Doktori (PhD) értekezés

Legárd Ildikó

2024. december

NEMZETI KÖZSZOLGÁLATI EGYETEM
Közigazgatás-tudományi Doktori Iskola

Legárd Ildikó

Kibervédelmi kihívások a közszolgálat személyi állományában

Doktori (PhD) értekezéstervezet

Témavezetők:

……..	……..
Dr. habil Budai Balázs Benjámin Phd	Dr. habil Krasznay Csaba Phd
tanszékvezető egyetemi docens	egyetemi docens

Budapest, 2024. december

TARTALOM

1. BEVEZETÉS

1.1 A TÉMA AKTUALITÁSA

A kibertér 1982-ben megjelenő fogalmát[1] néhány évtizeddel ezelőtt még misztikum, valamilyen futurisztikus megközelítés övezte, azonban az okos- és egyéb digitális eszközök, szolgáltatások használata, a világunkat behálózó online világ révén mostanra a mindennapi életünk részévé vált, még ha nem is tudatosan is, de aktív szereplői és alakítói lettünk a kibertérnek.

Az utóbbi néhány évtizedben bekövetkező technológiai fejlődés, a digitalizáció ugrásszerű megnövekedése, az infokommunikációs eszközök és szolgáltatások rendkívüli fejlődése, az internet széleskörű elterjedése, az adatokhoz, információkhoz történő gyors hozzáférés visszavonhatatlanul megváltoztatta az emberek és az egész társadalom életét, a vállalkozások működését és a közigazgatás szervezését.

Magyarországon a 2015-ben indított Digitális Jólét Program már alapvető célként határozza meg a digitális állam megteremtését és annak részeként a teljes közigazgatás digitális átalakítását, melynek segítségével az állami szolgáltatások digitálisan elérhetővé válnak, digitális közigazgatási folyamatok és szolgáltatások kerülnek kialakításra.

A digitális átalakulás szükségszerűségét felismerve, a Nemzeti Digitalizációs Stratégia 2022-2030 jövőképe értelmében Magyarország a digitális gazdaságot, a digitális kompetencia fejlesztését és a digitális közszolgáltatásokat, valamint a mesterséges intelligenciára épülő és automatizációs megoldásokat állítja a versenyképességi és modernizációs törekvéseinek középpontjába. További célkitűzésként jelenik meg, hogy hazánk a digitális gazdasági és társadalmi fejlettséget tekintve az európai országok rangsorában a jelenlegi 22. helyről[2], 2030-ra a legjobban teljesítő tíz ország közé kerüljön.[3]

A Nemzeti Digitalizációs Stratégiában megfogalmazott célok elérése és az egységesen magas szintű digitális környezet megteremtése érdekében került kidolgozásra és 2022. decemberében elfogadásra a Digitális Állampolgárság Program[4], amely megkönnyíti, és

[1] „A kibertér („cyberspace”) kifejezést William Gibson amerikai-kanadai sci-fi író használta először a számítógép-alapú hálózatok és az ember interaktív virtuális kapcsolatrendszerének leírására, az 1982-ben megjelent Burning Chrome című novellájában, majd a Neuromancer című regényében. In: Taktitkák és stratégiák a kiberhadviselésben.” (2023a) p. 11.

[2] Digital Economy and Society Index 2022, https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (Letöltve: 2023.09.25.)

[3] Nemzeti Digitalizációs Stratégia 2022-2030, p.88. https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf (Letöltve: 2023.03.20.)

[4] Digitális Állampolgárság Program: https://dap.gov.hu/program (Letöltve: 2024.11.09.)

egyszerűbb alapokra helyezi az állampolgárok és a kormányzat különböző szervei közötti kommunikációt, valamint az állami szolgáltatásokkal kapcsolatos ügyintézés folyamatát.

A közszolgáltatások digitalizációjával párhuzamosan, ugyanakkor a közigazgatás által döntően elektronikus információs rendszerekben tárolt, feldolgozott és továbbított adatok és információk mennyiségének, illetve mibenlétének köszönhetően a közigazgatás egyre több, a kibertér felől érkező fenyegetésnek van kitéve. A támadások irányulhatnak a rendszerekben kezelt adatok, információk bizalmassága, sértetlensége és rendelkezésre állása, valamint maga a rendszer vagy annak elemeinek sértetlensége és rendelkezésre állása ellen. Csak néhány hazai és nemzetközi példát említve: 2016-ban a Közigazgatási és Igazságügyi Hivatal honlapját (kih.gov.hu), a kormany.hu-t és a Külgazdasági és Külügyminisztérium publikus szolgáltatásait érte túlterheléses támadás, melynek eredményeképpen az érintett honlapok és szolgáltatások teljesen elérhetetlenné váltak több órára.[5] 2017-ben 45 kormányzati rendszert ért zsarolóvírus támadás Magyarországon. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet incidenskezeléssel foglalkozó egységei tájékoztatása szerint mindössze néhány száz eszköz fertőződött meg, melynek során a vírus zárolta a fájlokat a fertőzött számítógépeken, és a hackerek fizetést követeltek a hozzáférés visszaállításáért. A vírus egyébként elterjedt a világ 150 országában, az Egyesült Királyságban például a helyi kórházaktól 300 USD-t kértek minden egyes eszközük feloldásához, az érzékeny adatokhoz és betegnyilvántartásokhoz való hozzáférést blokkolták.[6] 2024. novemberben derült fény a magyar védelmi és biztonsági feladatokkal összefüggő beszerzéséért felelős állami cég, a Védelmi Beszerzési Ügynökség (VBÜ) informatikai rendszerei elleni hackertámadásra, melynek során egy nemzetközi hackercsoport letöltötte és titkosította a Védelmi Beszerzési Ügynökség teljes fájlszervertartalmát, az ügynökség által kezelt katonai beszerzésekkel kapcsolatos tervekért és adatokért cserébe pedig 5 millió dollárt követeltek. A Honvédelmi Minisztérium közlése szerint az ügyben az incidenst követően feljelentést tett a VBÜ.[7] 2024. januárban orosz hackerek 65 ausztrál kormányhivatalt és ügynökséget támadtak meg, és 2,5 millió dokumentumot loptak el Ausztrália történetének legnagyobb kormányzati kibertámadása

[5] Senki nem vállalta magára a kormányzati informatikai rendszerek elleni támadást: https://infoter.eu/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast (Letöltve: 2024.11.09.)

[6] Hungary under cyber attack: https://abouthungary.hu/news-in-brief/hungary-under-cyber-attack (Letöltve: 2024.11.09.)

[7] Meghackelték és ötmillió dollárral zsarolják a magyar Védelmi Beszerzési Ügynökséget, https://hu.euronews.com/2024/11/14/hackeles-otmillio-dollar-zsarolas-magyar-vedelmi-beszerzesi-ugynokseg-titkos-adatok (Letöltve: 2024.11.19.)

során. A hackerek bejutottak egy ausztrál ügyvédi iroda rendszereibe, amely a kormánnyal történő együttműködés folytán bizalmas kormányzati adatokat tárolt.[8] 2024. májusában Lengyelország és a Cseh Köztársaság azzal vádolt meg orosz hackereket, hogy kormányzati és infrastrukturális hálózatokat vettek célba. Mindkét ország azt állítja, hogy a támadások nagyjából egy időben történtek a szintén orosz hackerek általi, német kormány elleni támadással. A hackerek a Microsoft Outlook sebezhetőségét kihasználva jutottak hozzá adatokhoz.[9]

Az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA által a kiberfenyegetésekről készített éves jelentése már a 2020-as adatok alapján is megállapította, hogy a legtámadottabb szektor a közigazgatás. Ez a trend az elmúlt években nem változott, így a 2024. szeptember 19-én publikált fenyegetettségi riport, az ENISA Threat Landscape 2024 is megerősíti, hogy a vizsgált időszakban (2023. július – 2024. június) bekövetkezett kiberbiztonsági események száma alapján a legtöbb támadás –az összes detektált esemény 19%-a- a közigazgatási, kormányzati szektorral szemben következett be, a közlekedés a második (11%), a pénzügyi szektor pedig a harmadik (9%) helyre került.[10]

A támadók a sikeres támadás érdekében nagyon sok esetben nem is magukat a rendszereket támadják közvetlenül, hanem a sokkal könnyebb célpontban bizonyuló felhasználókat annak érdekében, hogy a szervezet által használt rendszerekhez hozzáférést szerezzenek, vagy megbénítsák azok működését. Az említett ENISA jelentés[11] az elsődleges fenyegetések közé sorolja az emberi hiszékenységre és együttműködési képességre építő, ún. social engineering támadásokat[12], és azt is kiemeli, hogy a social engineering támadások 15%-a a digitális infrastruktúrát, 10%-a pedig kifejezetten a közigazgatást, kormányzati szektort célozzák meg. A social engineering támadások 73%-a adathalász és egyéb csaló emailek segítségével valósul meg.
Éppen ezért a közigazgatási, kormányzati szektor számára alapvető jelentőségű az információbiztonság növelése, a kibervédelmi kapacitások bővítése, valamint a digitális kompetencia fejlesztése.

---

[8] Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Letöltve: 2024.11.09.)
[9] Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Letöltve: 2024.11.09.)
[10] ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024?v2=1 (Letöltve: 2024.11.09.)
[11] ld. 9. lábjegyzet
[12] A social engineering-ről ld. 3.2.2. Social engineering típusú támadások.

A nemzeti adatvagyon részét képező nemzeti elektronikus adatvagyon és az ezt kezelő elektronikus információs rendszerek és rendszerelemek biztonsága érdekében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), valamint a 2025. január 1-jétől hatályba lépő, az Ibtv.-t felváltó Magyarország kiberbiztonságáról szóló törvény (a továbbiakban: Kibertv.), a hatálya alá tartozó szervezetek számára számos elektronikus információbiztonsági követelmény megvalósítását teszi kötelezővé, melynek keretében külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatározniuk és végrehajtaniuk a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás, valamint a biztonsági események kezelése érdekében.
Bár az Ibtv.-ben és a Kibertv.-ben meghatározott feladatok közvetlen címzettjei a hatálya alá tartozó szervezetek vezetői, illetve az általa kinevezett/megbízott elektronikus információs rendszer biztonságáért felelős személy (továbbiakban: IBF), az elektronikus információk rendszerek védelméhez kapcsolódó feladatok végrehajtása elképzelhetetlen az érintett szerveknél dolgozó munkatársak közreműködése nélkül. A közszolgálatban dolgozó átlagfelhasználóknak a mindennapi munkájuk során számos, kiberbiztonsággal szorosan összefüggő feladatot kell végrehajtaniuk, melyek ellátása speciális ismereteket, készségeket és kompetenciákat kíván meg.

A kárt okozó kiberbiztonsági incidensek száma évről évre folyamatosan növekszik, a támadások egyre célirányosabbá és kifinomultabbá válnak. A közszolgálati dolgozók a kibertérből érkező támadások számára értékes és kiemelt célpontnak számítanak, hiszen általuk a támadók a nemzeti adatvagyon részét képző adatokhoz, információkhoz is hozzáférhetnek, vagy megbéníthatják egy egész szervezet és végső soron akár az egész ország működését is. Éppen ezért alapvető elvárás és meghatározó jelentőséggel bír, hogy a közigazgatásban dolgozók maguk is megfelelően felkészültek és tudatosok legyenek az kiberbiztonság területén, és erősödjön bennük a kiberfenyegetésekkel kapcsolatos tudatosság. Amennyiben a felhasználók ismerik a megfelelő biztonsági eljárásokat, követelményeket és technikákat, a lehetséges támadási és védekezési alternatívákat és azokat képesek alkalmazni is, akkor a kibertér felől érkező támadások bekövetkezésének valószínűsége is csökkenthető, mely összességében növeli a közigazgatási szervek működésének stabilitását, külső befolyástól mentes működését, valamint a nemzeti adatvagyon biztonságát. Nem utolsó sorban a biztonságtudatosság növelése

elengedhetetlen része Magyarország kibervédelmi képességei fejlesztésének és ezek keresztül az új típusú fenyegetésekkel szemben az állami szuverenitás megerősítésének.

1.2 A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A közigazgatási szervek kiberbiztonsága számos tényezőtől függ, többek között:

- az Ibtv.-ben, illetve a Kibertv.-ben, valamint a végrehajtási rendeleteikben megfogalmazott feladatok végrehajtásától, melyek alapvetően a szervezet vezetőjének, valamint az IBF felelősségi körébe tartoznak és hatósági ellenőrzés alatt állnak;
- a közigazgatási szervek munkatársai (továbbiakban: közszolgálati dolgozók) kiberbiztonsággal (elektronikus információbiztonsággal)[13] kapcsolatos feladatai ellátásától és biztonságtudatosságuktól;
- a szervezetet érintő kiberbiztonsági incidenstrendekre vonatkozó ismeretektől és az azokra történő reagálástól, valamint
- a megelőzésre, észlelésre és válaszadásra való szervezeti és egyéni képességektől.

Az Ibtv., illetve a Kibertv., valamint végrehajtási rendeleteik megfelelő jogszabályi garanciák előírásával igyekeznek biztosítani a hatályuk alá tartozó elektronikus információs rendszerek védelmét, a 41/2015. (VII. 15.) BM rendelet[14], valamint a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024 (VI. 24.) MK rendelet a szervezet vezetője, valamint az IBF számára konkrét feladatkatalógust határoz meg, ugyanakkor nem létezik olyan keretrendszer, dokumentum vagy tanulmány, amely az IBF-nek a feladatellátáshoz szükséges készségeit, ismereteit és kompetenciáit határozná meg.

[13] Ibtv. 1.§ (1) 26. kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez működtetéséhez.
A kiberbiztonság fogalmát az Ibtv. 1.§ (1) bekezdés 26. pontjában meghatározott definíció szerint alkalmazom, és minden olyan feladatot kiberbiztonsággal kapcsolatosként azonosítok, amelyek az Ibtv.-ben alapvető elektronikus információbiztonsági követelményként jelennek meg, és az Ibtv. hatálya alá eső elektronikus információs rendszerek védelmét szolgálják.
[14] 41/2015. (VII. 15.) BM rendelet 3.1.7. pont;

A közigazgatásban dolgozók biztonságtudatossága kialakítása érdekében, az Ibtv.-ben megfogalmazott kötelezettségek hatására az érintett szerveknél előremutató tudatosító tevékenység indult el, ugyanakkor a tudatosítás megvalósításra vonatkozó egységes szabályok és megoldások hiányában, a különböző szerveknél, a közigazgatás egyes területein teljesen eltérő módon valósult és valósul meg, illetve eredménnyel járt a tudatosítás. Az eredményesség tekintetében már a törvény hatályba lépését követő első felmérések (Illéssy - Nemeslaki - Som 2014; Nemeslaki, 2014; Nemeslaki - Sasvári, 2014; Nagy, 2015; Som - Papp, 2015; Som - Papp, 2016; Kollár, 2016) is nagy eltérést mutattak, és az eltelt közel nyolc évben végzett vizsgálatok is jelentős hiányosságokat tártak fel a munkatársak biztonságtudatossága terén.

Az Európai Bizottság 2024 júliusában hozta nyilvánosságra a Digital Decade 2024: Country reports elnevezésű jelentését, mely 2023-tól magában foglalja a korábbi években önállóan megjelent, a digitális gazdaság és társadalom fejlettségét mérő mutatót, a Digital Economy and Society Indexet (DESI). A jelentés megállapítja, hogy „Magyarország legnagyobb kihívása az elmúlt években egyértelműen a digitális kompetenciák lassú fejlődése volt, amelyek mind a gazdasági szektor, mind a közigazgatás további digitalizációjának alapját képezik.[15] „2023-ban a magyar lakosság 58,9%-a rendelkezett legalább alapvető digitális készségekkel. Bár az uniós átlag (55,6%) felett van, a figyelemnek továbbra is magasnak kell maradnia annak biztosítása érdekében, hogy a digitális készségek elterjedjenek a lakosság egészében, beleértve a legidősebb generációkat is.”[16]

A 2020-ban elfogadott Nemzeti Biztonsági Stratégia is kiemeli, hogy általános jelenség „a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme.”

A tudatosítás sikerességét akadályozza, hogy a közszolgálati dolgozók tekintetében még egyáltalán nem került feltérképezésre, hogy az Ibtv.-ben, valamint a Kibertv.-ben megfogalmazott feladatokkal összefüggésben, szervezeti szinten a munkatársaknak milyen kiberbiztonsággal kapcsolatos feladatokat kell ellátnia, így az sem, hogy ezekhez milyen készségekre és ismeretekre lenne szükségük. Kizárólag olyan kompetenciák azonosítására

[15] Digital Decade 2024: Country reports – Hungary Countra Report, https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports (Letöltve: 2024.11.09.)

[16] Magyarország 2024. évi országjelentése a digitális évtizedről https://digital-strategy.ec.europa.eu/hu/node/12860/printable/pdf (Letöltve:2024.11.14.)

került sor a közszolgálati digitális kompetencia referenciakeret részeként, amelyek általában határozzák meg a közigazgatásban dolgozó átlagfelhasználóknak a feladatellátáshoz szükséges digitális kompetenciáit, a kiberbiztonsággal kapcsolatos kompetenciákról viszonylag szűk körben, a „Biztonság, védelem és felelősség” területen fogalmaz meg néhány gondolatot.
Ahhoz, hogy érdemben növelni tudjuk a közigazgatási szervek kibervédelmi képességeit, nélkülözhetetlen, hogy az ott dolgozó átlagfelhasználók kibervédelmi képességeit is növeljük a megfelelő ismeretek, képességek, kompetenciák kialakítása segítségével.

A szervezetek megfelelő védelmi képességei kialakításához további elengedhetetlen ismeretek szükségesek az őket fenyegető kibertámadási típusokról. A hazai, közigazgatást érintő incidenstrendekkel kapcsolatos tanulmányok már születtek, ugyanakkor a teljes közigazgatás spektrumát átfogó, több évet elemző és összehasonlító írás még nem készült. Egy, a hazai incidenstrendekre irányuló kutatás érdemben hozzá tud járulni a szervezetek megfelelő védelmi képességének kialakításához, valamint a közszolgálatban dolgozók egyéni biztonságtudatossága fejlesztéséhez.

1.3 KUTATÁSI CÉLKITŰZÉSEK

A kibertér kérdésköre, jellegéből adódóan, csak korlátozottan értelmezhető nemzeti szinten, az Európai Unió részeként pedig minden esetben figyelemmel kell lennünk az uniós szintű jogalkotásra, a tagállamokra számára, a nemzeti jogrendbe kötelezően átültetendő jogi aktusokra. A Nemzeti Digitalizációs Stratégiával összhangban, mely az általa kitűzött célokat a nemzetközi stratégiai környezet és jó gyakorlatok figyelembevételével kívánja megvalósítani[17], disszertációmban a kutatási célok megfogalmazásakor, a hipotézisek bizonyítása során, valamint a várható tudományos eredmények tekintetében is kiemelt figyelmet fordítok a nemzetközi kontextusba való illeszkedésre, az Európai Unióban alkalmazott követelményeknek való megfelelésre.

[17] Nemzeti Digitalizációs Stratégia 2022-2030 p.93.
https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf
(Letöltve: 2023.03.20.)

Kutatásom célja, hogy elemezzem és összehasonlítsam a hazai és az Európai Unióban azonosított, közigazgatási szerveket érintő incidenstrendeket, valamint megvizsgáljam a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadási forma előfordulási arányát, ezáltal a humán faktor szerepét a kibertámadások sikerességében.

Kutatásom további célja, hogy az IBF, illetve a közszolgálatban dolgozó munkatársak esetében azonosítsam azokat a hazai jogszabályi környezeten alapuló, kiberbiztonsággal kapcsolatos feladatokat, valamint e feladatok ellátásához nélkülözhetetlen készségeket, ismereteket és kompetenciákat, amelyek biztosítják a szervezeti és az egyéni védelmi képességek növelését, valamint az Európai Unióban alkalmazott, kiberbiztonsággal kapcsolatos közös értelmezést és közös terminológia használatát is.

Kutatási céljaim elérése érdekében az alábbi részcélokat fogalmaztam meg:

1.	A információbiztonság területén használt fogalmak nemzetközi és hazai használatából eredő eltérések, és ezért a sok esetben tapasztalható következetlen alkalmazásuk miatt egy konzisztens fogalomkészlet létrehozása, érintve az kiberbiztonság, kibervédelem, információbiztonság, elektronikus információbiztonság, adatbiztonság kérdéskörét, valamint az információbiztonság tudatosság és tudatosítás fogalmát.
2.	A kiberbiztonságra vonatkozó hazai jogszabályi környezet bemutatása, elemzése.
3.	A magyar közigazgatási szerveket érő kiberbiztonsági incidensekre vonatkozó statisztikai adatok elemzése.
4.	Az európai kiberbiztonsági incidenseket bemutató dokumentumok elemzése, a meghatározó trendek azonosítása.
5.	A hazai kiberbiztonsági incidenstrendek összehasonlítása az európai trendekkel.
6.	A kiberbiztonsággal, kibervédelemmel és információbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó hazai és nemzetközi keretrendszerek meghatározása, elemzése, többszempontú összehasonlítása, valamint a magyar közigazgatási környezetben alkalmazható jó gyakorlatok azonosítása.
7.	Az IBF, valamint közszolgálatban dolgozók hazai jogszabályok alapján azonosítható kiberbiztonsági feladatainak meghatározása és a jó gyakorlatként megállapított

	nemzetközi keretrendszerekben történő beazonosítása.
8.	Az IBF, valamint a közszolgálatban dolgozók kiberbiztonsággal kapcsolatos feladatai ellátáshoz szükséges készségek, ismeretek, kompetenciák meghatározása a nemzetközi és hazai keretrendszerek segítségével.

1. táblázat: Kutatási célkitűzések (forrás: saját szerkesztés)

1.4 KUTATÁSI HIPOTÉZISEK

H1	A magyar közigazgatást érő kiberbiztonsági incidensek megfelelnek az európai incidenstrendeknek, melyekben meghatározó szerepe van a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadási formának.
H2	Meghatározható az elektronikus információs rendszer biztonságáért felelős személy számára egy olyan szerepprofil, amely azonosítja a mindennapi munkavégzés részét képező feladatokat, illetve a végrehajtáshoz szükséges készségeket, ismereteket és kompetenciákat.
H3	Azonosíthatók a közszolgálatban dolgozók mindennapi munkavégzése során ellátandó kiberbiztonsági feladatok, valamint a feladatellátást biztosító ismeretek, képességek és kompetenciák.

2. táblázat: Kutatási hipotézisek (forrás: saját szerkesztés)

1.5 KUTATÁSI MÓDSZERTAN[18]

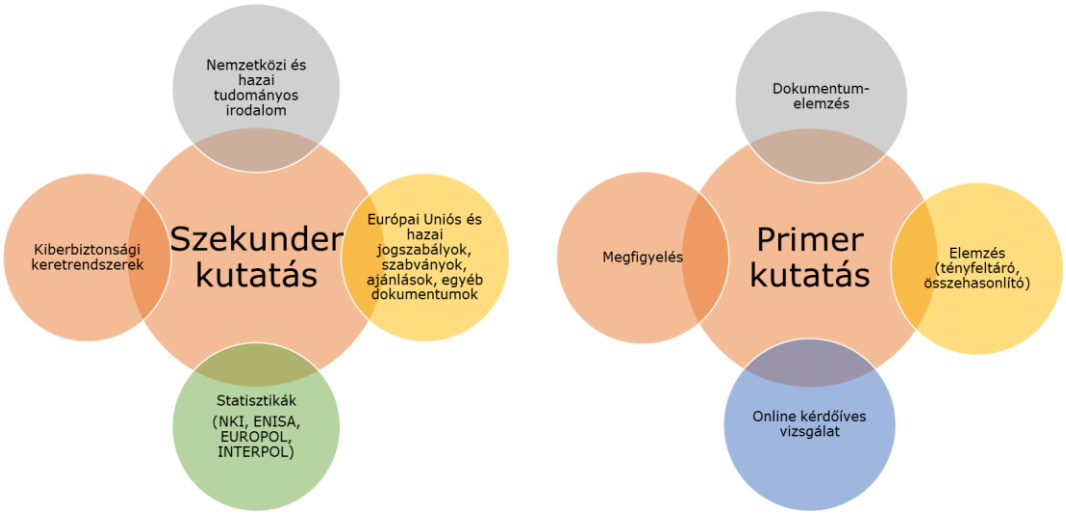
A hipotézisek bizonyítására primer, illetve szekunder kutatást végeztem az alábbi pillérekkel:

Szekunder kutatás: Széleskörű nemzetközi és hazai irodalomkutatás, a hatályos európai uniós és hazai jogszabályok, szabványok, ajánlások, kiberbiztonság tárgyú keretrendszerek, valamint a kibertér felől érkező fenyegetésekkel, támadásokkal kapcsolatos nemzetközi és hazai statisztikák vizsgálata, elemzése, rendszerezése, összehasonlítása.

[18] A disszertáció kutatási módszertani fogalmi rendszerének meghatározására Hornyacsek Júlia: A tudományos kutatás elmélete és módszertana című műve alapján kerül sor. (Hornyacsek, 2014)

Primer kutatás:

- dokumentumelemzés;
- online kérdőíves vizsgálat egy meghatározott célcsoportban;
- elemzés;
- megfigyelés.



1. sz. ábra: Kutatási módszertan (forrás: saját szerkesztés)

A kutatás során minőségi, valamint mennyiségi mutatókat is vizsgáltam, így kvalitatív és kvantitatív kutatási módszereket is alkalmaztam:

Kvalitatív módszerek:

- dokumentumelemzés;
- elemzés;
- megfigyelés.

Kvantitatív módszerek:

- kérdőív;
- statisztikai elemzés.

Az egyes hipotézisek vizsgálata során alkalmazott kutatási módszereket az alábbi táblázat foglalja össze:

	Szekunder kutatás				Primer kutatás			
	Nemzetközi és hazai tudományos irodalom	Európai Uniós és hazai jogszabályok, ajánlások, egyéb dokumentumok	Statisztikák (NKI, ENISA, EUROPOL, INTERPOL)	Kiberbiztonsági keretrendszerek	Dokumentum-elemzés	Elemzés (tényfeltáró, összehasonlító)	Online kérdőíves vizsgálat	Megfigyelés
H1	X	X	X		X	X		X
H2	X	X		X	X	X		X
H3	X	X		X	X	X	X	X

3. sz. táblázat: Kutatási módszertan áttekintő táblázat (forrás: saját szerkesztés)

Az egyes hipotézisek bizonyításához kapcsolódó részletes kutatási módszertan az adott fejezeteknél kerül ismertetésre.

Kutatásom részeredményeit tudományos folyóiratokban publikáltam, illetve számos tudományos és szakmai konferencián ismertettem.

1.6 A KUTATÁS FÓKUSZÁNAK SZŰKÍTÉSE

A kutatással érintett szervek:
A vizsgálatok kizárólag az Ibtv. hatálya alá tartozó szervezetek kibervédelmi képességei növelését célozzák, nem térnek ki a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény hatálya alá tartozó szervezetekre, valamint a magánszférában történő alkalmazhatóságra.

A kutatással érintett személyi kör:
A kutatások célcsoportját a „közszolgálatban dolgozó” kifejezés jelöli az értekezésben, ugyanakkor a vizsgálatok kifejezetten az Ibtv. hatálya alá tartozó közigazgatási szervezeteknél foglalkoztatott átlagfelhasználók biztonságtudatosságának fejlesztésére irányulnak. Az Ibtv.-t felváltó Kibertv. sem jelent e tekintetben változást, mivel annak 1. melléklete sorolja fel a hatálya alá tartozó, közigazgatási ágazathoz tartozó szervezeteket, amely két kiegészítéssel bővül: a központi szolgáltatóval, valamint a központi rendszerek szolgáltatóival.

A célcsoport szűkítése jelentőséggel bír, mivel ezen szervezetek és munkatársaik számára fogalmaznak meg a hatályos jogszabályok egyértelmű, kiberbiztonsággal kapcsolatos

feladatokat, így a vizsgálatok kiindulási pontja is a jogszabályokban megfogalmazott kötelezettségek voltak.
Ugyanakkor a „közszolgálati dolgozó” kifejezés arra kíván utalni, hogy a kutatási eredmények azon személyi kör számára is értelmezhetők, akiknek a jogszabályok ugyan nem írnak elő hasonlóan szigorú védelmi követelményeket, de a megfelelő kibervédelmi képesség kialakítása a számukra is jelentőséggel bír.
A közszolgálat fogalmának, illetve annak személyi állománya meghatározásának kérdése nem egyszerű feladat, arra egységesen elfogadott és használt definíciót nem találhatunk. A közszolgálati alkalmazott fogalma tekintetében is háromféle megközelítés létezik. A funkcionális megközelítés szerint, „a közszolgálati alkalmazottak a köz érdekében látnak el feladatokat, közszolgáltatásokat biztosítanak, gyakorta állami alapfunkciókat valósítanak meg”. Az organikus (vagy finanszírozási) felfogás szerint „a közszolgálati alkalmazottak olyan szerveknél dolgoznak, amelyeket a köz (az állam, az önkormányzat) tart fenn részben vagy egészben (tehát költségvetési szervek)”, a pragmatikusok szerint pedig „az a közszolgálati dolgozó, akit a jogállását rendező jogszabály (általában törvény) annak minősít” (Kiss, 2019., pp. 124-125.).
A disszertáció megközelítése az organikus felfogáshoz áll a legközelebb, ugyanakkor a kutatási eredmények bármely más elmélet alapján azonosított közszolgálati személyi kör számára segítségül szolgálhatnak a kiberbiztonsági kihívások kezelésében.

Átlagfelhasználó alatt egy adott elektronikus információs rendszert igénybe vevők körét azonosítom a foglalkoztatásra irányuló jogviszonyra tekintet nélkül. Olyan munkatársak, akik nem rendelkeznek informatikai vagy kiberbiztonsági végzettséggel, valamint nem informatikai vagy kiberbiztonsággal kapcsolatos munkakört látnak el.

A kutatás fókuszának egyéb szűkítése:

- A vizsgálatok kizárólag az elektronikus információs rendszerekben kezelt adatok, információk védelmére, valamint e rendszerek biztonságos használatára terjednek ki, a papír alapú adat, -illetve információvédelemre nem térnek ki.

- A disszertáció terjedelmi korlátai nem teszik lehetővé olyan speciális, szigorú szabályok által körül határolt és meghatározott területek biztonságtudatosításának vizsgálatát, mint a papír alapú vagy az elektronikus információs rendszerek által kezelt minősített adatok, illetve az európai vagy nemzeti létfontosságú

rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény[19] alapján kijelölt rendszerelemek védelme, valamint a honvédelmi célú elektronikus információs rendszerek biztonsága.

- A kutatás dedikált célja, hogy az átlagfelhasználó kiberbiztonsággal kapcsolatos feladatai meghatározásához, valamint biztonságtudatossága kialakításához és tovább fejlesztéséhez nyújtson segítséget, valamint olyan bázisként szolgáljon, amely a későbbi továbbképzések tekintetében is iránymutatást jelenthet.

- A disszertáció nem vizsgálja az átlagfelhasználók digitális kompetenciája közti különbségeket és nem célja a digitális kompetenciaterületek általános fejlesztése, kizárólag a digitális kompetencia részeként azonosított biztonságtudatosság növelését kutatja.

A kutatás időbeli lehatárolása:

Az értekezésben megfogalmazott kutatási kérdések és hipotézisek, illetve bemutatott vizsgálatok 2023. őszén zárultak le, így az Ibtv.-ben és végrehajtási rendeleteiben megfogalmazott szabályozást vették alapul. A NIS2 Irányelv implementációját biztosító Kibertv. megjelenését követően, a disszertáció tudományos eredményeinek jövőbeni felhasználhatóságára külön kitérek a 6. fejezetben.

[19] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

2. FOGALMI KERETRENDSZER, JOGSZABÁLYI HÁTTÉR

Az elektronikus információs rendszerek biztonságával kapcsolatos alapfogalmakat, valamint a hozzá kapcsolódó európai uniós és hazai szabályozást jelen fejezet mutatja be és elemzi.

Az egyes hipotézisekhez kapcsolódó kulcsfogalmak bemutatására az adott fejezet szakirodalmi áttekintésében kerül sor.

2.1. FOGALMI KERETRENDSZER

Az értekezés központi fogalma a kibervédelem, kiberbiztonság kérdése, így elengedhetetlen ezen fogalmak ismerete, és a hozzá kapcsolódó fogalmak bemutatása.

A **kibertér** („cyberspace") kifejezést William Gibson amerikai-kanadai sci-fi író használta először a számítógép-alapú hálózatok és az ember interaktív virtuális kapcsolatrendszerének leírására, az 1982-ben megjelent Burning Chrome[20] című novellájában, majd a Neuromancer[21] című regényében. A kibertér fogalma az elmúlt évtizedekben folyamatos változáson ment keresztül, tartalma a fejlődés ütemével párhozamosan bővül, ezért egységes meghatározással nem, csak egyedi megfogalmazásokkal találkozhatunk. Az Egyesült Államok Védelmi Minisztériuma által kiadott szótár szerint a kibertér „az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket".[22] Hazánkban a fogalmat a 2013-as Nemzeti Kiberbiztonsági Stratégia határozza meg, mely szerint: „[a] kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."[23][24]

[20] William Gibson: Izzó króm, In: GIBSON, W.: Izzó króm, ford.: Bárday Tamás, Gáspár András, Hoppán Eszter, Szántai Andrea, Szántai Zsolt, Valhalla Páholy, 1997, 133- 163

[21] William Gibson: Neurománc, ford.: Ajkay Örkény, Valhalla Páholy Kft., Budapest, 1992, 344

[22] JP 1-02 Department of Defense Dictionary of Military and Associated Terms, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (Letöltve: 2021.06.26.) Fordította: Berki Gábor (2013): A kibertéri konfliktusok változásai, Hadmérnök VIII. Évfolyam 1. szám, 173-185., 249.

[23] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

A kibertér különböző irányú folyamatok és ellenirányú folyamatok terepe. Míg a kibertér bizonyos szereplőinek tevékenysége az elektronikus információs rendszerben szereplő adatok, információk megszerzésére, vagy e rendszerek megbénítására, illetve elpusztítására irányulnak, addig velük szemben az ellenérdekű felek igyekeznek e rendszerek biztonságát garantálni. A **kiberbiztonság** nem más, mint „azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek”[25], tehát azon politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök alkalmazását jelentik, amelyek képesek a kibertérben létező kockázatok kezelésére[26]. A **kibervédelem** „a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését”[27]. Tehát egy aktív védelmi tevékenység, amelyet az érintett szereplő hajt végre a kiberbiztonság megteremtése érdekében, és amelyek a rendszerei, valamint az azokban kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása megőrzésére irányulnak.

Összefoglalva, a kiberbiztonság egy folyamatos, széleskörű törekvés és egyben állapot, a védelem pedig az erre irányuló tevékenységek összessége.

A kiberbiztonsággal szorosan összefügg, illetve annak részének tekinthető az egyes szervezetek információbiztonsága. A NATO információs műveletekkel foglalkozó 2009-ben kiadott doktrínája (továbbiakban AJP-3.10[28]) az **INFOSEC (information security), azaz információbiztonság** fogalmát, olyan információs képességként, eljárásként határozza meg, amely az információs műveletek célkitűzéseihez hozzájárul. Az információbiztonság (INFOSEC) célja a (tárolt, feldolgozott vagy továbbított) információk, valamint a fogadó rendszerek védelme a bizalmasság, a sértetlenség és rendelkezésre állás elvesztése ellen különféle eljárási, technikai és adminisztratív ellenőrzések révén.[29] E meghatározáson alapul az „információbiztonsági törvényként”

[24] Legárd Ildikó (2023a): A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintés - Legárd Ildikó: In: Taktikák és stratégiák a kiberhadviselésben.” p. 11.
[25] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (2019. április 17.) 2. cikk 1. pont (Letöltve: 2024.11.10.) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0881
[26] Ibtv. 1.§ (1) 26. pont
[27] Ibtv. 1.§ (1) 27. pont
[28] AJP-3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS, NATO/PfP UNCLASSIFIED publication. 2009, https://info.publicintelligence.net/NATO-IO.pdf (Letöltve: 2023. 09. 25.)
[29] AJP-3.10, fordította a szerző.

emlegetett, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint a Kibertv. gondolatrendszere is. Ez utóbbi szerint az elektronikus információs rendszer biztonsága: az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát"[30]

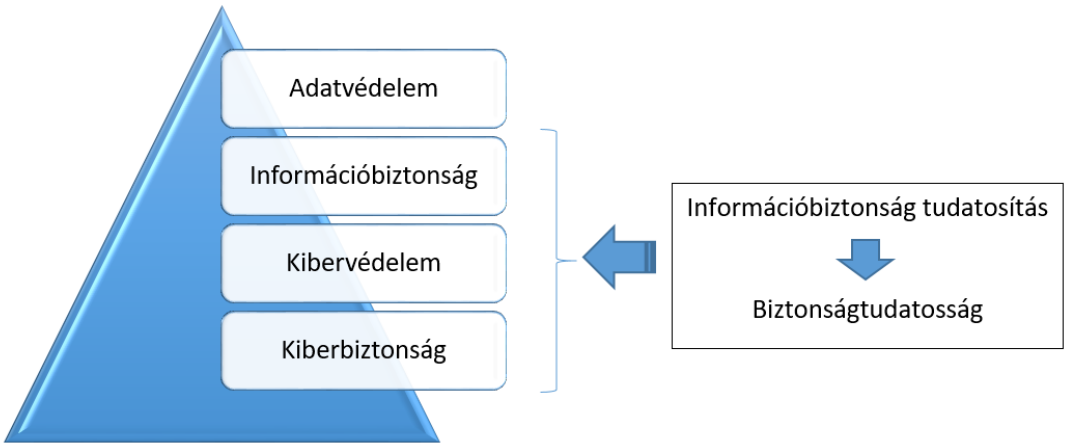
Ugyanakkor, ha az „információ" szó magyar nyelv értelmező szótára szerinti értelmét vizsgáljuk, a következő fogalom meghatározást kapjuk: az információ valamely személyre vagy ügyre vonatkozó tájékoztatás, felvilágosítás, de lehet értesülés vagy hír is.[31] Tehát ebben az ételemben beleérthetjük a információ bármely megjelenési formáját, így „a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információkat" (Muha, Krasznay, 2019., p.9.) is. A hazai jogszabályi környezet ugyanakkor –a nemzetközi fogalomhasználatnak megfelelően- az információbiztonság fogalma alatt, egyértelműen az elektronikus információs rendszerekben kezelt adatok, információk és az azt kezelő rendszerek biztonságát érti, amely három tényezőn, az ún. CIA-elven alapul: a bizalmasságon (confidentiality), a sértetlenségen (integrity) és az elérhetőségen (availability). **A disszertáció ennek megfelelően az információbiztonság, információbiztonsági tudatosság és tudatosítás fogalmak alatt, kizárólag az elektronikus információs rendszerekben kezelt adatok, információk biztonságát érti.**

Nem mehetünk el még egy, az értekezés témájához szorosan kapcsolódó fogalom, az adatvédelem mellett, melyet szükséges elhelyeznünk a fogalmi keretrendszerben. Az **adatvédelem**, kizárólag az adatok egy meghatározott csoportjára vonatkozik, függetlenül annak tárolási és megjelenési módjától. Az adatvédelem a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) értelmezésében: „a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége". Általában véve az elektronikus információs rendszerek által kezelt adatok csak egy részét teszik ki a személyes adatok, természetesen az elektronikus információs rendszerek által tárolt, kezelt, visszakeresett

[30] Kibertv. tervezete 4.§ 25. pont.

[31] A magyar nyelv értelmező szótára: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/i-i-31843/informacio-3225D/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2tfMUJFOEIiXX0sICJxdWVyeSI6ICJpbmZvcm1cdTAwZTFjaVx1MDBmMyJ9 (Letöltve: 2024.11.10.)

vagy továbbított más jellegű adatok, információk védelmét is magában foglalja az információbiztonság fogalma.



2. sz. ábra: Fogalmi keretrendszer (Forrás: saját szerkesztés)

Az információbiztonság fogalmának része minden olyan tevékenység, amely az elektronikus információs rendszerek biztonságához hozzájárul. Ilyen tevékenység a megfelelő védelmi képességek kialakításához szükséges, a rendszereket használó átlagfelhasználók információbiztonság-tudatosságának növelését célzó tudatosító tevékenység is.

Az **információbiztonság-tudatosság** a tudás, a képességek és a viselkedés olyan hármasa, mely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést (Legárd, 2020b, p. 95.).

A tudatosság kialakítása és fejlesztése érdekében, a szervezetek részéről megvalósuló **biztonságtudatosítás** olyan folyamatos erőfeszítésként írható le, amely felhívja az érdekeltek figyelmét az információbiztonságra és annak fontosságára, elősegíti a biztonságorientált magatartást[32], és ideális esetben ösztönzi az érdekelt feleket a biztonsági szabályok és irányelvek betartására.[33]

[32] Peltier (2005); ENISA, „A new users' guide: How to raise information security awareness," 2008. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide . (Letöltve: 2021.11.12.); Hansche (2001); Maeyer (2007)

[33] Tsohou, Karyda, El-Haddadeh (2012); Siponen (2000)

Az információbiztonság-tudatossággal, valamint a tudatosítással a V. fejezetben részletesebben is foglalkozok.

2.2. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁHOZ KAPCSOLÓDÓ JOGI SZABÁLYOZÁS

2.2.1. Stratégiaalkotás és szabályozás az Európai Unióban

Az Európai Unió az elektronikus információbiztonság területén konkrét jogszabályt 2005-ben alkotott először „**Az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat**” címmel, mely az ilyen típusú támadások esetén egységes, uniós szintű szankcionálási rendszert vezet be, valamint a tagállamok illetékes hatóságai közötti együttműködést mozdítja elő.[34]

2013-ban több, az Európai Unió belüli elektronikus információbiztonságot erősítő intézkedés történt:

- az Európai Parlament és a Tanács 2013-ban elfogadta **„Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról” szóló 2013/40/EU irányelvet**, mely meghatározza azokat a minimumszabályokat, amelyek mentén a tagállamoknak 2015. szeptember 4-ig harmonizálniuk kellett a vonatkozó nemzeti büntetőjogi szabályaikat[35];
- felállították a számítógépes szükséghelyzeteket elhárító állandó csoportot **(CERT-EU)**, amelynek tevékenysége az összes uniós intézményre, szervre és hivatalra kiterjed;
- megszületett az „**Európai Parlament és a Tanács 2013. május 21-i, 526/2013/EU rendelete az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről”**, mely jogszabály megerősítette a 2004-ben felállított ENISA szerepét;
- felállításra került a **Számítástechnikai Bűnözés Elleni Európai Központ**;

[34] A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról
[35] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

A kiberbiztonság kérdéskörének átfogó, stratégiai szintű áttekintése és rendezése érdekében az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága 2013 februárjában közzétette közös közleményét **„Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér”** címmel (továbbiakban: kiberbiztonsági stratégia).[36] A kiberbiztonsági stratégia célja a szabad és biztonságos internetes környezet biztosítása az Európai Unióban, melynek érdekében öt konkrét stratégiai prioritást és intézkedést fogalmaz meg úgy, mint: a kibertérből érkező fenyegetésekkel és támadásokkal szembeni hatékonyabb fellépés és védekezés, az elkövetett kiberbűncselekmények számának csökkentése, a közös kibervédelmi politika kidolgozása, a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése és a közös fellépés erősítése.

2016-ban két alapvető jelentőségű jogszabály került elfogadásra: a hálózati és információs rendszerek biztonságáról szóló, röviden **NIS irányelv (Directive on security of network and information systems)** és az **adatvédelmi rendeletet (General Data Protection Regulation – GDPR rendelet).**

A **NIS irányelv**[37] célja az európai szintű együttműködés megvalósítása, valamint egy közös intézmény és eszköztár kialakítása a tagállamok számára a hálózati és információs rendszerek általános szintű biztonságának garantálása érdekében. A cél megvalósításaként nemzeti szinten és közösségi szinten végrehajtandó feladatokat, valamint kötelező együttműködést ír elő a tagállamok és az egyes intézmények számára.
Az irányelv a hatálya alá tartozó szolgáltatók számára előírja, hogy a kockázatokkal arányos mértékű hálózat- és rendszerbiztonságot kell garantálniuk, illetve az illetékes hatóságok felé incidens bejelentési kötelezettségük van. Az alapvető és digitális szolgáltatást nyújtók azon körére, akik ellen intézett támadás a legközvetlenebbül érintheti a társadalom működését, a jogszabály további többletkötelezettségeket fogalmaz meg.
Az irányelvben foglalt rendelkezéseket a tagállamok 2018. május 9-ig átültették a nemzeti jogukba.

[36] Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér
[37] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Az Európai Parlament 2016. május 4-án fogadta el az Unió **általános adatvédelmi rendeletét**[38] (General Data Protection Regulation, a továbbiakban: **GDPR**), amelyet 2018. május 25-től kezdve kell a tagállamokban alkalmazni. A rendelet közvetlenül alkalmazandó és valamennyi tagállamra vonatkozóan állapít meg kötelezettségeket.
A szabályozás célja a személyes adatok és a magánszféra védelme, így a rendelet középpontjában a felhasználó, mint egyén áll. A GDPR hatálya valamennyi olyan vállalatra kiterjed, amely az unió polgárainak személyes adatait kezeli, így azon vállalatokra is, amelyek bár az Unión kívül működnek, azonban tevékenységük érinti az uniós polgárok személyes adatait. A rendelet értelmében súlyos szankciókkal sújthatók az előírásokat megszegő vállalatok.

2017. november 20-án az Általános Ügyek Tanácsa kijelentette, hogy az Unió egész területén meg kell erősíteni a kiberbiztonságot.[39] A miniszterek hangsúlyozták, hogy valamennyi uniós országnak biztosítania kell a kiberbiztonsághoz szükséges erőforrásokat és beruházásokat.[40]

A Tanács **2019. április 9-én** elfogadta azt a **kiberbiztonsági jogszabály**ként is ismert rendeletet, amely lehetővé teszi az EU számára, hogy „célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára”.[41]
„A szankciók kivethetők olyan személyekre vagy szervezetekre, akik, illetve amelyek:

- kibertámadásokért vagy megkísérelt kibertámadásokért felelősek,
- pénzügyi, technikai vagy anyagi támogatást nyújtanak ilyen támadásokhoz,
- azokban egyéb módon működnek közre.

Szankciók vethetők ki továbbá az ilyen személyekkel és szervezetekkel kapcsolatban álló személyekre és szervezetekre is.”[42]
A rendelet továbbá létrehozza az egész EU-ra kiterjedő tanúsítási rendszerek keretét, valamint felállítja az Európai Uniós Kiberbiztonsági Ügynökséget, amely átveszi a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepét.

[38] Az Európai Parlament és a Tanács (Eu) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
[39] http://www.consilium.europa.eu/hu/meetings/european-council/2017/10/19-20/ (Letöltve: 2023.09.25.)
[40] https://www.consilium.europa.eu/hu/policies/cyber-security/ (Letöltve: 2023.09.25.)
[41] https://www.consilium.europa.eu/hu/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ (Letöltve: 2023.09.25.)
[42] https://www.consilium.europa.eu/hu/policies/cybersecurity/timeline-cybersecurity/ (Letöltve: 2023.09.25.)

Európa kiberfenyegetésekkel szembeni ellenállóképességének erősítése érdekében az Európai Bizottság **2020**. decemberben **új kiberbiztonsági stratégiát** fogadott el. A dokumentum további célja, hogy az európai polgárok és vállalkozások megbízható szolgáltatásokat és digitális eszközöket vehessenek igénybe, és ezek előnyeit teljes mértékben ki tudják használni. A stratégia felhívja a figyelmet nem csak a tagállamokkal, hanem az uniós intézményekkel szembeni kibertámadásokra is, és a szükséges válaszlépések javítására.[43]

A megváltozott körülményekhez igazodva, a Tanács **2022**-ban fogadta el a **NIS 2 Irányelvet** az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről. A NIS 2 a kiberbiztonsági szabályok hatályát új ágazatokra, többek között a közigazgatásra és további szervezetekre terjeszti ki, melynek segítségével az Európai Unió egészének kibertámadásokkal szembeni ellenállóképességét, valamint a biztonsági eseményekre való reagálási kapacitásait kívánja erősíteni.[44] Az irányelv erősíti a tagállamok közötti szakmai együttműködést, valamint kötelezően előírja a tagállami számítógépes biztonsági eseményekre reagáló csoport (CSIRT) és egy, a nemzeti hálózati és információs rendszerek tekintetében illetékes hatóság felállítását. A jogszabály a hatálya alá tartozó szolgáltatók számára a korábbinál szigorúbb biztonsági és bejelentési követelményeket fogalmaz meg.
A tagállamoknak 2024. október 17-ig kell nemzeti jogszabályként végrehajtaniuk a NIS 2-ben foglalt intézkedéseket.

Az utóbbi években tehát az Európai Unió számos jogszabály megalkotásával, intézkedés bevezetésével, a kutatás és fejlesztés támogatásával járult hozzá a kibertérből érkező fenyegetések korai észleléséhez és a figyelmeztető rendszer kialakításához, a támadásokkal szembeni közös fellépéshez, az eseménykezeléshez, összességében egy biztonságosabb európai kibertér megvalósításához.

[43] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (Letöltve: 2023.09.25.)
[44] Irányelv az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv) https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive (Letöltve: 2023.09.21.)

2.2.2. Stratégiaalkotás és szabályozás hazánkban

Magyarországon a kiberbiztonság területén az első jelentős lépés a 2012. augusztus 31-én elfogadott **Magyary Zoltán Közigazgatási-fejlesztési Program (MP 12.0)** (továbbiakban: Magyary Program)[45] volt, mely az e-közigazgatás beavatkozási területei között sorolja fel az informatikai és információbiztonságot, valamint a területen végrehajtott illetve folyamatban lévő fejlesztéseket.

A 2012-ben elfogadott **Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat[46]** (továbbiakban: Nemzeti Biztonsági Stratégia) 1. mellékletének 31. pontja Magyarországot érintő biztonsági kihívásként azonosítja a kiberbiztonság megteremtését**,** és az ehhez kapcsolódó feladatként előírja a megfelelő kibervédelem kialakítása érdekében az állami szerepvállalás erősítését, a korai észlelést lehetővé tevő intézkedések bevezetését, az elektronikus információs rendszerek biztonságának növelését, a létfontosságú nemzeti információs infrastruktúra védelmének fokozását, továbbá az általános felhasználók tudatosítását.[47]

Az elektronikus információbiztonság szabályozási környezete kialakításának egyik első lépéseként – párhuzamosan a kapcsolódó törvény előkészítésével – 2013 márciusában került elfogadásra **Magyarország Nemzeti Kiberbiztonsági Stratégiája[48]** (továbbiakban: Kiberstratégia). A Kiberstratégiával Magyarország felelősséggel vállalja „a kibertér védelmével összefüggő feladatok ellátását" és kijelenti, hogy a „magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét, szabad, biztonságos és innovatív környezetté kívánja alakítani", melynek érdekében a legfontosabb feladatának tartja „a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelését, az ehhez szükséges kormányzati koordinációt és eszköztár erősítését"."[49]

2013. április 15-én, a korábbi stratégiákban megfogalmazott célok megvalósítása érdekében, első jogalkotási lépéseként, széles körű szakmai egyeztetést követően, az

[45] Magyary Zoltán Közigazgatási-fejlesztési Program (MP 12.0); https://www.uni-nke.hu/document/uni-nke-hu/gal_1_1modul.pdf (Letöltve: 2023.09.21.)
[46] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat;
[47] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat 31. pont a) és b).
[48] 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[49] Nemzeti Kiberbiztonsági Stratégia 1. pont

Országgyűlés elfogadta **az állami és önkormányzati szervek elektronikus információbiztonságáról_szóló 2013. évi L. törvényt**[50] (a továbbiakban: **Ibtv**.), mely a nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága megteremtésére irányul. A megfelelő védelem kialakítása érdekében a törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét, ezáltal a kibertér védelmét.[51]

Az Ibtv. 11. § (1) c) pontja alapján a kötelezett szervezet vezetője „az elektronikus információs rendszer biztonságáért felelős személyt nevez ki, vagy bíz meg", aki „felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért"[52].

Az Ibtv. végrehajtási rendeletei közül, az Ibtv.-ben meghatározott feladatok végrehajtása szempontjából kiemelkedő jelentőséggel bír **az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet**[53] (továbbiakban: BM rendelet),

---

[50] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)

[51] Ibtv. 1.§ (1)

8. bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

21. folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

31. kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

38. rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

39. sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

44. teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

48. zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem;

[52] Ibtv. 13.§ (2)

[53] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá

mely részletesen megfogalmazza és bemutatja azokat a konkrét feladatokat, amelyek az Ibtv. végrehajtása szempontjából elengedhetetlenek.

2020-ban került elfogadásra **Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV.21.) Korm. határozat**. A stratégia célul tűzte ki, hogy Magyarország 2030-ra bekerüljön a világ első tíz és Európa első öt legbiztonságosabb országa közé. A dokumentum 17 biztonsági kihívást és kockázatot jelölt meg, amelyek közül az első ötben szerepel a kiberfenyegetés is, a migráció, a váratlan fegyveres támadás, Magyarország hibrid fenyegetése és a terrorizmus mellett. A határozat kiemeli: „Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében."[54]

A stratégia –összhangban a nemzetközi szabályozással-, a kiberteret műveleti térnek ismeri el a hagyományos hadszínterek (szárazföld, a tengerek, a levegő és a világűr) mellett, sőt kiemeli, hogy „a jövőbeli konfliktusok nagy valószínűséggel még inkább ki fognak terjedni a kibertérre".[55] „A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia. Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése."[56]

Az új Nemzeti Biztonsági Stratégiához, valamint a megváltozott nemzetközi környezethez és uniós szabályozáshoz igazodó **Nemzeti Kiberbiztonsági Stratégia** jelenleg előkészítés alatt áll.

---

a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet

[54] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV.21.) Korm. határozat, 32. pont

[55] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV.21.) Korm. határozat, 71. pont

[56] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV.21.) Korm. határozat, 159. pont

A **NIS 2 irányelv implementációja** két lépcsőben valósult meg.

Első lépésként **a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény** (a továbbiakban : Kibertantv.) és annak végrehajtási rendelete a a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló **7/2024. (VI. 24.) MK rendelet** (a továbbiakban: 7/2024. MK rendelet) lépett hatályba. A Kibertantv. elsősorban a kiemelten kockázatos és kockázatos ágazatokban működő szolgáltatók és szervezetek vonatkozásában állapított meg kötelezettségeket, az Ibtv. hatálya alá tartozó szervezetek számára 2025. január 1-jéig továbbra is az Ibtv. maradt hatályban.

Második lépésként kerül elfogadásra a **Magyarország Kiberbiztonságáról szóló törvény,** amely hatályon kívül helyezi az Ibtv.-t, és a Kibertantv.-t is.[57] Az új törvény célja, hogy egységes szabályozás keretében biztosítsa a kibertámadások elleni védelem jogszabályi környezetének egységes kezelését, új és hatékony védekezési struktúra létrehozását, mely egyszerűsíti az állami információs rendszerek védelmét és irányt mutat a piaci szereplők számára, valamint maradéktalanul biztosítsa a NIS2 hazai jogba történő átültetését is.

Az új szabályozás, az Ibtv.-hez képest szigorúbb szabályokat ír elő a közigazgatási ágazat számára. A hatálya alá tartozó szervezeteknek többek között a törvényben meghatározott kockázatmenedzsment keretrendszert kell létrehozniuk és működtetniük, rendszeres belső kiberbiztonsági értékeléseket kell végrehajtaniuk a biztonsági követelmények megfelelőségének ellenőrzése céljából, valamint a 7/2024 MK rendeletnek megfelelően 19 követelménycsaládból, az adott rendszer biztonsági osztályának megfelelő védelmi kontrolokat kell megvalósítaniuk a kibertérből érkező kockázatok minimalizálás érdekében. Az új szabályozás a biztonsági eseménykezelés kapcsán bevezeti a nemzetközi terminológiának megfelelő kiberbiztonsági incidens[58] fogalmát. A szervezeteknek az elektronikus információs rendszereikben bekövetkezett kiberbiztonsági incidensek mellett (beleértve az üzemeltetési kiberbiztonsági incidenst is) a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket is haladéktalanul be kell jelenteniük a nemzeti kiberbiztonsági incidenskezelő központnak.

Az Ibtv. hatálya alá eső szervezetek számára 2025. január 1-től alkalmazandó a Kibertv, a 7/2024. MK rendelettel együtt.

[57] A tervezet lezárásakor a törvénytervezet még nem került elfogadásra, Törvényalkotási Bizottság eljárására vár.

[58] „kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát”, Kibertv. tervezete 4.§ 47. pont

3. KIBERBIZTONSÁGI INCIDENSTRENDEK A KÖZIGAZGATÁSBAN (ELSŐ HIPOTÉZIS)[59]

3.1. BEVEZETÉS

A kiberbiztonsági incidensek évről évre egyre nagyobb károkozásra képesek a privát- és a közszférában egyaránt. „A támadások okoztak globális károk mértéke a becslések szerint már 2018-2019 között – tehát a pandémia előtt – elérte az éves 375-575 milliárd dollárt", „amely összeg 2022-ben a becslések szerint meghaladta a 8.000 milliárd dollárt. A szakértők előrejelzése szerint 2025-re ez a szám eléri (és meghaladja) majd a 10.500 milliárd dollárt, 2028-ban pedig megközelítheti a 13.820 milliárd amerikai dollárt."[60]

Az anyagi károkozáson kívül azonban egy sikeres kibertámadás következményeként akár a megsérülhet az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása, a rendszerek leállása miatt emberi életek kerülnek közvetlen veszélybe, vagy megnőhet a személyi sérülések esélye, a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet, súlyos bizalomvesztés állhat elő a szervezettel szemben, a közigazgatási ágazatban a nemzeti adatvagyon helyreállíthatatlanul megsérülhet.[61] Éppen ezért kiemelkedő jelentőséggel bír, hogy a szervezetek megfelelő felkészültséggel rendelkezzenek a kibertámadásokkal szemben.

A kibertéri fenyegetések és az ezzel járó kockázatok kezelése leghatékonyabban a megelőzésre épülő hatékony védelmi intézkedések útján valósítható meg. Az elektronikus információs rendszerek biztonsága érdekében az Ibtv. hatálya alá eső szerveknek, a jogszabályokban meghatározott hatékony fizikai, logikai és adminisztratív intézkedéseket szükséges alkalmazniuk. E feladatok végrehajtásához elengedhetetlen, hogy megismerjék a

[59] E fejezet két tanulmányban került publikálásra: Legárd Ildikó: Információbiztonsági incidenstrendek a közigazgatásban. (Legárd, 2023d) és A közigazgatást érő hazai és európai incidenstrendek összehasonlítása (2023b).
[60] Bor Olivér: Egységesen magas kiberbiztonság az Európai Unióban. In: Szakmai Szemle XXII. évfolyam 1. szám 2024. április, Katonai Nemzetbiztonsági Szolgálat p.181.
[61] 7/2024. MK rendelet 1. melléklet 2.2. pont

közigazgatást fenyegető veszélyeket, az aktuális támadás típusokat, a kiberbiztonsági incidenstrendeket.
Amennyiben ismerik a fenyegetést jelentő kockázatokat, a megelőzésre épülő védelem is sikeresebben alakítható ki.

Bizonyítási cél:
Az európai és a hazai incidenstrendekre irányuló többszempontú, tudományos vizsgálat célja annak megállapítása, hogy a hazai, közigazgatást érő kiberbiztonsági incidensek típusai és annak változásai megfelelnek-e az európai trendeknek. Amennyiben az összehasonlító vizsgálat eredményeként megállapítható a megegyezés, a hazai közigazgatási szervezetek a hatékony kibervédelmi képességeiket az európai incidenstrendek figyelembevételével alakíthatják ki.

3.1.1. Hipotézisek

H1	**A magyar közigazgatást érő kiberbiztonsági incidensek megfelelnek az európai incidenstrendeknek, melyekben meghatározó szerepe van a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadási formának.**

4. táblázat: H1 hipotézis (forrás: saját szerkesztés)

A bizonyítás cél elérése érdekében első lépésként a magyar közigazgatást érintő incidenstrendek kerültek azonosításra a NBSZ NKI által, 2019 és 2021 közötti időszakban detektált információbiztonsági események átfogó elemzése alapján. Ezt követően az európai incidenstrendek meghatározására került sor az ENISA és az Europol, 2019-2021 közötti időszakra vonatkozó jelentései átfogó elemzése segítségével. Utolsó lépésként összehasonlításra kerültek a hazai és az európai incidenstrendek, különös tekintettel a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadási formákra.

3.1.2. Kutatási módszertan

A H1 hipotézis megválaszolására a következő lépéseket hajtottam végre, melyeket részleteiben a következő alfejezetekben ismertetek:

1. Hazai incidenstrendek azonosítása: Az NBSZ NKI által gyűjtött, a 2019-2021 években általuk kezelt incidensekre vonatkozó statisztikai adatok elemzése, az incidenstrendek azonosítása.
   - Kutatási módszer: statisztikai elemzés, megfigyelés.
   - Részfolyamatok leírása: az NBSZ NKI által gyűjtött adatok többszempontú elemzése: évenkénti bontásban, incidenstípusok szerint, szektorális bontásban (külön elemezve az állami és önkormányzati szerveket ért kibertámadásokat), illetve a pszichológiai manipulációra vonatkozó adatok szerint.

     Az elemzés további célkitűzése volt annak megállapítása, hogy mely szektort érte a legtöbb incidens a vizsgált időszakban, és mely incidenstípusok jellemzőek a „legtámadottabb" ágazatban. További kutatási kérdésként merült fel, hogy a pszichológiai manipuláció milyen százalékos arányban mutatható ki a detektált incidenstrendekben.

2. Európai incidenstrendek azonosítása: A jellemző európai incidenstípusokat bemutató jelentések meghatározása, elemzése és az európai incidenstrendek azonosítása.

   Kutatási módszer: dokumentumelemzés.

   Részfolyamatok leírása: Első lépésként azonosítottam a téma szempontjából releváns európai incidenstrendeket bemutató jelentéseket, majd részletes elemzést végeztem az incidensek típusai, valamint a szektorokat érintő kibertámadásokra vonatkozó adatok alapján.

3. Összehasonlítás: A hazai és az európai incidenstrendek összehasonlítása.

   Kutatási módszer: összehasonlító elemzés.

   Részfolyamatok leírása: Előre meghatározott szempontok szerint összehasonlítottam a hazai és az európai incidenstrendeket.

3.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

3.2.1. Hazai incidenstrendek vizsgálata

A biztonsági események típusaival, az eseménykezeléshez kapcsolódó eljárásokkal, feladatokkal több tanulmány is foglalkozik, ugyanakkor kifejezetten a közigazgatást érintő hazai incidenstrendekre vonatkozó tanulmány csupán kettő született.

Az incidenskezeléssel kapcsolatban a legátfogóbb kötet a Nemzeti Közszolgálati Egyetem gondozásában jelent meg **Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára** címmel, szerzői Berzsenyi Dániel, Bodó Attila Pál, Kapitány Sándor, Sági Gábor és Sebők Viktória (Berzsenyi et al., 2022). A kötet az alábbi témákba nyújt részletes betekintést: a kibertér aktuális nemzetközi biztonságpolitikai kihívásai, a biztonsági eseménykezeléssel kapcsolatos elvárások a hazai és a nemzetközi jogban, az eseménykezelés műszaki eszköztára – üzemeltetői, fejlesztői feladatok, valamint az incidenskezelés felhasználói oldala.

Bodó Attila Pál, Marsi Tamás, Sebők Viktória és Zámbó Nóra **Célzott Kibertámadások - Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára** című könyve (Bodó et al., 2022) bemutatja a kibervédelmi szabályozás újdonságait, az államok és szervezetek ellen irányuló legújabb támadás típusokat, kiemelten vizsgálja az ipari létesítmények elleni támadások új trendjeit, valamint a sérülékenységvizsgálatok jelentőségét a célzott támadások megelőzésében.

Beláz Annamária **A közigazgatás információbiztonsága: megjósolhatók az incidensek?** című tanulmányában (Beláz, 2019) elsősorban a valószínűségszámítás és a statisztikai elemzés módszereinek a biztonsági incidensek előrejelzésében és elhárításában betöltött szerepe vizsgálatára irányul, de röviden bemutatja a közigazgatás információbiztonságának védelmét, az információbiztonsági incidensek folyamatát és hatásait is.

Krasznay Csaba, Dobos László, Palla Gergely és Pollner Péter **Információbiztonsági incidensek a közigazgatásban** című közös tanulmánya (Krasznay et al., 2019) az

információbiztonsági folyamat egyik legfontosabb részterületével az incidensmenedzsmenttel foglalkozik a közigazgatásban, tehát olyan biztonsági események kezelésével, amelyek minden megtett védelmi intézkedés ellenére is bekövetkeznek és ezzel megbontják a szervezet biztonsági egyensúlyát. Az incidensekkel kapcsolatos jogi szabályozás kapcsán elsősorban az Ibtv., valamint e törvényben használt fogalmak meghatározásai kerülnek bemutatásra (pl. biztonsági esemény és annak kezelése, súlyos biztonsági esemény).

Az írás lépésenként elemzi az incidensmenedzsment folyamatát, melyek a következők: (1) felkészülés, (2) észlelés és elemzés, (3) elhatárolás, felszámolás és visszaállítás, (4) incidens utáni tevékenységek, valamint külön kitér a személyes adatokat érintő incidens esetén a Nemzeti Adatvédelmi és Információszabadság Hatóság felé történő értesítési kötelezettségre.

Az incidenstípusokat elhárítás szempontjából három csoportra bontották: végponti védelemmel, megfelelő üzemeltetéssel kezelhető incidensek, valamint a komoly védelmi intézkedéseket igénylő incidensek. Az incidensmenedzsment hosszú távú célja az lenne, hogy az első két kategóriába tartozó incidensek aránya csökkenjen a komoly védelmi intézkedéseket igénylő incidensekhez képest. Ugyanis ez azt jelenté, hogy Magyarország közigazgatásának kibervédelmi képességei érdemben javultak, hiszen a rövid távon megoldható intézkedéseket megtették, miközben kiépültek azok a struktúrák, amelyek a komoly hatású incidensek észlelését lehetővé teszik.

Az információbiztonsági incidensek elemzése egy példa segítségével történik, melynek során egy nagy hálózati forgalmat bonyolító szervezet tűzfalforgalmát elemezték a szerzők.

A szakirodalmi áttekintés során, a téma relevanciája szempontjából ki kell emelnem Bányász Péter és Krasznay Csaba tanulmányát, mely 2019-ben jelent meg **Kiberbiztonsági incidensek a magyar közigazgatásban címmel** (Bányász-Krasznay, 2019), mivel ez az egyetlen olyan írás, amely kifejezetten a közigazgatást érő incidenstrendeket azonosít.

A szerzők tanulmányukban a magyar közigazgatás kiberfenyegetettségének vizsgálatát végezték el annak érdekében, hogy feltárják az esetleges hiányosságokat és kezelésükre javaslatokat fogalmazzanak meg. A kritikus infrastruktúra fogalma és a vonatkozó legfontosabb jogszabályok ismertetését követően, a szerzők bemutatják a kritikus infrastruktúrák jelentőségét az állami működésben. Megállapításra kerül, hogy az államnak

kiemelt szerepe van a kibertér szabályozásában és komoly érdeke fűződik a kiberbiztonság megteremtéséhez, kiemelten a kritikus infrastruktúrák védelméhez. Ezt követően bemutatják az incidenskezelés legfontosabb fogalmait (kibertér, fenyegetés, fenyegetettség, bizalmasság, sértetlenség, rendelkezésre állás, biztonsági esemény), majd elemzik a legfontosabb incidens típusokat és azok kockázati besorolását. Az írás külön kitér a kibervédelem hazai intézményrendszerére, és felvázolja annak kezdeti (2015. október 1. előtti), majd a Nemzeti Kibervédelmi Intézet létrejöttét követő, jelenlegi struktúráját.
A magyar közigazgatás kiberfenyegetettségét a Nemzeti Kibervédelmi Intézethez 2015-2016-ban bejelentett incidensek száma alapján vizsgálja a tanulmány. A szerzők által kidolgozott mutató alapján három csoportba osztották az incidenseket: végponti védelemmel (28%), megfelelő üzemeltetéssel kezelhető incidensek (52%), valamint a komoly védelmi intézkedéseket igénylő incidensek (20%). Az eredmények alapján meghatározásra kerültek az ország kiberbiztonsági képessége növelése érdekében fejlesztendő területek, melynek keretében kiemelték a biztonságtudatosság jelentőségét és folyamatos fejlesztése szükségességét.

3.2.2. Social engineering típusú támadások

A bizonyítás során külön részben kerülnek bemutatásra a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadások kapcsán kimutatható hazai és az európai incidenstrendek, ezért a továbbiakban röviden bemutatom e támadási forma fogalmát, illetve jellemzőit a szakirodalom alapján.

Az elmúlt évtizedekben az információs rendszerek védelme egyre kifinomultabbá vált, ugyanakkor a rendszereket használók biztonságtudatossága nem tartott lépést a technikai fejlődés ütemével. Így nem meglepő, hogy a kiberbűnözők egy új és nagyon hamar népszerűvé vált támadási formát kezdtek el alkalmazni, az ún. **social engineering**-et.
A social engineering az emberi hiszékenységre, együttműködő képességére építő támadási forma. A támadók olyan alapvető emberi tulajdonságokat használnak ki, mint a segítőkészség, a hiszékenység, a befolyásolhatóság, a naivság, vagy a kíváncsiság, amely jó eséllyel minden emberben ott lakozik, melyekhez hozzáadódhat a biztonságtudatosság különböző okokból (alulképzettség, hanyagság stb.) bekövetkező hiánya, valamint a támadó általi szándékos megfélemlítés, zsarolás, vagy megvesztegetés. Ezek

kihasználásával már a támadó könnyen, vagy mindenesetre könnyebben megkerülheti a rendszerek fizikai és logikai védelmi vonalát, pl. tűzfalakat vagy behatolás detektáló rendszereket. (Muha - Krasznay, 2019., 50.)

Attól függően, hogy a támadó milyen módszereket használ, két fajta támadási csoportot tudunk megkülönböztetni[62]:

a) **Humán-alapú támadások**:

A humánalapú technikák alkalmazásához nem feltétlenül szükséges szaktudás, a támadó nem használ informatikai eszközöket, bárki által kivitelezhető, azonban előzetes megfigyelést és felkészülést igényel. A támadó és áldozata között közvetlen kontaktust feltételez, így a lebukás veszélye is nagyobb.

Típusai:

- segítség kérése;
- segítség nyújtása (fordított social engineering);
- megszemélyesítés, vagyis az identitás lopás;
- thumbstone theft, azaz a sírkő lopás, mely a megszemélyesítés egy speciális fajtája;
- shoulder surfing (képernyő lelesése);
- az irodai hulladék átvizsgálása, azaz a dumpster diving;
- tailgating, vagyis a szoros követés módszere a bejáraton történő bejutáshoz;
- piggybackin: a támadó az áldozat segítségével és tudtával jut át a bejáraton.

b) **Számítógép-alapú támadások:**

A közvetett kapcsolattartást preferáló, számítógép-alapú támadások sokkal elterjedtebbek, mivel a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal, így kisebb a lebukás veszélye.

Típusai:

- **adathalászat – phishing**: olyan, jellemzően e-mail küldése az áldozatnak, amely megtéveszti őt és olyan hamis weboldalra „irányítja át”, ahol kiadja személyes

[62] Deák Veronika A social engineering humán alapú támadási technikái (Deák, 2017a) és A számítógép alapú social engineer támadási technikák (Deák, 2017b), valamint Dr. Bányász Péter Social engineering and social media (Bányász, 2018) című tanulmányaikban részletesen elemzik e támadási csoportokat és formákat.

adatait, felhasználó nevét, jelszavát. (Több vállfaja ismert: hamisított e-mailek és hamisított weboldalak (scam); vishing (VOIP csalás), vagyis telefonos adathalászat; smishing, melynek során az adathalász üzenet sms-ben érkezik; pharming, azaz az eltérítéses adathalászat; whailing, vagyis „bálnavadászat", amelyek esetében a célpontok köre a vezetői réteg; nyereményjátékokat, ajándékokat vagy ingyenes szolgáltatásokat hirdető áloldalak.)

- **kártékony programok**: a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a file-on, amelyek segítségével megszerezhetik a célszemély vagy egy szervezet adatait. (Például: keylogger, azaz billentyűzet naplózó; baiting: fertőzött, kártékony kódokat tartalmazó adathordozó eszköz (pendrive, CD, DVD, SD kártya) „elvesztése" a kiszemelt szervezetnél vagy annak közelében, amit a gyanútlan és óvatlan alkalmazott csatlakoztat a saját gépéhez, így megfertőzve a saját, sőt jó eséllyel az egész szervezetet; javítás, frissítés felajánlása; trójai programok; veszélyes csatolmányok.)[63]
- **Wi-Fi hálózat veszélyei**: a hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat, így elsősorban a nyílt hozzáférésű Wi-Fi hálózatok rejtenek magukban veszélyeket, hiszen gyakran adathalász célokat szolgálnak, bár előfordulhat jelszóval védett hálózatok esetében is.
- **okostelefon alkalmazások általi hozzáférés** – alkalmazásengedélyekből fakadó kockázatok: az okostelefonra telepített alkalmazások nem csak a készülék alapvető funkcióihoz, hanem használatukért cserébe egyéb adatokhoz és információkhoz is kérnek és általában kapnak hozzáférést, mint pl. a felhasználó személyes adataihoz, névjegyeihez, fényképeihez, üzeneteihez stb.

Bár céljától függően a támadás más és más környezetben kerül végrehajtásra, általában négy lépésből áll, melyek egymásra épülve kerülnek végrehajtásra. A lépések a következők:

1. **információszerzés**: tipikusan internetről szerzett információk: közösségi hálózatok, keresőoldalak, a szervezet saját honlapja, telefonon keresztüli / írásban történő információszerzés, esetleg személyes felkeresés;
2. **kapcsolat kiépítése** a cél szempontjából legalkalmasabbnak ítélt és kiválasztott személlyel, aki akár egy vezető is lehet;

[63] A kártékony kódok social engineering technikákon keresztül történő terjedését Deák Veronika külön tanulmányban mutatja be (Deák, 2019.).

3. **kapcsolat kihasználása**;
4. **támadás végrehajtása**.[64]

A social engineering típusú támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Napjainkban az esetek döntő többségében a támadók az internet segítségével, online és elsősorban a közösségi oldalakról (pl. Facebook, Twitter, LinkedIn) gyűjtik a szükséges információkat, mivel ezeken az oldalakon kis költséggel, gyorsan, nagy mennyiségű adat érhető el (Deák, 2018., p. 396.).[65] A személyre utaló információk megszerzése elősegíti a tökéletes célpont, a leggyengébb láncszem kiválasztását a szervezetnél, akin keresztül majd a támadók sikeresen férhetnek hozzá a kívánt rendszerhez.

A social engineering, mint támadási forma különböző szempontú kutatásának hazánkban széleskörű és egyre bővülő irodalma van, ezért jelen szakirodalmi áttekintésben csupán kiemelném a témában jelentősebb számú publikációval rendelkező kutatókat, úgy mint Rajnai Zoltán (Albininé, Rajnai 2020; Albininé, Rajnai 2021), Póser Valéria (Szarvák, Póser 2021; Szarvák, Póser 2020), Oroszi Eszter Diána (Oroszi 2021.; Barna, Kollár, Oroszi 2023) és Kollár Csaba (Jagodics, Kollár 2023.; Kollár, Zakar 2020a; Kollár, Zakar 2020b).

A **nemzetközi tudományos világban** a pszichológiai manipuláció segítségével megvalósuló kibertámadásokról nagyszámú publikáció született, melyből ki kell emelni a social engineering fogalom megalkotóját Kevin Mitnicket. Mitnick korábban a világ egyik legkeresettebb hackere volt, aki számítógépes bűncselekményekért többször is börtönbe került. Később azonban, a hackerként eltöltött évek alatt megszerezett tudását és tapasztalatait felhasználva saját biztonsági céget alapított, oktatási programot dolgozott ki, valamint számos könyvet írt és tartott előadást a kibertámadások megelőzéséről. Leghíresebb könyvei **A legendás hacker. A megtévesztés művészete** (Mitnick, 2003), **A legendás hacker. A behatolás művészete** (Mitnick 2006), valamint **A legkeresettebb hacker. Az emberi hiszékenység sötét oldala** (Mitnick 2012).

[64] Muha - Krasznay, 2019., p. 55-57.
[65] Ez utóbbi témát Dr. Bányász Péter A közösségi média, mint a nyílt forrású információszerzés fontos területe (Bányász 2015) és Social engineering and social media (Bányász 2018) című tanulmányaiban elemzi.

A SANS Institue gondozásában már 2003-ban megjelent David Gragg írása **A Multi-Level Defense Against Social Engineering** címmel (Gragg 2003). A tanulmány áttekinti a social engineering támadási formákat, majd elemzi azokat a pszichológiai tényezőket, melyek hozzájárulnak a támadás sikerességéhez, végül bemutat egy többszintű védelmi mechanizmust (pl. biztonsági politika, biztonságtudatossági képzés, ellenállóképesség növelése, incidensekre való reagálás), amely segítséget nyújthat a megelőzésben.

Pekka Tetri és Jukka Vuorinen **Dissecting social engineering** című tanulmányának (Tetri – Vuorinen, 2012) célja a social engineering fogalmának meghatározása az elkövetésre jellemző technikák elemzésén keresztül. A támadási technika három dimenzióját különböztetik meg: a meggyőzést, a támadás felépítését és az adatgyűjtést. Álláspontjuk szerint a social engineering minden aspektusa megragadható és leírható e három dimenzió segítségével.

Az elmúlt években nagyon sok tanulmány foglalkozott a social engineering témakörével, ugyanakkor a legtöbb szakirodalom megjegyzi, hogy ennek ellenére még mindig lemaradás tapasztalható a kutatás területén a kapcsolódó keretrendszer megalkotásában, a formális definíciók, valamint a támadási minták meghatározásában. Mouton és társai **Social engineering attack examples, templates and scenarios** című írásukban éppen ezért a valóságban megtörtént social engineering támadások alapján határoznak meg támadási mintákat annak érdekében, hogy megalkossák a támadások részletes forgatókönyvét. (Mouton et al., 2016)

Joseph M. Hatfield **Social engineering in cybersecurity: The evolution of a concept** című tanulmánya (Hatfield, 2018) a kiberbiztonságban alkalmazott social engineering fogalmának történetét mutatja be, valamint nyomon követi a fogalom átterjedését a kiberbiztonságra az 1960-1980-as években. Végezetül a kiberbiztonságról 1990 és 2017 között írt tudományos cikkekben található 134 fogalom-meghatározás elemzésén keresztül feltárja a fogalom egyéb jelentéstartalmát is.

Conteh és Schmick **Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks** című írása (Conteh - Schmick, 2021) bemutatja a social engineering fogalmát, és elemezi a hálózati behatolásban és a kiberidentitás-lopásban, valamint a kiberbűnözés terjedésében játszott szerepét. A szerzők arra a

következtetésre jutnak, hogy bár a technológiának szerepe van a social engineering támadások hatásának csökkentésében, a sebezhetőség az emberi viselkedésben, az emberi impulzusokban és a pszichológiai jellemzőkben rejlik. A tanulmányban néhány megelőző intézkedést és lehetséges megoldást is javasolnak a social engineering jelentette fenyegetések ellen.

A social engineering típusú támadások megelőzésében kulcsszerepet játszó biztonságtudatosság és biztonságtudatosítás fogalmával, tartalmával, a vonatkozó nemzetközi és hazai szakirodalom áttekintésével az 5. fejezet foglalkozik részletesen.

3.3. HAZAI INCIDENSTRENDEK AZONOSÍTÁSA[66]

3.3.1. A biztonsági események kezelése

Az értekezés által bemutatott vizsgálatok a 2019-2021 közötti időszakra jellemző incidenstrendekre vonatkoznak, ezért a biztonsági események kezelésére vonatkozó fogalmak, szabályok, valamint az eseménykezelést ellátó hazai szervezetrendszer bemutatása a vizsgálatok elvégzésének idejében hatályos Ibtv. és végrehajtási rendeletei alapján kerülnek bemutatásra.

Az Ibtv. Preambuluma kimondja, hogy „A nemzet érdekében kiemelten fontos - napjaink információs társadalmát érő fenyegetések miatt - a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.”. Az elektronikus információs rendszer biztonsága érdekében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

[66] A fejezet Legárd Ildikó: Információbiztonsági incidenstrendek a közigazgatásban című tanulmányban került publikálásra. (Legárd, 2023d)

d) **a biztonsági események kezelését**.[67]

Az Ibtv. értelmező rendelkezése -1.§ (1)-értelmében:

- **biztonsági esemény**: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
- **súlyos biztonsági esemény**: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- **biztonsági esemény kezelése**: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.[68]

A biztonsági események kezelését -az eltérő ellátotti körre tekintettel- az alábbi szervezetek látják el:

- **NBSZ NKI**, mely kezeli:
    a) az Ibtv. 2. §-ában - az Ibtv. 19. § (2) bekezdése szerinti kivétellel - meghatározott szervek nyílt,
    b) a bejelentés-köteles szolgáltatók,

[67] Ibtv. 6.§

[68] A Kibertv. az alábbi fogalmakkal váltja fel a biztonsági esemény és eseménykezelés fogalmait:

- **kiberbiztonsági incidens**: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;
- **kiberbiztonsági incidenskezelés**: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;

c) a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,

d) a központosított informatikai és elektronikus hírközlési szolgáltató elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.

– **Katonai Nemzetbiztonsági Szolgálat**: az Ibtv. 19. § (2) bekezdése alapján a honvédelmi célú elektronikus információs rendszereket érintő biztonsági eseményeket és fenyegetéseket kezeli.

Az NBSZ NKI-n, illetve a KNBSZ-en kívül speciális eseménykezelési feladatokat lát el a **HUNCERT**, mely a Magyar Internet Szolgáltatókat segíti a számítógépes hálózati incidensek kockázatainak kezelésében, valamint az ilyen incidensek esetén az incidensesek felderítésében, kezelésében és elemzésében.[69]

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szakszolgálat szervezetén belül 2015. október 1-jével került létrehozásra a Nemzeti Kibervédelmi Intézet, melynek tevékenysége három pillérre épül:

– hatósági feladatok ellátása: az Ibtv.-ben, valamint a 187/2015 (VII.13.) Korm.rendeletben[70] meghatározott feladat-és hatáskörben a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozik;
– incidenskezelési tevékenység: az eseménykezelő központ a kibertérből érkező támadásokkal és fenyegetettségekkel kapcsolatos eseménykezelési feladatokat látja el;
– sérülékenységvizsgálat: az informatikai rendszerek gyenge pontjainak feltárására, a rendszer védelmi képességének tesztelésére irányul.

Biztonsági események kezelése során az NBSZ NKI:

– az Ibtv. 2. §-ában meghatározott szervek – a honvédelmi célú elektronikus információs rendszerek kivételével – nyílt,
– az alapvető szolgáltatást nyújtó szolgáltatók és a bejelentés-köteles szolgáltatók,

[69] https://www.cert.hu/ (Letöltve: 2022.11.11.)
[70] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

- a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,
- a központosított informatikai és elektronikus hírközlési szolgáltató, valamint
- a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat

elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket kezeli.[71]

Az **incidensek kezelésének alapszabályait** az Ibtv. felhatalmazása alapján az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet fekteti le, amely rendelkezik az intézmények és az eseménykezelő központ jogairól és kötelességeiről, valamint egyéb lehetőségekről is.

3.3.2. Az NKI által kezelt incidensek statisztikai adatai

Az NBSZ NKI az általa detektált és gyűjtött, incidensekre vonatkozó statisztikai adatokat az alábbi kategorizálás szerint tagolva, kutatási célból bocsátotta a rendelkezésemre 2022. februárban:

1. évenkénti bontás (havi bontásban is),
2. szektorális bontás,
3. incidensek típusai szerinti bontás.

1. **Évenkénti bontás**: 2019, 2020, 2021 évenként, havi bontásban is.

2. **Szektorális bontás**
   - **Állami és önkormányzati szervek**: Az Ibtv. 2.§-ában meghatározott szervek;
   - **Nemzeti létfontosságú rendszerelemek**: 2012. évi CLXVI. törvény (továbbiakban: Lrtv.)[72] alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással (energia, közlekedés,

[71] Ibtv. 19-20.§, 271/2018. (XII.20) Korm.rendelet 3.§ (1)
[72] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) 1.§ k)

agrárgazdaság, egészségügy, TB, pénzügy, infokommunikációs technológiák, víz, honvédelem, közbiztonság-védelem);

- **Alapvető szolgáltatásokat nyújtó szereplők**[73]: az Lrtv. alapján alapvető szolgáltatásokat nyújtó szereplőnek azon szervezet vagy gazdasági szereplő intézmény jelölhető ki, mely:
    - alapvető szolgáltatást nyújt (kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás),
    - az általa nyújtott alapvető szolgáltatás elektronikus információs rendszerektől függ,
    - az általa nyújtott alapvető szolgáltatást érintő biztonsági esemény - kormányrendeletben meghatározott - jelentős zavart okozna szolgáltatás nyújtásában és
    - az erre irányuló eljárásban alapvető szolgáltatást nyújtó szereplőként került azonosításra.
- **Bejelentés köteles szolgáltatók**: 2001. évi CVIII. törvény (továbbiakban: Ekertv.) alapján bejelentés köteles szolgáltatást nyújtónak minősül a magyarországi székhelyű gazdasági társaság, amely a következő információs társadalommal összefüggő szolgáltatások valamelyikét nyújtja:
    - aki online piacteret működtet vagy egy elérhető online piactér igénybevételével online adásvételi és szolgáltatási szerződések megkötését teszi lehetővé fogyasztók és kereskedők/ kereskedő és kereskedő között,
    - keresőszolgáltatást,
    - felhőalapú számítástechnikai szolgáltatást nyújt[74].
- **Közvetítő szolgáltatók**: Az Ekertv. alapján az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely
    - az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);

[73] 2012. évi CLXVI. törvény (Lrtv.) 1.§ d)

[74] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (továbbiakban: Ekertv.) 2.§ j)

- az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
- az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
- információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);
- alkalmazásszolgáltató;
- videómegosztóplatform-szolgáltató.[75]

– **Nemzetbiztonsági védelem alá eső szervezetek**: A nemzetbiztonsági védelem alá eső szervek és létesítmények köréről szóló 2009/2015. (XII. 29.) Korm. határozat 1. mellékletében felsorolt szervek (például: NAIH, AB, ÁSZ, KEH, OBH…)
– **Oktatási intézmények**
– **Egyéb szervezetek**:
  - a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők[76],
  - a központosított informatikai és elektronikus hírközlési szolgáltató[77],
  - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat[78],
  - egyéb bejelentések alapján.

3. Incidensek típusai szerinti bontás

Az NBSZ NKI az incidens típusok meghatározásánál a mai ENISA elődjeként működő, Európai Unió Hálózat- és Információbiztonsági Ügynökség által kidolgozott rendszer egy módosított változatát használja, ugyanis a magyar gyakorlat nem sorol be minden incidenst biztonsági eseménynek, amelyet az ENISA annak tekint (Marsi, 2018).

[75] 2001. évi CVIII. (Ekertv.) tv. 2.§ l)
[76] 271/2018. (XII. 20.) Korm. Rendelet 3.§ (1)
[77] 271/2018. (XII. 20.) Korm. Rendelet 3.§ (1)
[78] Ibtv. 20.§ (3)

Az eseménykezelő központ által 2019-2021 években detektált események az alábbi incidenstípusok szerint kerültek meghatározására:

- **Adminisztrátor fiók kompromittálódása (Privileged account compromise):** Privilegizált hozzáféréssel rendelkező (pl. rendszergazdai) fiók hitelesítő adatainak nyilvánosságra kerülése.
- **Behatolás (Intrusions)**: Ez jelentheti egy rendszer vagy alkalmazás (szolgáltatás) sikeres kompromittálását is, amely történhet távolról egy ismert vagy új sebezhetőség révén, de akár jogosulatlan helyi hozzáférés is okozhatja. Ide tartozik a botnet is.[79]
- **Behatolási kísérlet (Intrusion Attempts)**: Egy rendszer veszélyeztetésére vagy bármely szolgáltatás megzavarására irányuló kísérlet, például ismert vagy ismeretlen sérülékenység kihasználása révén, vagy többszöri bejelentkezési kísérlettel (jelszavak kitalálása / feltörése, brute force).[80]
- **Bejelentkezési kísérlet (Login attempts)**: többszöri bejelentkezési kísérlet pl. jelszavak kitalálása / feltörése, brute force segítségével.[81]
- **C&C szerver**: A parancs- és vezérlőkiszolgáló (C&C) egy támadó vagy kiberbűnöző által vezérelt számítógép, amelyet arra használnak, hogy parancsokat küldjenek a rosszindulatú programok által feltört rendszereknek, és fogadjanak ellopott adatokat a célhálózatról. Számos kampányban felhőalapú szolgáltatásokat, például webmail- és fájlmegosztó szolgáltatásokat használnak C&C-kiszolgálóként, hogy elvegyüljenek a normál forgalomban és elkerüljék a felderítést.[82]
- **DDoS**: Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás, olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatásigénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet (Muha-Krasznay (2014) p. 115.);
- **Defacement research**: weboldal rongálása.
- **DoS**: Denial of Service – szolgáltatásmegtagadással járó támadás (Berzsenyi et al, 2018, p. 392.)

[79] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[80] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[81] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[82] https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (Letöltve: 2022.11.11.)

- **Elérhetőség (Availability)**: Az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható.[83]
- **Erőforrások illetéktelen használata (Unauthorized use of resources)**: Az erőforrások jogosulatlan célokra történő felhasználása, beleértve a nyereségszerzést is (pl. az e-mail használata illegális profitszerző lánclevelekben való részvételre vagy piramisjátékokban).[84]
- **Féreg (Worm)**: Olyan program, amely a számítógép hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig és károkozó hatását önmaga – a számítógép összeomlásáig tartó – reprodukálásával, továbbításával éri el (Muha-Krasznay, 2014., p. 116.).
- **Illicit/Sértő tartalom (Abusive Content)**: például spam, harmful speech, azaz valakinek a lejáratása vagy diszkriminációja (pl. internetes zaklatás, rasszizmus, fenyegetések egy vagy több személy ellen), illetve ide tartozik a gyermekpornográfia és az erőszak magasztalásával kapcsolatos tartalmak is.[85]
- **Információbiztonság (Information Security)**: Az adatokkal és rendszerekkel való helyi visszaélés mellett az információbiztonságot veszélyeztetheti egy fiók vagy alkalmazás sikeres kompromittálása, valamint olyan támadások, amelyek révén információkat hallgatnak le és férnek hozzá átvitel közben (lehallgatás, hamisítás vagy eltérítés). Ugyanakkor az emberi/konfigurációs/szoftverhiba is veszélyeztetheti az információbiztonságot.[86]
- **Információgyűjtés (Information Gathering)**: például szkennelés (scanning) útján, melynek során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (pl. DNS-lekérdezés, portellenőrzés). Információ gyújthető lehallgatás (sniffing) útján is, mely a hálózati forgalom megfigyelése és rögzítése. A social engineering technikák is alkalmasak információgyűjtésre.[87]

[83] Ibtv. 1.§ (1) 38. pont
[84] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[85] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[86] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)
[87] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)

- **Információk illetéktelen hozzáférése (Unauthorised access to information)**: Az elkövető jogosulatlanul fér hozzá adatokhoz, információkhoz (pl. felhasználói fiókok feltörése).
- **Információk illetéktelen módosítása (Unauthorised modification of information)**: Az elkövető az információs rendszerben információt módosít vagy töröl.
- **Ismeretlen típusú káros kód:** ismeretlen rosszindulatú számítógépes program (pl. vírus, féreg, logikai bomba, kémprogram stb.).
- **Ismert sérülékenység kihasználása (Exploiting known vulnerabilities)**: A sérülékenység az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat (Muha-Krasznay, 2014., p.121.).
- **Káros tevékenység**: káros kód, fertőzött rendszer, C&C server, káros kód konfiguráció.
- **Letapogatás (Scanning)**: Szkennelés (scanning) során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (pl. DNS-lekérdezés, portellenőrzés).[88]
- **Logelemzés**: Például a vállalati informatikai rendszerek, tűzfalak, behatolás gátló-, és vírusirtó rendszerek naplóbejegyzéseinek, elemzése.
- **Megszemélyesítés (Masquerade)**: A social engineering egy esete, amikor egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel (Muha-Krasznay, 2014., p.119.).
- **Nem-adminisztrátor fiók kompromittálódása (Unprivileged account compromise)**: Nem privilegizált, átlagfelhasználói hozzáféréssel rendelkező fiók hitelesítő adatainak nyilvánosságra kerülése.
- **Nyitott port (Open port)**: „nyitott kapuk", amelyeken elérhetők a hálózat szolgáltatásai, így például a vírusok ezen a porton keresztül is bejuthatnak a szerveztek informatikai rendszereibe és gépeibe, ezáltal megbénítva a működést.
- **Pszichológiai manipuláció (Social engineering)**: A social engineering az emberi hiszékenységre, együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ

[88] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)

megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva (Muha-Krasznay, 2014., p.53.).

- **Ransomware**: zsarolóvírus.
- **Spam** (levélszemét): minden olyan kéretlen üzenet, amelyet tömegesen küldenek (kéretlen tömeges e-mail vagy UBE).[89]
- **SPAM IP**: Egy botnet fertőződésből fakadóan, spamelés miatt a használt IP cím feketelistákra kerülhet, és bizonyos levelező szerverek nem fogják befogadni az innen érkező, küldött leveleket.[90]
- **Trójai (Trojan)**: Olyan kártékony program, amelyet alkalmazásnak, játéknak, szolgáltatásnak, vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását (Muha-Krasznay, 2014., p.122.).
- **Visszaélés (Fraud)**: pl. erőforrások illetéktelen használata, megszemélyesítés, adathalászat, vagy licenc nélküli kereskedelmi szoftverek vagy egyéb szerzői jogi védelem alatt álló másolatok felajánlása vagy telepítése.[91]
- **Zaklatás (Harassment)**: bántó, valótlan üzenetek küldözgetése online (Monori, 2016., p. 247.).

3.3.3. Elemzés: Évenkénti összehasonlítás

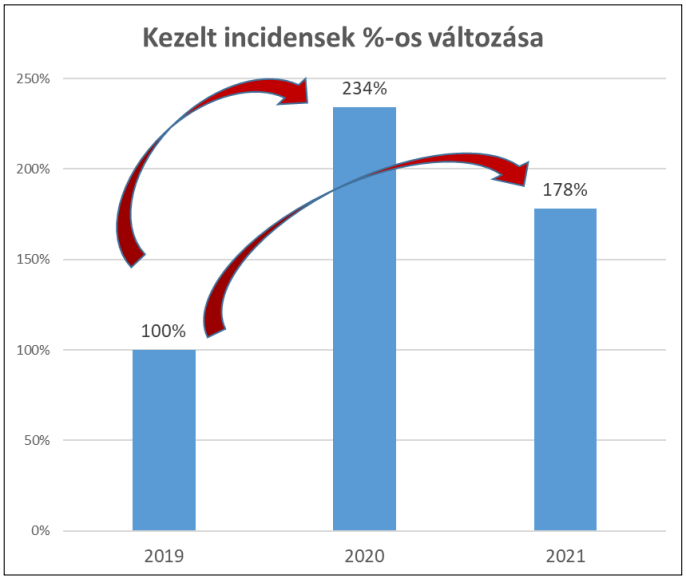
3.3.3.1. Az NKI által detektált incidensek összehasonlítása évenként és incidens típusokként

Az NKI az incidensekre vonatkozó átadott adatokat számszerűen – hónaponként, szektoronként és incidens típusonként- bocsátotta a rendelkezésemre. Tekintettel arra, hogy az Ibtv. 22.§ (4) bekezdése szerint az NBSZ NKI eljárásai során keletkezett adatok nem nyilvánosak továbbá, a konkrét számadatok tükrében olyan - a kapacitásaikra és képességeikre vonatkozó - következtetések is levonhatók, amelyek megnehezíthetnék a szolgáltatások ellátását, a konkrét számadatok nem publikálhatók. Az adatok feldolgozása során kizárólag a számadatokból levont következtetéseket, a számadatokban való változás százalékos mértékét, vagy egymáshoz viszonyított arányát lehet bemutatni. A disszertáció

[89] https://www.eset.com/hu/levelszemet/ (Letöltve: 2022.11.11.)
[90] https://nki.gov.hu/it-biztonsag/tudastar/keretlen-level-feketelista-spam-blacklist/ (Letöltve: 2022.11.11.)
[91] Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)

az adatok elemzése során a fenti követelmények figyelembevételével mutatja be a hazai incidenstrendeket.

Az NKI által kezelt incidensek százalékos eloszlását évenkénti összehasonlításban a 3.ábra szemlélteti.



3. ábra: Kezelt incidensek százalékos eloszlása évenkénti összehasonlításban (forrás: saját szerkesztés)

A grafikon segítségével egyértelműen kimutatható, hogy amennyiben a 2019-es évben, az összes kezelt incidens számát tekintjük 100%-nak, akkor a 2020-ban kezelt összes incidensek száma közel két és félszeres emelkedést mutat, és bár arányait tekintve csökkenés tapasztalható a 2021-es évben, ugyanakkor 2019-hez viszonyítva a kezelt incidensek aránya még mindig meredeken emelkedett.

A tapasztalható emelkedés lehetséges okai a következők lehetnek:

- Early Warning System (EWS): 2020. május 30-án hatályba lépett az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) kormányrendelet, melynek értelmében a korai figyelmeztető szolgáltatás nyújtására a NBSZ NKI került kijelölésre. Az EWS egy szignatúra alapú illetéktelen hálózati behatolást jelző rendszer (Network Based Intrusion Detection System - NIDS), amely kifejezetten nyílt internetről elérhető rendszerek (pl. weboldalak) elleni támadásokat képes felismerni és jelezni.
- koronavírushoz kapcsolódó világjárvány és az ezzel összefüggésbe hozható megtévesztő levelek, álhírek, közösségi média üzenetek, valamint az új

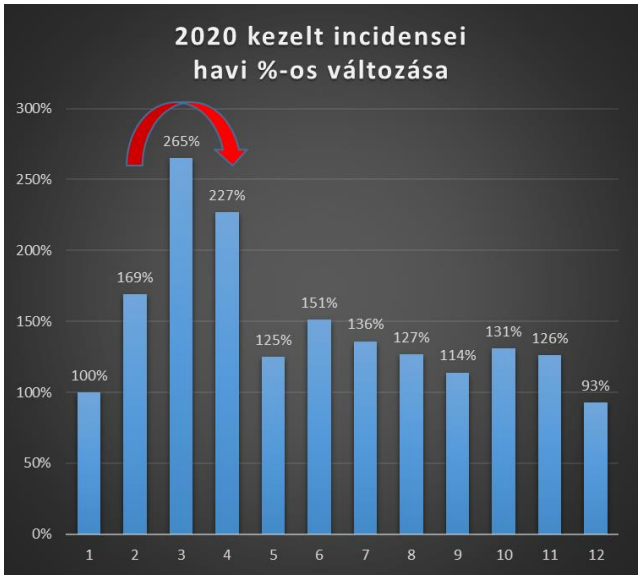
koronavírussal kapcsolatos, COVID-19 témájú káros tartalmú mobil alkalmazások és weboldalak;

– távmunka, otthoni munkavégzés kockázatai.

A Deloitte által készített, a COVID-19 járvány hatásait vizsgáló tanulmány szerint a felhasználók 47%-át érte adathalász támadás az otthoni munkavégzés során. 2020. február és május között a videókonferencia szolgáltatásokat igénybe vevő, több mint fél millió felhasználó adatait szerezték meg a támadók, és adták el a dark weben. Azon kibertámadások száma, amelyek korábban még nem ismert rosszindulatú programokat vagy módszereket alkalmaztak a korábbi 20%-ról a pandémia alatt 35%-ra emelkedtek.[92]
Az Interpol a COVID-19-hez kapcsolódó kiberfenyegetések kapcsán az adathalászatra, a különböző csalásokra, a rosszindulatú domain nevek, a malware-ek, a ransomware-ek valamint az álhírek gyorsan emelkedő terjedésére figyelmeztetett.[93]

2020. év vizsgálata

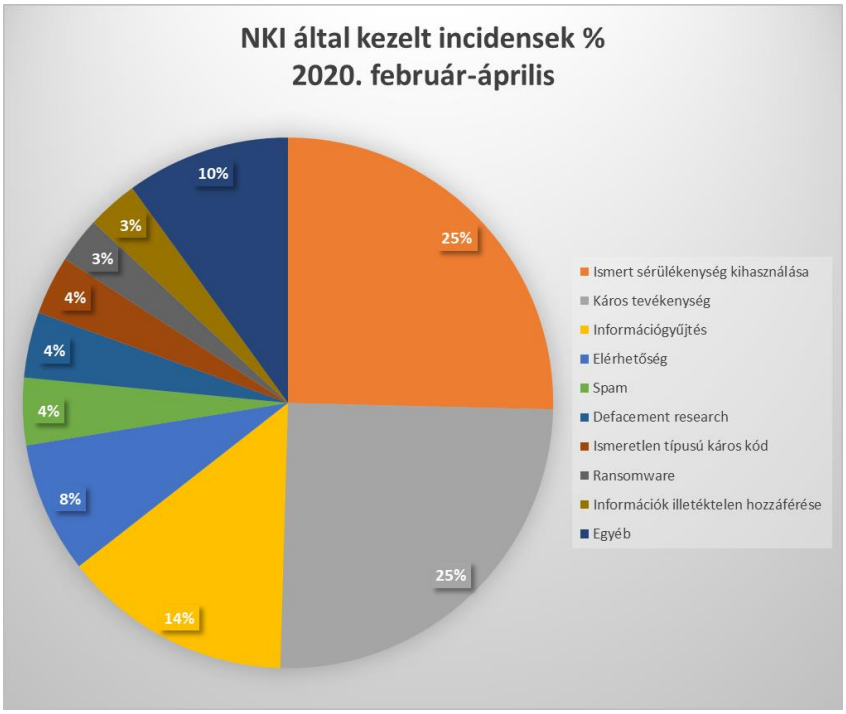
Ahhoz, hogy hazai viszonylatban is megvizsgáljam a világjárvány hatásait, elemezni szükséges a 2020. év emelkedő tendenciát mutató hónapjaiban azonosított incidens típusokat.



4. ábra: A 2020-ban kezelt incidensek havi eloszlása (forrás: saját szerkesztés)

[92] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (Letöltve: 2022.11.11.)
[93] https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats (Letöltve: 2022.11.11.)

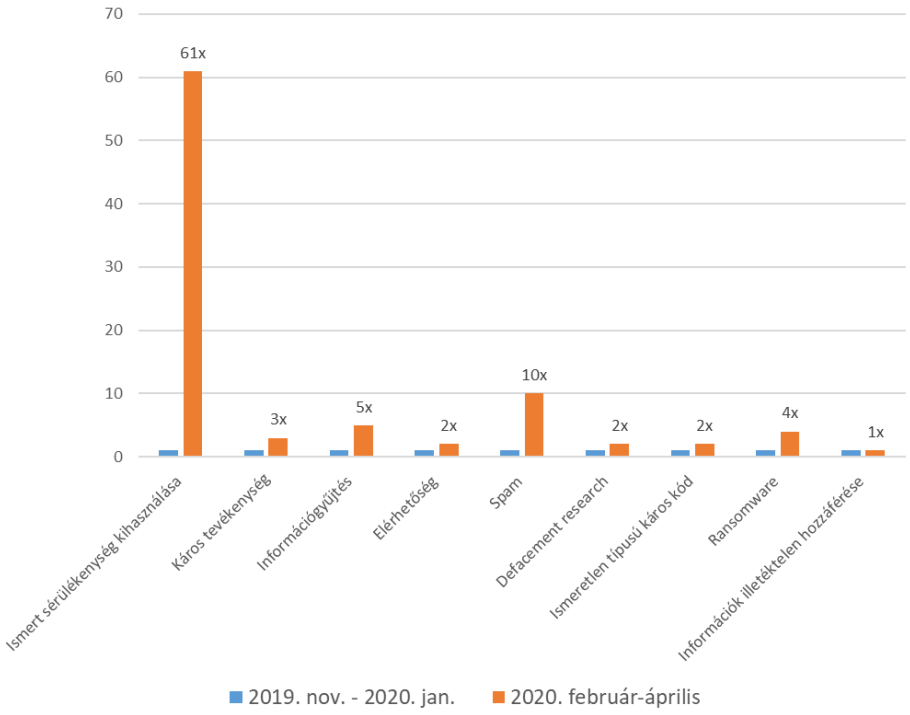
A havi eloszlásokból egyértelműen megállapítható, hogy az incidensek száma a COVID-19 első hullámában indult meredek emelkedésnek. A márciusban kezelt incidensek –a 2020-ban kezelt incidensek összesített számához viszonyított- százalékos aránya több, mint két és félszeres emelkedést mutat a januári eredménnyel összehasonlítva.
A 2020. február-április közötti időszakban az NKI által kezelt incidensek típusai a következők:



5. ábra: az NKI által kezelt incidens típusok 2020. február-április (forrás: saját szerkesztés)

Az incidensek képzeletbeli dobogóján az első három helyen az alábbi incidensek szerepelnek: első helyen megosztottan az ismert sérülékenység kihasználása (25%) és a káros tevékenység (25 %), második helyen az információgyűjtés (14%), a harmadik helyen pedig az elérhetőség (8%) szerepel.

Amennyiben összehasonlítjuk a 2020. február és április közti, valamint az azt megelőző három hónapot (2019. november és február között), az egyes incidens típusok esetén a következő emelkedést tapasztalhatjuk:



6. ábra: 2020. február-április és 2019. november -2020. január összehasonlító vizsgálata (forrás: saját szerkesztés)

A grafikon alapján megállapítható, hogy az ismert sérülékenység kihasználása mutatja a legnagyobb emelkedést (61-szeres), de a spam-ek (10x), az információgyűjtés (5x), a ransomware (4x), valamint a káros tevékenység is (3x) többszörös növekedést mutat.

Az ismert sérülékenység kihasználása tekintetében, amennyiben megvizsgáljuk a jelzett időszakban az NKI által kiadott riasztásokat, tájékoztatásokat, híreket, megállapíthatjuk, hogy az emelkedés hátterében több olyan konkrét fenyegetés is azonosítható, amelyek egyenként is okozhatták a kiemelkedő statisztikai eredményt. Ilyen fenyegetések többek között: Microsoft Windows 0. napi sérülékenysége[94][95], az Exchange mail szerverek ellen detektált támadások[96], a HP Support Assistant segédprogramjának kritikus sérülékenysége, az Adobe és Oracle szoftverek[97], valamint a VMware vCenter Server[98] sérülékenységei.

[94] A nulladik napi (más néven 0-day) sérülékenység olyan számítógépes szoftveres biztonsági rés, amely ismeretlen azok számára, akik érdekeltek lennének a sebezhetőség enyhítésében, befoltozásában (beleértve a célszoftver gyártóját is). A biztonsági rést kihasználva a hackerek hozzáférhetnek a számítógépes programokhoz, adatokhoz, további számítógépekhez vagy hálózatokhoz. Forrás: Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2018., p. 42. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7229/C%E9lzott%20kibert%E1mad%E1sok.pdf?sequence=1

[95] https://nki.gov.hu/figyelmeztetesek/riasztas/microsoft-windows-0-napi-serulekenysegek/ (Letöltve: 2022.11.11.)

[96] https://nki.gov.hu/it-biztonsag/hirek/exchange-szerverek-veszelyben/ (Letöltve: 2022.11.11.)

[97] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-adobe-szoftverek-serulekenysegeirol-4/ (Letöltve: 2021.11.11.), https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztato-oracle-szoftverek-serulekenysegeirol/ (Letöltve: 2022.11.11.)

A megnövekedett káros tevékenység és az információgyűjtéshez kapcsolódó incidensek hátterében a koronavírushoz, valamint az otthoni munkavégzéshez kapcsolódó fenyegetések állnak. A NKI 2020. márciusban tájékoztatást[99] adott ki az új koronavírus témájú kiberfenyegetésekről, amelyek az alábbiak:

7. ábra: Koronavírus témájú kiberfenyegetések (forrás: saját szerkesztés)

A vizsgált időszak további kiemelt fenyegetései közé tartozik az EMOTET vírus, melyet az Europol a világ legveszélyesebb rosszindulatú programjaként tart számon.[100] A 2014-ben felfedezett EMOTET egy fejlett, moduláris banki trójai, amely a kormányzati- és magánszektort egyaránt céloz. Alapképességeit tekintve elsősorban banki adatok lopására szakosodott, ugyanakkor az évek során megjelenő újabb változatai szinte bármilyen más káros tevékenységre alkalmasak (pl. személyes adatok ellopása vagy zsarolóvírus telepítése), nem véletlen tartják az egyik legköltségesebb és legpusztítóbb vírusnak.[101] Jellemző a kártevőre, hogy aktívan kihasználja az aktuális tendenciákat, híreket, így a

98 https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-vmware-vcenter-server-serulekenysegerol/ (Letöltve: 2022.11.11.)
99 https://nki.gov.hu/figyelmeztetesek/tajekoztatas/az-nki-tajekoztatoja-az-uj-koronavirus-temaju-kiberfenyegetesekrol/ (Letöltve: 2022.11.11.)
100 https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (Letöltve: 2022.11.11.)
101 https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/ (Letöltve: 2022.11.11.)

vizsgált időszakban jellemzően a COVID-19 témájához kapcsolódva terjedt a gyanútlan áldozatok között.

Elsősorban az otthoni munkavégzéshez kapcsolódó fenyegetésként jelentek meg a zsarolólevelek és a zsarolóvírusok. A Phobos ransomware például nyitott, vagy nem biztonságos távoli asztali kapcsolaton keresztül, RDP hitelesítő adatok brute-force támadásával, kiszivárgott, vagy megszerzett RDP hitelesítő adatok segítségével, valamint klasszikus és jól bevált adathalász technika segítségével terjedt.[102]

A 2020. évet tovább vizsgálva a következő kiugrást a júniusi hónapban láthatunk, melynek hátterében a COVID-19-hez kapcsolódó, újra erőre kapó, több esetben rosszindulatú csatolmányokat tartalmazó adathalász kísérletek, koronavírusra hivatkozó csaló honlapok, valamint a mobiltelefonokat veszélyeztető zsarolóvírusok állnak. Ebben az időszakban az NKI riasztást adott ki [103], az ORFK[104] pedig arra figyelmeztetett, hogy az országos tisztifőorvos, valamint a Nemzeti Népegészségügyi Központ nevében elektronikus leveleket küldtek elsősorban egészségügyi, állami intézményekbe és cégekhez, amelyek csatolmánya feltehetően rosszindulatú programot tartalmaz.


P 2020. 06. 12. 9:12

Nemzeti Egészségügyi Központ Magyarország <Muller.Cecilia@nnk.gov.hu>

Message has been disinfected :A Covid-19 védőfelszerelés ingyenes forgalmazása (Nemzeti Egészségügyi Központ Magyarország)

Címzett undisclosed-recipients:

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

Kedves mindenkinek,
A magyar kormány által kiadott covid-19 válaszadási utasítások szerint mi, a Magyar Nemzeti Egészségügyi Központ a covid-19 védőeszközöket ingyenesen kívánjuk eljuttatni a magyarországi összes regisztrált vállalathoz és iparághoz. Kérjük, töltse ki egyértelműen a mellékelt űrlapot. győződjön meg arról, hogy az alkalmazottak száma és a cég címe egyértelműen meg van írva ebben a formában.

Töltse ki a mellékelt űrlapot, és a mai bezárás előtt küldje vissza nekünk a másolatot, várva a gyors választ.

Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

- Dr. Müller Cecília
  osztályvezető
- Országos Tisztifőorvos
- NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT
- 1097 Budapest, Albert Flórián út 2-6.
- Müller.Cecília@nnk.gov.hu

---

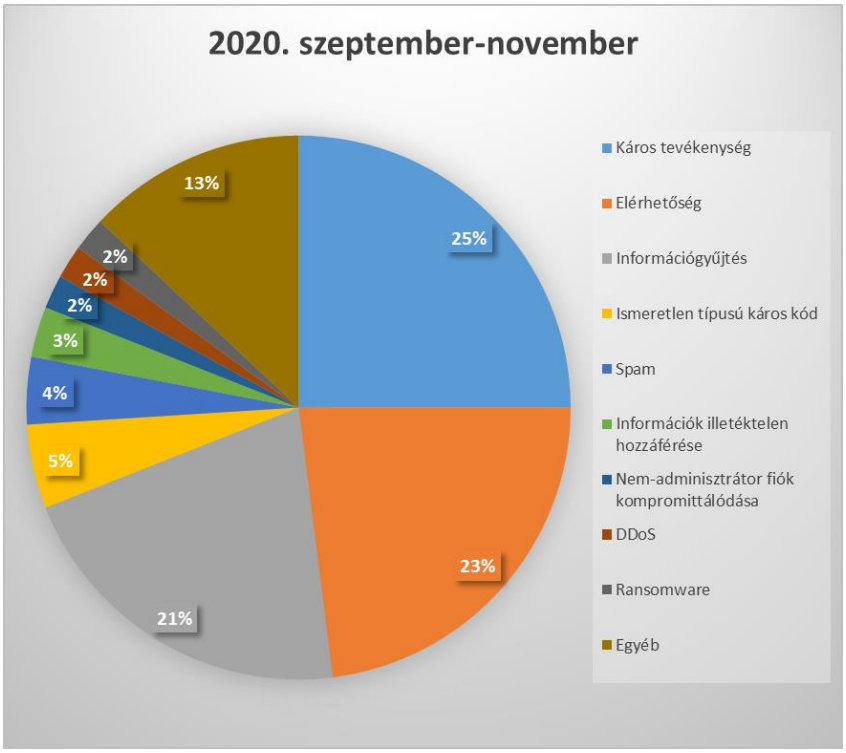
102 https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-phobos-zsarolovirus-terjedeserol/ (Letöltve: 2022.11.11.)

103 https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-nemzeti-nepegeszsegugyi-kozpont-neveben-kuldott-karos-csatolmanyt-tartalmazo-levellel-kapcsolatban/ (Letöltve: 2022.11.11.) https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nemzeti-nepegeszsegugyi-kozpont-arculati-elemeit-felhasznalo-adathalasz-levelekkel-kapcsolatban/ (Letöltve: 2022.11.11.)

104 https://koronavirus.gov.hu/cikkek/operativ-torzs-visszaeltek-az-orszagos-tisztifoorvos-es-az-nnk-nevevel (Letöltve: 2022.11.11.)

8. ábra: Riasztás a nemzeti népegészségügyi központ nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban (forrás: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-nemzeti-nepegeszsegugyi-kozpont-neveben-kuldott-karos-csatolmanyt-tartalmazo-levellel-kapcsolatban/)

A 2020-ban a detektált incidensek száma tekintetében a következő emelkedés az őszi, szeptember és november közötti időszakra, tehát a COVID-19 második hullámára tehető. Ezen időszakban az alábbi incidens típusokat azonosították:



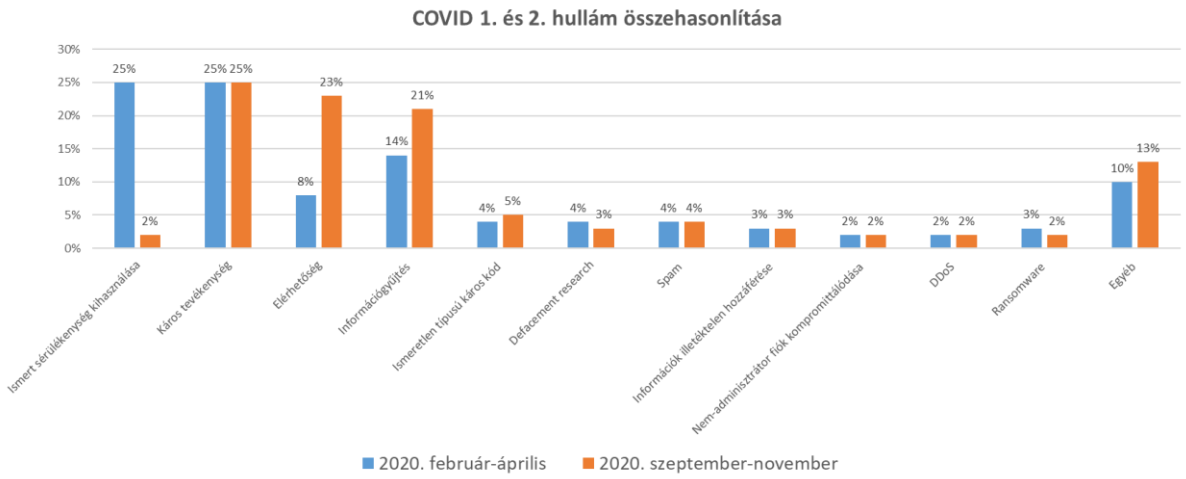
9. ábra: Az NKI által detektált incidensek eloszlása 2020. szeptember-november (forrás: saját szerkesztés)

A dobogó legfelső fokán elhelyezkedő káros tevékenység hátterében a megnövekedett EMOTET aktivitás áll, amely jellemzően egészségügyi intézmények nevében kiküldött, káros csatolmányt tartalmazó csaló levelekkel[105], valamint fertőzött e-mail fiókok kapcsolati listája útján terjedt[106]. Emellett a jelzett időszakban közüzemi szolgáltatók nevével visszaélő[107], valamint COVID-19 témájú adathalász/káros tartalmú levelek

[105] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/ (Letöltve: 2022.11.11.)
[106] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/ (Letöltve: 2022.11.11.)
[107] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kozuzemi-szolgaltatok-nevevel-visszaelo-adathalasz-uzenetekrol/ (Letöltve: 2022.11.11.)

okoztak incidenseket, a kormányzati és a pénzügyi szektorokat érintő DDoS támadások[108] mellett. Ez utóbbinak köszönhető, hogy az őszi időszakban az elérhetőség a dobogó második helyén végzett.

A következő grafikon a COVID-19 első és második hulláma során azonosított incidensek típusait hasonlítja össze:



10. ábra: A COVID 1. és 2. hulláma alatti incidens típusok összehasonlítása (forrás: saját szerkesztés)

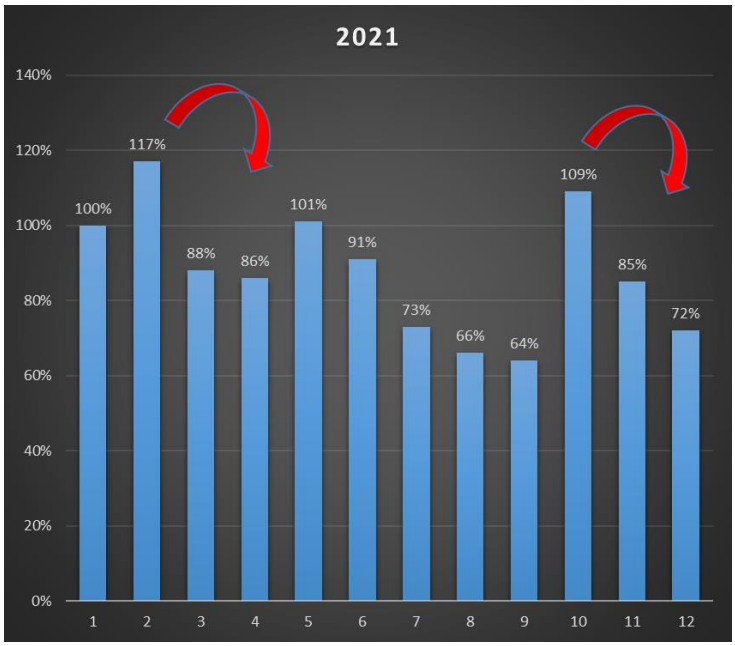
Az elemzésből egyértelműen megállapítható, hogy míg az első hullám során az ismert sérülékenység kihasználása, illetve a káros tevékenység voltak a domináló incidens típusok, addig a második hullámban a káros tevékenység mellett már az elérhetőség és az információgyűjtés voltak a legmeghatározóbbak. Egyéb típusok tekintetében, mint az ismeretlen típusú káros kód, defacement, spam, információk illetéktelen hozzáférése, nem-adminisztrátor fiók kompromittálódása, valamint a DDoS és a ransomware, kiegyenlített volt az összes incidenshez viszonyított arányuk mindkét időszakban.

2021. év vizsgálata

A 2021. évben, az NKI által detektált incidensek havi eloszlása tekintetében –a 2020. évhez hasonlóan- azonosítható a COVID tavaszi (harmadik) és ősz (negyedik) hulláma során történő százalékos emelkedés. (Az elemzés során –az előző két évhez hasonlóan- a

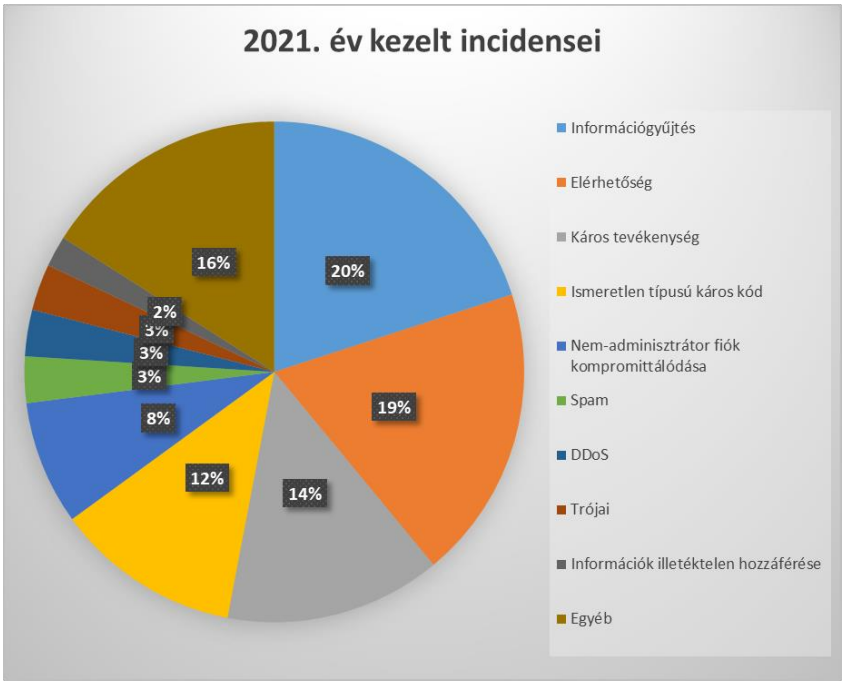
[108] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kormanyzati-es-penzugyi-szektorokat-erinto-ddos-tamadasokkal-kapcsolatban/ (Letöltve: 2022.11.11.)

januári hónapban azonosított incidenseket tekintem 100%-nak és az ehhez képest való elmozdulást vizsgálom havonkénti viszonylatban.)



11. ábra: 2021. év vizsgálat – Az incidensek havi eloszlása (forrás: saját szerkesztés)

A 2021-ben kezelt incidensek típusai szerinti eloszlást az alábbi grafikon mutatja be:



12. ábra: 2021. év NKI által kezelt incidensei (forrás: saját szerkesztés)

Az incidensek típus szerinti eloszlása tekintetében az előző évhez képest nem történt jelentős változás, az arányok tekintetében csupán néhány százalék eltérés mutatható ki. A három leggyakoribb incidens típusok az információgyűjtés (20%), az elérhetőség (19%), valamint a káros tevékenység (14%), de jelentős százalékban fordul elő az ismeretlen típusú káros kód (12%), valamint a nem-adminisztrátor fiókok kompromittálódása (8%) is.

A statisztikai eredmények hátterében a következő tendenciák azonosíthatók:

- a COVID-19 járványhoz kapcsolható kiberfenyegetések és incidensek száma csökkent;
- az EMOTET vírus a COVID harmadik hullámának elején (2021. február)[109], valamint az őszi következő hullámban (2021. november)[110] ismét fokozott aktivitást mutatott;
- 2021. márciusban a Microsoft Exchange szerverek esetében négy nulladik napi, tehát a fejlesztők által még fel nem fedezett sérülékenységet (ProxyLogon, illetve a ProxyShell) azonosítottak, melyek kihasználásával a támadók teljes irányítást szerezhettek a levelezőrendszer felett[111];
- 2021. márciusban megjelent, majd októberben[112] újra erőre kapott a Flubot malware, mely csomagküldő szolgáltatók nevével visszaélő, káros kód terjesztésével összefüggő sms üzenetek útján terjedt[113];
- 2021. októberben a Pécsi Tudományegyetem[114], valamint a Magyar Posta nevével és arculati elemeivel visszaélő[115] káros csatolmányt tartalmazó levelek terjedtek el a magán- és a közszférában egyaránt;
- 2021. októberben nagy mennyiségű kéretlen, adathalász tartalmú, káros csatolmánnyal rendelkező e-mail üzenetek terjedése volt megfigyelhető[116];

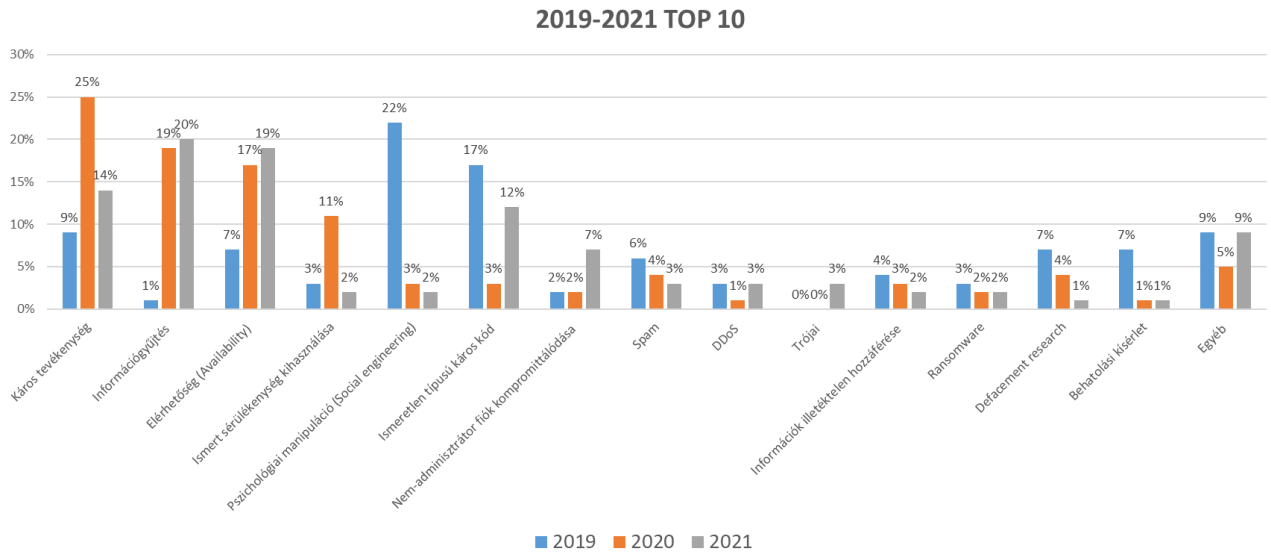
[109] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-emotet-malware-kapcsan/ (Letöltve: 2022.11.11.)
[110] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-emotet-malware-ismetelt-felbukkanasaval-osszefuggesben/ (Letöltve: 2022.11.11.)
[111] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szerverek-serulekenysegeivel-kapcsolatban/ (Letöltve: 2022.11.11.)
[112] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-flubot-malware-rel-kapcsolatban/ (Letöltve: 2022.11.11.)
[113] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/ (Letöltve: 2022.11.11.)
[114] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-pecsi-tudomanyegyetem-nevevel-visszaelo-karos-csatolmanyt-tartalmazo-levelekkel-kapcsolatban/ (Letöltve: 2022.11.11.)
[115] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-magyar-posta-nevet-es-arculati-elemeit-felhasznalo-adathalasz-uzenetekkel-kapcsolatban/ (Letöltve: 2022.11.11.)
[116] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-keretlen-adathalasz-tartalmu-e-mail-uzenetek-kapcsan/ (Letöltve: 2022.11.11.)

– 2021. novemberben a Microsoft Exchange szervereket érintő újabb 0. napi sérülékenységet (ProxyNotShell) azonosítottak. Sikeres kihasználás esetén a megfelelő jogosultsággal rendelkező támadó távoli kódfuttatást hajtott végre az érintett szerveren.[117];
– 2021. decemberben az azonosított Log4shell sérülékenység kihasználásával kapcsolatban ransomware/malware terjesztés volt megfigyelhető. A sérülékenység hitelesítés nélküli, tetszőleges, távoli kódfuttatást tett lehetővé a támadók számára, melynek sikeres kihasználása esetén teljes, rendszerszintű hozzáféréssel rendelkezhettek. [118].

Részkövetkeztetések - A vizsgált időszak (2019-2021) incidenstrendjei

A bemutatott elemzések során részletesen bemutattam az egyes évekre jellemző incidens típusokat, megtörtént esetekkel alátámasztva az előfordulásukat. Jelen összehasonlítás célja a vizsgált három évet jellemző incidenstrendek azonosítása és bemutatása.

A 2019-2021 közötti időszak évenként azonosított, leggyakoribb tíz incidens típusának összehasonlítása (az egyes évek tekintetében, az adott incidenshez kapcsolódó százalékos arány az adott évben detektált valamennyi incidenshez viszonyított aránya):



117 https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szervereket-erinto-0-napi-serulekenysegrol/ (Letöltve: 2022.11.11.)
118 https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-apache-log4j-konyvtart-erinto-kritikus-serulekenyseggel-kapcsolatban/ (Letöltve: 2022.11.11.)

13. ábra: 2019-2021 TOP 10 incidens típusai (forrás: saját szerkesztés)

A vizsgált három év viszonylatában megállapítható, hogy –néhány kivételtől eltekintve- az egyes incidens típusok arányában a 2019. évhez viszonyítva 2020-ban és 2021-ben százalékos emelkedés figyelhető meg. A **legmeredekebb emelkedést** a dobogó első három helyét elfoglaló incidens típusok esetén láthatjuk, melyek

- **a káros tevékenység,**
- **az információgyűjtés és**
- **az elérhetőség.**

Emelkedő tendencia mutatkozik meg:

- **a nem-adminisztrátor fiók kompromittálódása**, valamint
- **a trójai vírus** esetében is.

Az ismert sérülékenység kihasználásának 2020-ban tapasztalható kiugróan magas aránya a Microsoft Exchange mail szervereket érintő támadásnak volt köszönhető.

A **pszichológiai manipuláció** esetében a 2019-es évhez viszonyítva jelentős **visszaesés** tapasztalható a 2020-2021-es években. Szakmai tapasztalatom és megfigyelésem alapján **ez nem jelenti a social engineering típusú támadások tényleges csökkenését**, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Ugyanis, ha jobban megvizsgáljuk a grafikont, akkor látható, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya. Az ENISA referencia incidens taxonómiája[119] szerint a pszichológiai manipuláció az információgyűjtés fő kategóriájához tartozik, annak egyik alkategóriája, így feltételezhetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típust, tehát az információgyűjtést jelölték meg a 2020. és 2021. években.

Csökkenő tendencia figyelhető meg az adott évben detektált incidensek összesített számához képest, a 2020. és 2021. évben az alábbi incidens típusoknál:

- ismeretlen típusú káros kód,
- spam,
- információk illetéktelen hozzáférése,
- ransomware,

[119] Reference Incident Classification Taxonomy https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2022.11.11.)

- defacement
- behatolási kísérlet.

Természetesen ez nem jelenti feltétlenül az adott típushoz tartozó incidensek számszerű csökkenését, ez csupán arra a tendenciára utal, amely az adott incidens típus esetében, az adott évben bekövetkező összes incidenshez viszonyított arányában való változást szemlélteti.

3.3.4. Elemzés: Szektorális összehasonlítás

A disszertáció jelen részében, az NKI által detektált, a 3.3.2. részben részletesen bemutatott alábbi szektorok tekintetében azonosított incidensek kerülnek elemzésre:

- állami és önkormányzati szervek,
- nemzeti létfontosságú rendszerelemek,
- alapvető szolgáltatásokat nyújtó szereplők,
- bejelentés köteles szolgáltatók,
- közvetítő szolgáltatók,
- nemzetbiztonsági védelem alá eső szervezetek,
- oktatási intézmények,
- egyéb szervezetek.

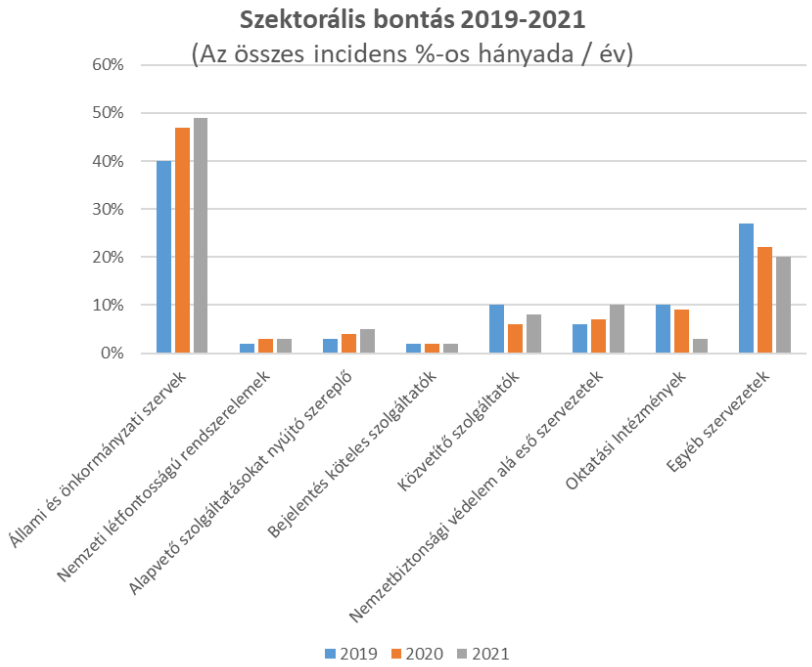
A 2019 és 2021 közötti időszakban az NKI az egyes vizsgált szektorokat érintően az állami és önkormányzati szervek tekintetében detektálta a legtöbb eseményt -a vizsgált három évben az összes incidens 47%-a-, míg a nemzetbiztonsági védelem alá eső szervezetek esetében ez az arány 8%, a közvetítő szolgáltatók és az oktatási intézmények tekintetében pedig 7%.

Az alábbi táblázat összefoglalja a 2019-2021 közötti időszakban az egyes szektorokat érő incidenseknek, az összes detektált incidenshez viszonyított százalékos arányát:

Az incidensben érintett szektor		Incidensek összesített százalékos aránya 2019-2021
Állami és önkormányzati szervek		47%
Nemzetbiztonsági védelem alá eső szervezetek		8%
Közvetítő szolgáltatók		7%
Oktatási Intézmények		7%
Alapvető szolgáltatásokat nyújtó szereplő		4%
Nemzeti létfontosságú rendszerelemek		3%
Bejelentés köteles szolgáltatók		2%
Egyéb szervezetek		22%

14. ábra: Az egyes szektorokban kezelt incidensek százalékos eloszlása a 2019-2021 évek összesített eredményei tükrében (forrás: saját szerkesztés)

Ahhoz, hogy az egyes szektorokat érintő trendek is kimutathatók legyen, meg kell vizsgálni, hogy az egyes szektorokat -évenkénti bontásban- milyen arányban érte támadás:



15. ábra: Szektorális bontás 2019-2021 közötti időszakban, évenkénti bontásban (forrás: saját szerkesztés)

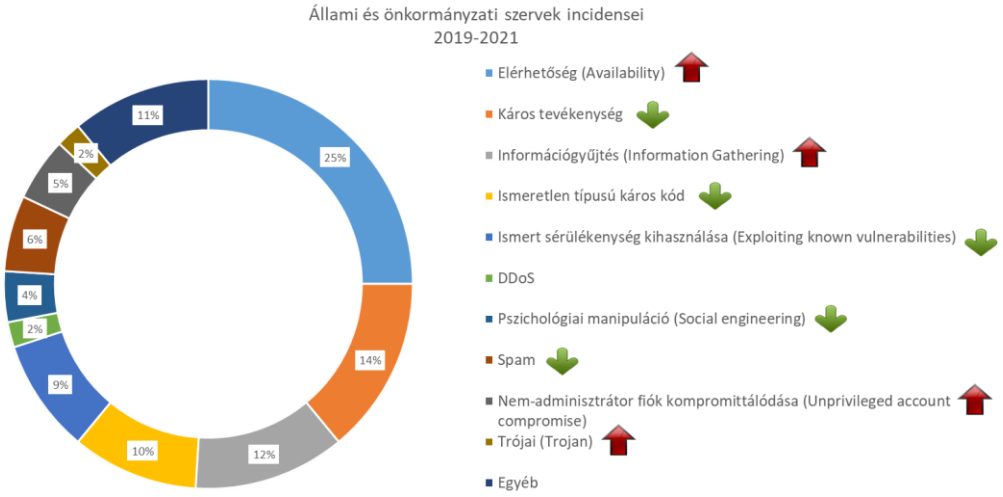
A grafikon alapján megállapítható, hogy **a leginkább támadott állami és önkormányzati szervek esetében az egyes években, az eseményeknek az összes detektált incidenshez viszonyított aránya -évről évre további emelkedést mutatva- nő,** így ezen szektor részéről fokozott védelmi intézkedések szükségesek a további emelkedés megakadályozása érdekében. Hasonló emelkedő tendencia mutatható ki a második legtámadottabb szektor, a

nemzetbiztonsági védelem alá eső szervek tekintetében is, valamint az alapvető szolgáltatásokat nyújtó szereplők és a nemzeti létfontosságú rendszerelemek esetében is. A bejelentés köteles szolgáltatók esetében stagnálás, míg a közvetítő szolgáltatók és az oktatási intézmények tekintetében csökkenés figyelhető meg.

Az állami és önkormányzati szervezeteket érintő, jellemző incidens típusok:

Az állami és az önkormányzati szervek –mint a legtámadottabb szektor-, különálló, incidens típusok szerinti vizsgálata is indokolt annak érdekében, hogy azonosíthatók legyenek a leginkább fenyegető támadási vektorok.

A 2019-2021 közötti időszakban, az állami és önkormányzati szerveket érő incidensek eloszlása a következő (piros nyíllal jelezve az emelkedő, zöld nyíllal pedig a csökkenő tendenciát):

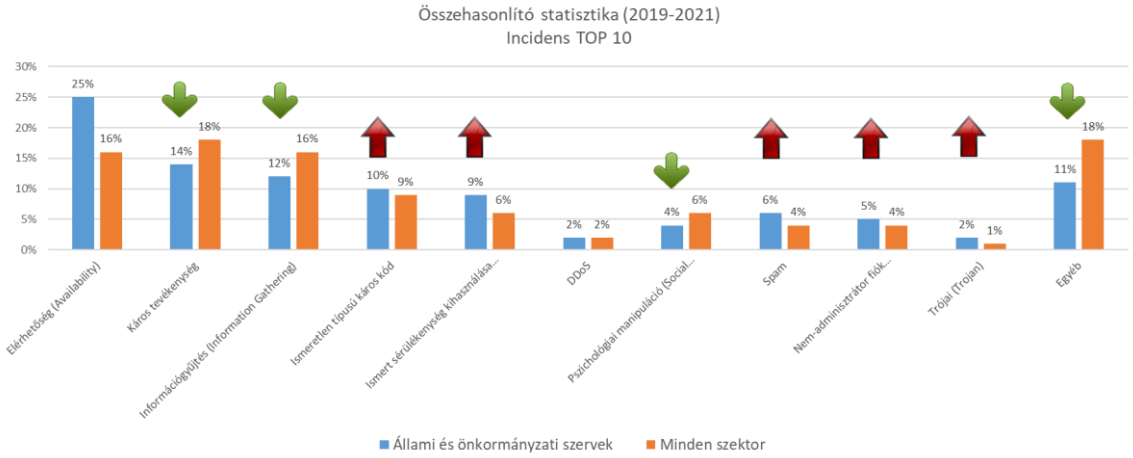


16. ábra: Az állami és önkormányzati szervek incidensei, 2019-2021 (forrás: saját szerkesztés)

A vizsgált időszakban az elérhetőség volt a legkritikusabb incidens típus, minden negyedik incidens eredményezte a rendelkezésre állás problémáját az állami és önkormányzati szerveknél (az összes detektált incidenshez viszonyított aránya 25%). Káros tevékenység az incidensek 8%-ában, információgyűjtés 12%-ban, míg ismeretlen típusú káros kód, illetve ismert sérülékenység kihasználása 10, illetve 9%-ban fordultak elő. Az összincidensekhez viszonyítva 10% alatti az aránya a spameknek, a nem-adminisztrátor

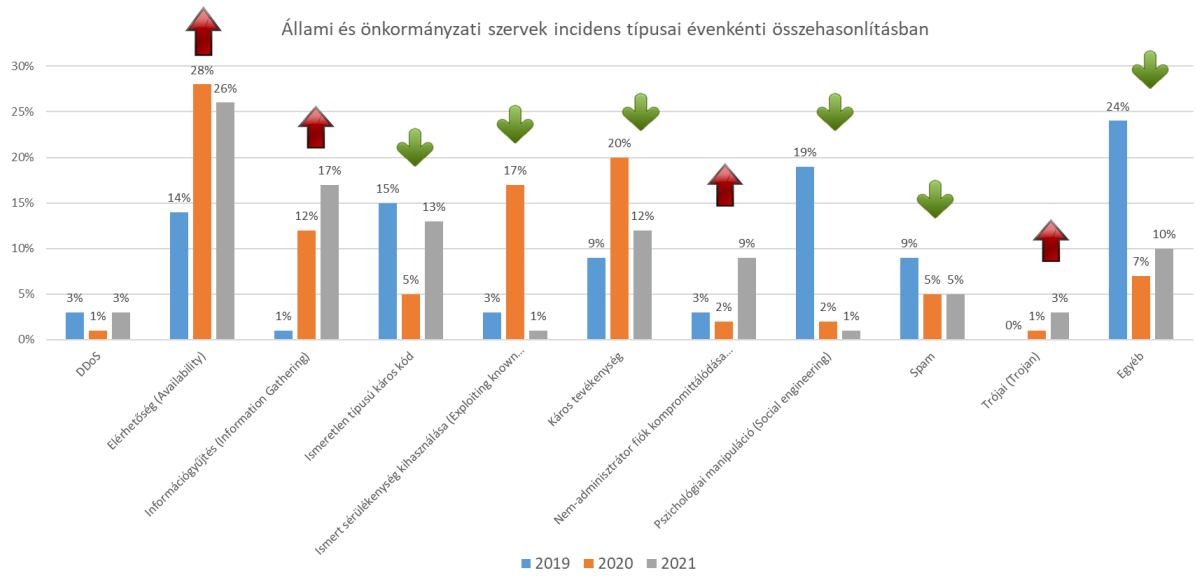
fiók kompromittálódásának, a pszichológiai manipulációnak, valamint a DDoS és a trójai vírus támadásoknak.

Amennyiben összehasonlítjuk az állami és önkormányzati szervezeteket érő leggyakoribb tíz incidens típus százalékos arányát az egyes incidens típusoknak, az összes szektoron belüli arányával, az alábbi összefüggéseket állapíthatjuk meg: az elérhetőség, az ismeretlen típusú káros kód, az ismert sérülékenység kihasználása, a spam, a nem-adminisztrátor fiók kompromittálódása, valamint a trójai vírus incidens típusok nagyobb arányban fordulnak elő az állami és önkormányzati szervek esetében (az összes szektort érintő átlaghoz viszonyítva), ugyanakkor a káros tevékenység, az információgyűjtés és a pszichológiai manipuláció kisebb százalékban mutatható ki.



17. ábra: Összehasonlító statisztika az állami és önkormányzati szervek és az összes szektor tekintetében, incidens típusok alapján (forrás: saját szerkesztés)

Az alábbi grafikon segítségével meghatározhatók az állami és önkormányzati szerveket érintő leggyakoribb incidens típusokhoz kapcsolódó trendek is:



18. ábra: Az állami és önkormányzati szervek incidens típusai évenkénti összehasonlításban (forrás: saját szerkesztés)

Részkövetkeztetések – Az állami és önkormányzati szerveket, mint a legtámadottabb szektort érintő incidenstrendek

A vizsgált időszakban **emelkedő trend azonosítható** az alábbi incidenstípusoknál:

- elérhetőség,
- információgyűjtés,
- nem-adminisztrátor fiók kompromittálódása,
- trójai vírus.

Csökkenő tendencia látható:

- az ismeretlen típusú káros kód,
- az ismert sérülékenység kihasználása,
- a káros tevékenység,
- a pszichológiai manipuláció, illetve
- a spamek esetében.

A **DDoS** esetében a 2020-ban történő csökkenést követően 2021-ben az arányszám ismét a 2019-es szintre emelkedett.

3.3.5. Elemzés: Pszichológiai manipuláció (Social engineering)

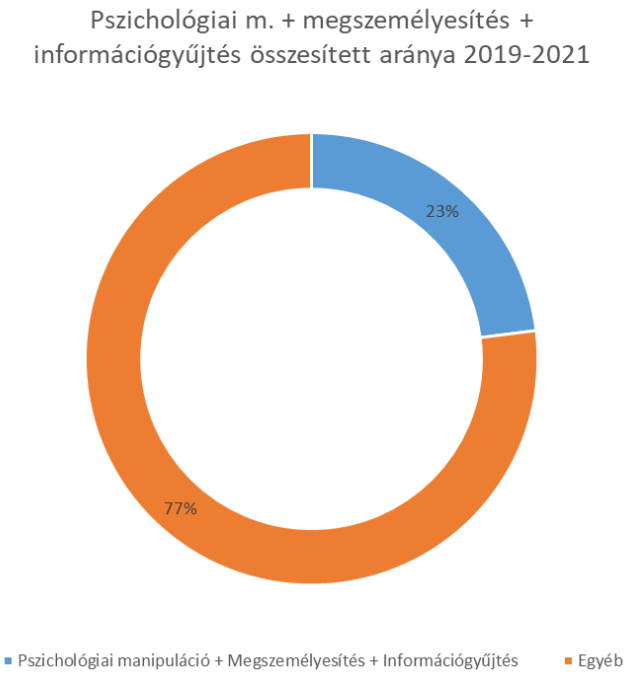
Ahogy a 3.2.2. részben már meghatároztam, a pszichológiai manipuláció (social engineering) az emberi hiszékenységre és együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva (Muha-Krasznay, 2014., p. 53.).

A NKI adatait évenként bontásban vizsgálva (3.3.3.) már megállapításra került, hogy a pszichológiai manipuláció esetében a 2019-es évhez viszonyítva jelentős visszaesés tapasztalható a 2020-2021-es években, amely azonban nem jelenti a social engineering típusú támadások tényleges csökkenését, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Az elemzett adatok alapján megállapítást nyert, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya, melynek hátterében az ENISA referencia incidens taxonómiája állhat, mely szerint a pszichológiai manipuláció az információgyűjtés alkategóriáját képzi. Így feltehetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típus, tehát az információgyűjtés került megjelölésre a 2020. és 2021. években.

E jelenségből adódó statisztikai eltérések kiküszöbölése érdekében a pszichológiai manipuláció vizsgálatánál az incidens típusok alábbi három kategóriájának összesített százalékos eloszlását vizsgáltam az 2019-2021 időszakban:

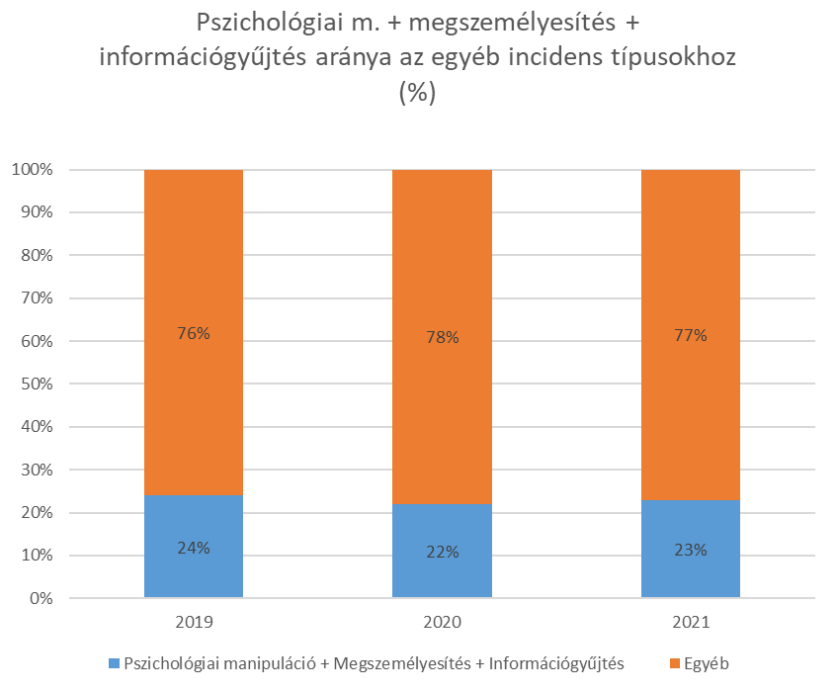
- pszichológiai manipuláció,
- megszemélyesítés (mely a pszichológiai manipuláció egyik támadási formája) és
- információgyűjtés.

A három incidens típus összesített aránya a 2019-2021 években detektált összes incidenshez képest 23%.



19. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés összesített aránya, 2019-2021 (forrás: saját szerkesztés)

A tágabb értelemben vett pszichológiai manipulációt jellemző trend meghatározása érdekében összehasonlítottam az egyes években kimutatható arányukat az összes incidensen belül, melyet az alábbi grafikon szemléltet:



20. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes, egyéb incidens típusokhoz viszonyított aránya, 2019-2021 (forrás: saját szerkesztés)

Részkövetkeztetések – Pszichológiai manipuláció érintő trendek

A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes aránya kiegyensúlyozott az egyes években, az egyéb incidens típusokhoz viszonyított arányuk 22% és 24% között mozog, tehát **stagnálást** mutat.
Ugyanakkor meg kell jegyezni, hogy még ha százalékos arányban a detektált incidensek majd egynegyedénél mutatható csupán ki tágabb értelemben vett pszichológiai manipuláció, sikerességük esetén jelentősen nagyobb és komolyabb károk következhetnek be, legyen szó akár információk jogosulatlan megszerzéséről, adatok titkosításáról, vagy egyéb káros tevékenységről.

3.4. EURÓPAI INCIDENSTRENDEK AZONOSÍTÁSA

Az összehasonlítás alapjául szolgáló európai dokumentumok bemutatása

Az NKI által detektált incidenstrendek összehasonlítása szempontjából meghatározó volt, hogy olyan trendekkel tudjam a kutatási eredményeimet összevetni, amely az Európai Unió területén azonosítható kibertámadásokra, fenyegetésekre vonatkozik, és amelynek forrása valamely európai uniós szerv. Ezen szempontok figyelembe vételével az alábbi jelentések szolgálnak az összehasonlítás alapjául:

- ENISA Threat Landscape 2020,
- ENISA Threat Landscape 2021,
- ENISA Threat Landscape 2022,
- Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol,
- Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol,
- Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol,
- EU Serious and Organised Crime Threat Assessment (SOCTA) 2021.

3.4.1. ENISA Threat Landscape 2020[120]

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) minden évben közzéteszi az ENISA „Fenyegetési Térkép” (ENISA Threat Landscape) jelentést, amelyben azonosítja és értékeli a legjelentősebb kiberfenyegetéseket. A 2019. január – 2020. április közötti időszak eseményeit feldolgozó 2020-as jelentés 2020 októberben került publikálásra. A kiadvány 22 különböző jelentésre oszlik. Az összevont jelentés a 2018-as fenyegetettséghez képest a legnagyobb változásként a digitális környezet átalakulását jelölte meg, amelyet a COVID-19 által kiváltott pandémia okozott. A világjárvány alatt azt tapasztalták, hogy a számítógépes bűnözők fejlesztik képességeiket, gyorsan alkalmazkodnak és hatékonyabban célozzák meg az érintett áldozatcsoportokat.

A) Incidenstrendek 2019-ben és 2020 első felében

TOP 15 kiberfenyegetés, kiemelve néhány, a téma szempontjából releváns megállapítást:

- Malware (rosszindulatú programok): A rosszindulatú szoftverek az első számú kiberfenyegetés az EU-ban, növekedő tendencia azonosítható.
- Web-based Attacks (web-alapú támadások): A COVID-19 világjárvány alatt megnőtt a hamis online vásárlási weboldalak és a csaló online kereskedők száma.
- Phishing (adathalászat): Növekedő tendencia mutatható ki. Az adathalászat áldozatainak száma az EU-ban tovább nő, és a rosszindulatú szereplők a COVID-19 témát használják fel a „csalogatásra”. A COVID-19 témájú támadások közé tartoznak a rosszindulatú fájl mellékleteket tartalmazó, illetve a rosszindulatú linkeket tartalmazó üzenetek, amelyek a felhasználókat adathalász oldalakra vagy rosszindulatú programok letöltésére irányítják át.
- Web Application Attacks (webes alkalmazások támadásai)
- SPAM
- Distributed Denial of Service, DDoS (elosztott szolgáltatás megtagadásos támadások)

[120] ENISA Threat Landscape 2020 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020 (Letöltve: 2022.11.11.)

- Identity Theft (személyazonosság-lopás): A számuk jelentősen növekszik. A rosszindulatú szereplők a célzott támadások hatékonyságának növelésére használják a közösségi médiaplatformokat.
- Data Breach (adatszivárgás)
- Insider Threat (belső fenyegetés)
- Botnets (botnetek)
- Physical Manipulation, Damage, Theft and Loss (fizikai manipuláció, sérülés, lopás és elvesztés)
- Information Leakage (információszivárgás)
- Ransomware (zsarolóvírus): A zsarolóvírusok továbbra is széles körben elterjedtek, és sok uniós szervezet számára költséges következményekkel járnak.
- Cyber Espionage (kiberkémkedés): A nagy értékű adatok, például szellemi tulajdon és államtitkok ellen irányuló, aprólékosan megtervezett és kitartó támadásokat (APT támadások) gyakran államilag támogatott szereplők tervezik és hajtják végre.
- Cryptojacking (fertőzött gépek segítségével, a felhasználó tudta és engedélye nélkül végzett kriptovaluta-bányászat[121])

B) **A pszichológiai manipulációra vonatkozó incidenstrendek**

Az ETL 2020-ban meghatározott, TOP 15 legveszélyesebbnek ítélt fenyegetés közé a social engineering nem került be önálló kategóriaként, ezért ezen jelentésből nem tudunk pontos következtetéseket levonni a pszichológiai manipulációval kapcsolatos trendekre. Ugyanakkor a bemutatott incidens típusokból egyértelműen látható, hogy a támadások jelentős részénél a pszichológiai manipulációs technikák alkalmazása áll a sikeres támadás hátterében (pl. a web-alapú támadások, az adathalászat, a személyazonosság-lopás vagy a zsarolóvírusok letöltése a legtöbb esetben az emberi hiszékenységre és segítőkészségre vezethetők vissza).

C) **A közigazgatási szektort érintő megállapítások (ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis (2019. január – 2020. április)**[122]

[121] https://www.eset.com/hu/hirek/eset-kiberbiztonsagi-elorejelzes-2019/ (Letöltve: 2022.11.11.)
[122] ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis
https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis (Letöltve: 2022.11.11.)

A ETL 2020-as jelentés részeként publikálásra kerülő „Ágazati/tematikus fenyegetéselemzés” az adott időszak tekintetében tíz különböző ágazatot érintő trendet mutat be, melynek részeként önálló ágazatként kezeli a közigazgatás, a védelmi és a szociális ellátások összevont területét. A közigazgatást is magában foglaló szektor tekintetében megállapításra került, hogy bár a malware-k, a web-alapú támadások és az adathalászat száma nőtt, mindemellett az ágazatot érő támadások száma alapján az incidenstrendek változatlannak tekinthetők, sőt **kissé csökkenő tendenciát mutatnak**.

3.4.2. ENISA Threat Landscape 2021[123]

Ebben az évben az ENISA összevonta a fenyegetések kategóriáit, amellyel az integráció és a hasonló fenyegetések jobb megjelenítése felé mozdult el.

A 2021. évi fenyegetettségi helyzetjelentés időintervalluma 2020. áprilistól 2021. júliusig tart. A jelentés általánosságban megállapította, hogy a 2020-as és 2021-es években a kiberbiztonsági támadások száma tovább növekedett, nemcsak az irányuk és a számuk, hanem a hatásuk tekintetében is. A COVID-19 járvány - a várakozásoknak megfelelően - szintén hatással volt a kiberbiztonsági fenyegetettségi helyzetre. A pandémia egyik maradandó fejleménye a hibrid irodai modell felé való tartós elmozdulás. Ez a tendencia megnövelte a támadási felületet, és ennek következtében **emelkedett a szervezeteket és vállalatokat a home office-okon keresztül célzó kibertámadások száma**.
Az egyre növekvő online jelenlét, a hagyományos infrastruktúrák online és felhőalapú megoldásokra való átállása, a fejlett összekapcsolhatóság és a feltörekvő technológiák - például a mesterséges intelligencia (AI) - új jellemzőinek kihasználása miatt a kiberbiztonsági környezet fenyegetettsége az egyre kifinomultabb, összetettebb és hatásosabb támadások révén növekedett.”[124]

A) Incidenstrendek a vizsgált időszakban:

[123] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (Letöltve: 2022.11.11.); https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf (Letöltve: 2022.11.11.)
[124] ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf, p. 6. Letöltve: 2022.11.11.)

Az elsődlegesen azonosított fenyegetések a következők[125]:

1. **Zsarolószoftverek (Ransomware)**
2. **Rosszindulatú szoftverek (Malware)**
3. **Cryptojacking**
4. **E-mail üzenetekhez kapcsolódó fenyegetések (E-mail related threats)**: Jellemzően olyan támadásokat sorolhatunk ide, amelyek nem a rendszerek technikai sebezhetőségeit, hanem az emberi befolyásolhatóságot, illetve a mindennapi szokások gyengeségeit használják ki (**social engineering típusú támadások**: pl. phishing, spear-phishing, whaling, smishing, vishing, business e-mail compromise (BEC), spam).[126]
5. **Adatok elleni fenyegetések (Threats against data)**: Ide tartoznak az adatvédelmi incidensek/szivárgások, melyek során érzékeny, bizalmas vagy védett adatok kerülnek jogosulatlan kézbe (pl. data breach, identity theft).[127]
6. **A rendelkezésre állás és az integritás elleni fenyegetések (Threats against availability and integrity)**: Igen változatos formában megjelenő támadási formák, de a legjellemzőbbek a szolgáltatásmegtagadás (DoS) és a webes támadások (pl. Distributed Denial of Service (DDoS) és Web-based Attacks, web application attack, Botnets).[128]
7. **Dezinformáció – félretájékoztatás (Disinformation – misinformation)**
8. **Nem rosszindulatú fenyegetések (Non-malicious threats)**: A hibákat és a hibás konfigurációkat gondatlanság, a tudatosság hiánya vagy egyszerűen emberi hibák okozzák, amelyeknél a rosszindulatú szándék nem nyilvánvaló.
9. **Ellátási láncot érintő támadások (Supply-chain attacks)**: Ebben az esetben a támadás nem közvetlen a célszervezet ellen következik be, hanem közvetetten, valamely partnerén, például beszállítókon, üzemeltetőkön keresztül érinti a szervezetet.[129]

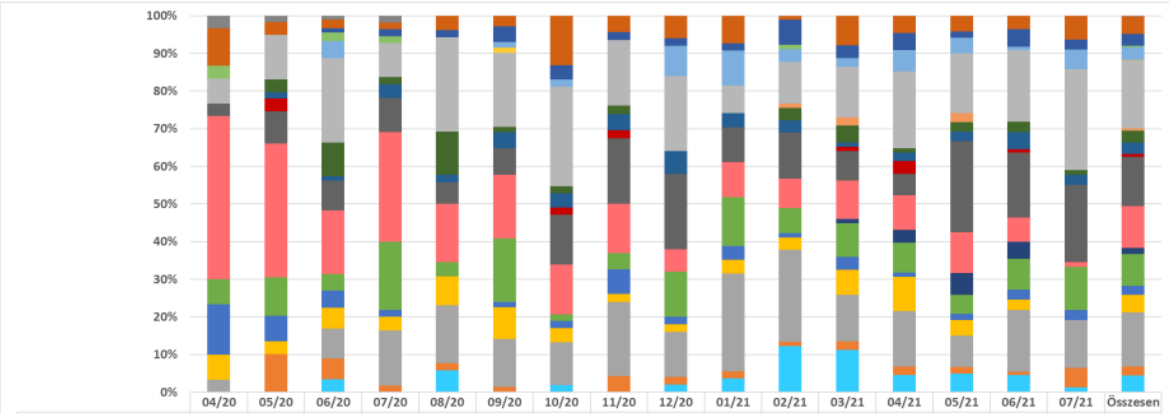
[125] ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf p. 7-8. (Letöltve: 2022.11.11.)
[126] ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf p. 7. (Letöltve: 2022.11.11.)
[127] ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf p. 7. (Letöltve: 2022.11.11.)
[128] ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf, p.7. (Letöltve: 2022.11.11.)
[129] https://nki.gov.hu/wp-content/uploads/2022/05/Supply-chain-attack_CTI_jelentes-2.pdf , p. 2. (Letöltve: 2022.11.11.)

B) A pszichológiai manipulációra vonatkozó incidenstrendek

Az ETL 2021 jelentésbe, a felsorolt elsődleges fenyegetések közé a social engineering ebben az évben sem került be önálló kategóriaként, ezért ezen dokumentumból sem tudunk pontos következtetéseket levonni a pszichológiai manipulációval kapcsolatos trendekre.
Ugyanakkor jelen esetben is igaz, hogy a bemutatott incidens típusokból egyértelműen megállapítható, hogy a támadások jelentős részénél a pszichológiai manipulációs technikák alkalmazása áll a sikeres támadás hátterében. A rosszindulatú szoftverek, így a zsarolóvírusok telepítése is a legtöbb esetben social engineering támadás során valósul meg, az e-mail üzenetekhez kapcsolódó, valamint az adatok elleni fenyegetések hátterében is valamilyen pszichológiai manipuláció áll az esetek jelentős részében.

C) A közigazgatási szektort érintő megállapítások

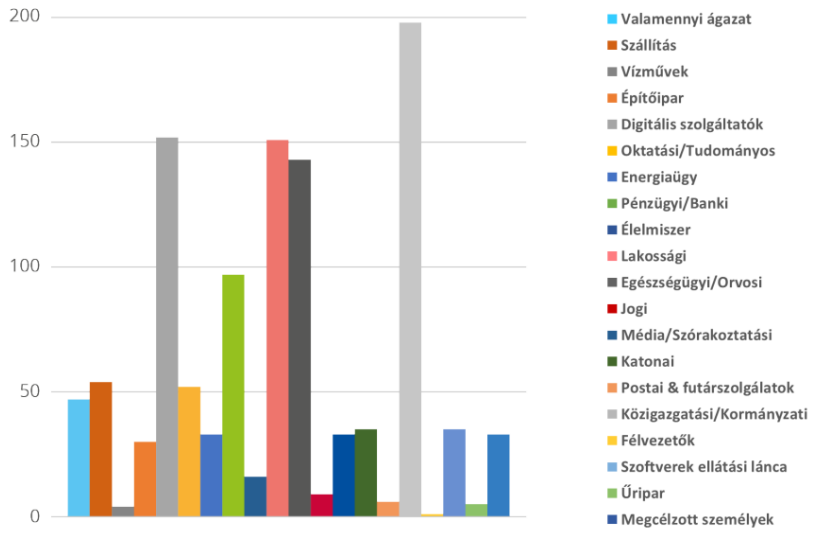
Az ETL 2021 -a 2020-as jelentéshez képest- sokkal letisztultabb ágazati besorolást vesz alapul, melynek keretében 19 szektort érintően tesz először kísérlete arra, hogy feltérképezze a fenyegetések egyes ágazatokra gyakorolt hatását. A 2021-es kategorizálásban a **közigazgatás/kormányzat önálló ágazatként** kerül besorolásra és vizsgálatra. A jelentés önállóan elemezi a fenyegetettségi helyzetjelentés szerinti elsődleges fenyegetésekhez kapcsolódóan megfigyelt incidensek számát az érintett ágazatban.
A közigazgatási/kormányzati szektort illetően, a 2020. április és 2021. július közti időszakban detektált incidensek száma, havi bontásban:



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Összesen
Vízművek	1	1	1	1													2
Szállítás	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Megcélzott személyek			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Úripar	1		2	1							1						4
Szoftverek ellátási lánca			4			1	1		4	5	3	2	5	5	1	4	35
Félvezetők						1											1
Közigazgatási/Kormányzati	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Postai & futárszolgálatok											1	2		3			6
Katonai		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Média/Szórakoztatási		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Jogi		2					1	1				1	3		1		7
Egészségügyi/Orvosi	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Lakossági	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Élelmiszer												1	3	7	5		16
Pénzügyi/Banki	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energiaügy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Oktatási/Tudományos	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitális szolgáltatók	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Építőipar		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Valamennyi ágazat			3		3		1		1	2	11	10	4	6	5	1	47

21. ábra: ETL 2021 - Az egyes szektorokat érő incidensek száma havi bontásban 2020. április és 2021. július között (forrás: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf)

A táblázat egyértelműen szemlélteti, hogy a közigazgatási/kormányzati ágazatot érő incidensek száma a legmagasabb (189 db) a vizsgált időszakban, így ezen szektor elsősége megkérdőjelezhetetlen a szektorok veszélyeztetettsége tekintetében.



22. ábra: ETL 2021- Az incidensek száma alapján megcélzott ágazatok 2020. április és 2021. július között (forrás: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf)

3.4.3. ENISA Threat Landscape 2022[130]

Az ETL 2022, a 2021. július – 2022. július közötti időszakot vizsgálja, és 2022. november 3.-án került publikálásra.
A jelentés általánosságban megállapítja, hogy a kiberbiztonsági támadások tovább nőttek, nemcsak a támadási vektorok és az elkövetési szám tekintetében, hanem a hatásukat illetően is. Az orosz-ukrán válság új korszakot nyitott meg a kiberhadviselés és a hacktivizmust szerepe, valamint a konfliktusokra gyakorolt hatásuk tekintetében.

A) Incidenstrendek a vizsgált időszakban

Az ETL 2022 jelentési időszakában a legfontosabb azonosított fenyegetések a következők:

1. Zsarolóvírusok (Ransomware): A zsarolóvírusok a jelentési időszak alatt a fő fenyegetést jelentették, több nagy nyilvánosságot és jelentős visszhangot kapott incidenssel.
2. Rosszindulatú szoftverek (Malware): Ebben a jelentési időszakban ismét nagyszámú, rosszindulatú szoftverekkel kapcsolatos incidenst figyeltek meg. Az elemzett incidensek főként az EU országaira összpontosítottak.
3. Social Engineering fenyegetések (Social Engineering threats):
A social engineering és különösen az adathalászat továbbra is népszerű technika a támadók számára. A Verzion Data Breach Investigations Report (DBIR) szerint a jogsértések mintegy 82%-a emberi tényezőre vezethető vissza, és az Európában, a Közel-Keleten és Afrikában elkövetett incidensek nem kevesebb mint 60%-a emberi tényező közreműködésével valósult meg.[131]
4. Az adatok elleni fenyegetések (Threats against data): A Verzion jelentése megjegyzi, hogy az összes adatvesztés mintegy 80%-a célszervezeten kívüli, míg mintegy 20%-a belső

[130] ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Letöltve: 2022.11.11.)
[131] Verizon DBIR https://www.verizon.com/business/resources/reports/dbir/ (Letöltve: 2022.11.11.)

okokra vezethető vissza. A motiváció továbbra is elsősorban a pénzügyi haszonszerzés (kb. 90%), a második pedig a kémkedés (kevesebb, mint 10%). A webes alkalmazások, az e-mailek és a figyelmetlenség (pl. hibák és hibás beállítások) a fő adatbetörési vektorok közé tartoznak, a lopott hitelesítő adatok, a zsarolóprogramok és az adathalászat használatával együtt, melyek a jogsértések alapját képező cselekménytípusok. Az adathalászat ismét a leggyakoribb módja a kezdeti hozzáférésnek. A zsarolási technikák tovább fejlődnek a kiszivárogtató oldalak népszerű használatával párhuzamosan.

5. A rendelkezésre állás elleni fenyegetések: Szolgáltatásmegtagadás (Threats against availability: Denial of Service): Az elérhetőség számos fenyegetés és támadás célpontja, melyek közül az elosztott szolgáltatásmegtagadásos támadás (DDoS) kiemelkedik.

6. A rendelkezésre állás elleni fenyegetések: Internetes fenyegetések (Threats against availability: Internet threats): A beszámolási időszak alatt a rendelkezésre állás elleni támadások, különösen a DDoS-támadások és a zsarolóvírusok állnak a legmagasabb helyen az elsődleges fenyegetések között, ami változást jelez az ETL 2021-hez képest, ahol a zsarolóvírusok önállóan álltak a dobogó tetején.

7. Dezinformáció – félretájékoztatás (Disinformation – misinformation): A dezinformáció a kiberhadviselés egyik eszközévé vált. Az Ukrajna elleni háborúban már a "fizikai" háború kezdete előtt is használták, mintegy Ukrajna orosz megszállásának előkészítéseként.

8. Ellátási láncot érintő támadások (Supply-chain attacks): Az ellátási lánc elleni támadás a szervezetek és beszállítóik közötti kapcsolatot célozza. A fenyegető csoportok egyre nagyobb érdeklődést mutatnak és egyre nagyobb képességekkel rendelkeznek az ellátási láncok, valamint a menedzselt szolgáltatók (MSP-k) elleni támadások iránt. A jelentési időszakban a SolarWinds volt az elsők egyike, aki felfedte ezt a fajta támadást, és rámutatott az ellátási láncot érintő támadások potenciális hatására.

A jelentés kiemeli, hogy a fenyegető szereplők **0. napos sérülékenységeket** használtak fel operatív és stratégiai céljaik eléréséhez.

B) A pszichológiai manipulációra vonatkozó incidenstrendek

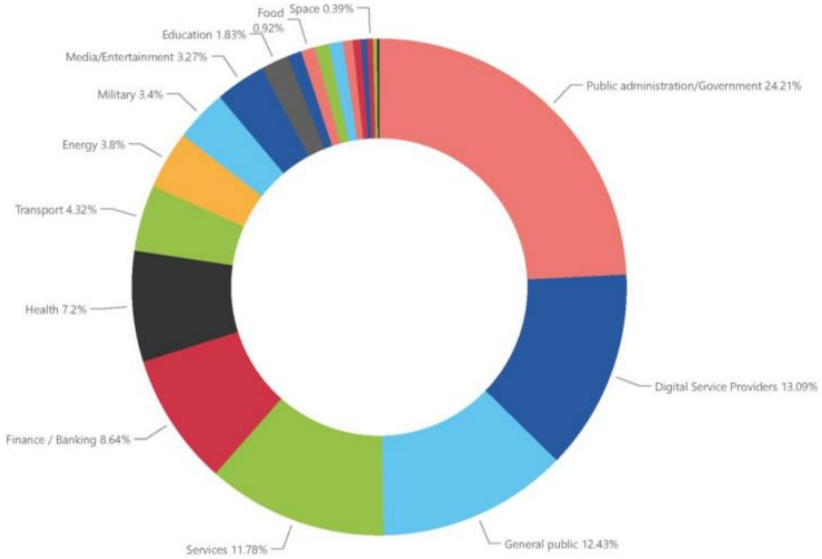
Az ETL 2022 az első jelentés, ahol **önálló fenyegetési tényezőként** szerepel a social engineering.

Lefontosabb megállapítások a social engineering-re vonatkozóan:

- A jelentés kiemeli, hogy a bűnözők nem véletlenül alkalmazzák a social engineering technikáját: a potenciális áldozataikat e-mailben érhetik el a legkönnyebben, és a tudatosságnövelő kampányok és gyakorlatok ellenére, a felhasználók még mindig bedőlnek ezeknek a trükköknek. A DBIR szerint a támadók továbbra is lopott hitelesítő adatokat használnak a célszemélyek további adatai megszerzéséhez vállalati e-maileken keresztül. A végső céljuk az, hogy ezeket az információkat felhasználják például a Business Email Compromise (BEC) támadások részeként.
- Az EMOTET 2021 januárjában a bűnüldöző és igazságügyi hatóságok munkájának köszönhetően egy időre eltűnt, azonban 2021 novemberében újra felbukkant, a pszichológiai manipulációnak köszönhetően gyorsan terjedt és hatalmas károkat okozott.
- Mind az Europol, mind az FBI arról számolt be, hogy az adathalászat és a social engineering továbbra is a fizetési csalások fő eszközei, amelyek mind számszerűségükben, mind kifinomultságukban növekednek.

C) A közigazgatási szektort érintő megállapítások

A jelentési időszakban ismét nagyszámú, a közigazgatás és a kormányzat ellen irányuló incidenst figyeltek meg, az összes incidens mintegy negyede 24,21% irányult a „Public administration/Government") felé, mely a legtámadottabb szektorként biztosította a helyét a dobogó tetején.



23. ábra: ETL 2022 - A megcélzott ágazatok az incidensek száma alapján (forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022)

3.4.4. Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol[132]

Az Europol Európai Számítógépes Bűnözés Elleni Központja (EC3) minden évben közzéteszi az Internetes Szervezett Bűnözés Fenyegetettségi Felmérését (IOCTA), amely az Europol kiemelt stratégiai jelentése a számítógépes bűnözés legfontosabb megállapításairól, valamint az új veszélyekről, az EU kormányait, vállalkozásait és polgárait érintő fenyegetésekről.

Az IOCTA kulcsfontosságú ajánlásokat fogalmaz meg a bűnüldöző szervek, a politikai döntéshozók és a szabályozó hatóságok számára, hogy hatékonyan és összehangoltan tudjanak reagálni a számítógépes bűnözésre.

A) Incidenstrendek a vizsgált időszakban

– Míg a **zsarolóvírusok** továbbra is a legfontosabb fenyegetés a jelentésben, a zsarolóvírus-támadások száma csökkent, mivel a támadók kevesebb, de jövedelmezőbb célpontokra és a nagyobb gazdasági károkra összpontosítanak.

[132] Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (Letöltve: 2022.11.11.)

- Az **adatok kompromittálódása** jelenti a második legfőbb kiberfenyegetést, melyekre leggyakrabban a pénzügyi adatok illegális megszerzése, például hitelkártyaadatok, online banki adatok vagy kriptovaluta-tárcák megszerzése révén kerül sor, például adathalászat, **adatszivárgás** vagy **információgyűjtő malware** segítségével.
- **Az adathalászat** és a **sebezhető távoli asztal protokollok (RDP-k)** a legfontosabb elsődleges **malware** fertőzési vektorok.
- Az **adatok** továbbra is kulcsfontosságú célpontok, a kiberbűnözés egyik legfontosabb eszközei.
- A bűnözők jellemzően néhány **banki trójai vírust** használnak, különösen azokat, amelyek moduláris felépítésűek és ezért változó funkcionalitásúak, mint például az **EMOTET és a Trickbot**, melyeket leginkább a hálózatba való behatolásra és a rosszindulatú programok terjesztésére használnak. Néhány esetben tehát a bűnözők az egyes **rosszindulatú szoftvereket** más rosszindulatú szoftverek telepítésére használják, beleértve a zsarolóprogramokat is.
- **Az elosztott szolgáltatásmegtagadásos (DDoS) támadások** egy újabb adatközpontú fenyegetések, amellyel meg kell küzdeni.
- Az új fenyegetések nem csak az új technológiákból, hanem a már létező technológiák ismert **sebezhetőségéből** is adódnak.
- Az **egyszerű weboldalrongálás**, mint az egyik prioritás jelenik meg a jelentésben, amely bár kisebb hattással bír, mégis nagyon gyakran fordul elő.
- A **"card not present" (CNP)** típusba tartoznak azok a csalások, amikor az elkövetéshez a fizikai kártyát nem használták. A CNP-csalás továbbra is a fő prioritás a fizetési csalásokon belül, és továbbra is az illegális tevékenység más formáinak elősegítője.
- Az **adathalászat** továbbra is fontos eszköz a kiberbűnözők fegyvertárában mind a kiberbűnözés, mind pedig a nem készpénzes csalás (NCPF) esetében.
- Míg a kriptovaluták továbbra is megkönnyítik a kiberbűnözést, a hackerek és csalók most már rendszeresen célba veszik a **kriptovalutákat** és a vállalkozásokat.

B) A pszichológiai manipulációra vonatkozó incidenstrendek

- A felmérés során a bűnüldöző szervek és a magánszektor képviselői következetesen beszámoltak a social engineeringről, mint az egyik legfőbb fenyegetésről.

- A célzott kibertámadások esetében a social engineering és a célzott adathalászat elsődleges fertőzési vektorként történő alkalmazása a 2020-as évhez képest is folytatódik.
- A Business Email Compromise (BEC) esetében gyakran alkalmaznak a bűnözők social engineering technikákat, melynek segítségével megszemélyesítik a vállalat munkatársait.

C) A közigazgatási szektort érintő megállapítások

Az Europol által összeállított IOCTA egyes jelentései nem vizsgálják az egyes ágazatokat célzó incidensek számát és arányát.

3.4.5. Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol[133]

A COVID-19 krízis megmutatta, hogy a bűnözők hogyan használják ki aktívan a társadalom legkiszolgáltatottabb helyzetét és élnek vissza a pandémia következtében kialakult válsággal a kibertámadások területén is.

A) Incidenstrendek a vizsgált időszakban

A jelentés főbb megállapításai:

- A **zsarolóprogram** továbbra is a legdominánsabb fenyegetés.
- A **rosszindulatú szoftverek** széles körben jelen vannak a számítógépes bűnözésben. A bűnözők néhány hagyományos **banki trójai** vírust átalakítottak **fejlett moduláris malware**-ré, hogy szélesebb körben tudják azokat terjeszteni. Ezek a továbbfejlesztett rosszindulatú szoftverek az EU-ban a legnagyobb fenyegetést jelentik.

[133] Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (Letöltve: 2022.11.11.)

- A rosszindulatú szoftverek jellemzően **trójaiak** és távoli hozzáférési eszközök (RAT), amelyek lehetővé teszik a bűnözők számára, hogy megszerezzék a fertőzött számítógépek feletti távoli irányítást.
- A bűnözők egyre körültekintőbben választják ki a célpontjaikat, így jelentős figyelmet fordítanak a belső üzleti folyamatok megértésére és **rendszerek sebezhetőségének** megismerésére.
- Az **adatok kompromittálása** ismét központi szerepet játszik számos fenyegetésben.
- A **social engineering** továbbra is a legfőbb fenyegetések között található, mivel elősegíti a kiberbűnözés egyéb típusainak sikerességét.
- Az **EMOTET** sokoldalú felhasználása miatt mindenütt jelen van és ez az egyik legkorszerűbb malware.
- A **DDoS-támadások** fenyegetettségi potenciálja nagyobb, mint annak jelenlegi hatása az EU-ban.
- **Online csalások**: A SIM-cserés csalások száma az elmúlt évben meredeken emelkedett és egy olyan kulcsfontosságú trend, amely lehetővé teszi az elkövetőknek, hogy átvegyék a számlák feletti rendelkezést. A **BEC csalások, tehát az üzleti e-mailekhez kapcsolódó visszaélések** továbbra is aggodalomra adnak okot, mivel egyre növekszik a számuk, és egyre kifinomultabbá és célzottabbá váltak. Az **online befektetési csalás** az egyik leggyorsabban növekvő bűncselekmények közé tartozik, milliós veszteségeket okozva és több ezer áldozatot érint.
- Az elmúlt két évben megnőtt a **zsaroló spamek** száma, amelyekben az elkövető megpróbálja megijeszteni és rávenni az áldozatot jellemzően meghatározott összegű bitcoin megfizetésére, a fizetés megtagadása esetén hátrányos esemény kilátásba helyezésével.

B) A pszichológiai manipulációra vonatkozó incidenstrendek

- A social engineering továbbra is a legfőbb fenyegetések között található, mivel elősegíti a kiberbűnözés egyéb típusainak sikerességét.
- A social engineering és az adathalászat számszerűsége és kifinomultsága jelentős növekedést mutat. Az ember gyengeségeinek célba vétele, a social engineering és az adathalászat megalapozzák a számítógépes bűncselekmények többségét, a

csalásoktól és a zsarolástól kezdve egészen az érzékeny információk megszerzéséig és a fejlett malware-támadások végrehajtásáig.

- A sikeres social engineering és az adathalász támadások hátterében a nem megfelelő biztonsági intézkedések és a felhasználók elégtelen biztonságtudatossága áll.

C) A közigazgatási szektort érintő megállapítások

Az Europol által összeállított IOCTA egyes jelentései nem vizsgálják az egyes ágazatokat célzó incidensek számát és arányát, így a későbbi szektorális összehasonlítás során nem kerülnek külön elemzésre.

3.4.6. Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol[134]

A COVID-19 világjárvány jelentősen befolyásolta a kiberfenyegetések alakulását, hatása még a 2021-es évben is kimutatható.

A) Incidenstrendek a vizsgált időszakban

A jelentés főbb megállapításai:

- A **zsarolóvírusok** továbbra is kulcsfontosságú fenyegetések, melyek egyre inkább kihasználják a széles körben elterjedt távmunkát a potenciális célpontok hálózatának **letapogatásával (scanning)**, a **nem biztonságos távoli asztali protokoll (RDP)** után kutatva, illegve nyomon követik a nyilvánosságra hozott virtuális magánhálózati **(VPN) sebezhetőségeket**.
- **A mobil rosszindulatú programok** üzemeltetői kihasználják az **online vásárlások** számának növekedését a szállítási szolgáltatások nevének visszaélésével, akiket **adathalász csaliként** használnak annak érdekében, hogy áldozataikat rávegyék a rosszindulatú kód letöltésére, vagy ellopják a hitelesítő adataikat, vagy a szállítási

[134] Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 (Letöltve: 2022.11.11.); https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (Letöltve: 2022.11.11.)

csalás egyéb formáit kövessék el. Ezek a programok SMS spammelési képességekkel is rendelkezhetnek.

- A **mobil banki trójaiak** kifejezett fenyegetéssé váltak a mobilbankolás megnövekedett népszerűségnek köszönhetően.
- A bűnözők továbbra is a **COVID-19 témáját** használják fel az online értékesítésre szánt hamisított gyógyászati termékek és a vishing révén történő bejelentkezési adatok megszerzéséhez.
- A **DDoS-támadások** egyes jelentések szerint visszatértek, melynek hátterében az online szolgáltatásokra való egyre nagyobb mértékű támaszkodás áll.
- A fenyegetési szereplők tovább fejlesztették módszereiket és szervezettségüket. A kiberbűnözőket továbbra is a kiszámíthatóbb célpontválasztás vezérli, ugyanakkor sokkal inkább **kombinálják a támadás különböző technikáit**. Például egy ransomware támadást további DDOS támadással egészítik ki az áldozatokra történő, a váltságdíj megfizetésére vonatkozó nyomásgyakorlás érdekében.
- A ransomware műveletek egyre inkább a nagy értékű, szervezetek és ellátási láncok elleni támadásokra összpontosítanak és új, többrétegű zsarolási módszereket alkalmaznak, míg a **social engineering** fokozattan a felső vezetőket helyezi az érdeklődése középpontjába.
- **Az adathalászat** és a social engineering tekintetében mind a támadások gyakorisága, mind pedig a csalás mértéke és kifinomultsága növekszik.
- A **befektetési csalás** virágzik, mivel a polgárok óriási veszteségeket szenvednek el, de az üzleti **Business Email Compromise** (BEC) és a **vezérigazgatói csalás** is kulcsfontosságú fenyegetések maradtak.
- Az **EMOTET** vírus terjedését kiemeli a jelentés.

B) A pszichológiai manipulációra vonatkozó incidenstrendek

- Az adathalászat és a social engineering tekintetében mind a támadások gyakorisága, mind pedig a csalások kiterjedtsége és kifinomultsága növekszik.
- A social engineering a vizsgált időszakban fokozattan a felső vezetőket helyezi az érdeklődése középpontjába.

C) A közigazgatási szektort érintő megállapítások

Az Europol által összeállított IOCTA egyes jelentései nem vizsgálják az egyes ágazatokat célzó incidensek számát és arányát, így a későbbi szektorális összehasonlítás során nem kerülnek külön elemzésre.

3.4.7. EU Serious and Organised Crime Threat Assessment (SOCTA) 2021[135]

Az EU SOCTA 2021 egy részletes, az Europol által készített, a súlyos és szervezett bűnözés fenyegetettségének elemzésére vonatkozó jelentés, amely információkat nyújt a szakemberek, a döntéshozók és a szélesebb nyilvánosság számára. A SOCTA 2021 megállapításai az EU-ban a súlyos és szervezett bűnözésről valaha végzett legnagyobb adatgyűjtés részeként gyűjtött adatok (adatbázis, kérdőív) részletes elemzésének eredményeit mutatja be. A SOCTA 2021-hez szolgáltatott adatok mennyisége körülbelül 60%-kal nőtt az azt megelőző jelentés, a SOCTA 2017-hez képest.

A) Incidenstrendek a vizsgált időszakban

A jelentés főbb megállapításai:

- Az olyan eszközök, mint a **rosszindulatú programok, zsarolóprogramok, adathalászat közvetítők**, **szimatolás (sniffing)** és elosztott szolgáltatásmegtagadás (**DDoS**) támadások már online, különösen a sötét weben elérhetőek. Ezen kívül a csalás áldozatainak adatait úgynevezett hitelkártya-adatként értékesítik dumps néven. A **szolgáltatásként nyújtott bűnözés üzleti modellje** a bűnügyi szolgáltatásokat bárki számára könnyen elérhetővé teszi, csökkentve ezzel a szakértelem szintjét, amelyre korábban szükség volt az egyes bűncselekmények elkövetéséhez.
- A **DDoS-támadások** jól ismert és tartós fenyegetést jelentenek, melynek segítségével közintézményeket és kritikus infrastruktúrákat is támadás alá vesznek.

[135] Europol (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Letöltve: 2022.11.11.)

- A bűnözők továbbra is kihasználják a meglévő **sebezhetőségeket**, mintegy a bűncselekmények elkövetésének lehetőségeként.
- A **kriptovalutákat** gyakran használják a csalók.
- Az **EMOTET** újabb aktivitást mutat, mely sokkal több, mint egy átlagos malware. Az EMOTET-et az teszi olyan veszélyessé, hogy a kártevőt kiberbűnözőknek „bérbe adják", hogy más típusú kártevőket telepítsenek, például banki trójaiakat vagy zsarolóprogramokat az áldozat számítógépére.
- **Üzleti e-mailekhez kapcsolódó visszaélések (BEC)**, amely vállalkozások és szervezetek ellen irányul, és a számuk és kifinomultságuk folyamatosan növekszik.
- Új technikák, mint például a **SIM-csere és a SMishing**, amelyek jelentős kockázatot jelentenek az áldozatok személyazonossága és pénzügyei tekintetében. A bűnözők a telefonszolgáltatókat kihasználva teszik meg a cserét a nevükben, akár egy korrupt bennfentes révén, akár social engineering technikákat alkalmazva.
- **Online befektetési csalások**, melyek évente több ezer uniós állampolgárt céloznak meg, és egyre inkább támaszkodnak az újszerű befektetésekre, például kriptovaluták értékesítésére.
- **Adathalászat**, amely továbbra is jelentős fenyegetést jelent és a kifinomultsága egyre nő.

B) A pszichológiai manipulációra vonatkozó incidenstrendek

- A világjárvány alatt a csalók előszeretettel alkalmaztak social engineering technikákat az emberi viselkedés manipulálására és a gyenge pontok kihasználására az információk megszerzése érdekében.
- A bűnözők a social engineering támadásokhoz egyre gyakrabban használják az online platformokat annak érdekében, hogy hozzáférjenek olyan érzékeny információkhoz, amelyek segítik őket a csalások elkövetésében.
- A social engineering jellemző technikái a következők:
  - Cold Calling - Hideghívás call centereken keresztül. A telefonon jelentkező csalók meggyőzik az áldozatokat, hogy fizessenek például pénzátutalás vagy előlegfizetés formájában valamilyen kitalált történet ürügyén.
  - Imperszonáció - Megszemélyesítés: a csalás során a támadó valamely hiteles személynek adja ki magát, és így szerez jogosulatlan hozzáférést.

- Identify Theft - személyazonosság lopás: személyes adatok jogellenes gyűjtése, felhasználása vagy a személyes adatokkal történő manipulálás az érintett előzetes hozzájárulása nélkül.
- Phishing (vishing, spear phishing) – Adathalászat: Csalárd kísérlet arra, hogy érzékeny információkat vagy adatokat, például felhasználóneveket, jelszavakat és hitelkártya adatokat szerezzenek meg, miközben a támadók megbízható személynek adják ki magukat az elektronikus kommunikációban (pl. emailben, sms-ben, telefonon).

C) A közigazgatási szektort érintő megállapítások

A SOCTA 2021 nem vizsgálja az egyes ágazatokat célzó incidensek számát és arányát, így a későbbi szektorális összehasonlítás során nem kerülnek külön elemzésre.

3.5. ÖSSZEHASONLÍTÁS: A HAZAI ÉS AZ EURÓPAI INCIDENSTRENDEK ÖSSZEHASONLÍTÁSA[136]

A H1 hipotézisem bizonyítása érdekében, mely szerint „a magyar közigazgatást érő kiberbiztonsági incidensek megfelelnek az európai incidenstrendeknek”, a disszertáció 3.3. részében részletesen elemzett hazai incidenstrendeket összehasonlítani szükséges a 3.4. részben bemutatott európai jelentésekben meghatározott incidens típusokkal és trendekkel. Az összehasonlító elemzésre a következő fejezetekben kerül sor a hazai incidenstrendek elemzésénél alkalmazott tagolás szerint:

- az NKI által, 2019 és 2021 között kezelt incidens típusok összehasonlítása az európai trendekkel;
- az NKI által, 2019 és 2021 között kezelt incidensek szektorális összehasonlítása az európai trendekkel;
- az NKI által, 2019 és 2021 között kezelt, tágabb értelemben vett pszichológiai manipulációhoz kapcsolódó incidensek összehasonlítása az európai trendekkel.

[136] A fejezet Legárd Ildikó: A közigazgatást érő hazai és európai incidenstrendek összehasonlítása (2023b) című tanulmányokban kerültek publikálásra.

3.5.1. Évenkénti és incidens típusok szerinti összehasonlítás

Az összehasonlítás alapjául szolgáló európai dokumentumok közül az ENISA jelentései az elnevezésével ellentétben nem a naptári évekhez igazították a vizsgálati időszakot, így lehetséges, hogy az ENISA Threat Landscape (továbbiakban: ETL) 2020, a 2019. január – 2020. április közötti időszak adatait dolgozza fel, az ETL 2021, a 2020. áprilistól 2021. júliusig tartó periódust, míg az ETL 2022, a 2021. július – 2022. július közötti hónapokat elemzi. Hasonlóképpen az Eurpol által összeállított EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 jelentése sem naptári évhez kötött, mivel az előző jelentés 2017-ben készült el, így az azóta eltelt időszakban azonosítható trendeket elemzi, bár hangsúlyosan a koronavírus járvánnyal érintett éveket és a pandémiához kapcsolódó jelenségeket vizsgálja. A szintén az Eurpol által készített Internet Organised Crime Threat Assessment (továbbiakban: IOCTA) 2019, 2020 és 2021 jelentések mindig a publikálást megelőző 12 hónapra vonatkozó megállapításokat tartalmaznak, így szintén nehezen feleltehetők meg az NKI által évenként gyűjtött incidenseknek. A vizsgálati időtartamból keletkező eltérések kezelése érdekében az összehasonlításhoz az NKI által detektált incidensek tekintetében a 2019-2021 időszakra vonatkozó összegzett statisztikai adatokat vettem alapul.

Ahhoz, hogy a hazai trendek összehasonlíthatók legyenek az európai trendekkel, szükséges megvizsgálni a három év viszonylatában összesítve az egyes incidens típusok arányát és adott típushoz kapcsolódó trendeket. Az alábbi táblázat összefoglalja a 2019-2021 években azonosított incidensek TOP 10-es listáját, az adott évekhez köthető eltérések miatt (évenként a TOP 10-es lista némileg változott) az összesített lista 14 incidens típust sorol fel. A második oszlop megmutatja, hogy az adott típus, az összes 2019-2021-es években detektált incidens hány százalékát teszi ki. Az utolsó négy oszlop az adott incidenshez kapcsolódó emelkedő / csökkenő tendenciát hivatott bemutatni, az adott évben, az adott incidens típushoz hozzárendelhető, valamennyi detektált incidenshez viszonyított arányuk feltüntetésével.

Incidensek típusai	2019-2021 összes incidenshez viszonyított arány	Tendencia	2019	2020	2021
Káros tevékenység	18%		9%	25%	14%
Elérhetőség (Availability)	16%		1%	19%	20%
Információgyűjtés	16%		7%	17%	19%
Ismeretlen típusú káros kód	9%		3%	11%	2%
Pszichológiai manipuláció (Social engineering)	6%		22%	3%	2%
Ismert sérülékenység kihasználása	6%		17%	3%	12%
Spam	4%		2%	2%	7%
Nem-adminisztrátor fiók kompromittálódása	4%		6%	4%	3%
Defacement research	4%		3%	1%	3%
Információk illetéktelen hozzáférése	3%		0%	0%	3%
Ransomware	2%		4%	3%	2%
DDoS	2%		3%	2%	2%
Behatolási kísérlet	2%		7%	4%	1%
Trójai	1%		7%	1%	1%
Egyéb	7%		9%	5%	9%

5. táblázat: 2019-2021 évek incidens típusai – TOP 10 áttekintés (forrás: saját szerkesztés)

Az incidens típusok összehasonlítása a terminológiai eltérések miatt nem könnyű feladat. Az elemzést nehezíti, hogy maga az ENISA is eltérő terminológiai megközelítést alkalmaz 2021 óta, ugyanis ekkor az ENISA összevonta a fenyegetések kategóriáit, és a korábbi jól azonosítható incidens típusok helyett összefoglaló kategóriákat vezetett be. Ennek tükrében, az NKI által vizsgált incidens típusok azonosításához és a trendek összehasonlításához az európai jelentések átfogó dokumentumelemzésére volt szükség, melyet a 3.4. rész mutat be részletesen. A 3.4. részben a jelentések elemzése során külön kitértem az NKI által vizsgált incidens típusokhoz köthető megállapításokra és az azokból azonosítható trendekre, így jelen részben csupán az összehasonlítás eredményeinek ismertetésére kerül sor.

Az összehasonlítás során arra kerestem a választ, hogy az NKI által leggyakrabban detektált incidens típusok („Incidens típusok, NKI 2019-2021 összesített TOP 10” oszlop) azonosíthatók-e elkövetési trendként az ENISA Threat Landscape 2020, 2021 és 2022, valamint az IOCTA 2019, 2020, 2021 és a SOCTA 2021 jelentésekben. Amennyiben a megfeleltetés igaznak bizonyult, „pipa” került jelölésként a táblázat megfelelő részébe, ahol azonban az adott hazai incidens típus nem volt azonosítható a jelentésben, „negatív” jelzés került a releváns cellába.

Az alábbi táblázat bemutatja az összehasonlító elemzés eredményeit az NKI által vizsgált incidens típusonként jelölve, hogy azok mely európai jelentés konkrét megállapításainak feleltehetők meg, tehát mely hazai incidens típus azonosítható a vizsgált időszakban meghatározó trendként az Európai Unióban is.

Incidens típusok, NKI 2019-2021 összesített TOP 10	ENISA Threat Landscape 2020	ENISA Threat Landscape 2021	ENISA Threat Landscape 2022	IOCTA 2019	IOCTA 2020	IOCTA 2021	SOCTA 2021
Káros tevékenység - malicious actions (pl. káros kód, fertőzött rendszer, C&C server, káros kód konfiguráció)	✓	✓	✓	✓	✓	✓	✓
Elérhetőség - Availability (pl. DoS, DDoS, szabotázs, kiesés - nem rosszindulatú)	✓	✓	✓	✓	✓	✓	✓
Információgyűjtés - Information Gathering (pl. scanning, sniffing)	✓	✓	✓	✓	✓	✓	✓
Ismeretlen típusú káros kód - Unknown malware	✓	✓	✓	✓	✓	✓	✓
Pszichológiai manipuláció - Social engineering	✓	✓	✓	✓	✓	✓	✓
Ismert sérülékenység kihasználása - Exploiting known vulnerabilities	✓	✓	✓	✓	✓	✓	✓
Spam	✓	✓	✓	—	✓	✓	—
Nem-adminisztrátor fiók kompromittálódása - Unprivileged account compromise	✓	✓	✓	✓	✓	✓	✓
Defacement research	✓	✓	✓	—	—	—	—
Információk illetéktelen hozzáférése - Unauthorised access to information	✓	✓	✓	✓	✓	✓	✓
Ransomware	✓	✓	✓	✓	✓	✓	✓
DDoS	✓	✓	✓	✓	✓	✓	✓
Behatolási kísérlet - Intrusion Attempts	✓	✓	✓	✓	✓	✓	✓
Trójai - Trojan	✓	✓	✓	✓	✓	✓	✓
Egyéb	✓	✓	✓	✓	✓	✓	✓

6. táblázat: Az NKI által, 2019 és 2021 között kezelt incidens típusok általános összehasonlítása az európai trendekkel (forrás: saját szerkesztés)

A vizsgálatból kiderült, hogy a spam, illetve a defacement (honlaprongálás) kivételével valamennyi, az NKI által detektált incidens típus meghatározó trendként került azonosításra a 2019-2021 közötti évekre vonatkozó európai jelentésekben is. A **spamre** vonatkozóan az IOCTA 2019, valamint a SOCTA 2021 nem tartalmaz megállapításokat. Ezzel szemben az ETL 2020 a spam kategóriáját az 5. leggyakoribb fenyegetésként jelöli meg, míg az ETL 2021-ben az email-ekhez kapcsolódó fenyegetések között szerepel, az ETL 2022-ben pedig a malware-k terjesztésében, valamint a dezinformáció és félretájékoztatásban betöltött szerepe miatt kerül kiemelésre. Az IOCTA 2020 a zsaroló spam-ekre hívja fel a figyelmet, míg az IOCTA 2021 a rosszindulatú programok sms spamelési képességeit emeli ki. Tehát megállapítható, hogy bár a spam a legtöbb jelentésben nem kerül önálló kategóriaként megjelölésre, ugyanakkor számos incidens

típus hátterében, ahhoz kötődően jelenik meg, mely egyértelműen bizonyítja, hogy nem elhanyagolható szerepe van a támadások sikerességében.

A **defacement**, mint meghatározó fenyegetési vektor egyik IOCTA jelentésben, illetve a SOCTA 2021-ben sem szerepel, ugyanakkor valamennyi ETL-ben azonosíthatók trendként. Az ETL 2020-ban, a TOP 15-ös lista második helyen szereplő web-alapú támadásokhoz sorolható a honlaprongálás esete, az ETL 2021-ben az új, összefoglaló kategóriaként megjelenő „rendelkezésre állás és az integritás elleni fenyegetések" között szerepel a webes támadások családja részeként. Az ETL 2022-ben a „rendelkezésre állás elleni fenyegetések: Internetes fenyegetések" kategóriába sorolható a defacement.

Összességében megállapítható, hogy az NKI által, a 2019-2021 időszakban leggyakrabban detektált incidens típusok megfelelnek az vizsgált időszakban elemzett európai trendeknek. A spam-ek, illetve a defacement esetében, melyek az összes detektált hazai incidens mintegy 4%-4%-ában állnak a biztonsági események hátterében, az európai megfelelés a fentebb leírtak figyelembevételével nem önálló kategóriaként, hanem az egyes összesítő kategóriák részeként, e főkategóriákhoz kapcsoló trendek keretében értelmezhetők.

A Koronavírus járvány hatása a hazai és az európai incidenstrendekre

A disszertáció 3.3.3.1. részében bemutatott, **2020. évre** vonatkozó elemzésből kiderül, hogy a koronavírus egyes hullámaihoz kapcsolódóan szignifikánsan megemelkedett az NKI által detektált incidensek száma, a tavaszi (2020. február-április) és az őszi hullám (2020. szeptember-november) incidenseinek összesített aránya eléri az összes éves incidens közel 60 %-át.

Amennyiben az NKI által detektált incidens típusokat és a hozzájuk kötődő biztonsági eseményeket összehasonlítjuk az ENISA által, a Threat Landscape 2020 keretében bemutatott, COVID-19-hez kapcsolódó elemzésével[137], illetve az Interpol által összeállított pandémiával kapcsolatos jelentésével[138], megállapíthatjuk, hogy a járvány első és másik hullámában azonosított hazai incidenstrendek megfelelnek az európai trendeknek.

[137] Threat Landscape Mapping, ENISA: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/threat-landscape-mapping-infographic-2020 (Letöltve: 2022.11.11.)

[138] https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (Letöltve: 2022.11.11.)

ENISA Threat Landscape 2020 -COVID 19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek		Interpol - COVID 19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek
Távmunkához kapcsolódó infrastruktúrákhoz köthető támadások	✓		Adathalászat / Átverés/csalás	✓
Koronavírussal kapcsolatos domain-ek	✓		Malware / Ransomware	✓
Sms-es adathalászat	✓		Rosszindulatú domain-ek	✓
Email-es adathalászat	✓		Álhírek	✓
Hamis tesztelési alkalmazások				
Támadások egészségügyi szervezetek ellen	✓			

7. táblázat: A COVID-19 idején, az NKI által 2020-ban detektált hazai incidensek összehasonlítása az európai incidenstrendekkel (forrás: saját szerkesztés)

A **2021**. évre is igaz, hogy az NKI által detektált incidensek százalékos aránya a tavaszi (2021. február-április) és az őszi (2021. szeptember-november) hullám során jelentősen megemelkedett. Az incidenstrendek hátterében a korábban (3.3.3.1., 2021. év vizsgálata) azonosított és részletesen bemutatott olyan incidens típusok állnak, mint a COVID -19 járványhoz kapcsolódó kiberfenyegetések, a rosszindulatú malware-ek (pl. EMOTET, Flubot) és zsarolóvírusok, a káros csatolmányokat tartalmazó kampányszerűen terjedő levelek, a kéretlen, adathalász tartalmú email üzenetek, valamint a Microsoft Exchange szerveket érintő ProxyLogon és ProxyShell sérülékenységek, illetve az Apache Log4j könyvtárt érintő Log4shell érintő sérülékenység.

Amennyiben a 2021. év vonatkozásában összehasonlítjuk az NKI által legnagyobb arányban detektált incidens típusokat az ENISA és az Europol által készített jelentésekben azonosítható elkövetési formákkal és bemutatott európai trendekkel, megállapíthatjuk, hogy a hazánkban detektált incidensek valamennyi típusa megjelenik a vizsgált európai jelentésekben is. Az összehasonlítás eredményét az alábbi táblázat szemlélteti:

NKI 2021	ETL 2021	ETL 2022	IOCTA 2020	IOCTA 2021	SOCTA 2021
Információgyűjtés	✓	✓	✓	✓	✓
Elérhetőség	✓	✓	✓	✓	✓
Káros tevékenység	✓	✓	✓	✓	✓
Ismeretlen típusú káros kód	✓	✓	✓	✓	✓
Nem-adminisztrátor fiók kompromittálódása	✓	✓	✓	✓	✓
Spam	✓	✓	✓	✓	–
DDoS	✓	✓	✓	✓	✓
Trójai	✓	✓	✓	✓	✓
Információk illetéktelen hozzáférése	✓	✓	✓	✓	✓

8. táblázat: A COVID-19 idején, az NKI által 2021-ban detektált hazai incidensek összehasonlítása az európai incidenstrendekkel (forrás: saját szerkesztés)

Részkövetkeztetések:

A hazai és az európai incidenstrendek összehasonlító vizsgálata során megállapítottam, hogy a koronavírus járvány és ennek hatására a mindennapi munkavégzés és szabadidő eltöltésének az online térbe áthelyeződése kapcsán, a kiberbiztonsági incidensek számának jelentős emelkedése figyelhető meg a járványt megelőző időszakhoz képest.
A leggyakoribb támadás típusok a különböző káros tevékenységet megvalósító rosszindulatú szoftverek voltak, ideértve a zsarolóvírusokat is, amelyek hatalmas károkat okoztak a megtámadott személyeknek, szervezeteknek, cégeknek. Jelentős emelkedés figyelhető meg a vizsgált években a rendelkezésre állást célzó támadások tekintetében is, különös tekintettel a DDOS-ra. Az ismert sérülékenységek kihasználása szintén jellemző tendencia volt, az adatszivárgásokkal, az információgyűjtéssel, valamint a nem-adminisztrátori fiókok kompromittálódásával együtt.
A támadók gyorsan alkalmazkodtak a megváltozott körülményekhez, ezért egyre hatékonyabban célozták meg az áldozatokat különböző social engineering technikák segítségével. (Ez utóbbi incidensek elemzésére a 3.5.3. részben kerül sor.)

Összességében megállapítottam, hogy 2020 és 2021-es években, mind a COVID-19 világjárvány kapcsán kialakuló hullámok időszakában, mind pedig a teljes évet figyelembe véve azonosított hazai incidens típusok megfelelnek az európai jelentésekben megjelenített legfőbb fenyegetéseknek, így az összehasonlítás eredményeképpen megállapítottam, hogy a magyar közigazgatást érő incidenstrendek megfelelnek az európai trendeknek.

3.5.2. Szektorális összehasonlítás

A disszertáció 3.3.4. részében bemutatott elemzés segítségével megállapítást nyert, hogy az NKI által végzett eseménykezeléssel érintett és az értekezésben vizsgált ellátotti körben az állami és önkormányzati szerveket érte a legtöbb kibertámadás, a 2019 és 2021 közötti időszakban detektált incidensek 47%-a e szektor ellen irányult.

Az incidensben érintett szektor		Incidensek összesített százalékos aránya 2019-2021
Állami és önkormányzati szervek		47%
Nemzetbiztonsági védelem alá eső szervezetek		8%
Közvetítő szolgáltatók		7%
Oktatási Intézmények		7%
Alapvető szolgáltatásokat nyújtó szereplő		4%
Nemzeti létfontosságú rendszerelemek		3%
Bejelentés köteles szolgáltatók		2%
Egyéb szervezetek		22%

24. ábra: Az egyes szektorokat érintően kezelt incidensek százalékos eloszlása, 2019-2021 (forrás: saját szerkesztés)

A hazai szektorális eredmények európai trendekkel történő összehasonlítása érdekében az előző részekben bemutattam az egyes európai jelentésekben azonosított, az állami és önkormányzati szerveknek leginkább megfeleltethető szektorokkal kapcsolatos trendeket. Az „állami és önkormányzati szervek” terminológiának a nemzetközi dokumentumokban azonosítható megfelelője a „Public Administration”, azaz a közigazgatás, vagy a szűkebb fogalmat takaró „Government” (kormányzat) feleltethető meg.

Az egyes jelentések alapján, minden évben a közigazgatás ágazata bizonyult a legtámadottabb szektornak, ugyanakkor a tendenciák tekintetében az egyetlen a 2020-a ETL jelentés, amely megállapította, hogy az ágazatot érő támadások száma alapján az incidenstrendek változatlannak tekinthetők, sőt kissé csökkenő tendenciát mutatnak.
A jelentések megállapításait összevetve a hazai szektorális eredményekkel megállapítható, hogy a közigazgatási ágazat az európai incidenstrendeknek is meghatározó része, ugyanakkor az ETL 2020 által kimutatott kissé csökkenő tendencia a hazai tendenciákkal ellentétes. A 2019-2021 között időszakban, az NKI által detektált, az állami és önkormányzati szervek felé irányuló incidensek növekvő tendenciát mutattak az egyes években.
Ugyanakkor az összehasonlításból eredő eltérés oka a nem pontosan egymásnak megfeleltethető szektorokkal is magyarázható, hiszen az ETL 2020 szélesebb körben határozta meg az ágazathoz tartozó szerveket, és ide sorolta a védelmi és szociális ellátásokat is.

Az ETL 2021 -a 2020-as jelentéshez képest- sokkal letisztultabb ágazati besorolást vesz alapul, melynek keretében 19 szektort vizsgál, melyek között önállóan jelenik meg a közigazgatási/kormányzati szektor.
A jelentés megállapítja, hogy a közigazgatási/kormányzati ágazatot érő incidensek száma a legmagasabb (189 db) a vizsgált időszakban, így ezen szektor elsősége megkérdőjelezhetetlen a szektorok veszélyeztetettsége tekintetében.
Az ETL 2021 vizsgálati eredményeit összehasonlítva a hazai, szektorokat érintő incidenstrendekkel megállapítható, hogy a közigazgatási/kormányzati ágazatot éri szignifikánsan a legtöbb támadás, tehát ez a szektor van kitéve a leginkább a kibertérhez kapcsolódó fenyegetéseknek.

Az ETL 2022 hasonló következtetésre jut: a jelentési időszakban ismét nagyszámú, a közigazgatás és a kormányzat ellen irányuló incidenst figyeltek meg, az összes incidens mintegy negyede 24,21% irányult e szektor felé.

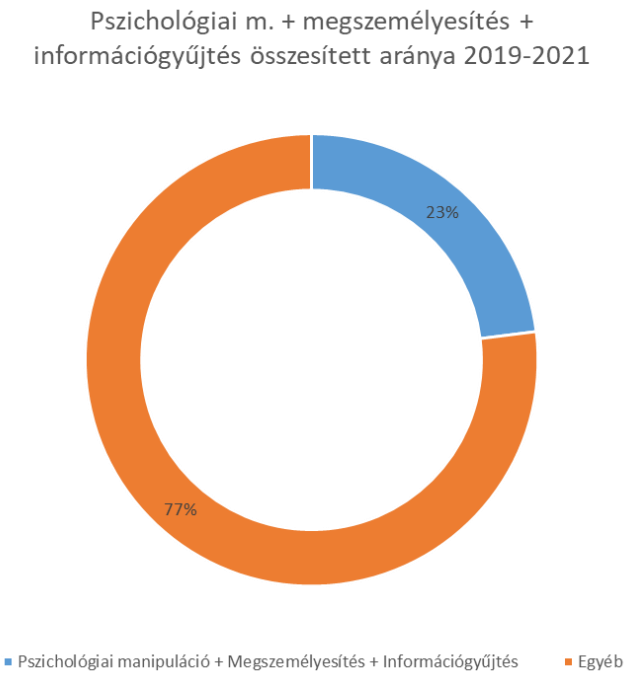
Az Europol által összeállított IOCTA egyes jelentései, valamint a SOCTA 2021 nem vizsgálják az egyes ágazatokat célzó incidensek számát és arányát, így a szektorális összehasonlítás során nem kerülnek külön elemzésre.

Részkövetkeztetések:
Az ágazati szempontból bemutatott ETL jelentések hazai vizsgálatokkal történő összehasonlítása alapján megállapítottam, hogy a magyar közigazgatást érő kiberbiztonsági incidensek megfelelnek az európai incidenstrendeknek és e tekintetben a szektorális összehasonlítás sem képez kivételt.
Hazánkban és az Európai Unióban egyaránt, a 2019-2021 közötti időszakban a közigazgatási/kormányzati szektort érte a legtöbb incidens, tehát a közigazgatási/kormányzati szervek a kibertámadók leggyakoribb célpontjai.

3.5.3. Pszichológiai manipulációhoz kapcsolódó incidensek

A hazai adatok elemzése során a 3.3.5. részben bemutatásra került, hogy az NKI által detektált incidensek tekintetében szükséges a pszichológiai manipuláció fogalmát tágan értelmezni és a statisztikai eltérések kiküszöbölése érdekében a pszichológiai manipuláció

vizsgálatánál a megszemélyesítés, valamint az információgyűjtés incidens típusokkal kiegészített, összesített százalékos eloszlását vizsgálni az 2019-2021 közötti időszakban. Vizsgálatom eredményeit az alábbi grafikon szemlélteti:



25. ábra: A tágabb értelemben vett pszichológiai manipulációnak az összes incidenshez viszonyított aránya a 2019-2021 közötti időszakban (forrás: saját szerkesztés)

Amennyiben a tágabb értelemben vett pszichológiai manipulációt érintő trendeket elemezzük a vizsgált három év -2019, 2020 és 2021- viszonylatában, azt láthatjuk, hogy az egyes években az összes incidenshez viszonyított arányuk stagnáló tendenciát mutat, 22% és 24% között mozog.

Az európai trendekkel történő összehasonlítás érdekében, dokumentumelemzés segítségével azonosítottam az egyes jelentésekben detektálható pszichológiai manipulációhoz, azaz az angol terminológiának megfelelő, social engineeringhez kapcsolódó trendeket, melyeket bemutattam az előző részekben.

Az ETL 2020-ban meghatározott TOP 15 legveszélyesebbnek ítélt fenyegetés, valamint az ETL 2021-ben felsorolt elsődleges fenyegetések közé a social engineering nem került be önálló kategóriaként, ezért ezen jelentésekből nem tudunk pontos következtetéseket levonni a pszichológiai manipulációval kapcsolatos trendekre, ugyanakkor számos, a

jelentésekben megjelölt elsődleges fenyegetés első lépéseként azonosíthatók a social engineering technikák.
Az **ENISA Threat Landscape 2022** az első jelentés, ahol önálló fenyegetési tényezőként szerepel a social engineering, így az európai és a hazai trendek összehasonlítása alapjául elsődlegesen ezt a dokumentumot lehet számításba venni.

Az Europol által készített **Internet Organised Crime Threat Assessment (IOCTA)** jelentések nem határoznak meg rangsort, százalékos eloszlást vagy konkrét számadatokat az egyes incidens típusok tekintetében. A riportok az egyes támadási vektorokhoz (pl. social engineering) kapcsolódó trendekre, és az egyes incidens típusok közötti összefüggésekre hívják fel a figyelmet. Tekintettel a tényre, hogy a social engineering a támadások jelentős részében a sikeresség hátterében áll, így a dokumentumokban elszórtan, jellemzően nem önállóan, hanem más támadás típusokhoz való kapcsolata alapján kerül bemutatásra.

Részkövetkeztetések:
Az elemzett dokumentumokból megállapítottam, hogy a vizsgált időszakban a különböző social engineering technikákat egyre növekedő számban és jelentős százalékban sikeresen használták fel a csalók egyéb támadás típusok elkövetése érdekében, amely jellemző nem csak hazánkban, hanem az Európai Unióban egyaránt. Bár a bemutatott jelentések nem határozzák meg a pszichológiai manipulációhoz köthető incidensek számát vagy százalékos arányát, a felsorolt megállapítások megkérdőjelezhetetlenné teszik, hogy a social engineeringre az egyik legfőbb fenyegetésként kell tekintenünk, elsősorban növekvő kifinomultsága, és az egyéb támadás típusok sikerességéhez történő hozzájárulása szempontjából.

Az összehasonlítás eredményeként összességében megállapítottam, hogy a social engineering az **európai incidenstrendek tekintetében az elsődleges fenyegetések közé tartozik, melynek szerepe, számszerűsége és kifinomultsága tekintetében is növekedő tendenciát mutat**. A tágabb értelemben vett pszichológiai manipuláció **a hazai trendek tekintetében is kulcsfontosságú jelentőséggel bír,** mivel hozzávetőlegesen minden negyedik támadás social engineeringhez kötődik. Bár az NKI által gyűjtött adatok a pszichológiai manipuláció kifinomultságára, valamint az egyéb támadási vektorokban betöltött szerepére nem szolgáltatnak információt, mégis a sikeres támadások egyre

növekvő számából és a korábban bemutatott konkrét esetekből többek között arra is lehet következtetni, hogy a social engineering technikákat az elkövetők egyre növekvő számban, egyre célzottabban és kifinomultabban alkalmazzák a céljaik elérése érdekében.

3.6. KÖVETKEZTETÉSEK

A fejezet elején meghatározott bizonyítási célom az volt, hogy többszempontú, tudományos vizsgálatokkal bizonyítsam, hogy a hazai, elsősorban közigazgatást érő kiberbiztonsági incidenstrendek megfelelnek-e az európai trendeknek!

A bizonyítási cél elérése érdekében jelen fejezet első részében bemutattam, majd évenkénti és incidens típusok szerinti bontásban, illetve szektorális bontásban elemeztem az NKI által, a 2019-2021 közötti években detektált incidensekre vonatkozó statisztikai adatokat, külön kitérve a koronavírushoz kapcsolódó világjárvány hatásaira, valamint a pszichológiai manipuláció különböző szempontú vizsgálatára is.
A következő részben dokumentumelemzés segítségével bemutattam az összehasonlítás alapjául szolgáló -az ENISA, illetve az Europol által összeállított- jelentéseket.
A fejezet harmadik részében több szempontú vizsgálatot végeztem a hazai és az európai incidenstrendek összehasonlítása érdekében, melynek keretében összevetettem az NKI által a vizsgálat időszakban kezelt incidens típusokat –évenkénti bontásban és összesítve- az európai trendekkel, majd az incidensek szektorális megoszlását, valamint a tágabb értelembe vett pszichológiai manipulációra vonatkozó adatokat hasonlítottam össze az európai adatokkal.
Az NKI által, 2019 és 2021 között kezelt incidens típusok és az európai trendek általános összehasonlítása érdekében -a terminológiai és a vizsgált időszakokból adódó eltérések miatt- az európai dokumentumok részletes elemzésére volt szükség. Vizsgálati eredményeimet a 6-8. táblázatokban foglaltam össze pontosan megjelölve, hogy az NKI által detektált incidens típus azonosítható-e, és ha igen, mely dokumentum megállapításai szerint, meghatározó európai trendként.
Az incidens típusokra irányuló vizsgálat alapján megállapítottam, hogy az NKI által közölt adatok alapján detektált incidenstrendek megfelelnek az európai trendeknek.

A szektorális összehasonlítás kizárólag a 2020. év tekintetében mutatott némi különbséget a trendek tekintetében: míg a hazai adatok alapján a közigazgatás felé irányuló támadások százalékos aránya növekedett, addig az ENISA kissé csökkenő tendenciát észlelt. Ugyanakkor a 2020-a Threat Landscape is megjegyezte, hogy a közigazgatási ágazat az európai incidenstrendeknek meghatározó része. A 2021-es és 2022-es évek tekintetében mind az NKI, mind pedig az ENISA megállapította, hogy a közigazgatási / kormányzati szektorral szemben következik be a legtöbb kibertámadás.

A pszichológiai manipuláció (social engineering) tekintetében az elemzett európai dokumentumokból egyértelműen megállapítható, hogy a támadási formára az egyik legfőbb fenyegetésként kell tekintenünk és meghatározó szerepe van az egyéb támadási típusok sikeressége szempontjából. A hazai adatok is alátámasztják a social engineering jelentőségét, hiszen a vizsgált években kiegyensúlyozottan az arányuk 22-24 % között mozgott, ugyanakkor az egyéb támadás típusok hátterében, a bemutatott konkrét példák alapján egyértelműen megállapítható, hogy pszichológiai manipuláció állt.

Összehasonlító vizsgálataim eredményeként megállapítottam, hogy a 2019-2021 közötti időszakban a magyar közigazgatást érő kibertámadások alapján meghatározható incidenstrendek, mind az évenkénti összehasonlítás és ennek keretében a pandémiás időszakban tapasztalható változások, mind pedig a három év összesített adatai, valamint az egyes szektorokat érő támadások és a pszichológiai manipuláció önálló vizsgálata tekintetében is, megfelelnek az európai incidenstrendeknek.

4. AZ IBF SZEREPPROFIL (MÁSODIK HIPOTÉZIS)[139]

4.1. BEVEZETÉS

A 2022-es Digitális Gazdasági és Társadalmi Index (DESI) megállapította, hogy 2021-ben 8,9 millió személy dolgozott IKT-szakemberként az Európai Unióban, amely a munkaerőpiac 4,5 %-át teszi ki. Bár 2013 óta folyamatos a növekedés, az IKT-szakemberek aránya lassan növekszik (2020-ban az összes foglalkoztatott 4,3%-át tették ki az IKT szakemberek), gyorsulásra van szükség, hiszen 2030-ra 20 millió foglalkoztatott IKT-szakértő elérése a cél az EU-ban, a nők és a férfiak közötti konvergenciával.[140]

Az Európai Bizottság által Magyarországról kiadott „2024. évi országjelentés a digitális évtizedről" megállapítja, hogy a „foglalkoztatott IKT-szakemberek aránya Magyarországon 4,2 %, szemben az EU-ban mért 4,8 %-kal, és ami még fontosabb, az éves előrehaladása (+2,4 %, szemben az EU-ban mért 4,3 %-kal) nem elegendő a 2030-ra kitűzött cél eléréséhez."[141] Magyarországon egyébként az informatikai felsőoktatási szakokon végzettek aránya az alapképzésben 2020-ban 4,9% volt, a cél, hogy 2030-ra ez arány 10%-ra növekedjen[142].

A kiberbiztonsági munkaerő és szakképzettség hiánya mind a gazdasági fejlődés, a versenyképesség, mind pedig nemzetbiztonsági szempontból komoly aggodalomra ad okot, különösen a globális gazdaság gyors digitalizációja miatt. Ezért az Európai Unió 2020-ban kiadott kiberbiztonsági stratégiája[143] is felhívja a figyelmet a kiberbiztonsági szakemberek hiányának veszélyeire, melynek megoldására egy uniós szintű kiberbiztonsági pályafutási rendszer kidolgozását és bevezetését javasolja.

---

[139] E fejezet két tanulmányban került publikálásra: Legárd Ildikó: A nemzetközi keretrendszerek összehasonlítása és a jó gyakorlatok azonosítása az IBF szerepprofil definiálása érdekében (Legárd, 2022a); Legárd Ildikó: Az elektronikus információs rendszer biztonságáért felelős személy szerepprofilja (Legárd, 2023c)

[140] Digitális Gazdasági és Társadalmi Index (DESI) 2022 https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (Letöltve: 2022.10.12.)

[141] Magyarország 2024. évi országjelentése a digitális évtizedről https://digital-strategy.ec.europa.eu/hu/factpages/hungary-2024-digital-decade-country-report (Letöltve: 2024.11.14.)

[142] Nemzeti Digitalizációs Stratégia (2022-2030) p.9; https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030

[143] Az Európai Gazdasági és Szociális Bizottság (2021/C 286/14) véleménye közös közleményéről az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre (JOIN(2020) 18 final)

Napjaink közigazgatási környezete a digitalizáció felgyorsuló térnyerésének köszönhetően teljes átalakuláson ment keresztül, a közigazgatási folyamatok mára már elképzelhetetlenek az információs és kommunikációs technológiák használata nélkül. E fejlődési folyamattal párhuzamosan a közigazgatás kiemelkedő célpontjává vált az évről évre célzottabb és szofisztikáltabb kibertámadásoknak. Az Európai Unió Kiberbiztonsági Ügynöksége, az ENISA által készített, az előző fejezetben bemutatott jelentések évről évre a legtámadottabb ágazatként azonosítják a közigazgatást, melyet az előző fejezetben bemutatott hazai incidenstrend-elemzések is megerősítenek.

Ahhoz, hogy a közigazgatás területén ki tudjuk használni a digitalizációban rejlő lehetőségeket, **szükséges, hogy a kibertér felől érkező fenyegetések tekintetében is megfelelő felkészültséggel rendelkezzünk, és megfelelő képzettségű és számú kiberbiztonsággal foglalkozó szakember álljon rendelkezésre**. A Nemzeti Digitalizációs Stratégia (2022-2030) is kiemeli, hogy „ágazati és központi szinten kiemelten szükséges az információbiztonsági elemek és a kibervédelmi kapacitások bővítése, összhangban a hazai és az EU-s szintű törekvésekkel”[144].

A kibertámadások megelőzése érdekében az Ibtv., majd 2025. január 1-től a Kibertv. a hatálya alá tartozó szervezetek elektronikus információs rendszereinek védelmét biztosító kötelezettségei körében, mind a szervezet vezetője, mind pedig az általa megbízott vagy kinevezett elektronikus információs rendszer biztonságáért felelős személy (IBF) számára meghatározott feladatok ellátását teszik kötelezővé. Az Ibtv., és a végrehajtására szolgáló 41/2015. (VII. 15.) BM rendelet[145] konkrét feladatkatalógust határoz meg az IBF részére, ugyanakkor nem létezik olyan hazai dokumentum, amely segítséget nyújtana a sikeres feladatellátáshoz nélkülözhetetlen készségek, ismeretek és kompetenciák meghatározásához, ezáltal a megfelelő kibervédelmi képességek és felkészültség biztosításához.

Bizonyítási cél:

A következő részekben bemutatott vizsgálatokkal azt kívánom bizonyítani, hogy nemzetközi keretrendszerek segítségével, tudományos alapokon megalkotható az

[144] Nemzeti Digitalizációs Stratégia (2022-2030) p.68; https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030

[145] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet. A rendeletet a 7/2024 MK váltja fel az Ibtv. hatála alá tartozó szervezetek számára 2025. január 1-től.

elektronikus információs rendszer biztonságáért felelős személy részére egy olyan szerepprofil, amely meghatározza az általa ellátandó feladatokat, valamint a végrehajtáshoz szükséges készségeket, ismereteket, kompetenciákat, és nem utolsó sorban szervesen illeszkedik a tágabb, európai környezetbe.

4.1.1. Hipotézisek

H2	**Meghatározható az elektronikus információs rendszer biztonságáért felelős személy számára egy olyan szerepprofil, amely azonosítja a mindennapi munkavégzés részét képező feladatokat, illetve a végrehajtáshoz szükséges készségeket, ismereteket és kompetenciákat.**

9. táblázat: H2 hipotézis (forrás: saját szerkesztés)

E kutatási cél elérése érdekében az alábbi alhipotéziseket állítottam fel:

H2-1.	Azonosíthatók a kiberbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó nemzetközi keretrendszerek segítségével olyan jó gyakorlatok, amelyek átültethetők a magyar közigazgatási környezetbe.
H2-2.	Az elektronikus információs rendszer biztonságáért felelős személy jogszabályokban meghatározott feladatai, és e feladatok ellátásához szükséges készségek, ismeretek és kompetenciák azonosíthatók a jó gyakorlatként bemutatott nemzetközi keretrendszerekben.
H2-3.	Kidolgozható az elektronikus információs rendszer biztonságáért felelős személy számára egy olyan szerepprofil, amely meghatározza a mindennapi munkavégzés részét képező feladatokat, illetve a végrehajtáshoz szükséges készségeket, ismereteket és kompetenciákat.

10. táblázat: H2 hipotézis alhipotézisei (forrás: saját szerkesztés)

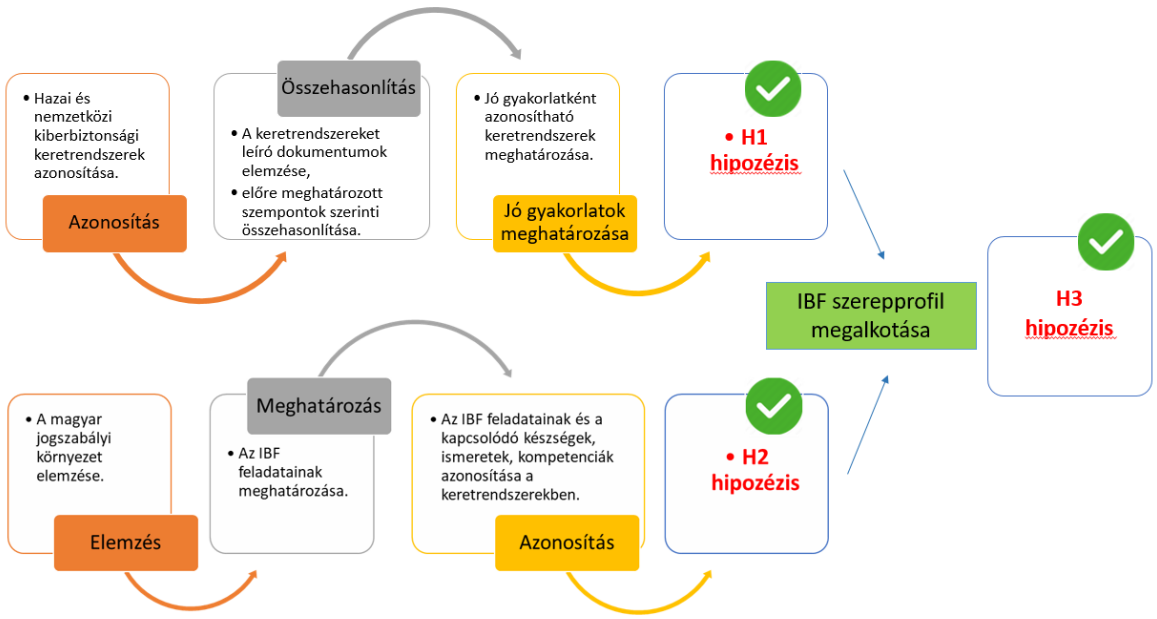
4.1.2. Kutatási módszertan

A bemutatott alhipotézisek megválaszolására a következő lépéseket hajtottam végre, melyeket részleteiben a következő részekben ismertetek.

Az H2-1. hipotézis vizsgálata során elsőként meghatároztam a kiválasztás kritériumrendszerét, melynek segítségével feltérképeztem a kiberbiztonsággal, kibervédelemmel, illetve információbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó hazai és nemzetközi keretrendszereket. Ezt követően dokumentumelemzést hajtottam végre, mely a keretrendszereket leíró dokumentumok elemzésén, illetve előre meghatározott szempontok szerinti összehasonlításán alapult. Az összehasonlítás eredményeként azonosítottam azokat a keretrendszereket, amelyek jó gyakorlatként, kiindulási pontként szolgálhatnak az IBF szerepprofiljának definiálásában, majd meghatároztam a releváns keretrendszerek azon elemeit, amelyek átültethetők a magyar közigazgatási környezetbe.

A H2-2. hipotézis esetén, a magyar jogszabályi környezet elemzését követően megfogalmaztam azon kiberbiztonsági feladatokat, amelyeket az IBF-nek a hatályos jogszabályok alapján ellátnia szükséges, majd e feladatokat és a hozzá kapcsolódó készségeket, ismereteket és kompetenciákat azonosítottam a kiválasztott keretrendszerekben.

A H2-3. hipotézis igazolása érdekében a nemzetközi keretrendszerekben, a H2-2. hipotézis bizonyítása során bemutatott elemek segítségével meghatároztam azokat a magyar közigazgatási környezetben értelmezhető feladatokat és a feladatok ellátásához szükséges ismereteket, készségeket és kompetenciákat, amelyek nélkülözhetetlenek az IBF feladatai ellátásához, végül megalkottam az IBF szerepprofilját, valamint annak tartalmi elemeit.



26. ábra: A kutatási folyamat bemutatása a H2 hipotézis esetében (forrás: saját szerkesztés)

4.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

A hazai jogszabályokban alkalmazott „az elektronikus információs rendszer biztonságáért felelős személy”[146] elnevezés ismeretlen a nemzetközi szakirodalomban, a feladatkörében legközelebb álló kiberbiztonsági munkakörök a CISO (Chief Information Security Officer), illetve a CISM (Certified Information Security Manager). Az általuk ellátandó feladatok közös metszéspontja, az Informatikai Biztonsági Irányítási Rendszer (IBIR), angolul Information Security Management System létrehozása és működtetése.

Az Informatikai Biztonsági Irányítási Rendszer „egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az IBIR magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat. Az IBIR akkor hatékony, ha hasznos a szervezet számára.” (Muha - Krasznay, 2019., 37.). Az IBIR, vagy ahogy szakmai körökben nevezik, az információbiztonsági irányítási rendszer kialakításával és működtetésével kapcsolatos alapvető követelményeket az ISO/IEC 27001:2013 szabvány határozza meg.

Az ISO/IEC:27001 szabványsorozat első elemét ISO/IEC 27001:2005 számon Informatika – Biztonsági technikák – Informatikai biztonsági irányítási rendszer – Követelmények címmel 2005-ben fogadták el. Ezt követően a szabványcsalád részeként számos, az informatikai rendszerek biztonságával foglalkozó szabvány jelent meg. A IBIR az ISO/IEC 27001:2005 szabvány alapvető fogalma, melynek célja, hogy mintát nyújtson a rendszer létrehozásához, megvalósításához, működtetéséhez, felügyeletéhez és felülvizsgálatához.

Az Ibtv. és a végrehajtására szolgáló 41/2015 (VII.15.) BM rendelet alapvetően az ISO/IEC 27001:2013 szabvány által előírt követelményekből indul ki, a jogszabályban meghatározott feladatok operatív végrehajtására pedig bevezeti az elektronikus információs rendszer biztonságáért felelős személy fogalmát.

A Magyarország kiberbiztonságára vonatkozó, 2025-ben hatályba lépő új szabályozás végrehajtását biztosító 7/2024 MK rendelet a védelmi intézkedések alapjaként az Amerikai Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Technológiai és Szabványügyi Testülete által SP 800-53 számon kiadott, az információs rendszerek és

[146] Ibtv. 11.§ (1) c) pont

szervezetek számára kibocsátott, a biztonsági és adatvédelmi kontrollok átfogó katalógusának jelenleg hatályos 5. kiadását (NIST SP 800-53 Rev. 5) veszi alapul.[147]

A nemzetközi szakirodalomban az IBIR bevezetésével és működésével kapcsolatban számtalan publikációt találhatunk, melyek közül csak néhányat, a téma szempontjából releváns írást emelnék ki.

Omar és társai **A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard** című tanulmányukban (Fonseca-Herrera et al., 2021) bemutatják az információbiztonsági irányítási rendszer modelljét az NTC-ISO/IEC 27001:2013 szabványhoz igazodva, amely bármely szervezetre alkalmazható, és lehetővé teszi a szervezetek számára, hogy rendszerszerűen és megfelelő módon hajtsák végre az információs eszközök integritásának, bizalmas jellegének és sértetlenségének megőrzéséhez szükséges ellenőrzéseket, eljárásokat és politikákat.

Oppliger **Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale** című tanulmányában (Oppliger, 2015) útmutatót nyújt az ISO/IEC 27000 biztonsági szabványokról és azok végrehajtásáról, illetve gyakorlati információkkal szolgál a szabványok akkreditációjáról és tanúsításáról is. Az írás külön kitér az információbiztonsági irányítási rendszer tervezésére, a bevezetésre, a rendszerfelügyeletre, a felülvizsgálatra és a frissítésre.

Culot és társai a **The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda** címmel megjelent írásukban (Culot et al., 2021) az ISO/IEC 27001 szabvány tudományos szakirodalmának áttekintését helyezik a vizsgálatuk középpontjába. Emellett felvázolnak egy sor kutatási lehetőséget azzal a céllal, hogy ösztönözzék az információbiztonság és a minőségirányítás metszéspontjába tartozó kérdéseket vizsgáló tanulmányok megszületését.

Ţigănoaia tanulmánya **Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard** címmel (Ţigănoaia, 2015) kiemeli az információbiztonság jelentőségét, mint a szervezti célok elérésének egyik legfontosabb eszközét, mely nagyban hozzájárul a szervezet

[147] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (Letöltve: 2024.11.14.)

hatékonyságához és eredményességéhez. Álláspontja szerint a megfelelő információbiztonságot egy szervezetben kizárólag az információbiztonsági irányítási rendszer bevezetésével és tanúsításával lehet biztosítani, ezért bemutat egy útmutatót arra vonatkozóan, hogy a szervezet -önértékelése segítségével- hogyan tudja megállapítani, hogy hol tart és milyen konkrét lépéseket kell tennie az ISO/IEC 27001:2013 szabvány bevezetése érdekében.

A hazai szakirodalomban, az információbiztonsági irányítási rendszernek az Ibtv. hatálya alá szerveknél történő bevezetését segítő több tanulmány is született, melyek közül csak a téma szempontjából legrelevánsabbakat emelem ki.
Muha Lajos számos írása foglalkozik a témával, melyek közül –összefoglaló jellegük és átfogó megközelítésük okán- kiemelném **Az Informatikai Biztonsági Irányítási Rendszer** című konferenciaközleményt (Muha 2010), mely bemutatja az IBIR fogalmát, a rendszer bevezetésének és működtetésének előnyeit, valamint a PDCA modellen alapuló megvalósítás és fejlesztés lehetőségeit.

Muha Lajos és Krasznay Csaba **Az elektronikus információs rendszerek biztonságának menedzselése** (Muha-Krasznay, 2019), valamint **Az elektronikus információs rendszerek biztonságáról vezetőknek** (Muha - Krasznay, 2014) című könyvükben részletes bemutatják az elektronikus információs rendszer fogalmát ás annak tartalmát, a vonatkozó jogi szabályozást, a kapcsolódó nemzetközi és hazai szabványokat, ajánlásokat, valamint az IBIR bevezetésének és működtetésének legfontosabb elemeit.

Muha Lajos és Szádeczky Tamás **Irányítási rendszerek** című egyetemi jegyzetében (Muha – Szádeczky, 2014) összehasonlításra kerülnek az információbiztonsági irányítási és más irányítási rendszerek, bemutatásra kerül a PDCA elv alkalmazása az IBIR bevezetése és működtetése kapcsán, majd részletesen elemzik a rendszer bevezetéséhez és működéséhez, valamint az ellenőrzéshez és felülvizsgálathoz, továbbfejlesztéshez és karbantartáshoz kapcsolódó egyes feladatok.

Dr. Haig Zsolt **Az információbiztonság szabályozói és szervezeti keretei** című írása (Haig, 2007) áttekinti az információbiztonsággal kapcsolatos hazai és nemzetközi szabványokat és incidenskezelő szervezeteket, valamint a hazai gyakorlatot.

Michelberger Pál **Információ-, folyamat- és vállalatbiztonság** című írásában (Michelberger, 2018) bemutatja az információbiztonsághoz kapcsolódó szabványokat, az IBIR kialakításának egyes lépéseit, az információbiztonság humán oldalát, valamint a vállalati kockázatmenedzsmentet és a folyamatalapú vállalati működést.

Oroszi Eszter **Információbiztonsági stratégia és vezetés** című egyetemi jegyzetében (Oroszi, 2014) bemutatja az információbiztonsági irányítási rendszer célját, kialakítását és egyes elemeit, majd részletesen elemzi a rendszer részét képző információbiztonsági stratégia egyes kérdéseit, kialakítását és megvalósítását, különös tekintettel az információbiztonság szervezeti felépítésére, a szabályzati környezetre, a védelmi intézkedésekre, valamint a visszamérés és ellenőrzés lehetőségeire.

4.3. A HAZAI ÉS A NEMZETKÖZI KIBERBIZTONSÁGI KERETRENDSZEREK AZONOSÍTÁSA ÉS BEMUTATÁSA[148]

Annak érdekében, hogy azonosítani tudjam, hogy egy IBF-nek pontosan milyen feladatokat kell ellátnia és ehhez milyen ismeretekre, készségekre, kompetenciák kialakítására van szükség a mindennapi munkavégzés során, kiindulási pontként dokumentumelemzés segítségével megvizsgáltam és összehasonlítottam a témában már létező keretrendszereket.

A keretrendszerekre vonatkozó kiválasztás kritériumrendszere

Vizsgálatom olyan keretrendszerek felkutatására irányult, amelyek minimum a felsorolt kritériumok egyikének megfelelnek:

- valamely kiberbiztonsági és/vagy közigazgatási szerepkörhöz rendelve, kiberbiztonsággal kapcsolatos feladatokat határoz meg;
- kiberbiztonsággal kapcsolatos ismereteket, tudásterületeket határoz meg;
- kiberbiztonsággal kapcsolatos készségeket határoz meg;
- kiberbiztonsággal kapcsolatos humán képességeket határoz meg;
- kiberbiztonsággal kapcsolatos kompetenciákat határoz meg;

[148] E fejezet Legárd Ildikó: A nemzetközi keretrendszerek összehasonlítása és a jó gyakorlatok azonosítása az IBF szerepprofil definiálása érdekében (Legárd, 2022a) című tanulmány alapján készült.

– a közigazgatási szerepkörök tekintetében feladatokat, ismereteket, készségeket, képességeket, kompetenciákat határoz meg.

A hazai és a nemzetközi kiberbiztonsági keretrendszerek azonosítása

A felsorolt feltételeknek az alábbi hazai és nemzetközi keretrendszerek feleltek meg:

- DigKomp Állampolgári Digitális Kompetencia-keret (A DigComp 2.1. hazai átültetése) - The Digital Competence Framework for Citizens: DigComp 2.2.;
- Közszolgálati digitális kompetencia referenciakeretrendszer;
- National Initiative for Cybersecurity Education (NICE);
- The Cyber Security Body of Knowledge (CyBOK);
- European e-Competence Framework (e-CF);
- ESCO (European Skills, Competences, Qualifications and Occupations);
- European Cybersecurity Taxonomy;
- European Cybersecurity Skills Framework - ECSF (Európai Kiberbiztonsági Készség-keretrendszer);
- CONCORDIA;
- ECHO Cyberskills Framework;
- SPARTA;
- CyberSec4Europe.

A következő alfejezetekben dokumentumelemzés segítségével bemutatom az azonosított keretrendszereket és azok legfontosabb tartalmi elemeit.

4.3.1. DigKomp Állampolgári Digitáliskompetencia-keret - The Digital Competence Framework for Citizens: DigComp 2.2.[149]

Az Európai Unió 2006-ban az egész életen át tartó tanuláshoz szükséges kulcskompetenciákról szóló ajánlásával (2006/962/EK) a digitális kompetenciát elismerte, mint az egész életen át tartó tanuláshoz szükséges nyolc kulcskompetencia egyikét: „A

[149] DigKomp Állampolgári Digitáliskompetencia-keret - The Digital Competence Framework for Citizens: DigComp 2.2. https://dpmk.hu/2019/07/25/a-digitalis-kompetencia-unios-referenciakerete-magyarul/ (Letöltve: 2022.10.11.) https://joint-research-centre.ec.europa.eu/digcomp_hu (Letöltve: 2022.04.20.)

digitális kompetencia magában foglalja az információs társadalmi technológiák (IST) magabiztos és kritikus használatát a munka, a szabadidő és a kommunikáció terén. Ez az IKT terén meglévő alapvető készségeken alapul: számítógép használata információ visszakeresése, értékelése, tárolása, előállítása, bemutatása és cseréje céljából, valamint a kommunikáció és az együttműködő hálózatokban való részvétel céljából az interneten keresztül."[150]

A DigComp (Carretero, S. et all, 2017) az Európai Bizottság tudományos és ismeretterjesztő szolgálata, a Közös Kutatóközpont (JRC) által indított projekt, mely 2013-ban jelent meg „The Digital Competence Framework for Citizens", azaz az „Állampolgári digitáliskompetencia-keret" címmel. A JRC 2016-ban készítette el a DigComp 2.0-t, amelyben a terminológia és a fogalmi modell frissítésre került, illetve a keretrendszer európai, nemzeti és regionális megvalósulását példákon keresztül mutatták be. A DigComp 2.1 verzió a korábbi három helyett nyolc jártassági szintet alkalmaz gyakorlati példákkal kiegészítve. A 2022. március 22-től elérhető DigComp 2.2 már több mint 250 új példát kínál a tudásra, készségekre és attitűdökre, amelyek segítik a polgárokat abban, hogy magabiztosan, kritikusan és biztonságosan kapcsolódjanak be a digitális világba.

A digitális kompetencia keretrendszer 5 területen azonosítja a digitális kompetencia kulcsfontosságú összetevőit:

1. Információs és adatműveltség,
2. Kommunikáció és együttműködés,
3. Digitális tartalom létrehozása,
4. **Biztonság,**
5. Problémamegoldás.

[150] Az Európai Parlament és a Tanács ajánlása (2006. december 18.) az egész életen át tartó tanuláshoz szükséges kulcskompetenciákról

DigComp 2.0 (megjelenés éve: 2016)		DigComp 2.1 (megjelenés éve: 2017)	
Kompetenciaterületek (1. dimenzió)	Kompetenciák (2. dimenzió)	Jártassági szintek (3. dimenzió)	Gyakorlati példák (5. dimenzió)
1. Információ- és adatmenedzsment	1.1 Adatok, információk és digitális tartalmak böngészése, keresése és szűrése 1.2 Adatok, információk és digitális tartalmak értékelése 1.3 Adatok, információk és digitális tartalmak kezelése	Nyolc jártassági szint mind a 21 kompetenciához	Gyakorlati példák a nyolc jártassági szinthez tanulási és foglalkoztatási környezetben a 21 kompetencia terén
2. Kommunikáció és együttműködés	2.1 Interakció digitális technológiákon keresztül 2.2 Megosztás digitális technológiák segítségével 2.3 Állampolgári részvétel digitális technológiák segítségével 2.4 Együttműködés digitális technológiák segítségével 2.5 A hálózati kommunikáció általános illemszabályai (Netikett) 2.6 A digitális személyazonosság kezelése		
3. Digitális tartalmak	3.1 Digitális tartalmak létrehozása 3.2 Digitális tartalmak szerkesztése 3.3 Szerzői jog és engedélyek 3.4 Programozás		
4. Biztonság	4.1 Eszközök védelme 4.2 A személyes adatok és a magánélet védelme 4.3 Az egészség és a jóllét védelme 4.4 Környezetvédelem		
5. Problémamegoldás	5.1 Technikai problémák megoldása 5.2 Igények és technológiai válaszok megfogalmazása 5.3 Digitális technológiák kreatív alkalmazása 5.4 Digitális kompetencia hiányosságok felismerése		

27. ábra: DigComp 2.0 és 2.1 kulcsfontosságú összetevői (Forrás: https://dpmk.hu/wp-content/uploads/2019/07/DigComp2.1_forditas_6_20200130.pdf (Letöltve: 2022.04.26.))

Az értekezés témája szempontjából a „Biztonság” kompetenciaterülete az egyetlen releváns terület, így a következőkben a „Biztonság”-hoz tartozó kompetenciákat mutatom be részleteiben.

Biztonság kompetenciaterület meghatározása: Az eszközök, a tartalom, a személyes adatok és a magánélet védelme digitális környezetben. A testi és lelki egészség védelme, valamint a társadalmi jólétet és társadalmi befogadást szolgáló digitális technológiák ismerete. A digitális technológiák és használatuk környezeti hatásainak ismerete.

A Biztonság egyes területei:

1. **Eszközök védelme**

Képes az eszközök és a digitális tartalom védelmére, valamint a digitális környezetben jelentkező kockázatok és veszélyek megértésére. Ismeri a biztonsági intézkedéseket, és kellően figyelembe veszi a megbízhatóságot és a magánélet védelmét.

2. A személyes adatok és a magánélet védelme

Képes a személyes adatok és a magánélet védelmére digitális környezetben. Megérti a személyazonosításra alkalmas információk felhasználásával és megosztásával kapcsolatos ismereteket, képes megvédeni saját magát és másokat az esetleges károktól. Megérti, hogy a digitális szolgáltatások „Adatvédelmi szabályzatban" határozzák meg a személyes adatok felhasználásának módját.

3. Az egészség és a jólét védelme

Képes elkerülni az egészségügyi kockázatokat, valamint a testi és lelki jólétet fenyegető veszélyeket a digitális technológiák használata során. Képes megvédeni magát és másokat a digitális környezetben előforduló lehetséges veszélyektől (pl. cyber bullying). Ismeri a digitális technológiákat és azok alkalmazását a társadalmi jólét és a társadalmi befogadás érdekében.

4. A környezet védelme

Tisztában van a digitális technológiák és használatuk környezeti hatásával.

Hazánkban a 1341/2019. (VI. 11.) Korm. határozat döntött a Digitális Kompetencia Keretrendszer fejlesztéséről és bevezetésének lépéseiről, melynek „célja, hogy a digitális felkészültség és kompetenciák hiánya miatt Magyarországon senki ne szoruljon ki a digitális világból és a digitális gazdaságból, továbbá folyamatosan bővüljön a digitálisan felkészült munkavállalók köre".[151] Alapját adja a DigComp digitáliskompetencia-keret, így a digitális kompetenciák öt fő fejlesztési területét határozza meg: 1. Információ és adatmenedzsment, 2. Kommunikáció és együttműködés, 3. Digitális tartalmak létrehozása, 4. Biztonság, 5. Problémamegoldás. A jelenlegi változat 5 területen, 21 kompetenciaelemet definiál 8 jártassági szinten. A „állampolgári digitáliskompetencia-keret" célja a polgárok digitális kompetenciájának fejlesztése, mely két részre tagolódik: az állampolgári alap szintre, mely az önálló eszközhasználatig viszi a felhasználót, valamint az állampolgár plusz szintre, mely összetettebb, több területre kiterjedő kompetenciákat sorol fel, melyet meghatározott digitális szolgáltatások igénybevételéhez nyújtanak. (Molnár - Sasvári – Tarpai, 2017)

[151] 1341/2019. (VI. 11.) Korm. határozat a Digitális Kompetencia Keretrendszer fejlesztéséről és bevezetésének lépéseiről

Részkövetkeztetések:

A Digitális Kompetencia Keretrendszer általánosságban az állampolgárok szintjén határozza meg és mutatja be a szükséges kompetenciákat, nem tartalmaz közszolgálat-specifikus elemeket, továbbá nem azonosítja a kompetenciák alapjaként szolgáló ismereteket, valamint készségeket, képességeket, így az IBF szerepprofilja meghatározása szempontból nem tekinthető releváns keretrendszernek.

4.3.2. Közszolgálati Digitális Kompetencia Referenciakeret (munkaanyag)[152]

A Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló 1456/2017. (VII. 19.) Korm. határozat[153] értelmében, a közigazgatásban dolgozók digitális kompetenciáinak fejlesztése érdekében, a Belügyminisztérium és a Nemzeti Közszolgálati Egyetem együttműködésében kidolgozásra került a közszolgálati digitális kompetencia referenciakeretről (továbbiakban: Referenciakeret) szóló munkaanyag.

A kompetenciarendszer 3 nagy elemből áll: az alapkompetenciákból, a szakmai, szervezeti, valamint a digitális kompetenciákból. A **digitális kompetenciák** meghatározása a DigKomp 2.1.-ben meghatározott kompetenciákat veszi alapul, azokat tovább fejlesztve, illetve a közigazgatásra specializálva jelennek meg a Referenciarendszerben. A DigComp 2.1.-hez képest lényeges különbség, hogy míg az előbbi nyolc jártassági szintet határoz meg, a Referenciakeret –a hat szintű nyelvi keretrendszerhez igazítva- hat szintet különít el kezdő, kísérletező, gyakorlott, szakértő, szaktekintély, valamint újító kategóriákkal.

[152] A Közszolgálati Digitális Kompetencia Referenciakeret (összefoglaló dokumentum), munkaanyag; Szerző: Közszolgálati Referenciakeret Előkészítő Munkacsoport

[153] 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

A referenciakeret **7 fő digitális kompetenciát és 19 digitális alkompetenciát** határoz meg, mindezt **6 jártassági szinten** definiálva, **gyakorlati példákkal** szemléltetve a közigazgatás és a rendészet területéről:

Digitális Kompetencia	Digitális Alkompetenciák
1. Információ és adatmenedzsment	1.1 Adatok, információk és digitális tartalmak böngészése, keresése és szűrése
	1.2 Adatok, információk és digitális tartalmak kiértékelése
	1.3 Adatok, információk és digitális tartalmak kezelése
2. Digitális tartalmak kezelése	2.1 Digitális tartalmak létrehozása
	2.2 Digitális tartalmak szerkesztése
	2.3 Szerzői jog és engedélyek
3. Digitális kommunikáció	3.1. Digitális technológiával támogatott interakció (kommunikáció, digitális platformon való tartalom- és információ megosztás)
	3.2 A hálózati kommunikáció általános illemszabályainak (Netikett) ismerete, alkalmazása
4. Digitális együttműködés	4.1 Digitális inklúzió kezelése az ügyfél digitális felzárkóztatása az ügyintézésben
	4.2 Együttműködés digitális platformokon
5. Biztonság, védelem, felelősség	5.1 A digitális eszközök védelme
	5.2 Adatvédelem
	5.3 Információszabadság biztosítása
	5.4 A rendelkezésre álló adatvagyon felelős hasznosítása
6. Digitális problémák megoldása	6.1 Alapvető felhasználói problémák kezelése
	6.2 Igények megfogalmazása
	6.3 Digitális technológiák kreatív alkalmazása
7. Digitális önismeret, önfejlesztés	7.1 Digitális kompetencia erősségek és hiányosságok felismerése és fejlesztése
	7.2 A hatósági és magán digitális identitás szétválasztása

28. ábra: A Közszolgálati Digitális Kompetencia Referenciakeret (Forrás: A közszolgálati digitális kompetencia referenciakeret (összefoglaló dokumentum), munkaanyag; Szerző: Közszolgálati Referenciakeret Előkészítő Munkacsoport)

A Referenciakeret a téma szempontjából releváns „Biztonság, védelem, felelősség” kompetenciát és alkompetenciáit az alábbiak szerint határozza meg:

5. „Biztonság, védelem, felelősség”: A kompetencia megmutatja, hogy a közszolgálatban dolgozó milyen szinten képes megvédeni az általa használt elektronikus eszközöket, programokat. Milyen módon tudja megelőzni, hogy a rajtuk tárolt adatokhoz és tartalmakhoz illetéktelenek ne férjenek hozzá. Megvédi saját és mások személyes adatait a digitális közszolgáltatások használata, a közfeladat ellátása során. Felelősen szét tudja választani a hivatali és a magánszféráját érintő adatokat és információkat. Meg tudja ítélni, hogy a közfeladat ellátása során keletkezett mely információk oszthatók meg az azokra

jogosultakkal és az adatok igénylőivel. Tisztában van azzal, hogy a munkája során kezelt, tárolt adatokat csak célhoz kötötten, a feladat ellátásával összefüggésben használhatja fel és hasznosíthatja.

Alkompetenciák:

5.1 A digitális eszközök védelme

Fizikailag és digitális módszerekkel megvédi a feladatai ellátásához használt digitális eszközöket és tartalmakat. Felismeri a digitális környezetre jellemző kockázatokat és veszélyeket. Az általa ismert digitális biztonsági megoldásokat a veszélyek elkerülésére és elhárítására az adott veszélyhelyzethez legjobban illeszkedő módon alkalmazza és használja.

5.2 Adatvédelem

A hatályos szabályozás előírásainak és a szervezet adatvédelmi szabályzatának megfelelően óvja a hivatali, valamint az ügyfelek (állampolgárok) személyes adatait digitális környezetben is. Az általa ismert és használt eszközökkel gondoskodik arról, hogy a védett személyes adatok, valamint hivatali adatok ne kerüljenek illetéktelen személyek, szervezetek kezébe.

5.3 Információszabadság biztosítása

A hatályos jogi szabályozásnak megfelelő tartalommal biztosítja a közérdekű és közérdeklődésre számot tartó adatok és információk elérhetőségét digitális környezetben is. Gondoskodik az ilyen adatok digitális közzétételéről a megfelelő platformokon.

5.4 A rendelkezésre álló adatvagyon felelős hasznosítása

Feladatainak ellátása során célhoz kötötten gyűjti, kezeli, hasznosítja a rendelkezésre álló adatokat digitális környezetben is. Különbséget tud tenni a hivatalos és személyes adatok és tartalmak között és ezeket elkülönítetten használja. Tudatában van, hogy a hivatalos adatvagyon személyes célokra nem használható fel.

Részkövetkeztetések:

Az előzőekben részletesen ismertetett Referenciakeret szervesen illeszkedik a közszolgálatban már létező egyéb kompetenciarendszerekhez, és megfelelő alapul szolgálhat a digitális kompetenciák fejlesztésére irányuló képzéseknek, illetve módszertani

és tananyagfejlesztéseknek, ugyanakkor mindezt csupán az átlagfelhasználó szintjén igaz, a kiberbiztonsággal foglalkozó szakemberek, így az IBF számára nem nyújt megfelelő ismeretanyagot a szükséges kompetenciák tekintetében.

4.3.3. National Initiative for Cybersecurity Education (NICE)[154]

Az amerikai National Institute of Standards and Technology (NIST) 2013-ban adta ki a National Initiative for Cybersecurity Education (NICE) elnevezésű keretrendszert, melynek célja, hogy azonosítsa a kiberbiztonsághoz kapcsolódó munkaköröket, illetve részletesen meghatározza a kiberbiztonsági munkakörök tartalmát és e munkakörök betöltéséhez szükséges, elsajátítandó ismeretköröket, készségeket és képességeket. A keretrendszer egyes részei mintegy építőelemként szolgálnak az egyének és csapatok által végzett kiberbiztonsági munka elvégzéséhez szükséges feladatok, ismeretek és készségek leírásához. A NICE-keretrendszert a köz-, a magán- és az akadémiai szektorban is alkalmazható.

A kiberbiztonsággal kapcsolatos munkaköröket 7 kategóriába (Category), 33 szakterületbe (Speciality Area) sorolja, és 52 munkakört (Work Role) határoz meg részletes munkaköri leírással. Mindehhez „szuperkészletként" nyújtja az egyes munkakörökhöz kapcsolódó kiberbiztonsági ismereteket (Knowledge), készségeket (Skill), képességeket (Ability) és a feladatok (Tasks) összefoglalóját.

A NICE Framework fő építő kövei:

- Feladatok (Tasks) - olyan tevékenység, amely a szervezeti célok elérésére irányul;
- Tudás (Konwledge)– a memórián belüli visszakereshető fogalmak halmaza;
- Készségek (Skill, Ability) – képesség egy megfigyelhető cselekvés végrehajtására.

A keretrendszer egyes építőelemei egymáshoz való viszonyát a 33. ábra mutatja be, ahol a „T" – Feladatok (Tasks), „K" - Tudás (Knowledge) és „S" – Készségek (Skill).

[154] National Initiative for Cybersecurity Education (NICE) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (Letöltve: 2022.03.10.)

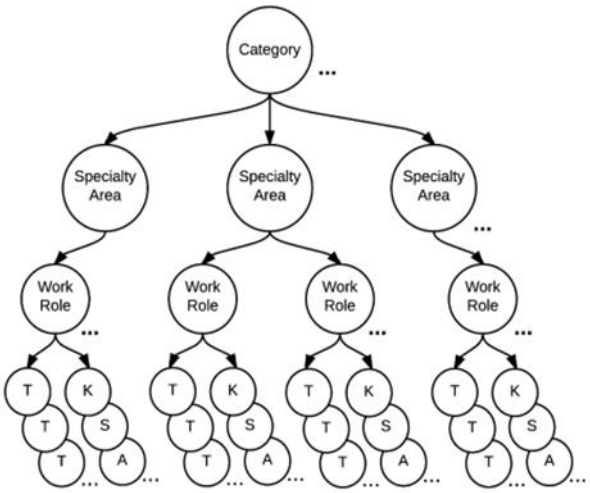


Figure 1 - Relationships among NICE Framework Components

29. ábra: Kapcsolat a NICE Keretrendszer építőelemei között (Forrás: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf Letöltve: 2022.04.26.)

A keretrendszer alapvetően a következő szereplőknek nyújt segítséget:

- a munkaadóknak, hogy segítsenek felmérni és leírni a kiberbiztonsági munkaerőt (a nem technikai személyzet, pl. humánerőforrás-menedzsment feladatokat ellátó munkatárs számára nyújt kiindulási alapot a betöltendő kiberbiztonsági pozíció leírásához);
- a jelenlegi és jövőbeli kiberbiztonsági dolgozóknak abban, hogy felfedezzék a feladatokat és a munkaszerepeket, illetve megértsék, hogy a munkáltatók milyen tudást és készségeket várnak el az egyes kiberbiztonsági pozíciók esetében;
- képzési és tanúsítási szolgáltatóknak abban, hogy segíteni tudják a jövőbeni kiberbiztonsági munkaerőt a megfelelő tudás és készségek megszerzésében;
- oktatási szolgáltatóknak, akik a NICE-keretrendszert referenciaként használják a tananyag, a tanfolyamok, a szemináriumok és a kutatások kidolgozásához.

A Keretrendszerben meghatározott „szuperkészlet” segítséget nyújthat annak meghatározásában is, hogy milyen ismeretanyagra, készségekre és képességekre van szüksége egy IBF-nek. A felsorolt elemek meghatározása érdekében a NICE keretrendszeren belül azonosítani szükséges azt a kiberbiztonsági munkakört, amely a legközelebb áll az IBF feladatköréhez. Mivel az IBF Ibtv.-ben megfogalmazott egyik legfontosabb és legátfogóbb feladata a szervezeten belüli információbiztonsági irányítási rendszer kialakításához és fenntartásához kapcsolódik, így az IBF szerepekörének

leginkább a NICE által meghatározott „Information Systems Security Manager” (Információs Rendszerek Biztonsági Vezetője) munkaköre feleltethető meg. E munkakört a keretrendszer a „Felügyelet és kormányzás” (Oversee and Govern) kategóriában, a „Kiberbiztonsági Management” (Cybersecurity Management) szakterületen belül helyezi el.

Részkövetkeztetések:

A NICE segítségével meghatározhatók azok a kiberbiztonsági feladatok (Tasks), amelyeket az IBF-nek a munkája során ellátni szükséges, a keretrendszer segítségével a feladatellátáshoz szükséges ismeretek (Knowledge), készségek (Skills), illetve képességek (Abilities) is azonosíthatók. Az átültetés nehézséget az képzi, hogy a felsorolt kiberbiztonsági szerepkörök, illetve az azokhoz kapcsolható elemek nem mindig igazodnak az EU igényeihez, jogszabályaihoz és éppen ezért nehezen összeegyeztethetők az európai egyéb keretrendszerekkel.

4.3.4. The Cyber Security Body of Knowledge (CyBOK)[155]

Az Egyesült Királyság nemzeti kiberbiztonsági készségekre vonatkozó stratégiája[156] elismeri a kiberbiztonsági készségek piaci hiányát és annak folyamatos növekedését. E probléma kezelése érdekében az Egyesült Királyság kormánya célul tűzte ki egy olyan kiberbiztonsági tudásanyag létrehozását, amely meghatározza a kiberbiztonság területét. A Cyber Security Body of Knowledge (CyBOK) v1.0 2019 októberében jelent meg. 19 tudásterület (KA) sorol fel, amelyek öt magas szintű kategóriára oszthatók.

Magas szintű területek és tudásterületeik[157]:

1. Humán, szervezeti és szabályozási szempontok:
   - Kockázatkezelés és irányítás
   - Jogszabályok és szabályozás
   - Humán faktor
   - Adatvédelem és online jogok

[155] The Cyber Security Body of Knowledge (CyBOK) https://www.cybok.org/ (Letöltve: 2022.03.10.)
[156] National Cyber Security Skills Strategy https://www.gov.uk/government/publications/cyber-security-skills-strategy (Letöltve: 2022.04.10.)
[157] https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf (Letöltve: 2022.03.10.)

2. Támadások és védekezés:
   - Malware és támadási technológiák
   - Ellenséges magatartás
   - Biztonsági műveletek & Incidenskezelés
   - Csalásfelderítés
3. Rendszerbiztonság:
   - Kriptográfia
   - Operációs rendszerek & virtualizáció biztonság
   - Elosztott rendszerek biztonsága
   - A biztonság formális módszerei
   - Hitelesítés, engedélyezés & elszámoltathatóság
4. Szoftver- és platformbiztonság:
   - Software biztonság
   - Web és mobil biztonság
   - Biztonságos szoftver életciklus
5. Az infrastruktúra biztonsága:
   - Alkalmazott kriptográfia
   - Hálózatbiztonság
   - Hardware biztonság
   - Kiber-fizikai rendszerek biztonsága
   - Fizikai réteg & távközlés biztonság

Részkövetkeztetések:

Noha a CyBOK előre mozdítja a kiberbiztonság tudásterületeinek tisztázását, azonban nem foglalkozik közvetlenül a szerepek és tudáskategóriák összefüggéseivel.

4.3.5. European e-Competence Framework (e-CF)[158]

Az Európai Szabványügyi Bizottság (CEN) által közzétett European e-Competence Framework, azaz az Európai e-Kompetencia Keretrendszer (e-CF) egy nemzetközi ágazati keretrendszer, amely az informatikai szakemberek besorolására szolgál a különböző

[158] European e-Competence Framework (e-CF) https://itprofessionalism.org/ (Letöltve: 2022.03.25.)

szektorokban/iparágakban. Az e-CF 3.0 verziója az Európai Unió "e-készségek a 21. századra" című stratégiájának részét képzi. Az e-CF új verziója 2019-ben jelent meg, tükrözve a keretrendszer jelentőségét a versenyképesség, az átláthatóság és az európai IT-készségek konvergenciája szempontjából a globális digitális környezetben.

A keretrendszer a kompetenciák, készségek, ismeretek és jártassági szintek közös nyelvét alakította ki, melyet Európa-szerte alkalmaznak. Az e-CF által meghatározott négy dimenzió: 5 kompetenciaterület, 41 széles körben elismert infokommunikációs kompetencia, 5 CF jártassági szint, ismeretek és készségek példái.

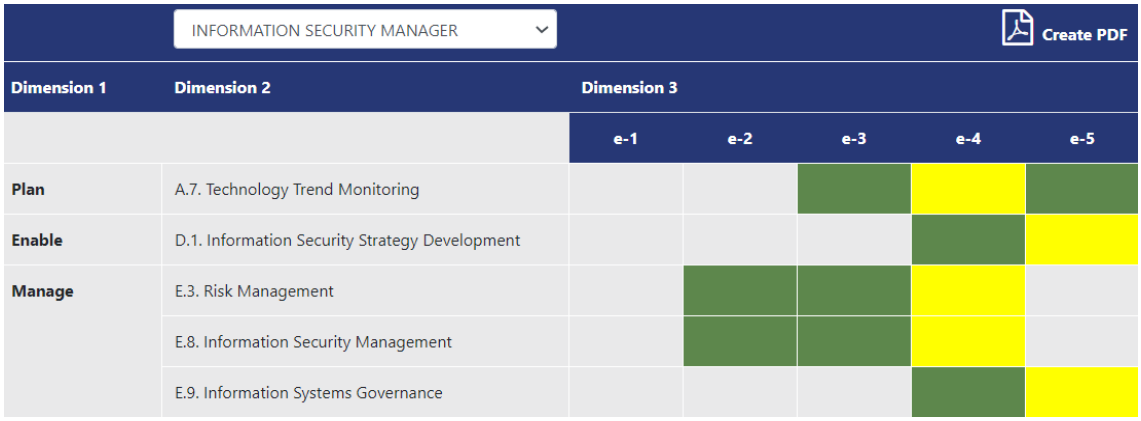
Az Európai e-Kompetencia Keretrendszer elősegíti az IKT-hoz kapcsolódó kompetenciáknak az Európai Képesítési Keretrendszernek (EKKR; European Qualification Framework) megfelelő beazonosítását és meghatározását, továbbá röviden ismerteti az EKKR kidolgozása mögött álló módszertani szempontokat is.

Az e-CF dimenziói:

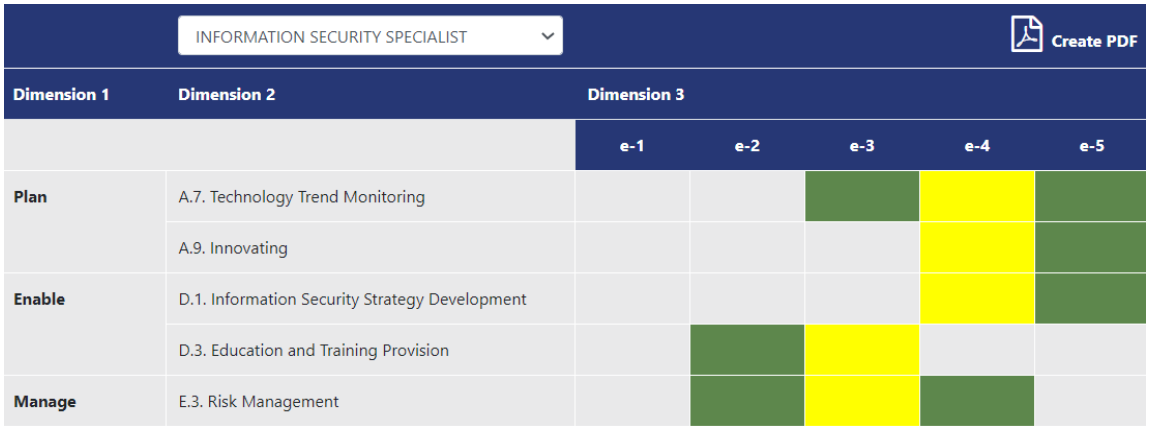
1. dimenzió - 5 e-kompetencia terület: Az IT makró folyamatokból származó: Tervezés (Plan)–Építés (Build) –Futtatás (Run)– Engedélyezés (Enable) – Kezelés (Manage). E kompetencia területek belépési pontot biztosítanak az e-kompetenciákhoz.
2. dimenzió - 41 e-kompetencia: Összesen 41 e-kompetencia biztosítja az informatikai szakmai kompetenciák európai szabványos referenciáit az informatikai munkakörökben megkövetelt szakmai kompetenciák tekintetében. Az egyes kompetenciákat szervezeti szempontból határozzák meg és írják le.
3. dimenzió - 5 e-CF jártassági szint (5 e-kompetencia készségszint): A jártassági szint növekedésével párhuzamosan a kompetencia komplexitása, a feladatellátás autonómiája és a befolyásolási képesség növekvő szintjei jellemzők. Minden egyes e-kompetenciához meghatározott, releváns készségszint van hozzárendelve. Ugyanakkor a 3. dimenzió szintleírásai a kompetencia fejlesztésének egyéni perspektíváit is megadják.
4. dimenzió - ismeretek és készségek példái: Az ismeretekre és készségekre vonatkozó példák a 2. dimenzióban szereplő 41 e-kompetencia általános leírásához kapcsolódnak. Ezek a példák nem tekinthetők kimerítő jellegűnek, pusztán inspirációt és iránymutatást nyújtanak a további konkrét ismeretek és készségek meghatározásához az adott igényeknek megfelelően.

A keretrendszer 30 IKT szakmai szerepprofilon keresztül fedi fel az e-CF működését, és mutatja be, hogy ez az interaktív eszköz hogyan szolgál a kompetenciák azonosításának alapjaként. A bemutatott szerepprofilok bármely szervezetben betöltött tipikus szerepek, amelyek lefedik a teljes IKT üzleti folyamatot.

Az e-CF kizárólag két kiberbiztonsághoz kapcsolódó szerepkört azonosít, az „Information Security Manager" és az „Information Security Specialist" szerepeket, és ezekhez határozza meg az egyes IKT kompetenciákat és a hozzájuk tartozó releváns jártassági szinteket.



30. ábra: Az e-CF által meghatározott „Information Security Manager" szerepkörhöz kapcsoló kompetenciák és jártassági szintek (Forrás: https://itprofessionalism.org/ Letöltve: 2022.04.26.)



31. ábra: Az e-CF által meghatározott „Information Security Manager" szerepkörhöz kapcsoló kompetenciák és jártassági szintek (Forrás: https://itprofessionalism.org/ Letöltve: 2022.04.26.)

Az Information Security Manager és az Information Security Specialist esetében három közös e-kompetencia kerül megjelölésre: a technológiai trendek nyomon követése (A.7.), az információbiztonsági stratégia kidolgozása (D.1.), valamint a kockázatkezelés (E.3.). Eltérő kompetenciaként jelenik meg az Information Security Managernél az

információbiztonsági irányítás (E.8.) és az információs rendszerek irányítása (E.9.). Az Information Security Specialist két speciális e-kompetenciája az innováció (A.9.) és az oktatás és képzés biztosítása (D.3.).

Részkövetkeztetések:

Az e-CF 3.0-s verziója egy magasan absztrakt szintű készségmátrixot tartalmaz, amelyben a kiberbiztonság csak az egyik összetevő. Ugyanakkor az IBF feladatköréhez legközelebb álló két bemutatott kiberbiztonsági szerepkörhöz kapcsolható kompetenciát a releváns jártassági szinten nagyon jól azonosítja, ezért a keretrendszer kiindulási alapként szolgálhat az IBF szerepprofilja tekintetében, a szükséges kompetenciák meghatározásában.

4.3.6. ESCO (European Skills, Competences, Qualifications and Occupations)[159]

Az ESCO az Európa 2020 stratégia egyik kezdeményezése, az Európai Bizottság projektje, amelyet a Foglalkoztatás, Szociális Ügyek és Társadalmi Befogadás Főigazgatóság (DG EMPL) irányít.

Az ESCO 2942 foglalkozás és 13 485, e foglalkozásokhoz kapcsolódó készség leírását, illetve 500 transzverzális készség és kompetencia meghatározását tartalmazza, 27 nyelvre (az EU összes hivatalos nyelvére, valamint izlandi, norvég és arab nyelvre) lefordítva.

Az ESCO célja, hogy támogassa a munkahelyi mobilitást, valamint az integráltabb és hatékonyabb munkaerőpiacot Európa-szerte azáltal, hogy a foglalkozások és készségek tekintetében "közös nyelvet" kínál, amelyet a különböző érdekelt felek használhatnak a foglalkoztatási, oktatási és képzési témákban egyaránt.

Az ESCO összekapcsolja a foglalkoztatást az oktatással: segít az oktatási és képzési szolgáltatóknak abban, hogy megértsék, milyen készségekre van szükségük a munkaerőpiacoknak. Ezután tanterveiket ennek megfelelően tudják módosítani, annak érdekében, hogy jobban felkészítsék diákjaikat a jövőbeni munkaerőpiacokra. Az ESCO abban is segít a potenciális munkaadóknak, hogy jobban megértsék, mit tanultak a diákok.

Az ESCO osztályozás olyan modulokból áll, mint a foglalkozások hierarchiája a nemzetközi szabványos osztályozás (International Standard Classification of Occupations -

[159] ESCO (European Skills, Competences, Qualifications and Occupations) https://ec.europa.eu/esco/portal/howtouse/21da6a9a-02d1-4533-8057-dea0a824a17a (Letöltve: 2022.04.22.)

ISCO) alapján, ismeretek, készségek, kompetenciák, valamint képesítések. A modulok egyes elemei kombinálva és egymáshoz kapcsolódva alkotják a teljes osztályozást.

Rendelkezésre álló adatkészletek:

A) Foglalkozások:

0. Fegyveres erők
1. Vezetők
2. Felsőfokú képzettséget igénylő foglalkozások
3. Technikusok és hasonló foglalkozások
4. Irodai foglalkozások
5. Szolgáltatási és értékesítési foglalkozások
6. Szakképesített mezőgazdasági és halászati foglalkozások
7. Szakképzettséget igénylő ipari foglalkozások
8. Gépkezelők, összeszerelők és járművezetők
9. Egyszerű foglalkozások

B) Készségek/ Kompetenciák:

- Tudás (K)
- Nyelvi készségek és ismeretek (L)
- Készségek (S)
- Transzverzális készségek és kompetenciák (T)

C) Képesítések:

- AZ ESCO támogatja az egyes képesítések által igazolt tanulási eredmények leírását és megértését.
- Az ESCO használatával tovább fejleszthetők a személyre szabott/digitális pályaorientációs szolgáltatások.
- Az ESCO támogatja a nem formális és informális tanulás eredményeinek érvényesítését.

Az ESCO azonban csupán két foglalkozáshoz kapcsolva jelenít meg kiberbiztonsághoz kapcsolódó készségeket, illetve kompetenciákat, ugyanakkor a tudás tekintetében nem határoz meg kiberspecifikus ismereteket.

FOGLALKOZÁSOK	TUDÁS
Információs és kommunikációs technológiai foglalkozások: – Adatbázis- és hálózati foglalkozások (252) – Szoftver- és alkalmazásfejlesztők, -elemzők (251)	Információs és kommunikációs technológiák (IKT): Az információs és kommunikációs technológiákat (IKT) érintő interdiszciplináris programok és képesítések
KÉSZSÉGEK	**KOMPETENCIÁK**
Számítógéppel végez munkát - Számítógépes rendszereket hoz létre és véd: – **S 5.2.0. számítógépes rendszereket hoz létre és véd** – **S 5.2.2. gondoskodik az IKT eszközök védelméről**	Transzverzális készségek és kompetenciák -> alapkészségek és –kompetenciák -> munkavégzés digitális eszközökkel és alkalmazásokkal -> **digitális biztonsági intézkedéseket alkalmaz (kéretlen elektronikus hirdetések elleni védelmet telepít, ügyel az internetes adatvédelemre, tűzfalat telepít és frissít)**

11. táblázat: Az ESCO-ban azonosított kiberbiztonság kapcsolódású elemek (forrás: saját szerkesztés)

Részkövetkeztetések:

Az ESCO keretrendszerét áttekintve megállapítható, hogy bár széleskörűen, az ISCO nemzetközi szabványa szerint határozza meg a foglalkozásokat és a hozzá kapcsolódó tudást, készségeket és kompetenciákat, azonban az IBF tekintetében egyáltalán nem azonosítható a betöltött szerepkör, illetve feladatkör, így a kapcsolódó ismeretek, készségek és kompetenciák meghatározására sem kerülhet sor.

4.3.7. European Cybersecurity Taxonomy[160]

A Bizottság 2018-ban elfogadott közleményében kötelezettséget vállalt arra, hogy a Horizont 2020 keretprogram keretében kísérleti kutatást indít annak érdekében, hogy segítse a nemzeti kiberbiztonsági központok hálózatba tömörítését. Ezzel a céllal összhangban a Bizottság Közös Kutatóközpontja (JRC) 2019-ben különböző nemzetközi szabványok alapján egy kutatási kiberbiztonsági osztályozási rendszert dolgozott ki és javaslatként fogalmazott meg azzal a céllal, hogy a kutatási egységek (nemzeti kiberbiztonsági központok) Európa-szerte referencia indexként használhassák az általuk javasolt keretrendszert. A közösen használt terminológia javítja a helyzetfelismerést és a koordinációt, valamint segít annak pontos megállapításában, hogy mi jelent veszélyt és kockázatot.

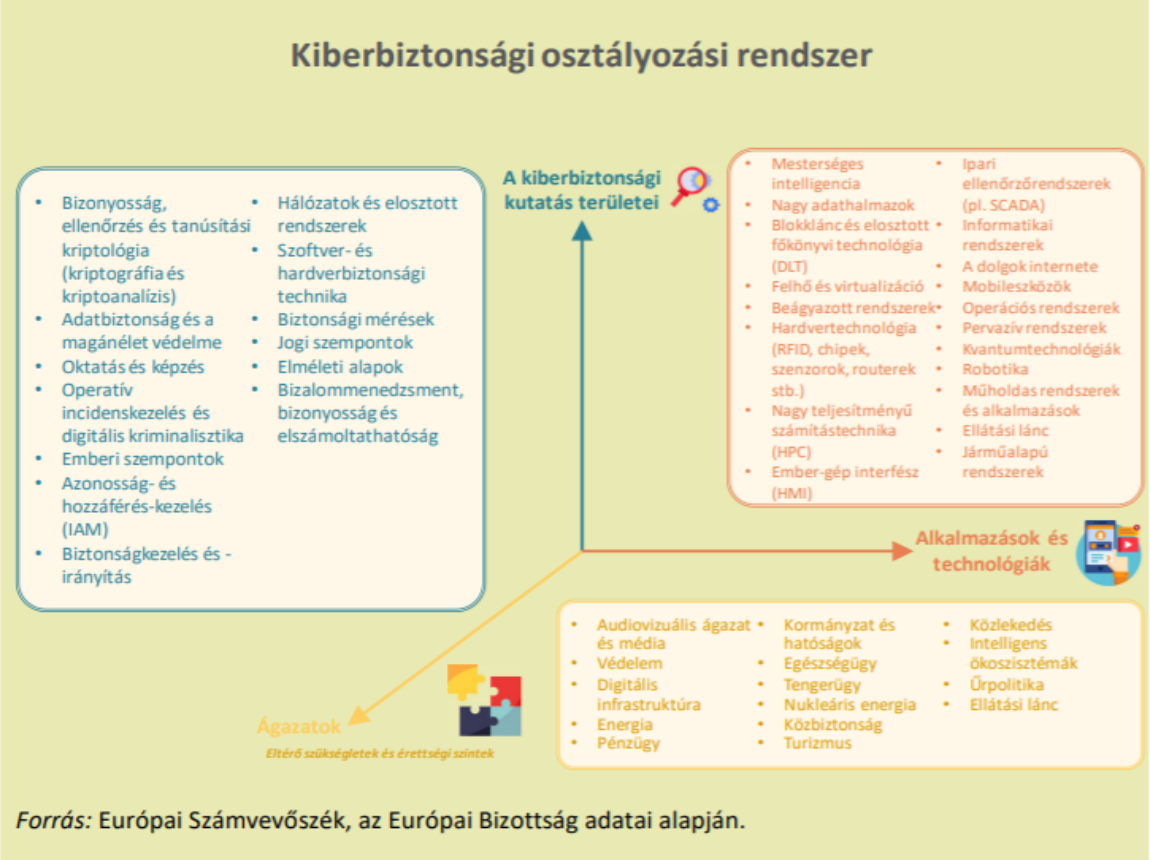
[160] European Cybersecurity Taxonomy https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy (Letöltve: 2022.04.21.)

A JRC javaslata háromdimenziós taxonómiából áll, és e dimenziókon alapuló kiberbiztonsági területeken alapul:

- a kiberbiztonság kutatási területei (pl. adatbiztonság és a magánélet védelme, oktatás és képzés, humán szempontok, operatív incidenskezelés, jogi szempontok),
- ágazatok (pl. digitális infrastruktúra, energia, pénzügy, kormányzat és hatóságok) és
- alkalmazások és technológiák (pl. MI, felhő és virtualizáció, informatikai rendszerek, mobileszközök).

A dokumentumban javasolt taxonómia a rendelkezésre álló európai kiberbiztonsági kompetenciák feltérképezésének támogatását is szolgálja.

A Kiberbiztonsági osztályozási rendszer elemei az Európai Számvevőszék, az Európai Bizottság adatai alapján:



Forrás: Európai Számvevőszék, az Európai Bizottság adatai alapján.

32. ábra: Kiberbiztonsági osztályozási rendszer (Forrás: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_HU.pdf Letöltve: 2022.04.26.)

Részkövetkeztetések:

A kiberbiztonsági osztályozási rendszer jelentős előrelépés a kiberbiztonság fogalomkörébe tartozó kutatási területek, alkalmazási területek, illetve a releváns ágazatok meghatározása tekintetében, és megalapozza a kiberbiztonság terminológiájának európai „közös nyelvét", a technológiai koherencia kialakítását. Az osztályozási rendszer által bemutatott dimenziók, valamint a hozzá kapcsolódó kiberbiztonsági területek kiegészítő jelleggel bírhatnak az IBF kiberbiztonsági feladatainak, valamint a szükséges ismeretek meghatározásában, ugyanakkor nem nyújtanak információt a végrehajtáshoz nélkülözhetetlen készségekről és kompetenciákról.

4.3.8. European Cybersecurity Skills Framework - ECSF (Európai Kiberbiztonsági Készség-keretrendszer) [161]

Az Európai Unió 2020-ban kiadott kiberbiztonsági stratégiája[162] felhívja a figyelmet a kiberbiztonsági szakemberek hiányának veszélyeire, melynek megoldására egy uniós szintű kiberbiztonsági pályafutási rendszer kidolgozását és bevezetését javasolja. "Az Európai Gazdasági és Szociális Bizottság úgy véli, hogy e készséghiányt csak egy uniós szintű kiberbiztonsági pályafutási rendszer segítségével lehet orvosolni, amely segítséget nyújt az egyének számára egy lehetséges kiberbiztonsági pályafutás meghatározásában, kiépítésében és megvalósításában azáltal, hogy segít megérteni, milyen ismeretekre, készségekre és képességekre van szükség a kiberbiztonsági pálya elkezdéséhez vagy fejlesztéséhez, illetve az ilyen pályára való átálláshoz".

Az ENISA „Kiberbiztonsági készségek fejlesztése az EU-ban" című jelentése[163] szerint Európa le van maradva a kiberbiztonság területén releváns szerepkörök és készségek meghatározására szolgáló átfogó megközelítés kidolgozásában. Bár a kiberbiztonság

[161] European Cybersecurity Skills Framework - ECSF (Európai Kiberbiztonsági Készség-keretrendszer) https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.11.20.); https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf (Letöltve: 2022.11.20.)

[162] Az Európai Gazdasági és Szociális Bizottság (2021/C 286/14) véleménye közös közleményéről az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre (JOIN(2020) 18 final)

[163] Európai Uniós Kiberbiztonsági Ügynökség, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees (A kiberbiztonsági készségek fejlesztése az EU-ban: a kiberbiztonsági diplomák tanúsítása) https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (Letöltve: 2022.04.21.)

világméretű, minden országot érintő kérdés, a nemzetállamok között számos különbség van. Emiatt a meglévő kiberbiztonsági keretrendszerek összeegyeztethetetlenek lehetnek az európai szükségletekkel, törvényekkel és szabályozásokkal, vagy általában nem azokra irányulnak. Szükségessé vált és alapvető lépésnek tekinthető Európa digitális jövője felé egy európai kiberbiztonsági készségek keretrendszerének kidolgozása, amely figyelembe veszi az EU és az egyes tagállamok szükségleteit.

Az ENISA az európai kiberbiztonsági készségek keretrendszer kidolgozása érdekében 2020-ban ad hoc munkacsoportot hozott létre. A multidiszciplináris szakértői csoport célja az volt, hogy elősegítse a kiberbiztonsági oktatás, képzés és munkaerő-fejlesztés ökoszisztémájának harmonizációját, valamint egy közös európai nyelvet dolgozzon ki a kiberbiztonsági készségek kontextusában. A csoport tanácsot adott és segítette az ENISA-t egy európai kiberbiztonsági készségkeretrendszer kidolgozásában, amely lehetővé teszi az egyének, a munkáltatók és a képzési szolgáltatók által az EU tagállamaiban használt szerepek, kompetenciák, készségek és ismeretek közös megértését. Ezen túlmenően a figyelemfelkeltést is elősegítheti azáltal, hogy azonosítja a kiberbiztonsági környezet azon hiányosságait, amelyek áthidalhatók egy közös európai kiberbiztonsági készségkeretrendszer létrehozásával. A keretrendszer támogatja a kiberbiztonsággal kapcsolatos készségek felismerését, és segíti a kiberbiztonsággal kapcsolatos készség- és karrierfejlesztési képzési programok tervezését.

Az ad hoc munkacsoportnak 17 kinevezett tagja van és összességében 14 ország vesz részt a működésében.[164] A munkacsoport 2020. decemberében kezdte meg a működését két csoportra bontva: az egyik szemantikai, a másik munkaerőpiaci szempontokból vizsgálta a kiberbiztonság kérdéseit. A két csoport javaslatai alapján került kidolgozásra 2020. júliusában a keretrendszer első tervezete. Ezt követően vette kezdetét a tesztelés fázisa, majd a visszajelzések alapján a keretrendszer felülvizsgálatára és korrekciójára, finomítására került sor. 2022 első felében elkészült a második tervezet, mely a külső érdekelt felekkel történő véleményeztetést követően javításra, majd a keretrendszer végső változata[165] 2022. szeptember 19-én kiadására kerül.

[164] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls) (Letöltve: 2022.04.20.)
[165] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.10.12.)

Az ad hoc munkacsoport a probléma elemzését két oldalról közelítette meg: a létező keretrendszerek, taxonómiák és tudományos irodalom, valamint a munkaerő-piaci trendek és igények elemzése alapján. Az elemzés eredményeként sor került:

- a **tudás** azonosítására (strukturált megközelítéssel a meglévő tudásosztályok alkalmazásával);
- a kulcsfontosságú **kiberbiztonsági készségek** azonosítására a piaci igények alapján, amelyek összekapcsolhatók a szakmai profilokkal, illetve a kompetenciákkal;
- a tipikus **kiberbiztonsági szakmai profilok** meghatározására a piaci igények alapján:
  a) a profilhoz kapcsolható kulcselemek leírásával (a profil alternatív elnevezése, összefoglaló megállapítások, küldetés, tipikus feladatok, kulcs ismeretek és készségek, e-CF kompetenciák),
  b) a választott részletezettségi szinten azonosítva (ESCF jelenleg: 12 szint).

ECSF szakmai profilok:

1. Chief Information Security Officer (CISO)
2. Cyber Incident Responder
3. Cyber Legal, Policy and Compliance Officer
4. Cyber Threat Intelligence Specialist
5. Cybersecurity Architect
6. Cybersecurity Auditor
7. Cybersecurity Educator
8. Cybersecurity Implementer
9. Cybersecurity Researcher
10. Cybersecurity Risk Manager
11. Digital Forensics Investigator
12. Penetration Tester

A szakmai profilok felépítése:

- A szakmai szerepprofil neve.
- Alternatív elnevezés: a szakmai szerepprofil alternatív elnevezései.
- Összegzés: a szerepkör fő célkitűzései.
- Küldetés: a szerepkör legfőbb elemeinek bemutatása.

- Eredménytermékek: a szerepkör tipikus eredményeinek listája, amely a profil relevanciáját is magyarázza egy nem szakértő számára.
- Fő feladatok: a szerepkörhöz kapcsolódó fő feladatok felsorolása.
- Kulcs készségek: a szerepkör munkafeladataihoz kapcsolódó és ellátásukhoz szükséges képességek felsorolása. A puha készségek (pl. kommunikáció, időgazdálkodás, együttműködési képesség) és az etika alapelvei is néhány esetben kifejezetten megjelennek a profilokban.
- Kulcs ismeretek: a munkakörhöz tartozó feladatok elvégzéséhez, valamint a szerepkör betöltéséhez szükséges alapvető ismeretek listája.
- E-Kompetenciák: Az e-kompetencia keretrendszer (e-CF) alapján kerül meghatározásra.

Az e-kompetenciák a 4.3.5. pontban bemutatott Európai e-Kompetencia Keretrendszer (e-CF) alapján kerülnek meghatározásra az adott szakmai profil által megjelölt szinten.

A kulcs készségek között megjelennek a **puha készségek**, illetve az etikai alapelvek is. A puha készségek olyan tulajdonságok, amelyek minden szakmai készséghez szükségesek, így az ilyen készségekre a szakemberek számára is szükség van. A készségek széles skálája tartozik a puha készségek közé, mint például a kommunikáció, a másokkal való együttműködés, a jelentéstétel, a befolyásolás, a kritikus gondolkodás, az időgazdálkodás és a stressz kezelése.
Az **etika** szintén fontos átfogó elem, amely a kiberbiztonság valamennyi aspektusára hatással van, ezért az európai kiberbiztonsági készségek egyik alapvető készségkomponense és a keretrendszer alapvető eleme. A kiberbiztonság összefüggésében az etika arról szól, hogy milyen döntések azok, amelyek megfelelnek az értékeinknek, mi az, ami erkölcsileg elfogadható mind az adatgazda, mind pedig a szervezet számára. A kiberbiztonsági szakemberek gyakran kerülnek akár érzékeny információk, adatok birtokába, így az etikai tudatosság fontos érték, az etikus döntéshozatal pedig fontos készség, amelyekkel rendelkezniük kell.

Példa az ECSF által meghatározott szerepprofilra (1. Chief Information Security Officer (CISO)- Információbiztonsági Vezető):

2. PROFILES

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources
Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans

	• Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people	
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring D.1. Information Security Strategy Development E.3. Risk Management E.8. Information Security Management E.9. IS-Governance	Level 4 Level 5 Level 4 Level 4 Level 5

33. ábra: Példa az ECSF profilra (CISO) (Forrás: ECSF – European Cybersecurity Skills Framework, 2022.09.19. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)

Az ECSF gyakorlati használata:

1. Helyzetfelmérés: a kiberbiztonsággal kapcsolatos megfelelő információk összegyűjtése és feldolgozása, pl. egy szervezet állapotáról, az érintett felek azonosítása, távlati célok meghatározása.
2. Azonosítás: az elérendő konkrét célok azonosítása. A kiberbiztonsággal kapcsolatos konkrét követelmények és célok megfogalmazása.
3. Kiválasztás: az ECSF megfelelő összetevőinek kiválasztása aszerint, hogy az adott helyzetre mely ECSF profilok a leginkább alkalmazhatók. Ezután ki kell választani azokat az összetevőket, amelyek segítik az igények lefedését vagy a kívánt célok elérését.
4. Átültetés: a kiválasztott komponensek igényeknek megfelelő alkalmazása. Amennyiben szükséges, a kiválasztott komponenseken módosítás hajtható végre, hogy jobban illeszkedjenek az adott helyzethez.
5. Alkalmazás: a testreszabott komponensek átültetése a célkörnyezetre. A személyre/szervezetre szabott ECSF-összetevők felhasználásával lépéseket tehetünk a biztonsággal kapcsolatos célkitűzések és a szervezeti célok megvalósítása érdekében.

34. ábra: Az ECSF gyakorlati használata (saját szerkesztés)

A szakmai szerepprofilok nem szakértő személyek számára is készültek, hiszen segítenek megérteni a kiberbiztonság komplex környezetét, és közös uniós nyelvet biztosítanak minden érdekelt fél számára.

Az ECSF szerepprofilok nem egyediek, hanem egy általános szerepkör egyszerű leírását tartalmazzák a széleskörű használhatóság érdekében. Magát a munkakört egy szervezeten belül természetesen egyedi módon határozzák meg, hozzárendelve a fizetést, a feltételeket és kikötéseket. A gyakorlatban egy kiberbiztonsági munka számos ECSF szerepkörből és / vagy szerepekörök részéből áll.

Részkövetkeztetések:

Az ECSF a kiberbiztonsági szakmai szerepprofilok kidolgozásán keresztül, közvetett módon meghatározza azokat a kiberbiztonsággal kapcsolatos feladatokat is, amelyeket a szervezeteknek a működésük során ellátniuk szükséges. Az azonosított kiberbiztonsági feladatokhoz az ellátáshoz szükséges kulcs ismereteket, kulcs készségek és e-kompetenciák is feltérképezésre és pontosan meghatározásra kerültek a keretrendszerben. Az ECSF használata egységes terminológiát biztosít minden európai szervezet számára, és kiindulási pontként szolgál az IBF feladatainak azonosításában. A feladatok ellátásához nélkülözhetetlen ismeretek, készségek és kompetenciák hozzárendelése révén a keretrendszer segítségével pontosan meghatározhatók azok a humánerőforrás-fejlesztési irányok, amelyek az IBF és a munkáját segítő egyéb kiberbiztonsági feladatokat ellátó munkatársak képzése segítségével hozzájárulnak a kibertámadások elleni fokozott védelem eléréséhez és az elektronikus információs rendszerek biztonságához.

4.3.9. Egyéb, kiberbiztonsági készségek azonosítására szolgáló keretrendszerek

A 2018-as Horizont 2020, „A Biztonsági Unió (SU) hatékonyságának növelése” című kiberbiztonsági felhívására 12 pályázat érkezett, melyek közül négy került nyertesként kiválasztásra: a CONCORDIA, az ECHO, a SPARTA és a CyberSec4Europe kísérleti projektek. A projektek célja, hogy segítséget nyújtsanak Európa kiberbiztonsági szakértelmének egyesítésében és az európai kiberbiztonsági környezet előkészítésében annak érdekében, hogy hatékonyan megvalósulhasson a biztonságosabb digitális Európára vonatkozó elképzelés. Ezek a kísérleti projektek több mint 160 partnert, köztük nagyvállalatokat, kkv-kat, egyetemeket és kiberbiztonsági kutatóintézeteket vontak össze 26 EU-tagállamból.

A kutatási cél szem előtt tartásával, a négy projekt releváns eredményei a következők:

- **CONCORDIA** (Cyber Security Competence for Research and Innovation)[166]: A CONCORDIA egy jelentős H2020 konzorcium, amelynek célja Európa kiberbiztonsági képességeinek összekapcsolása. Módszertant dolgozott ki a kiberbiztonsági tanfolyamok fejlesztésére, a készséghiányok megszüntetése érdekében.
- **ECHO**[167]: Az ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) fő célja az Európai Unió proaktív kibervédelmének és Európa technológiai szuverenitásának erősítése hatékony és eredményes több ágazatot és több területet érintő együttműködés révén. A projekt egy európai kiberbiztonsági ökoszisztémát fejleszt ki, amely támogatja az európai piac biztonságos együttműködését és fejlődését, valamint megvédi az Európai Unió polgárait a kiberfenyegetésekkel és incidensekkel szemben. Célja az egészségügyben, a közlekedésben és az energiaiparban tapasztalható tudás- és készséghiányok pontosabb meghatározása, valamint a kiberbiztonsági oktatási és képzési programok kidolgozása.

[166] CONCORDIA (Cyber Security Competence for Research and Innovation) http://www.concordia-h2020.eu/press_release/CONCORDIA_Press_release_FInal_1_Page.pdf (Letöltve: 2022.10.12.)
[167] ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) https://echonetwork.eu/project-summary/ (Letöltve: 2022.10.12.)

- **SPARTA** (Strategic programs for advanced research and technology in Europe) [168]: A SPARTA célja egy olyan hosszú távú közösség létrehozása, amely képes együttműködni olyan megoldások meghatározására, fejlesztésére, megosztására, amelyek segítik a szakembereket a kiberbűnözés megelőzésében és a kiberbiztonság fokozásában. A projekt azonosította azokat a készségeket, amelyeket a kiberbiztonsági tantervekbe beépíteni szükséges. 11 alapvető témakört és 16 kiberbiztonsági témakört határoztak meg, melyeket 6 technológiai csoportra osztottak: informatika, kriptológia, matematika, humán és társadalomtudományok, adatvédelem és biztonság.
- **CyberSec4Europe**[169]: A CyberSec4Europe fő célja az európai demokrácia és a digitális egységes piac integritásának biztosításához és fenntartásához szükséges kiberbiztonsági képességek konszolidációja. A kiberbiztonsággal kapcsolatos európai egyetemi diplomát adó programok áttekintésére fókuszált azzal a céllal, hogy támogassák az oktatásban szükséges kiberkészségek azonosítását és rangsorolását.

Részkövetkeztetések:

A Horizont 2020 négy nyertes pályázata, a CONCORDIA, az ECHO, a SPARTA és a CyberSec4Europe kísérleti projektek nagyon fontos eredményeket értek el az általános, illetve szakterületi (pl. egészségügy) kiberbiztonsági képzések terén, mivel számos, az oktatásban szükséges kiberbiztonsággal kapcsolatos készséget azonosítottak, valamint kiberbiztonsági oktatási és képzési programokat dolgoztak ki a felmért készséghiányok csökkentése érdekében. A kutatási célkitűzések elérése szempontjából azonban a projektek eredményei kifejezetten oktatási/képzési fókusszal kerültek megállapításra, és általánosságban, vagy szakterület specifikusan azonosították a szükséges készségeket, mint képzendő területeket. A projektek nem nyújtanak információt a közigazgatás-specifikus készségekről, illetve a hozzájuk kapcsolható ismeretekről és kompetenciákról.

[168] SPARTA (Strategic programs for advanced research and technology in Europe) https://www.sparta.eu/ (Letöltve: 2022.10.12.)
[169] CyberSec4Europe https://cybersec4europe.eu/ (Letöltve: 2022.10.12.)

4.3.10. Összehasonlító elemzés

A 4.3. pont bevezetésében felállított kritériumrendszer segítségével 13 keretrendszer került azonosításra és elemzésre, melyek közül:

- valamely kiberbiztonsági és/vagy közigazgatási szerepkörhöz rendelve, kiberbiztonsággal kapcsolatos feladatokat határoz meg: a NICE, és az ECSF keretrendszer;
- kiberbiztonsággal kapcsolatos ismereteket, tudásterületeket határoz meg: a NICE, a CYBOK, a European Cybersecurity Taxonomy és az ECSF keretrendszer;
- kiberbiztonsággal kapcsolatos készségeket határoz meg: a NICE és az ECSF keretrendszerek, illetve részben érintve a kérdéskört, az ESCO és a Horizont 2020 projektek;
- kiberbiztonsággal kapcsolatos humán képességeket határoz meg: a NICE keretrendszer;
- kiberbiztonsággal kapcsolatos kompetenciákat határoz meg: a DigComp 2.2., a Közszolgálati Referenciakeret, az e-CF, az ESCO és az ECSF keretrendszerek;
- a közigazgatás szerepkörök tekintetében feladatokat, ismereteket, készségeket, képességeket, kompetenciákat határoz meg: a Közszolgálati Referenciakeret, az e-CF, az ESCO és az ECSF keretrendszerek, illetve részben érintik a Horizont 2020 projektek is.

Az alábbiakban ismertetem az elemzett keretrendszerek összehasonlítását táblázat formájában a kutatási cél szempontjából meghatározó jellemzők alapján:
(Amennyiben egy adott jellemző azonosításra került az elemzett keretrendszerben, „X” –el került jelölésre, néhány indokolt esetben az **„X”** jelölése helyett **konkrét tartalmi elemek** kerültek felsorolásra a vizsgált jellemző kapcsán. Abban az esetben, ha az adott jellemző nem azonosítható a vizsgált keretrendszerben, a táblázat megfelelő cellájába **„-„** jel került.)

Keretrendszer	Kiberbiztonság	Feladatok (Tasks)	Tudás (Konwledge)	Készségek (Skills)	Képességek (Ability)	Kompetenciák	IBF	Közigazgatási kapcsolódás
DigComp 2.2.	„Biztonság"	-	-	-	-	1. Eszközök védelme 2. A személyes adatok és a magánélet védelme 3. Az egészség és a jólét védelme 4. A környezet védelme	-	(X) nem specifikus
Közszolgálati Referenciakeret	„Biztonság"	-	-	-	-	1. A digitális eszközök védelme 2. Adatvédelem 3. Információszabadság biztosítása 4. A rendelkezésre álló adatvagyon felelős hasznosítása	-	X
NICE	X	X	X	X	X	-	X	X
CyBok	X	-	X	-	-	-	-	-
e-CF	A kiberbiztonság csak az egyik összetevő az e-CF-en belül!	-	-	-	-	5 kompetenciaterület 41 infokommunikációs kompetencia 5 CF jártassági szint	X	(X) nem specifikus
ESCO	-	-	-	S 5.2.0. számítógépes rendszereket hoz létre és véd S 5.2.2. gondoskodik az IKT eszközök védelméről	-	Digitális biztonsági intézkedéseket alkalmaz (kéretlen elektronikus hirdetések elleni védelmet telepít, ügyel az internetes adatvédelemre, tűzfalat telepít és frissít)	-	X
European Cybersecurity Taxonomy	X	-	X	-	-	-	-	X
ECSF	X	X	X	X	-	X	X	X
Horizont 2020 projektek	X	-	-	X	-	-	-	(X)

12. táblázat: Keretrendszerek összehasonlító táblázata (forrás: saját szerkesztés)

Kiberbiztonsági munkakörre vonatkozó feladatokat, ismeretanyagot, készségeket/képességeket, illetve kompetenciákat határoznak meg: a NICE, a CyBok, az e-CF és az ECSF keretrendszerek.

Az összehasonlított keretrendszerek közül a NICE az Egyesült Államokban, a CyBok az Egyesült Királyságban került kidolgozásra, a összes további keretrendszer az Európai Unió megfelelő szervei által kezdeményezett projektek, kettő kivételével: a magyar Állampolgári digitális kompetencia-keret (DigComp 2.1.), amely ugyanakkor az Unióban kidolgozott DigComp 2.2. hazai megfelelője, illetve a Közszolgálati digitális kompetencia referenciakeret, mely a Belügyminisztérium és a Nemzeti Közszolgálati Egyetem együttműködésében megvalósuló, kidolgozás alatt álló projekt.

Az elemzés szempontjából további fontos támpontot nyújtott, hogy az egyes keretrendszerekben meghatározott elemek az IBF szerepkörében is értelmezhetők-e. E tekintetben a NICE, az e-CF, valamint az ECSF keretrendszerek nyújthatnak segítséget a szerepprofil vonatkozásában.

Az elemzés további feladata volt annak meghatározása, hogy az IBF számára meghatározandó feladatok és az ahhoz kapcsolódó ismeretek, készségek, kompetenciák azonosítása szempontjából, mely elemzett keretrendszer bír relevanciával, tehát mely

keretrendszerek elemei ültethetők át a magyar közigazgatási környezetbe legjobb gyakorlatként.

4.4. JÓ GYAKORLATOK AZONOSÍTÁSA, MAGYAR KÖZIGAZGATÁSBA ÁTÜLTETHETŐ ELEMEK MEGHATÁROZÁSA

Az összehasonlító táblázat segítségével az alábbi megállapításokat tettem a jó gyakorlatként történő alkalmazhatóság tekintetében:

Az európai DigComp 2.2. mintájára kidolgozott **hazai Állampolgári digitális kompetencia-keret (DigComp 2.1.)** jelentős előrelépést biztosít az átlagfelhasználók, így a közigazgatásban dolgozók digitális és annak részeként, a biztonsághoz kapcsolódó kompetenciái meghatározása terén, ugyanakkor a keretrendszer nem bír relevanciával az IBF szerepprofilja meghatározásában. A DigComp jó gyakorlatként történő alkalmazása a közszolgálati szerepprofil kidolgozása szempontjából bírhat jelentőséggel.

A **Közszolgálati digitális kompetencia referenciakeret** a DigComp 2.2. keretrendszerhez képest sokkal részletesebben és közigazgatás-specifikusan határozza meg az átlagfelhasználók kompetenciáit a „Biztonság, védelem és felelősség" területen, ugyanakkor a Referenciakeret kidolgozása, pontosítása még folyamatban van, ráadásul szintén nem jelent támpontot az IBF szerepprofil kidolgozása tekintetében.

A **CyBok**, illetve a **European Cybersecurity Taxonomy** a kiberbiztonság tudásterületeit azonosítja, azonban nem foglalkoznak az alkalmazáshoz szükséges készségekkel, kompetenciákkal. E két keretrendszernek a szükséges ismeretanyagok későbbi részletes kidolgozása során lehet szerepe, azonban a kutatásnak kizárólag a feladatellátáshoz szükséges ismeretanyag, készségek és kompetenciák azonosítása a célja, a képzési anyagok bővebb meghatározása nem képezi a vizsgálat tárgyát. A jövőben, önálló kutatásként ugyanakkor vizsgálandó e terület is.

A **Horizont 2020 projektek (CONCORDIA, ECHO Cyberskills Framework, SPARTA, CyberSec4Europe)** speciális készségek megállapítását tűzték ki célul, több

esetben egy-egy sajátos szakterületre (pl. közlekedés) fókuszálva, és az azonosított készségek a kiberbiztonsági tanfolyamok, tantervek fejlesztésére, valamint azok oktatási célú felhasználására koncentráltak. E projektek nem azonosíthatók a kitűzött kutatási célok szempontjából jó gyakorlatként.

Az **ESCO** ugyan 2942 foglalkozást és e foglalkozásokhoz kapcsolódó 13 485 készség leírását, illetve 500 transzverzális készség és kompetencia meghatározását tartalmazza, ugyanakkor kiberbiztonsági kapcsolódás csak érintőlegesen mutatható ki. A felsorolt készségek és kompetenciák nem nyújtanak megfelelő támpontot az IBF szerepprofil kidolgozásához.

Az amerikai **NICE keretrendszer** megfelelő kiindulási alap lehetne az IBF szerepprofil szempontjából, hiszen az általa azonosított kiberbiztonsági szerepkörök vonatkozásában pontosan meghatározza a szükséges ismereteket, készségeket és képességeket. Az átültetés nehézséget –ahogy már a korábbi fejezetben utaltam rá- az képezi, hogy a felsorolt kiberbiztonsági szerepkörök nem mindig igazodnak az EU igényeihez, jogszabályaihoz és éppen ezért nehezen összeegyeztethetők az európai egyéb keretrendszerekkel. A NICE-hez felépítésében és gondolatmenetében nagyon hasonló ECSF keretrendszer átültethetőség szempontjából inkább megfeleltethető jó gyakorlatnak, és értelemezhető a magyar közigazgatási környezetben is.

Az **Európai Kiberbiztonsági Készség-keretrendszer** (**ECSF**) az általa azonosított kiberbiztonsági szerepkörök vonatkozásában meghatározza a feladatellátáshoz szükséges ismereteket, készségeket és kompetenciákat is, ez utóbbit a szintén elemzett **European e-Competence Framework (e-CF)** segítségével teszi, biztosítva ezzel a két európai keretrendszer közti átjárhatóságot is. Az ECSF segítségével jól azonosíthatók az IBF számára a mindennapi munkavégzéshez kapcsolódó kiberbiztonsági feladatok, illetve a keretrendszer segítségével a szükséges ismeretek, készségek és kompetenciák is. **Az ECSF moduláris felépítése alkalmassá teszi, hogy a szerepprofilokban azonosításra kerülő elemek rugalmasan átültethetők legyenek a magyar közigazgatási környezetbe. Alkalmazásával, az általam kidolgozott IBF szerepprofil szervesen beilleszthető az európai keretrendszerek által alkalmazott „közös nyelvi" környezetbe, és a segítségével meghatározásra kerülő ismeretek, készségek és kompetenciák biztosítják a más európai országokkal történő átjárhatóságot is.**

A következő összehasonlító táblázat áttekinthetően szemlélteti az összehasonlító elemzés eredményeit:

Keretrendszerek	Jó gyakorlatként alkalmazása az IBF szerepprofil kidolgozásához	Átültethető elemek a magyar közigazgatási környezetbe	Jövőben további kutatási terület
DigComp 2.2.	-	-	-
Közszolgálati Referenciakeret	-	-	-
NICE	-	-	-
CyBok	-	-	✓
e-CF	✓	Kompetenciák	-
ESCO	-	-	-
European Cybersecurity Taxonomy	-	-	✓
ECSF	✓	Feladatok Ismeretek Készségek Kompetenciák	-
Horizont 2020 projektek	-	-	-

13. táblázat: Keretrendszerek jó gyakorlatként történő azonosítása (forrás: saját szerkesztés)

Az összehasonlítás eredményeként azonosítottam azokat a keretrendszereket, amelyek jó gyakorlatként kiindulási pontként szolgálnak az IBF szerepprofiljának definiálásában, majd meghatároztam a releváns keretrendszerek azon elemeit, amelyek átültethetők a magyar közigazgatási környezetbe.

4.5. AZ IBF KIBERBIZTONSÁGI FELADATAINAK MEGHATÁROZÁSA, A FELADATOK AZONOSÍTÁSA A RELEVÁNS KERETRENDSZEREKBEN

A nemzetközi keretrendszerek összehasonlítása eredményeként azonosítottam azokat a keretrendszereket, amelyek jó gyakorlatként kiindulási pontként szolgálhatnak az IBF szerepprofiljának megalkotásában, majd meghatároztam a releváns keretrendszerek azon elemeit, amelyek átültethetők a magyar közigazgatási környezetbe, tehát az H1-1. hipotézisem bizonyítást nyert.

Következő lépésként meg kell határozni azokat a konkrét kiberbiztonsági feladatokat, amelyeket az IBF-nek végre kell hajtania a mindennapi munkája során, majd e feladatokat meg kell feleltetni az azonosított keretrendszerekben.

Ahhoz, hogy meghatározzam, hogy az IBF-nek munkája ellátása során milyen feladatokat kell ellátnia és ahhoz milyen ismeretanyag, készség és kompetencia szükséges, a következő lépéseket kell végrehajtani:

1. meg kell vizsgálni az Ibtv. szerinti elektronikus információs rendszerek biztonságáért felelős személy jelenlegi, törvényben felsorolt feladatait,
2. a feladatokat be kell azonosítani az European Cybersecurity Skills Framework (Európai Kiberbiztonsági Készség-keretrendszer, továbbiakban: ECSF)[170] szerepprofilokban,
3. az ECSF-ben beazonosított feladatok alapján ki kell jelölni a feladatokhoz kapcsolódó ECSF-ben meghatározott ismereteket, készségeket és kompetenciákat (e-CF[171]).

1. Az Ibtv. 13.§-a határozza meg részletesen az IBF feladatait, ugyanakkor a 11. és 12.§-ban, a szervezet vezetője számára megfogalmazott feladatok is megjelennek az IBF mindennapi feladatellátása során a szervezet vezetőjét támogató, előkészítő, végrehajtó tevékenységként.

Az IBF Ibtv. alapján meghatározott feladatai a következők:

[170] European Cybersecurity Skills Framework Role Profiles (ECSF) : https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.11.20.)

[171] European e-Competence Framework (e-CF) https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework/ (Letöltve: 2022.03.25.)

1. Jogszabályokkal való összhang megteremtése és fenntartása Ibtv. 11.§ (1) a)-b), k)-l); 13.§ (2) a)-b) d), (5) a)-b)
2. Szabályozás / Véleményezés Ibtv. 11.§ (1) f); 13.§ (2) c), e)
3. Tudatosítás Ibtv. 11.§ (1) g)
4. Kockázatkezelés Ibtv. 11.§ (1) h)
5. Biztonsági események kezelése Ibtv. 11.§ (1) i)-j), m)
6. Ellenőrzés / Audit Ibtv. 11.§ (1) h)
7. Tájékoztatás / Jelentés (vezetés, érintettek) Ibtv. 13.§ (1), (3)
8. Kapcsolattartás Ibtv. 13.§ (2) f)
9. Egyéb feladatok Ibtv. 11.§ (1) n)

14. táblázat: Az IBF Ibtv. alapján meghatározott feladatai (forrás: saját szerkesztés)

A felsorolt feladatok az alábbi profilokban azonosíthatók be:

35. ábra: IBF profil meghatározása az ECSF szerepprofilok alapján (forrás: saját szerkesztés)

Az IBF jogszabályban meghatározott feladatai szerint, az ECSF-ben beazonosított feladatokat és a hozzá kapcsolódó készségeket, ismereteket, kompetenciákat a Függelék 1. sz. melléklete mutatja be részletesen, jelen rész kizárólag a táblázatban szereplő adatok elemzésére és értékelésére szorítkozik.

A következő táblázat összefoglalja, hogy az Ibtv. alapján meghatározott egyes feladatok, mely ECSF profilban kerültek azonosításra, tehát mely profilokban szereplő elemek segíthetnek az adott feladat mindennapi ellátásában. Pirossal kerültek megjelölésre azok a

szerepprofilok, amelyekből az adott feladat kapcsán a legtöbb elem került azonosításra, tehát amelyik szerepprofil –az adott feladat alapján- a legjellemzőbbnek mondható.

		CISO	Cyber Incident responder	Cyber Legal, Policy and Compliance Officer	Cyber Threat Intelligence Specialist	Architect	Auditor	Educator	Implementer	Researcher	Risk Manager	Digital Forensics Investigator	Penetration Tester
1	Jogszabályokkal való összhang megteremtése és fenntartása	x		x						x			
2	Szabályozás / Véleményezés	x	x	x				x					
3	Tudatosítás	x						x					
4	Kockázatkezelés	x			x		x			x	x		
5	Biztonsági események kezelése	x	x		x								
6	Ellenőrzés / Audit	x		x	x		x		x	x			
7	Tájékoztatás / Jelentés (vezetés, érintettek)	x	x	x	x		x		x	x			
8	Kapcsolattartás	x		x	x	x			x	x			
9	Egyéb feladatok	x		x		x			x	x			

15. sz. táblázat: Az IBF egyes feladatainak ECSF elemei (forrás: saját szerkesztés)

Az adatokból egyértelműen kimutatható, hogy az IBF szerepe és feladatai a CISO szerepprofiljához állnak a legközelebb. A jogszabályokkal való összhang megteremtésével és fenntartásával, a szabályozással, a tájékoztatással/ jelentéssel, a kapcsolattartással összefüggő feladatok esetében is a CISO szerepprofiljában azonosított fő feladatok, kulcs készségek és ismeretek, valamint e-kompetenciák szolgálhatnak irányadóként és segítségként az IBF-k feladatellátása és fejlesztése, illetve a vele szemben támasztott követelmények megfogalmazása szempontjából. A többi feladat kapcsán is megjelennek elemek a CISO szerepprofilból, ugyanakkor ezek esetében a legtöbb elem más profilból kerül kiemelésre.

A tudatosítás területén a cybersecurity educator, a kockázatkezelés esetében a risk manager, a biztonsági eseménykezelésnél a cyber incident responder, az ellenőrzéseknél pedig az auditor szerepprofilok elemi dominálnak a Ibtv.-ben megfogalmazott feladatok kapcsán.

Három további szerepprofilt találhatunk, amelyekből számos elem releváns lehet az IBF számára: a cyber legal, policy and compliance officer, a cyber threat intelligence specialist, valamint a cybersecurity researcher. Ennek legfőbb oka, hogy az IBF kiemelt feladata, hogy átfogóan biztosítsa az adott szervezet, illetve rendszerek jogszabályi megfelelőségét, a megfelelésről pedig ellenőrzések révén kell megbizonyosodnia. A „kutatói” szerepkör leginkább a gyorsan változó körülmények és ismeretek követésére és alkalmazására vonatkoznak.

A digital forensics investigator, illetve a penetration tester profilok egyetlen eleme sem jelenik meg az IBF vonatkozásában, mely leginkább azzal magyarázható, hogy ezek a

kiberbiztonsági feladatkörök nagyon speciális szakértelmet és tapasztalatot igényelnek, így képzési igényük is jelentősen eltér a többi területtől.

Részkövetkeztetések:
Összességében a táblázat egyértelműen megmutatja, hogy az IBF-nek milyen sokszínű és széleskörű ismerettel kell rendelkeznie a feladatai megvalósításához és ezek mennyire különböző készségek és kompetenciák meglétét igénylik.
A vizsgálattal bebizonyítottam, hogy az elektronikus információs rendszer biztonságáért felelős személy magyar jogszabályokban meghatározott feladatai, és e feladatok ellátásához szükséges készségek, ismeretek és kompetenciák azonosíthatók a jó gyakorlatként bemutatott nemzetközi keretrendszerekben (ECSF, e-CF), tehát a H1-2. hipotézis is igaznak bizonyult.

4.6. AZ IBF SZEREPPROFIL DEFINIÁLÁSA[172]

Ahhoz, hogy egy koherens, logikailag egységes szerepprofilt lehessen alkotni, szükség volt az Függelék 1. sz. mellékletében bemutatott táblázatok részletes áttekintésére, az esetleges ismétlődések és párhuzamosságok kiszűrésére, valamint a hazai jogszabályokban meghatározott terminológiának megfelelő megfogalmazások alkalmazására.

Az egyes kategóriákhoz tartozó, véglegesnek tekinthető szerepprofil elemek összegyűjtését követően, az alábbi összefoglaló táblázatban mutatom be a vizsgálataim eredményeként kidolgozott IBF szerepprofilt.

Az IBF szerepprofilja az Ibtv.-ből levezethető kiberbiztonsági feladatok alapján, az Európai Kiberbiztonsági Készség-keretrendszer (ECSF), valamint az Európai E-Kompetencia Keretrendszer (e-CF) bázisán, a magyar jogszabályi környezettel összehangolva került kidolgozásra. A szerepprofil meghatározza a mindennapi munkavégzéséhez kapcsolódó feladatokat és az ellátásukhoz szükséges kulcs készségeket, ismereteket és kompetenciákat.

[172] E fejezet Legárd Ildikó: Az elektronikus információs rendszer biztonságáért felelős személy szerepprofilja (Legárd, 2023c) című tanulmány alapján készült.

IBF SZEREPPROFIL	
Alternatív elnevezés	Elektronikus információs rendszerek biztonságáért felelős személy Informatikai Biztonsági Felelős (IBF) Informatikai Biztonsági Vezető (IBV)
Összegzés	Felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért a szervezet elektronikus információs rendszereiben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a szervezet elektronikus információs rendszereinek és elemeinek sértetlensége és rendelkezésre állásának zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítása érdekében.
Küldetés	A szervezet elektronikus információs rendszerei, valamint a rendszerekben kezelt adatok, információk védelme érdekében jogszabályokban meghatározott logikai, fizikai és adminisztratív védelmi intézkedéseket hajt végre. Ennek keretében gondoskodik: a szervezet elektronikus információs rendszerei biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, melynek részeként irányítja és elvégzi a szükséges tevékenységek tervezését, szervezését, koordinálását és ellenőrzését; előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, illetve e rendszerek biztonsági osztályba sorolását; véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit; kapcsolatot tart a hatósággal és az eseménykezelő központtal.
Fő feladatok	
– Biztosítja a kiberbiztonsággal és az információbiztonsággal kapcsolatos törvényeknek, rendeleteknek és szabványoknak való megfelelést, többek között jogi és szakmai tanácsadás, iránymutatás nyújtása segítségével. – Irányítja az Információbiztonsági Irányítási Rendszer (IBIR) működését és fejlesztését. – Előkészíti és bemutatja a szervezet felső vezetése jóváhagyása céljából a kiberbiztonság jövőképét, stratégiáját és politikáját, az Informatikai Biztonsági Szabályzatot, valamint biztosítja ezek megvalósítását és végrehajtását. – Kiberbiztonsági terveket dolgoz ki (pl. incidenskezelési terv). – Tervezési, szervezi, és végrehajtja a kiberbiztonsággal és az információbiztonsággal kapcsolatos tudatosságnövelő tevékenységeket, melynek keretében kidolgozza, frissíti a kiberbiztonsággal és az információbiztonsággal kapcsolatos tanterveket és oktatási anyagokat a tudatosság növelése érdekében. A képzések során, a tartalom, a módszer és az eszközök kiválasztásánál figyelembe veszi a résztvevők igényeit, innovatív megoldásokat keres a hatékonyság növelése érdekében. Nyomon követi, értékeli és jelentést készít a képzés hatékonyságáról és a képzésben részt vevők teljesítményéről. – Kidolgozza a szervezet kiberbiztonsági kockázatkezelési stratégiáját, kidolgozza, fenntartja, jelenti és kommunikálja a teljes kockázatkezelési ciklust. Tájékoztatja a felső vezetést a kiberbiztonsági	

kockázatokról, fenyegetésekről és azok hatásáról a szervezetre és biztosítja, hogy a szervezet felső vezetése jóváhagyja a szervezet kiberbiztonsági kockázatait. Biztosítja, hogy valamennyi kiberbiztonsági kockázat a szervezet számára elfogadható szinten maradjon. Értékeli a kiberbiztonsági kockázatokat és javaslatot tesz a legmegfelelőbb kockázatkezelési lehetőségekre, beleértve a biztonsági kontrollokat, valamint azokat a kockázatcsökkentő és a kockázatok elkerülését segítő intézkedéseket, amelyek a legjobban illeszkednek a szervezet stratégiájába. Nyomon követi a kockázatok javítására irányuló tevékenységeket.

- Azonosítja, értékeli és kezeli az elektronikus információs rendszerek sebezhetőségeit. Alkalmazza és irányítja a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.
- Kidolgozza, végrehajtja és értékeli az incidensek kezelésével kapcsolatos eljárásokat. Azonosítja, elemzi, mérsékli és kommunikálja a kiberbiztonsági incidenseket. Jelentést tesz a felső vezetésnek a kiberbiztonsági incidensekről. Azonosítja a fenyegetettségi környezetet, beleértve a támadók profilját és a támadási potenciál becslését. Biztosítja a szervezet ellenállóképességét a kiberbiztonsági incidensekkel szemben. Méri a kiberbiztonsági incidensek észlelése és a válaszadás hatékonyságát. Dokumentálja és értékeli a kiberbiztonsági incidenst követően hozott enyhítő intézkedések ellenálló képességét. Együttműködik a biztonsági műveleti központokkal (SOC) és a számítógépes biztonsági eseményelhárítási csoportokkal (CSIRT). Szorosan együttműködik az üzemeltetésben résztvevő informatikusokkal a kiberbiztonsággal kapcsolatos intézkedések során.
- Kiberbiztonsági ellenőrzéseket hajt végre. Kidolgozza az ellenőrzési tervet, melyben meghatározza az alkalmazni kívánt keretrendszereket, szabványokat, módszertant és ellenőrzési teszteket. Meghatározza az ellenőrzés hatókörét, célkitűzéseit és az ellenőrzéssel szemben támasztott követelményeket, irányítja az ellenőrzési tevékenységeket. Az ellenőrzések eredményeként dokumentálja és jelentést készít az elektronikus információs rendszerek, szolgáltatások és termékek biztonságáról.
- Egyeztet a felső vezetéssel a kiberbiztonsággal kapcsolatos költségvetésről. Biztosítja a kiberbiztonsági stratégia végrehajtásához szükséges erőforrásokat. Irányítja a szervezeten belüli folyamatos kapacitásépítést.
- Kapcsolatot alakít ki, együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szakmai szervezetekkel.
- Támogatást nyújt a kiberbiztonsággal kapcsolatos kérdésekben a felhasználók és az érdekelt felek számára.
- Nyomon követi a kiberbiztonság fejlődési irányait. Elemzi és értékeli a kiberbiztonsági technológiákat, megoldásokat, fejlesztéseket és eljárásokat. Elvégzi a kiberbiztonsági megoldások integrálását, és biztosítja a megfelelő működésüket. Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát.

Kulcs készségek

- A kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok elemzése, betartása és betartatása, a jogszabályváltozások nyomon követése.
- Kiberbiztonsági irányelvek, tanúsítványok, szabványok, módszertanok és keretrendszerek elemzése

és végrehajtása.

- Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása.
- Az üzleti stratégia, modellek és termékek átfogó megértése.
- A kiberbiztonsági stratégia, politika és az Informatikai Biztonsági Szabályzat kidolgozása, illetve végrehajtásának irányítása, szükség esetén módosítása vagy új tervek kidolgozása például jogszabályváltozás esetén.
- Információbiztonsági irányítási rendszer (IBIR) kialakítása, alkalmazása, ellenőrzése és felülvizsgálata közvetlen irányítással, vagy kiszervezés révén.
- Az üzleti igényeknek és a jogi követelménynek megfelelő kiberbiztonsági tervek és eljárások kidolgozása.
- A kiberbiztonsági tudatossággal, képzéssel és oktatással kapcsolatos igények azonosítása, a célközönségnek megfelelő pedagógiai megközelítések kiválasztása. A kiberbiztonsági igények lefedésére irányuló tanulási programok tervezése, fejlesztése és megvalósítása. Értékelési programok kidolgozása a tudatosságnövelő, képzési és oktatási tevékenységekhez. A szervezet kiberbiztonsági kultúrájának befolyásolása.
- Kiberbiztonsági gyakorlatok kidolgozása, beleértve a kibertér tágabb értelemben vett környezetét alkalmazó szimulációkat.
- A szervezet kiberbiztonsági helyzetének értékelése és javítása, a kiberbiztonsággal kapcsolatos problémák azonosítása és megoldása.
- Kiberbiztonsági kockázatkezelési keretrendszerek, módszertanok és iránymutatások átültetése, valamint a vonatkozó szabályozásoknak és szabványoknak való megfelelés biztosítása. A szervezet kockázatkezelési gyakorlatának elemzése és megerősítése. Kockázatmegosztási lehetőségek tervezése és kezelése, kiberbiztonsági „kockázattudatos” környezet kialakítása. A vezetők és az érdekelt felek számára a kockázatokra vonatkozó információk biztosítása az alátámasztott döntéshozatal érdekében.
- Auditálási eszközök és technikák alkalmazása, auditálási információk összegyűjtése, értékelése, megőrzése és védelme. Az ellenőrzés integránsan, pártatlanul és függetlenül történő elvégzése.
- A kiberfenyegetésről szóló, többféle forrásból származó információk összegyűjtése, elemzése és összefüggéseinek feltárása. Üzleti folyamatok elemzése, a szoftver- vagy hardverbiztonság értékelése és felülvizsgálata, technikai és szervezeti ellenőrzések végrehajtása.
- A biztonsági dokumentumok, jelentések, SLA-k felülvizsgálata és javítása.
- A kiberbiztonsági erőforrások tervezése és vezetése.
- A kiberbiztonsággal kapcsolatos technológiák új fejlesztéseinek nyomon követése. Kiberbiztonsági megoldások integrálása a szervezet infrastruktúrájába, a megoldások értékelése azok biztonságossága és teljesítménye alapján.
- Kommunikálás, koordinálás és együttműködés a belső és külső érdekelt felekkel.
- Új ötletek megfogalmazása és az elmélet átültetése a gyakorlatba.
- Az etikai követelmények és szabványok megértése, gyakorlása és betartása.
- Nyomás alatti munkavégzés.
- A munkatársak motiválása és ösztönzése.

- Együttműködés más csapattagokkal és kollégákkal.

Kulcs ismeretek

- Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok;
- kiberbiztonsági tanúsítványok, szabványok, módszertanok és keretrendszerek;
- kiberbiztonsági ajánlások és legjobb gyakorlatok;
- etikus kiberbiztonsági szervezeti követelmények;
- kiberbiztonsági érettségi modellek;
- kiberbiztonsági eljárások;
- erőforrás-gazdálkodás;
- irányítási gyakorlatok;
- kiberbiztonsági tudatosítás, oktatás és képzési programok fejlesztése, kiberbiztonsági oktatási és képzési szabványok, módszertanok és keretrendszerek;
- kiberbiztonsági kockázatok*:* kockázatkezelési szabványok, módszertanok és keretrendszerek, kockázatkezelési eszközök, kockázatkezelési ajánlások és legjobb gyakorlatok;
- kiberfenyegetések, számítógépes rendszerek sebezhetőségei;
- incidenskezelési szabványok, módszertanok és keretrendszerek, eseménykezelési ajánlások és legjobb gyakorlatok, incidenskezelési eszközök, kibertámadási formák, kiberbiztonsági trendek;
- operációs rendszerek biztonsága;
- számítógépes hálózatok biztonsága;
- biztonsági műveleti központok (SOC) működése;
- számítógépes biztonsági eseményelhárítási csoportok (CSIRT) működése;
- kiberbiztonsági ellenőrzések és megoldások, auditálási szabványok, módszertanok és keretrendszerek, auditálással kapcsolatos tanúsítás;
- kiberbiztonsággal kapcsolatos technológiák és megoldások.

E-kompetenciák

- **A.1. Az információs rendszerek és az üzleti stratégia összehangolása 4. szint:** Vezető szerepet vállal a hosszú távú innovatív informatikai megoldások kialakításában és végrehajtásában.
- **A.7. Technology Trend Monitoring 5. szint:** Megtervezi és vezeti a szisztematikus technológiai megfigyelés szervezeti struktúráját és támogatási rendszerét. Tanácsot ad és befolyásolja a stratégiai döntéseket a jövőbeli IKT-megoldások megtervezésében és megfogalmazásában.
- **B.3. Tesztelés 4. szint:** Széleskörű szaktudást használ a teljes tesztelési tevékenység folyamatának kialakítására, beleértve a belső gyakorlati szabályok kialakítását is. Szakértői útmutatást és tanácsadást nyújt a tesztelési csoportnak.
- **B.5. Dokumentumok előállítása 3. szint:** A részletesség szintjét a célcsoport igényeihez igazítja.
- **C.4. Problémakezelés 3. szint:** Az IKT-infrastruktúra és a problémakezelési folyamat speciális ismereteit használja fel a hibák azonosítása és minimális kieséssel történő megoldása érdekében. Nyomás alatt is megalapozott döntéseket hoz az üzleti hatás minimalizálása érdekében szükséges megfelelő intézkedésekről.
- **C.4. Problémakezelés 4. szint:** Vezető szerepet tölt be és felelős a teljes problémakezelési

folyamatért. Beosztja és biztosítja, hogy jól képzett emberi erőforrások, eszközök és diagnosztikai berendezések álljanak rendelkezésre a vészhelyzeti események kezelésére. Mély szakértelemmel rendelkezik a kritikus komponensek meghibásodásának előrejelzéséről és a minimális leállási idővel történő helyreállításról. Kialakítja az eszkalációs folyamatokat annak érdekében, hogy minden egyes incidenshez megfelelő erőforrásokat lehessen alkalmazni.

- **D.1. Információbiztonsági stratégia kidolgozása 5. szint:** Stratégiai vezetést biztosít az információbiztonságnak a szervezet kultúrájába való beillesztése érdekében.
- **D.3. Oktatási és képzési szolgáltatás 3. szint:** Kreatívan jár el a készséghiányok elemzése érdekében; konkrét követelményeket dolgoz ki és azonosítja a képzési kínálat lehetséges forrásait. Szakterületi ismeretekkel rendelkezik a képzési piacról, és visszajelzési mechanizmust hoz létre az alternatív képzési programok hozzáadott értékének értékelésére.
- **D.9. Humánerőforrás-fejlesztés 3. szint:** Figyelemmel kíséri és kezeli az egyének és csoportok fejlesztési igényeit.
- **D.10. Információ- és tudásmenedzsment 3. szint:** Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és ennek megfelelően biztosítja a legmegfelelőbb információs struktúrát.
- **E.3. Kockázatkezelés 4. szint:** Vezető szerepet vállal a kockázatkezelési politika meghatározásában és annak alkalmazásában, figyelembe véve az összes lehetséges korlátozó tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál.
- **E.4. Kapcsolatmenedzsment 3. szint:** Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során.
- **E.6. IKT minőségbiztosítás 4. szint:** Értékeli és megállapítja a minőségi követelmények teljesítésének mértékét, és irányítja a minőségpolitika végrehajtását. Gyakorlati vezetést biztosít a minőségi szabványok meghatározásához és teljesítéséhez.
- **E.8. Információbiztonsági irányítás 3. szint:** Értékeli a biztonságirányítási intézkedéseket és mutatókat, dönt ezek információbiztonsági politikának való megfelelőségéről. Vizsgálatot és korrekciós intézkedéseket kezdeményez a biztonsági előírások megsértése esetén.
- **E.8. Információbiztonsági irányítás 4. szint:** Vezeti az információs rendszerekben tárolt adatok integritásának, bizalmasságának és rendelkezésre állásának biztosítását, és megfelel az összes jogi követelménynek.
- **E.9. Információs rendszerek irányítása 4. szint**: Az információs rendszerek irányítási stratégiájának vezetése a vonatkozó folyamatok kommunikálásával, terjesztésével és ellenőrzésével a teljes IKT-infrastruktúrában.

16. táblázat: IBF szerepprofil (forrás: saját szerkesztés)

4.7. KÖVETKEZTETÉSEK

E fejezet bevezetésében meghatározott bizonyítási cél annak alátámasztása volt a bemutatott vizsgálatok segítségével, hogy nemzetközi keretrendszerek alapján, tudományos alapokon megalkotható az elektronikus információs rendszer biztonságáért felelős személy részére egy olyan szerepprofil, amely meghatározza az általa ellátandó feladatokat, valamint a végrehajtáshoz szükséges készségeket, ismereteket, kompetenciákat, és nem utolsó sorban szervesen illeszkedik a tágabb, európai környezetbe.

Az IBF szerepprofilja létrehozása érdekében három alhipotézist állítottam fel, melyek bizonyítását és annak lépéseit jelen fejezet részei részletesen bemutatták.

A H2-1. hipotézis esetében azt vizsgáltam, hogy vajon meghatározhatók-e a kiberbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó nemzetközi és hazai keretrendszerek segítségével olyan jó gyakorlatok, amelyek átültethetők a magyar közigazgatási környezetbe. Első lépésként meghatároztam a kiválasztás kritériumrendszerét, melynek segítségével feltérképeztem a kiberbiztonsággal, kibervédelemmel, illetve információbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó hazai és nemzetközi keretrendszereket. Dokumentumelemzés segítségével előre meghatározott szempontok szerint összehasonlítottam a keretrendszereket leíró dokumentumokat, majd meghatároztam a jó gyakorlatként azonosított keretrendszerek azon elemeit, amelyek kiindulási pontként szolgálhatnak az IBF szerepprofiljának definiálásában és átültethetők a magyar közigazgatási környezetbe. Kutatási lépéseim eredményeként a H2-1. hipotézis igaznak bizonyult.

A H2-2. hipotézis esetében arra kerestem a választ, hogy az IBF magyar jogszabályokban meghatározott feladatai, és e feladatok ellátásához szükséges készségek, ismeretek, és kompetenciák azonosíthatók-e a jó gyakorlatként bemutatott nemzetközi keretrendszerekben. Kutatási célom elérése érdekében a hazai jogszabályi környezet elemzését követően meghatároztam azon kiberbiztonsági feladatokat, amelyeket az IBF-nek a hatályos jogszabályok alapján ellátnia szükséges, majd e feladatokat és a hozzá kapcsolódó készségeket, ismereteket és kompetenciákat azonosítottam a kiválasztott keretrendszerekben, ezzel bizonyítva a H2-2. hipotézist. Eredményeimet a Függelék 1. sz. mellékletében foglaltam össze.

A H2-3. hipotézis esetén azzal a feltételezéssel éltem, hogy kidolgozható az IBF számára egy olyan speciálisan rászabott szerepprofil, amely meghatározza a mindennapi munkavégzés részét képző feladatokat, illetve a végrehajtáshoz szükséges ismereteket, képességeket és kompetenciákat. E hipotézis igazolása érdekében a nemzetközi keretrendszerekben, a H2-2. hipotézis bizonyítása során bemutatott elemek segítségével meghatároztam azokat a magyar közigazgatási környezetben értelmezhető feladatokat, ismereteket, készségeket és kompetenciákat, amelyek nélkülözhetetlenek IBF számára az Ibtv-ben megfogalmazott feladatok végrehajtásához, végül a megfelelő elemek implementációjával megalkottam az IBF szerepprofilját, valamint annak tartalmi elemeit, ezzel bizonyítva a H2-3. hipotézisben megfogalmazott feltételezésemet.

A részhipotézisek eredményeképp kidolgoztam egy tudományos alapokon nyugvó szerepprofilt az IBF részére.

Az Európai Kiberbiztonsági Készség-keretrendszer (ECSF) és az általa alkalmazott Európai e-Kompetencia Keretrendszer (e-CF) segítségével kidolgozott IBF szerepprofil biztosítja az Európai Unióban alkalmazott, kiberbiztonsággal kapcsolatos közös értelmezést és közös terminológia használatát, továbbá meghatározza a munkakörhöz kapcsolódó kritikus készségeket, ismereteket és kompetenciákat, amelyek egyben biztosítják e területek további fejlesztését is. A szerepprofil támogatja az egyéni fejlesztési lehetőségeket, ugyanakkor megfelelő alapot szolgáltat a képzési programok kidolgozásához és folyamatos fejlesztéséhez, valamint segítséget nyújt a humánerőforrás menedzsment számára a jelöltekkel, illetve a foglalkoztatott IBF-vel szembeni követelmények megfogalmazásában, felelősségük megalapozásában. A szerepprofil megfelelő tájékoztatást nyújt a felső vezetés számára is az IBF szervezeti környezetében értelmezhető feladatairól.

5. A KÖZSZOLGÁLATI KIBERBIZTONSÁGI „SZEREPPROFIL” (HARMADIK HIPOTÉZIS)[173]

5.1. BEVEZETÉS

Az Ibtv. értelmében a hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét. E feladat ellátása érdekében a szervezetnek megfelelő védelmi intézkedéseket kell végrehajtania, amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, valamint a biztonsági események kezelését. Bár, ahogy az az előző fejezetekben bemutatásra került, az Ibtv.-ben meghatározott feladatok közvetlen címzettjei a hatálya alá tartozó szervezetek vezetői, illetve az általa kinevezett/megbízott elektronikus információs rendszer biztonságáért felelős személy, az elektronikus információk rendszerek védelméhez kapcsolódó feladatok végrehajtása elképzelhetetlen az érintett szerveknél dolgozó munkatársak közreműködése nélkül. A közszolgálatban dolgozó átlagfelhasználóknak a mindennapi munkájuk során számos, kiberbiztonsággal szorosan összefüggő feladatot kell végrehajtaniuk, melyek ellátása speciális ismereteket, készségeket és kompetenciákat kíván meg. A lehetséges támadási és védekezési alternatívák, a szervezeti szintű biztonsági szabályok egyéni ismerete elengedhetetlen a szervezet biztonsági szintjének megőrzésében, hiszen elegendő egyetlen gyenge láncszem, akin keresztük a támadók különböző pszichológiai manipulációs technikák segítségével utat törnek maguknak a bizalmas szervezeti adatokhoz, információkhoz.

Bizonyítási cél

A fejezet következő részeiben bemutatott vizsgálatok célja annak bizonyítása, hogy azonosíthatók olyan kiberbiztonsági feladatok, amelyekkel a közszolgálatban dolgozó

[173] E fejezetet megalapozó kutatások az alábbi tanulmányokban kerültek publikálásra: Legárd Ildikó: A nemzetközi keretrendszerek összehasonlítása és a jó gyakorlatok azonosítása az IBF szerepprofil definiálása érdekében (Legárd, 2022a); Legárd Ildikó: Az elektronikus információs rendszer biztonságáért felelős személy szerepprofilja (Legárd, 2023c) E fejezet a következő tanulmányban került publikálásra: Legárd Ildikó (2023e): Közszolgálati kiberbiztonsági szerepprofil (Legárd, 2023e) – Megjelenés alatt!

átlagfelhasználó is találkozik, sőt ellátni köteles a mindennapi feladatellátása során, valamint e feladatok segítségével meghatározhatóak az ellátáshoz szükséges speciális ismeretek, készségek és kompetenciák a témával foglalkozó hazai és nemzetközi keretrendszerek segítségével.

A bemutatott vizsgálatok szorosan kapcsolódnak az IBF szerepprofil kidolgozása érdekében végzett korábbi kutatásomhoz, melynek keretében megtörtént a kiberbiztonsággal kapcsolatos feladatokkal, készségekkel, ismeretekkel és kompetenciákkal foglalkozó hazai és nemzetközi keretrendszerek elemzése és összehasonlító vizsgálata, illetve e keretrendszerek jó gyakorlatként, a magyar közigazgatásba átültethető elemeinek azonosítása (Legárd, 2022a, pp. 43-55.). Az eredmények felhasználásra kerültek az IBF szerepprofil egyes elemeinek meghatározásakor (Legárd, 2023c, pp.39-48.), illetve kiindulási alapként szolgáltak jelent kutatás elvégzéséhez.

5.1.1. Hipotézisek

H3	**Azonosíthatók a közszolgálatban dolgozók mindennapi munkavégzése során ellátandó kiberbiztonsági feladatok, valamint a feladatellátást biztosító ismeretek, képességek és kompetenciák.**

17. táblázat: H3 hipotézis (forrás: saját szerkesztés)

A bizonyítás cél elérése érdekében az alábbi két alhipotézist állítottam fel:

H3-1.	A közszolgálatban dolgozók szervezeti szinten értelmezhető kiberbiztonsági feladatai, valamint az ellátásukhoz szükséges készségek, ismeretek és kompetenciák levezethetők az IBF Európai Kiberbiztonsági Készség-keretrendszer (ECSF)[174] segítségével azonosított feladataiból.
H3-2.	Az ECSF segítségével meghatározott ismerethalmazok kiegészítése szükséges további, átlagfelhasználó-specifikus elemekkel annak érdekében, hogy pontosan definiálni tudjuk a nem kiberbiztonsági munkakörökhöz kapcsolódó

[174] European Cybersecurity Skills Framework Role Profiles : https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.11.20.); European Cybersecurity Skills Framework (ECSF) - User Manual: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

	kiberbiztonsági feladatokat, és a biztonságtudatosság kialakításához nélkülözhetetlen ismereteket, készségeket és kompetenciákat.

18. táblázat: H3 hipotézis alhipotézisei (forrás: saját szerkesztés)

5.1.2. Kutatási módszertan

A H3-1. hipotézis bizonyítása érdekében megvizsgáltam az IBF-nek az ECSF keretrendszerben azonosított feladatait, majd ezek közül kiválasztottam azokat a feladatokat, amelyek végrehajtása nem nélkülözi az adott szervezet, nem kiberbiztonsági munkakörben foglalkoztatott munkatársai közreműködését. A magyar jogszabályi környezetet figyelembe véve módosításokat hajtottam végre, illetve kiegészítéssel éltem a közszolgálati dolgozókra vonatkozó elemek tekintetében.
Az H3-2. hipotézis esetében áttekintettem a korábbi kutatásom során elemzett, kiberbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó hazai és nemzetközi keretrendszereket. A dokumentumelemzést követően meghatároztam a releváns keretrendszerek azon elemeit, amelyek átültethetők a magyar közigazgatási környezetbe. A releváns elemek implementációját követően, egy egységes rendszerbe foglalva meghatároztam a közszolgálati dolgozó azon kiberbiztonsági feladatait, készségeit, ismereteit és kompetenciáit, amelyek nélkülözhetetlenek a magyar jogszabályok által meghatározott, szervezeti szintű kibervédelmi és kiberbiztonsági feladatok ellátásához.

Bizonyítási kísérlet:
Egy kérdőíves vizsgálat segítségével bizonyítási kísérletet tettem a közszolgálati „szerepprofil” elemeivel kapcsolatos szakértői attitűdök mérésére, valamint a kutatási eredményeim árnyalására, esetleges módosítására.
A kísérletet és annak eredményeit az 5.6. rész mutatja be részletesen.

5.2. KAPCSOLÓDÓ SZAKIRODALMI ÁTTEKINTÉS

A közszolgálatban dolgozó átlagfelhasználó kiberbiztonsági feladatai, és az ellátásukhoz szükséges készségek, ismeretek és kompetenciák- egymáshoz való viszonyát, illetve az

információbiztonságban együttesen betöltött szerepüket és jelentőségüket leginkább a biztonságtudatosság fogalmán keresztül és vonatkozó szakirodalom alapján tudjuk megvilágítani.

5.2.1. Információbiztonság-tudatosság

Az információbiztonság-tudatosságnak (information security awareness) nincs egy általánosan elfogadott fogalma, annak összetevőit több magyar és nemzetközi kutatás is megkísérelte meghatározni (Legárd 2020b, p.95.). Egyes szerzők a fogalom egyéni aspektusait hangsúlyozzák, minthogy a biztonságtudatos személy nem csak a megfelelő szintű tudással rendelkezik az információbiztonság területén, hanem megérti és elfogadja annak jelentőségét, és képes az elsajátított ismereteknek megfelelően cselekedni és viselkedni (Veseli, 2011; Shaw, Chen, Harris, Huang, 2009). **Aldawood és Skinner** a felhasználó azon képességeit emelik, ki, hogy képes felismerni, beazonosítani, elkerülni vagy megbénítani egy rosszindulatú támadási kísérletet (Aldawood – Skinner, 2018; Aldawood - Skinner 2019a, Aldawood és Skinner 2019b).

Nemeslaki András és Sasvári Péter a definíció szervezeti aspektusait emelik ki, mint hogy „az információbiztonság-tudatosság a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket” (Nemeslaki - Sasvári 2014., p. 169.).

Bulgurcu és társai úgy határozzák meg az információbiztonság-tudatosságot, mint a munkavállaló általános ismereteinek és attitűdjének halmazát az információs rendszerek használatával kapcsolatban úgy, ahogy azt a szervezeti környezetben értelmezik (Bulgurcu et el., 2010., p. 532.). Az információbiztonság-tudatosság ebben a vonatkozásban két fő területből áll, egyrészt általában az információbiztonsággal kapcsolatos tájékozottságból, másrészt az információbiztonsági szabályozások és stratégiák ismeretéből (Illéssy, Nemeslaki, Som, 2014., p. 54.).

Összességében **az információbiztonság-tudatosság fogalmát** úgy lehet meghatározni, mint amely a tudás, a képességek és a viselkedés olyan hármasa, mely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső

igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést (Legárd, 2020b, p. 95.).

36. ábra: Az egyéni biztonságtudatosság és a biztonságtudatos szervezeti kultúra kialakítása (forrás: saját szerkesztés)

5.2.2. Biztonságtudatosító programok

A tudatosítás jelentőségét mutatja, hogy számos nemzetközi informatikai biztonsági szabvány –például az ISO 27001, COBIT, vagy az ISO 9001:2000- utal a minősítés megszerzésének előfeltételeként a tudatosítási program megvalósítására.
Az információbiztonsági tudatossági program tartalma és megvalósítása tekintetében ugyanakkor nem találkozhatunk egy nemzetközileg elfogadott keretrendszerrel, a témát vizsgáló korábbi tanulmányok is - a fogalom meghatározása helyett - a programok különféle aspektusaira és céljaira összpontosítottak.

Prah, Otchere és Opan - követve Chent és társait (Chen et al., 2008) - megállapította, hogy a biztonságtudatossági programok megfelelő ismeretekkel szolgálnak a felhasználók számára a biztonsági problémák káros következményeinek értékeléséhez, és megteszik a megfelelő intézkedéseket a biztonsági események megelőzéséhez és a helyreállításhoz. Az információbiztonsági tudatossági programok segítségével a szervezetek tudatosítani képesek a munkatársaikban, hogy milyen biztonsági fenyegetésekkel kell szembenézniük, illetve, hogy azokat milyen biztonsági intézkedésekkel és hogyan lehet megelőzni, elhárítani. A programok legfontosabb célja, hogy pozitívan befolyásolja az alkalmazottak viselkedését és hozzáállását az információbiztonsággal kapcsolatban. (Prah, Otchere és Opan, 2016, p. 62.)

A nemzetközi szakirodalomban ismertetett, tudatosító programokra vonatkozó leírások, elemzések alapján, a **biztonságtudatosítás** olyan folyamatos erőfeszítésként írható le, amely felhívja az érdekeltek figyelmét az információbiztonságra és annak fontosságára, elősegíti a biztonságorientált magatartást[175], és ideális esetben ösztönzi az érdekelt feleket a biztonsági szabályok és irányelvek betartására.[176]

A biztonságtudatosság fogalmával és tartalmával, a biztonságtudatosító programok tervezésével, megvalósításával, a tudatosítás kulcsfontosságú tématerületeivel, valamint a megfelelő tudástranszfert biztosító csatornák kiválasztásával részletesen foglalkoztam az alábbi tanulmányokban, konferenciaközleményekben:

- **Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre** - In. Hadmérnök, 2020. 15. évf., 1. szám, p. 91-105. (Legárd, 2020e)
- **Building An Effective Information Security Awareness Program** - In: Thomas, Hemker; Robert, Müller-Török; Alexander, Prosser; Dona, Scola; Tamás, Szádeczky; Nicolae, Urs (szerk.) Central and Eastern European e|Dem and e|Gov Days 2020, Wien, Ausztria: Österreichische Computer Gesellschaft (ÖCG) (2020) - p. 189-200. (Legárd, 2020d)
- **A humán faktor szerepe a kiberbiztonság megteremtésében** - In: Tick, József; Kokas, Károly; Holl, András (szerk.) Networkshop 2020. Országos Online Konferencia. 2020. szeptember 2-4., Budapest, Magyarország: Hungarnet, 2020, pp. 124-132. (Legárd, 2020b)
- **Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével** – In. Polgári Szemle: Gazdasági És Társadalmi Folyóirat 2021. 17.: 1-3 p. 358-373.) (Legárd, 2021b)
- **Effective methods for successful information security awareness** – In. Pro Publico Bono: Magyar Közigazgatás; A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi szakmai folyóirata 9 : 1, 2021 pp. 108-127. (Legárd, 2021a)

[175] Peltier (2005); ENISA, „A new users' guide: How to raise information security awareness," 2008. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide . (Letöltve: 2021.11.12.); Hansche (2001); Maeyer (2007)
[176] Tsohou, Karyda, El-Haddadeh (2012); Siponen (2000)

5.2.3. Az információbiztonságtudatosság és tudatosítás megjelenése a hazai jogszabályokban

A kiberbiztonságra vonatkozó magyarországi dokumentumokban, szabályozásokban kiemelt figyelmet fordítanak a tudatosság és a tudatosítás jelentőségének hangsúlyozására. A 2013-ban elfogadott **Nemzeti Kiberbiztonsági Stratégia** a kiberbiztonság fogalmi elemeként határozza meg a tudatosságnövelő eszközök folyamatos és tervszerű alkalmazását.[177]

Az **Ibtv**. kimondja, hogy az elektronikus információs rendszerek védelme érdekében a szervezet vezetője köteles gondoskodni „az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról”[178].

A **41/2015. (VII. 15.) BM rendelet**[179] értelmében az Ibtv. hatálya alá eső szervek kötelesek az Informatikai Biztonsági Szabályzatukban (továbbiakban: IBSZ) rögzíteni, hogy az adminisztratív védelmi intézkedések[180] körében, a tudatosítás érdekében milyen lépéseket tesznek meg. A rendelet 4. melléklete további részletszabályokat fogalmaz meg a biztonságtudatossági képzés kapcsán: „Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára az új felhasználók kezdeti képzésének részeként, amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, illetve az érintett szervezet által meghatározott gyakorisággal.”[181]

A hálózati és információs rendszerek biztonságára vonatkozó Stratégia[182], mely 2018-ban került elfogadásra, kiemeli:

---

[177] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat
[178] Ibtv. 11. § (1)
[179] 41/2015. (VII. 15.) BM rendelet 3.1.7. pont;
[180] Az információbiztonsági követelményeket alapvetően három csoportba oszthatjuk: fizikai, logikai és adminisztratív védelem. In: 41/2015. (VII. 15.) BM rendelet
[181] 41/2015. (VII. 15.) BM rendelet , 3.1.7.3.pont, Biztonság tudatosság képzés
[182] Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján készült Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégia https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf (Letöltve: 2021.11.12.)

„A digitalizálódó világban egyre fontosabb feladattá válik, és fokozott aktivitást igényel az állampolgárok, a társadalom különböző szereplőinek a tudatosítása annak érdekében, hogy a mindennapok részévé váló digitális eszközök és szolgáltatások biztonságos használatát elsajátítsák. (…) A szakosított intézmények – a civil, a gazdasági és a tudományos területek szereplőinek együttműködésével – támogatják a kibertér biztonságos használatát célzó, gyakorlati tudást elősegítő, figyelemfelhívó-tudatosító tevékenységeket, annak érdekében, hogy az egyéni felhasználók, a vállalatok és a szervezetek magabiztos és biztonságos módon használhassák digitális eszközeiket, valamint a kormányzati és piaci elektronikus szolgáltatásokat."

Magyarország 2020-ban kiadott **Nemzeti Biztonsági Stratégiájának** bevezető része rögzíti, hogy általános jelenség a felhasználók információbiztonsági tudatosságának alacsony szintje, „holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme".[183]

A **Nemzeti Digitalizációs Stratégia 2022-2030** átfogó céljainak megvalósítása érdekében, a digitális kompetencia pillér tekintetében alapvető célként határozza meg a munkavállalók digitális jártasságának folyamatos fejlesztését a digitálisan felkészült munkavállalók arányának növelése érdekében.[184]

A 2025-ben hatályba lépő **Kibertv.**, valamint a 7/2024 MK rendelet is kiemelt figyelmet szentel a tudatosításnak. A Kibertv. értelmében „a szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak kiberbiztonsági képzéséről, továbbképzéséről;".[185]
A **7/2024 MK rendelet** 2. mellékletét képző Védelmi intézkedések katalógusa önálló követelménycsaládként jeleníti meg a „Tudatosság és képzés" területét, melyben részletszabályokat fogalmaz meg a biztonságtudatossági, valamint a szerepkör-alapú képzésre vonatkozóan, melyek megvalósítása már alap biztonsági osztály esetében is kötelező. A képzést minden, a szervezet rendszereit használó munkatárs számára

[183] A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 32. pont
[184] Nemzeti Digitalizációs Stratégia 2022-2030, p. 89.
[185] Kibertv. tervezete 6.§ (5) a)

biztosítania kell, beleértve a vezetőket és a felső vezetőket, valamint a szerződéses partnereket is. A képzésbe integrálni szükséges a biztonsági eseményekből levont tanulságokat.

A 2015. október 1-jén alakult, Nemzetbiztonsági Szakszolgálat irányítása alatt működő **Nemzeti Kibervédelmi Intézetnek** (továbbiakban: NKI) kiemelkedő szerepe van az információbiztonság-tudatosság növelésében. Tevékenysége számos réteget céloz: a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését) és a felhasználókat, akiket pedig meg kell tanítani az internet és az információs technológiák biztonságos használatára, a saját és a rájuk bízott adatok felelős és szakszerű kezelésére. Az NKI szakmai anyagokat és útmutatókat tesz közzé, oktatási vagy képzési tevékenységet folytat, valamint a médiában megjelenő tudatosítási kampányokkal segíti a cél elérését.[186]

A biztonságtudatossággal és tudatosítással foglalkozó hazai jogszabályokat áttekintve kijelenthető, hogy Magyarország élen jár e terület szabályozásában és nem csak elvi szintű állásfoglalásokat fogalmaznak meg, hanem gyakorlati kötelezettségeket is meghatároznak az érintett szervek számára.

Jelen kutatás e stratégiai, jogszabályokban és egyéb dokumentumokban megfogalmazott célok megvalósítását kívánja elősegíteni –hiánypótló módon- a közszolgálatban dolgozók kiberbiztonsági feladatai, és az ellátásukhoz szükséges készségek, ismeretek és kompetenciák meghatározásával.

5.3. A KÖZSZOLGÁLATBAN DOLGOZÓK KIBERBIZTONSÁGI FELADATAINAK MEGHATÁROZÁSA AZ ECSF PROFILOK SEGÍTSÉGÉVEL

A Jegyző és Közigazgatás folyóiratban megjelent tanulmányomban (Legárd, 2023c) az Európai Készség-keretrendszer (ECSF), valamint az Európai e-Kompetencia Keretrendszer (e-CF) segítségével azonosításra kerültek az IBF-nek az Ibtv.-ben meghatározott feladatai, a végrehajtáshoz szükséges készségekkel, ismeretekkel és kompetenciákkal együtt.

[186] https://nki.gov.hu/intezet/tartalom/szolgaltatasok/ (Letöltve: 2020. 10.31.)

Jelen fejezetben a korábban, az IBF szerepprofil részeként azonosított elemekből kiindulva meghatározom a közszolgálati dolgozók kiberbiztonsággal kapcsolatos feladatait, valamint az ellátásukhoz szükséges készségeket, ismereteket és kompetenciákat. A dokumentumelemzés eredményeit a Függelék 2. mellékletében található táblázatok mutatják be.

A feladatok meghatározására az IBF-nek az Ibtv. alapján azonosított kilenc feladatcsoportja szerint került sor:

1. Jogszabályokkal való összhang megteremtése és fenntartása
2. Szabályozás / Véleményezés
3. Tudatosítás
4. Kockázatkezelés
5. Biztonsági események kezelése
6. Ellenőrzés / Audit
7. Tájékoztatás / Jelentés (vezetés, érintettek)
8. Kapcsolattartás
9. Egyéb feladatok

Az IBF ECSF-ben azonosított feladatai közül a táblázatokban kizárólag azokat szerepeltetem („IBF” oszlop), amelyek a közszolgálati dolgozók mindennapi feladatellátása szempontjából relevánsnak számítanak. A közszolgálati dolgozók szempontjából így azok a feladatok és a hozzá kapcsolódó készégek, ismeretek és kompetenciák kerülnek meghatározásra, amelyek az IBF feladatai szervezeti szintű végrehajtásához kapcsolódnak, ugyanakkor értelmezhetők és figyelembe veendők a közszolgálati dolgozók munkavégzése során. Ugyanakkor a közszolgálati dolgozókra vonatkozóan, az adott feladat kapcsán azonosított elemeket kiegészíteni szükséges további olyan specifikus elemekkel, amelyek a hazai jogszabályokkal való összhang megteremtését célozzák, és a közszolgálati dolgozók számára nélkülözhetetlenek a kiberbiztonsággal kapcsolatos feladatok ellátása, valamint a szervezeti szintű kiberbiztonság megteremtése szempontjából. (A kiegészítések piros színnel kerültek megjelölésre a táblázatban.)

A táblázatokból levonható következtetések:

A „jogszabályokkal való összehang megteremtése” keretében a jogszabályoknak, valamint a szervezetszabályozó eszközöknek való megfelelés biztosítása minden közszolgálti dolgozó alapvető és általános feladata, ez alól a kiberbiztonsággal kapcsolatos szabályok sem kivételek. Természetesen ennek ellátásához képesnek kell lenni a vonatkozó jogszabályok és szabályzatok megértésére és alkalmazására. Tekintettel arra, hogy a kiberbiztonság egy kevéssé ismert szakterület, fejleszteni javasolt ezen a területen a munkatársak alapvető ismereteit is. Megfelelő ismeretek és képesség birtokában a munkatárs részt tud venni szervezeti szinten a rendszerek és a bennük tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, valamint az információbiztonságnak a szervezeti kultúrába történő beillesztésében.

A „szabályozás/véleményezés” feladata kapcsán a közszolgálati dolgozónak általában nincsen a különböző kiberbiztonsági jogszabályok, szabályzatok kidolgozásával kapcsolatos feladata, ugyanakkor bizonyos szakterületeken ezekkel kapcsolatos véleményezési jogkör felmerülhet. Azonban a legtöbb közszolgálati dolgozónak csupán az előző pontban bemutatott végrehajtással és megfeleléssel kapcsolatos feladatokat kell ellátnia.

A „tudatosítás” egy olyan központi terület, amelyben minden munkatársnak aktívan szerepet kell vállalnia, a tudatosító programban történő részvétele és a követelmények teljesítése kulcsfontosságú és egyben kötelező is! E területhez kapcsolódó ismeretek tekintetében, az előző pontokban megjelölt ismeretanyagon kívül el kell sajátítani a lehetséges támadási és védekezési alternatívákat, a munkakör ellátásához szükséges kiberbiztonsági eljárásokat, technikákat, a vonatkozó ajánlásokat és szabványokat.

A „kockázatkezelés” szintén egy olyan feladat, amelyben minden munkatársnak ki kell vennie a részét a szervezetben. Bár a kockázatok feltérképezése, értékelése és kezelése alapvetően vezetői hatáskörbe tartozik, ugyanakkor az adott feladat ellátását – természetesen- ügyintézői szinten ismerik a legjobban, így a kockázatkezelés egyes lépései nem nélkülözhetik az ő közreműködésüket. Ehhez mindenképpen szükséges a kiberbiztonsági problémák azonosításának, a kockázatok értékelésének, valamint a kockázatcsökkentő intézkedések megértésének és végrehajtásának képessége. A vezetők

esetében kiemelten fontos a kockázatokra vonatkozó információkkal alátámasztott döntéshozás képessége. E szakterülettel kapcsolatban megfelelő ismeretek szükségesek a kiberbiztonsági kockázatokról, a kiberfenyegetésekről, és a rendszerek sebezhetőségéről, valamint a kockázatkezelés folyamatáról és abban betöltött szerepekről. Amennyiben a munkatárs rendelkezik az említett képességekkel és ismeretekkel, képes lesz megérteni és alkalmazni a kockázatkezelés elveit, részt venni az IBSZ-ben meghatározott, kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében.

A „biztonsági események kezelése" alapvetően az IBF feladata, ugyanakkor amennyiben egy munkatárs érintett egy incidensben, akkor –szükség szerint- részt kell vennie az incidenskezelési eljárásban is. Ugyanakkor a megelőzésben is óriási szerepe van az átlagfelhasználóknak, hiszen azonosítania és jelentenie kell az IBF-nek a kiberbiztonsági incidenst vagy annak gyanúját, és részt kell vállalnia az felmerülő károk enyhítésében is. Ehhez természetesen megfelelő ismeretekkel kell rendelkezni a kibertámadási formák és a számítógépes rendszerek sebezhetősége területén. illetve képesnek kell lennie az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatok ellátására, valamint a problémák és hibák segítséggel történő elhárítására.

Az „ellenőrzés/audit" lefolytatása alapvetően nem a munkatársak, hanem az IBF, vagy egy megbízott, harmadik személy feladata. Ugyanakkor, amennyiben a szakterület érintett egy kiberbiztonsági belső, vagy hatósági ellenőrzésben, akkor a munkatársaknak együtt kell működniük az ellenőrzést végző személyekkel, melynek során át kell adniuk a szükséges információkat, adatokat, dokumentumokat. Ezek a feladatok elsősorban az önálló szervezeti egység vezetőket terhelik, így nekik alapszinten ismerniük kell a kiberbiztonsági ellenőrzésekhez kapcsolódó auditálási módszertanokat és keretrendszereket, a szükséges tanúsítványok követelményrendszerét, valamint képesnek kell lenniük a felsorolt ismeretek feladatkörhöz kapcsolódó alkalmazására, az ellenőrzési jelentések elkészítésére vagy az abban való részvételre. Ennél a területnél már releváns lesz egy speciális, kizárólag vezető szerepkörben értelmezhető kompetencia is: számot kell tudnia adni „saját és mások tevékenységéről korlátozott számú érintett irányítása során."

A „tájékoztatás/jelentés (vezetés, érintettek)” terület kapcsán az átlagfelhasználóknak gyakorlatilag széleskörű együttműködést kell végrehajtania az IBF-fel, melynek keretében be kell jelenteni az IBF-nek az észlelt biztonsági eseményt vagy annak gyanúját, valamint az azonosított kockázatot, illetve be kell vonnia az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, azok folyamataiba. A kiberbiztonsággal kapcsolatos intézkedések során szorosan együtt kell működnie az IBF-fel, illetve az üzemeltetést végző informatikusokkal. A feladatok ellátásához –a megfelelő kommunikációs képességeken kívül- szükség van arra is, hogy az üzleti igények kiberbiztonsági vonatkozásai is megfogalmazásra és megfelelően továbbításra kerüljenek. Az ismeretek ezen a területen a korábbiakban bemutatott ismeretanyagokra épülnek, speciális tudást nem igényelnek. Megfelelő ismeretek és képességek birtokában a munkatárs képes lesz részt venni az Információbiztonsági Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában.

A „kapcsolattartás” témaköre az átlagfelhasználók szintjén szorosan kapcsolódik a „tájékoztatás/jelentés”, valamint az „ellenőrzés/audit” területekhez, ugyanakkor egy elemmel, a hatóságokkal történő kapcsolattartással és a részükre történő információ-megosztással egészült ki. Ez utóbbi lehetősége természetesen egyedi eset, legtöbbször kiberbiztonsági incidens esetén fordulhat elő az NBSZ NKI-val, mint hatósággal történő kommunikáció során. Éppen ezért -kizárólag az alapvető ismeretekre koncentrálva- szükséges megismerni az elektronikus információs rendszerek biztonsága felügyeletének, valamint az incidenskezelésnek a hazai szervezeti rendszerét.

Az „Egyéb feladatok és a hozzá kapcsolódó ismeretek, képességek, kompetenciák” kategóriába került be minden olyan feladat, amelyet más területhez nem lehetett besorolni, mégis fontos az átlagfelhasználó szempontjából. Ide került többek között a feladatkörhöz kapcsolódó kiberbiztonsági megoldások integrálása és a megfelelő működés biztosítása, valamint a rendszerek, szolgáltatások frissítése. Természetesen ehhez a kiberbiztonsággal kapcsolatos technológiák és megoldások megfelelő ismerete, az alkalmazás képessége, az etikai követelmények és szabványok megértése, gyakorlása és betartása is szükséges. Fontos kompetenciaként jelent meg az üzleti folyamatok és a kapcsolódó információs követelmények elemzése, és az IBF-vel együttműködve a legmegfelelőbb információs struktúra biztosítása.

Az ECSF-ben, a kiberbiztonsághoz szorosan nem kapcsolódó, úgynevezett puha készségek is megjelentek a szerepprofilok részeként, melyek közül néhány az átlagfelhasználó esetében is szükséges a kiberbiztonsággal kapcsolatos feladatok ellátásához, melyek az alábbiak:

- a munkatársak motiválása és ösztönzése,
- a nyomás alatti munkavégzés,
- az etikai követelmények és szabványok megértése, gyakorlása és betartása,
- együttműködés más csapattagokkal és kollégákkal,
- a belső és külső érdekelt felekkel történő kommunikáció, koordináció és együttműködés,
- az összetett problémák és biztonsági kihívások alapszintű elemzése és megoldása.

A Függelék 2. mellékletében bemutatott táblázatok, valamint a fentebb ismertetett elemzés segítségével bebizonyítottam, hogy a közszolgálatban dolgozók szervezeti szinten értelmezhető kiberbiztonsági feladatai, valamint az ellátásukhoz szükséges készségek, ismeretek és kompetenciák levezethetők és azonosíthatók az IBF Európai Kiberbiztonsági Készség-keretrendszer (ECSF) segítségével meghatározott feladataiból, ezzel bizonyítva a H3-1. alhipotézist.

5.4. A KÖZSZOLGÁLATI „SZEREPPROFIL” KIEGÉSZÍTÉSE A DIGITÁLIS KOMPETENCIA KERETRENDSZERREL, A DIGCOMP-PAL[187]

A közszolgálati „szerepprofil” egyes elemeinek azonosítása során az Európai Kiberbiztonsági Készség-keretrendszert (ECSF) és az által alkalmazott Európai e-Kompetencia Keretrendszert (e-CF) használtam a kompetenciák meghatározására, azonban már az elemzés során egyértelművé vált, hogy az e-CF alkalmazása nem kiberbiztonsághoz kapcsolódó munkakörre nehezen, illetve bizonyos feladatok esetén egyáltalán nem alkalmazható. Annak érdekében, hogy a közszolgálati „szerepprofil” további elemekkel kerüljön kiegészítésre, megvizsgáltam a korábbi kutatásom eredményeként azonosított és

[187] DIGITÁLIS KOMPETENCIA Keretrendszer (DIGCOMP) https://dpmk.hu/wp-content/uploads/2019/07/DigComp2.1_forditas_6_20200130.pdf (Letöltve: 2022.04.20.)

elemzett kiberbiztonsággal foglalkozó keretrendszereket (Legárd, 2022a), hogy melyek nyújthatnak segítséget a közszolgálati dolgozók kompetenciái tekintetében.

Az összehasonlító elemzés eredményeként, a közszolgálati profil szempontjából jó gyakorlatként történő alkalmazhatóság tekintetében az alábbi megállapításokat tettem:

Az európai DigComp 2.2. mintájára kidolgozott **hazai Állampolgári digitális kompetencia-keret (DigComp 2.1.)** jelentős előrelépést biztosít az átlagfelhasználók, így a közigazgatásban dolgozók digitális és annak részeként, a biztonsághoz kapcsolódó kompetenciái meghatározása terén, ugyanakkor a keretrendszer önmagában történő alkalmazása nem elegendő, hiszen nem ad információt a közszolgálati dolgozók mindennapi kiberbiztonság-kapcsolódású feladatairól és a végrehajtásukhoz szükséges ismeretekről, készségekről. A DigComp jó gyakorlatként történő alkalmazása a közszolgálati „szerepprofil" kidolgozása szempontjából csupán **kiegészítő jelleggel bír**.

A **Közszolgálati digitális kompetencia referenciakeret** már sokkal részletesebben és közigazgatás-specifikusan határozza meg az átlagfelhasználók kompetenciáit a „Biztonság, védelem és felelősség" területen, ugyanakkor nem azonosítja a kompetenciák alapjaként szolgáló ismereteket, készségeket és képességeket. Mivel a Referenciakeret kidolgozása, pontosítása még folyamatban van, annak közszolgálati profilban történő alkalmazása a **jövőben további kutatási célként** fogalmazható meg.

A **CyBok** (The Cyber Security Body of Knowledge), illetve a **European Cybersecurity Taxonomy** a kiberbiztonság tudásterületeit azonosítja, azonban nem foglalkoznak az alkalmazáshoz szükséges készségekkel, kompetenciákkal. E két keretrendszernek a szükséges ismeretanyagok későbbi részletes kidolgozása során lehet szerepe, azonban a disszertációnak kizárólag a feladatellátáshoz szükséges ismeretanyag, készségek és kompetenciák azonosítása a célja, a képzési anyagok bővebb meghatározása nem képzi a vizsgálat tárgyát. A jövőben, mintegy a disszertáció folytatásként ugyanakkor vizsgálandó e terület is.

A **Horizont 2020 projektek (CONCORDIA, ECHO Cyberskills Framework, SPARTA, CyberSec4Europe)** speciális készségek megállapítását tűzték ki célul, több

esetben egy-egy sajátos szakterületre (pl. közlekedés) fókuszálva, és az azonosított készségek a kiberbiztonsági tanfolyamok, tantervek fejlesztésére, valamint azok oktatási célú felhasználására koncentráltak. E projektek nem azonosíthatók a kitűzött kutatási célok szempontjából jó gyakorlatként.

Az **ESCO** (European Skills, Competences, Qualifications and Occupations) keretrendszerét áttekintve megállapítható, hogy bár széleskörűen, az ISCO nemzetközi szabványa szerint határozza meg a foglalkozásokat és a hozzá kapcsolódó tudást, készségeket és kompetenciákat, azonban a közszolgálati tisztviselők tekintetében (ESCO kategóriák szerint: 1112 –országos közigazgatási vezetők / igazgatásszervező, 2422 – közigazgatási ügyintéző, köztisztviselő, politikai szakértő, 335 – közhivatali ügyintéző) egyáltalán nem határoz meg kiberbiztonsághoz kapcsolódó ismereteket, készségeket és kompetenciákat.

Az **Európai e-Kompetencia Keretrendszer** (**e-CF) 3.0-s verziója** egy magasan absztrakt szintű készségmátrixot tartalmaz, amelyben a kiberbiztonság csak az egyik összetevő, és a keretrendszer kizárólag a kiberbiztonsági munkaerőhöz kapcsolható kompetenciákat azonosítja a releváns jártassági szinten. Az e-CF a közszolgálatban dolgozó, nem kiberbiztonsági munkakört ellátó személy számára szükséges ismeretanyagról, készségekről, valamint kompetenciákról hiányosan nyújt információt.

Az amerikai **NICE keretrendszer** (National Initiative for Cybersecurity Education) megfelelő kiindulási alap lehetne egy hazai közszolgálati „szerepprofil” szempontjából, hiszen az általa azonosított kiberbiztonsági szerepkörök vonatkozásában pontosan meghatározza a szükséges ismereteket, készségeket és képességeket. Az átültetés nehézséget az képezi, hogy a felsorolt kiberbiztonsági szerepkörök a szakterület számára készültek, ráadásul ezek nem mindig igazodnak az EU igényeihez, jogszabályaihoz és éppen ezért nehezen összeegyeztethetők az európai egyéb keretrendszerekkel. A NICE-hez felépítésében és gondolatmenetében nagyon hasonló ECSF keretrendszer átültethetőség szempontjából inkább megfeleltethető jó gyakorlatnak, és értelemezhető a magyar közigazgatási környezetben is.

Az **Európai Kiberbiztonsági Készség-keretrendszer** (European Cybersecurity Skills Framework – **ECSF**) az általa azonosított kiberbiztonsági szerepkörök vonatkozásában

meghatározza a feladatellátáshoz szükséges ismereteket, készségeket és kompetenciákat is, ez utóbbit a szintén elemzett **European e-Competence Framework (e-CF)** segítségével teszi, biztosítva ezzel a két európai keretrendszer közti átjárhatóságot is. Az ECSF ugyan kiberbiztonsági munkakörökből indul ki, így tehát nem az átlagfelhasználó számára készült, ugyanakkor –ahogy az előző részben bemutatásra került-, segítségével jól azonosíthatók egy közigazgatásban dolgozó átlagfelhasználó számára is a mindennapi munkavégzéshez kapcsolódó kiberbiztonsági feladatok, illetve a keretrendszer segítségével a szükséges ismeretek, készségek és kompetenciák is. Az ECSF moduláris felépítése alkalmassá teszi, hogy a szerepprofilokban azonosításra kerülő elemek rugalmasan átültethetők legyenek a magyar közigazgatási környezetbe, egy átlagfelhasználó számára is. Alkalmazásával, az általam kidolgozott közszolgálati „szerepprofil" szervesen beilleszthető az európai keretrendszerek által alkalmazott „közös nyelvi" környezetbe, és a segítségével meghatározásra kerülő ismeretek, készségek és kompetenciák biztosítják a más európai országokkal történő átjárhatóságot is.

Az összehasonlítás eredményét a 19. táblázat mutatja be.

Keretrendszerek	Jó gyakorlatként alkalmazása a közszolgálati „szerepprofil" kidolgozásához	Átültethető elemek a magyar közigazgatási környezetbe
DigComp 2.2.	✓	Kompetenciák a „Biztonság" területről
Közszolgálati Referenciakeret	-	-
NICE	-	-
CyBok	-	-
e-CF	✓	Kompetenciák
ESCO	-	-
European Cybersecurity Taxonomy	-	-
ECSF	✓	Feladatok Ismeretek Készségek Kompetenciák
Horizont 2020 projektek	-	-

19. táblázat: Keretrendszerek jó gyakolatként történő azonosítása (forrás: saját szerkesztés)

Mivel a DigComp, az Európai Bizottság tudományos és ismeretterjesztő szolgálata, a Közös Kutatóközpont (JRC) által indított projekt, amely kifejezetten a nem kiberbiztonsággal foglalkozó átlagfelhasználók kompetenciáit hivatott meghatározni, így megvizsgáltam annak lehetőségét, hogy a európai DigComp 2.2. mintájára kidolgozott hazai Állampolgári digitális kompetencia-keret (DigComp 2.1.) alkalmas lehet-e a közszolgálatban dolgozó átlagfelhasználó kompetenciáinak meghatározására is.
A vizsgálat érdekében először azonosítottam a DigComp kiberbiztonsággal összekapcsolható kompetenciaterületét, illetve a hozzá kapcsolódó kompetenciákat, majd meghatároztam a kompetenciák esetén azokat a releváns jártassági szinteket, amelyek a közszolgálati környezetben értelmezhetők.

Kompetenciaterület:
A DigComp egyetlen kiberbiztonsággal összekapcsolható kompetenciaterülete, a „Biztonság", amely **négy kompetenciát** foglal magában:

1. Eszközök védelme,
2. A személyes adatok és a magánélet védelme,
3. Az egészség és a jóllét védelme,
4. Környezetvédelem.

A felsorolt négy kompetenciából az első három esetében mutatható ki kiberbiztonsággal kapcsolat, így a negyedik, tehát a „Környezetvédelem" kompetenciájának elemzése nem képezi jelen vizsgálat tárgyát.

Mindhárom kompetencia négy jártassági szinten és szintenként két-két, tehát összesen nyolc tudásszinten értelmezhető. Az Alap-, illetve Középszinthez tartozó első négy tudásszint csupán a kompetenciák megértését biztosítják, az alkalmazás és értékelés kognitív területe a Haladó szinthez tartozó 5., illetve 6. tudásszinthez kapcsolódik. Tekintettel arra, hogy biztonságtudatosság fogalmi eleme az ismeretek alkalmazásának képessége is, így az 5. tudásszinttől vehetők figyelembe a meghatározott kompetenciák. Ugyanakkor a Mesterszinthez kapcsolódó 7. és 8. tudásszint már a létrehozás kognitív területét feltételezik, amely alapján képes az átlagfelhasználó választani a komplex problémák adott megoldási lehetőségei közül, illetve rendkívül összetett, sok tényező által befolyásolt problémák önálló megoldására képes, amely azonban szervezeti környezetben nem, vagy nagyon ritka esetben értelmezhetők. Egy közszolgálati szervezetnél az összetett,

elektronikus információbiztonsághoz kapcsolódó problémák esetében a választás, illetve a megoldáshoz vezető szakmai döntés a szervezet vezetője és/vagy az IBF feladata, így a tudatosító programnak nem kell kiterjednie e Mesterszinthez kapcsolódó kompetenciák kialakítására, elsődlegesen a Haladószinthez kapcsolódó kompetenciák kialakítása a cél.

Az alábbi táblázatokban elemzésre kerül, hogy az egyes kompetenciákhoz kapcsolódó Haladó szintű képességek mely elemei és milyen szinten relevánsak, és azok hogyan kapcsolódnak a korábbiakban meghatározott közszolgálati „szerepprofilhoz".

1. Az „eszközök védelme" kompetencia

Haladó szintű (5. vagy 6. tudásszint), releváns képességek *„Akár másokat is segítve képes vagyok" (5)* vagy *„Haladó szinten, saját igényeim és mások igényei szerint, komplex helyzetekben képes vagyok"(6):*	**Közszolgálati „szerepprofilba" illesztés**
különböző módszereket alkalmazni eszközeim és digitális tartalmaim megóvására, (5)	**9. Egyéb feladatok, ismeretek, képességek, kompetenciák**
megkülönböztetni a kockázatokat és veszélyeket digitális környezetben, (6)	**4. Kockázatkezelés** **5. Biztonsági események kezelése**
biztonsági intézkedéseket alkalmazni, (5)	**1. Jogszabályokkal való összhang megteremtése és fenntartása** **5. Biztonsági események kezelése**
értékelni a legmegfelelőbb módszereket, amelyekkel kellő mértékben figyelembe lehet venni a megbízhatósági és adatvédelemi szempontokat. (6)	**4. Kockázatkezelés**

20. táblázat: DigComp - Az „eszközök védelme" kompetencia azonosítása a Közszolgálati szerepprofilban (forrás: saját szerkesztés)

2. A „személyes adatok és a magánélet védelme" kompetencia

Haladó szintű (6. tudásszint), releváns képességek *„Haladó szinten, saját igényeim és mások igényei szerint, komplex helyzetekben képes vagyok"(6):*	**Közszolgálati „szerepprofilba" illesztés**
kiválasztani a megfelelőbb módszereket a személyes adatok és a magánélet megóvására digitális környezetben, (6)	**4. Kockázatkezelés**
értékelni a legmegfelelőbb módszereket arra, hogyan lehet felhasználni és megosztani személyazonosításra alkalmas adatokat úgy, hogy közben megvédem magamat és másokat a nem megfelelő adatkezeléssel kapcsolatos, lehetséges károktól, (6)	**4. Kockázatkezelés**
értékelni az adatvédelmi nyilatkozatok megfelelőségét a személyes adatok felhasználásával kapcsolatban. (6)	**4. Kockázatkezelés**

21. táblázat: DigComp - A „személyes adatok és a magánélet védelme" kompetencia azonosítása a Közszolgálati szerepprofilban (forrás: saját szerkesztés)

3. Az „egészség és a jóllét védelme" kompetencia

Haladó szintű (6. tudásszint), releváns képességek *„Haladó szinten, saját igényeim és mások igényei szerint, komplex helyzetekben képes vagyok”(6):*	**Közszolgálati „szerepprofilba” illesztés**
megkülönböztetni a legmegfelelőbb módszereket, amelyekkel elkerülhetők a digitális technológiák használata során felmerülő, az egészségre, illetve a fizikai és pszichológiai jóllétre veszélyt jelentő kockázatok, (6)	**4. Kockázatkezelés**
adaptálni a legmegfelelőbb módszereket, amelyekkel megvédhetem magamat és másokat digitális környezetben, (6)	**5. Biztonsági események kezelése**
a célnak megfelelően kiválasztani a társadalmi jóllétet és befogadást elősegítő digitális technológiákat. (6)	**9. Egyéb feladatok, ismeretek, képességek, kompetenciák**

22. táblázat: DigComp - Az „egészség és a jóllét védelme” kompetencia azonosítása a Közszolgálati „szerepprofilban” (forrás: saját szerkesztés)

Részkövetkeztetések:

Az elemzésből kiderül, hogy a DigComp-ban meghatározott egyes kompetenciáknak és képességeknek helyük van az ECSF segítségével meghatározott közszolgálati „szerepprofilban”, annak hasznos kiegészítését, árnyalását jelentik. A „kockázatkezelés” további hat kompetenciával bővíthető az átlagfelhasználók tekintetében, amelyek érintik az eszközök, valamint a személyes adatok és a magánélet védelme, illetve az egészség és a jóllét védelme területeken alkalmazható, legmegfelelőbb védekezési módszerek ismeretét és alkalmazását. A „biztonsági események kezelése” további három kompetenciával gazdagítható, amelyek az eszközök, valamint az egészség és a jóllét védelme területeket érintik. Ez utóbbi kompetenciák elsősorban a megelőzésre, így a veszélyek felismerésére, a leghatékonyabb védelmi módszerek és biztonsági intézkedések ismeretére és adaptációjára épülnek. További fontos elemként kerülhet be a közszolgálati dolgozók kompetenciái közé, hogy az illető képes saját és mások igényei szerint, komplex helyzetekben a célnak megfelelően kiválasztani a társadalmi jóllétet és befogadást elősegítő digitális technológiákat.

Az ismertetett dokumentumelemzés segítségével bebizonyítottam, hogy az ECSF segítségével meghatározott ismerethalmazok kiegészítése indokolt további, átlagfelhasználó-specifikus elemekkel annak érdekében, hogy pontosan definiálni tudjuk a nem kiberbiztonsági munkakörökhöz kapcsolódó kiberbiztonsági feladatok ellátását támogató ismereteket, készségeket és kompetenciákat (H3-2. alhipotézis).

5.5. KÖZSZOLGÁLATI KIBERBIZTONSÁGI „SZEREPPROFIL”

Az előző részekben bemutatott vizsgálatok segítségével bebizonyítottam, hogy az Ibtv.-ből levezethető kiberbiztonsági feladatok alapján, az Európai Kiberbiztonsági Készség-keretrendszer (ECSF) és az Európai e-Kompetencia Keretrendszer (e-CF) bázisán, a DigComp 2.2. keretrendszerrel kiegészítve a közszolgálati átlagfelhasználó számára meghatározhatók a mindennapi munkavégzéshez kapcsolódó kiberbiztonsági feladatok és az ellátásukhoz szükséges kulcs készségek, ismeretek és kompetenciák, tehát bizonyítást nyert a H3 hipotézis.

Megállapításaimat egy ún. közszolgálati kiberbiztonsági „szerepprofilban” összegeztem. Az idézőjeles „szerepprofil” -nevével ellentétben- nem egy adott munkakörhöz köthető (mint az ECSF-ben található szerepprofilok, vagy az IBF szerepprofil), hanem munkakörtől és betöltött pozíciótól függetlenül valamennyi átlagfelhasználónak szól, aki a meghatározott közigazgatási szervezetnél lát el, nem kiberbiztonsággal kapcsolatos feladatokat.

Az előző részekben ismertetett kutatási lépésekben, valamint a Függelék 2. mellékletében bemutatott táblázatokban előforduló ismétlődések kiküszöbölése, az ismeretek rendszerezése, valamint a felsorolt elemek összefoglalása érdekében az alábbi táblázatban összesítettettem a vizsgálatom eredményeként definiált „szerepprofilt”:

KÖZSZOLGÁLATI KIBERBIZTONSÁGI „SZEREPPROFIL”
Fő feladatok
– Biztosítja a munkaköréhez kapcsolódóan a kiberbiztonsággal kapcsolatos szabványoknak, törvényeknek és rendeleteknek, illetve szervezetszabályozó eszközöknek való megfelelést.
– Részt vesz a feladatköréhez kapcsolódóan a szervezet kiberbiztonsága jövőképét, stratégiáját és politikáját meghatározó dokumentumok végrehajtásában.
– Részt vesz az Informatikai Biztonsági Szabályzat végrehajtásában.
– Részt vesz a feladatkörét érintő kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.
– Részt vesz a kiberbiztonsággal kapcsolatos tudatosságnövelő programokon, az előírt

követelményeket teljesíti.

- Részt vesz a feladatköréhez kapcsolódóan a kockázatkezelés folyamatában.
- Részt vesz az IBF által azonosított kockázatok értékelésében, valamint a kockázatkezelésben (a kockázatra adott válaszlépések meghatározásában, a kockázatcsökkentő intézkedések végrehajtásában).
- Részt vesz a szervezet belső szervezetszabályozó eszközeiben rögzített incidenskezelési eljárásban a feladatköréhez kapcsolódóan.
- Azonosítja és jelenti az IBF-nek a kiberbiztonsági eseményeket vagy annak gyanúját, részt vesz az esetleges károk enyhítésében.
- Kapcsolatot tart, bejelentést tesz, tájékoztatja az IBF-et az esetleges biztonsági eseményről vagy annak gyanújáról, a felmerülő kockázatokról, továbbá bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába.
- A kiberbiztonsággal kapcsolatos intézkedések során szorosan együttműködik az IBF-fel, illetve az üzemeltetést végző informatikusokkal.
- Indokolt esetben (pl. egy információbiztonsági incidens esetén) együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel.
- Részt vesz és/vagy együttműködik a kiberbiztonsági ellenőrzésekben.
- Együttműködik az ellenőrzések során a szükséges információk, adatok, dokumentumok átadásában.
- Integrálja a feladatkörhöz kapcsolódó kiberbiztonsági megoldásokat és biztosítja a megfelelő működésüket.
- Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát.
- Alkalmazza a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.

Kulcs készségek

- Képes a feladatai ellátása során alkalmazni a kiberbiztonságra vonatkozó jogi követelményeket, szervezetszabályozó eszközöket, valamint a vonatkozó ajánlásokat és bevált gyakorlatokat.
- Képes megérteni és feladatai ellátása során figyelembe venni a szervezeti célokat, jövő képet, a biztonsággal kapcsolatos politikát és stratégiát, a jogi, szabályozási és szabvány követelményeket.
- Képes részt venni a szervezet kiberbiztonsági jövőképének, stratégiájának, politikájának, valamint az Informatikai Biztonsági Szabályzatnak a feladatköréhez kapcsolódó végrehajtásában.
- Képes részt venni a feladatköréhez kapcsolódó, a szervezetszabályozó eszközöket és egyéb jogi követelményeket kiegészítő, megfelelő kiberbiztonsági irányelvek, eljárások és szabályok kidolgozásában és végrehajtásában.
- Képes részt venni a feladatkörét érintő, kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.
- Képes a jogi és szabályozási környezet, valamint a műszaki üzleti igények alapszintű megértésére és kommunikációjára.
- Képes az üzleti igények kiberbiztonsági vonatkozásai kommunikálására a felső vezetés és az IBF felé.
- Képes a biztonságtudatosító programokon való aktív részvételre, a tananyag elsajátítására és alkalmazására.

- Képes megfogalmazni az elsajátítandó ismeretekre, készségekre vonatkozó igényét.
- Képes a feladatköréhez kapcsolódóan a kiberbiztonsági problémák azonosítására, a kockázatok értékelésére, valamint a kockázatcsökkentő intézkedések megértésére és végrehajtására.
- Képes a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozni.
- Képes gyakorolni az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatokat.
- Képes a social engineering típusú támadásokat felismerni.
- Képes a problémák és hibák segítséggel történő elhárítására.
- Képes kommunikálni és kapcsolatot építeni az IBF-el, illetve az érdekelt felekkel, a feladatkörét érintő kiberbiztonsági kockázatok kezelése, illetve az incidensek megelőzése és kezelése érdekében.
- Képes jelentéseket kidolgozni, vagy az elkészítésükben közreműködni, valamint a jelentéseket megfelelően kommunikálni.
- Képes kommunikálni, koordinálni és együttműködni a belső és külső érintettekkel (pl. hatóságok, auditorok, alvállalkozók) a feladatkörét érintő, kiberbiztonság tárgyú vagy azzal kapcsolatos feladatok ellátása során.
- Képes részt venni és együttműködni a kiberbiztonsági tárgyú ellenőrzésekben.
- Képes részt venni az ellenőrzési jelentések elkészítésben.
- Képes az auditálási és megfelelőség-értékelési módszertanok, eszközök és technikák – feladatköréhez kapcsolódó- alkalmazására. (Kizárólag vezetői szerepben.)
- Képes a feladatköréhez kapcsolódóan a kiberbiztonsági ajánlások és legjobb gyakorlatok implementálására, valamint a kiberbiztonsági megoldások integrálására a szervezet infrastruktúrájába.
- Képes a feladatköréhez kapcsolódóan az etikai követelmények és szabványok megértésére, gyakorlására és betartására.
- Képes a szervezet kiberbiztonsági kultúrájának befolyásolására, a munkatársak motiválására és ösztönzésére.
- Képes a nyomás alatti munkavégzésre.
- Képes az érdekelt felek számára történő megfelelő kommunikációra, prezentációra és jelentéstételre.
- Képes együttműködni más csapattagokkal és kollégákkal.
- Képes a belső és külső érdekelt felekkel történő kommunikációra, koordinációra és együttműködésre.
- Képes az összetett problémák és biztonsági kihívások alapszintű elemzésére és megoldására.

Kulcs ismeretek

- Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete.
- Általános kiberbiztonsági ismeretek, szervezeti szinten az információbiztonsági előírások és stratégiák feladatkörhöz kapcsolódó ismerete.

- Az elektronikus információs rendszerek biztonságának felügyelete rendszerének, valamint az incidens-, illetve kockázatkezelésnek az alapszintű ismerete.
- A kockázatkezelés folyamatának és abban betöltött szerepének az alapszintű ismerete.
- A megfelelő biztonsági eljárások, követelmények, technikák, valamint ajánlások és szabványok feladatkörhöz kapcsolódó, a lehetséges támadási és védekezési alternatívák alapszintű ismerete.
- A potenciális kiberfenyegetések, kibertámadási formák és a számítógépes rendszerek sebezhetőségeinek alapszintű ismerete.
- A kiberbiztonsági ellenőrzések, auditálási szabványok, módszertanok és keretrendszerek feladatkörhöz kapcsolódó alapszintű ismerete. (Kizárólag vezetői szerepben.)
- Az auditálással és a kiberbiztonsággal kapcsolatos tanúsítások feladatkörhöz kapcsolódó, alapszintű ismerete.
- Kiberbiztonsággal kapcsolatos technológiák, megoldások és kontrollok feladatkörhöz kapcsolódó ismerete.
- Etikus kiberbiztonsági szervezeti követelmények.

E-kompetenciák

- Részt vesz az információs rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, valamint a vonatkozó jogi követelménynek való megfelelésben.
- Részt vesz az Információbiztonsági Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában.
- Részt vesz az információbiztonságnak a szervezet kultúrájába való beillesztése folyamatában.
- Részt vesz a tudatosító képzések során elsajátított ismeretek, készségek segítségével a biztonságtudatos szervezeti kultúra kialakításában, fenntartásában és kommunikálásában.
- Megérti és alkalmazza a kockázatkezelés elveit, részt vesz az IBSZ-ben meghatározott kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében a feladatköréhez kapcsolódóan.
- A kockázatokra vonatkozó információkkal alátámasztott megalapozott döntéseket hoz a feladatköréhez kapcsolódó kockázatok kezelése és mérséklése érdekében. (Kizárólag vezetői szerepben.)
- Különböző módszereket alkalmaz eszközei és digitális tartalmai megóvására.
- Értékeli a legmegfelelőbb módszereket, amelyekkel kellő mértékben figyelembe lehet venni a megbízhatósági és adatvédelemi szempontokat.
- Kiválasztja a megfelelőbb módszereket a személyes adatok és a magánélet megóvására digitális környezetben.
- Értékeli a legmegfelelőbb módszereket arra, hogyan lehet felhasználni és megosztani személyazonosításra alkalmas adatokat úgy, hogy közben megvédje önmagát és másokat a nem megfelelő adatkezeléssel kapcsolatos, lehetséges károktól.
- Értékeli az adatvédelmi nyilatkozatok megfelelőségét a személyes adatok felhasználásával kapcsolatban.
- Megkülönbözteti a legmegfelelőbb módszereket, amelyekkel elkerülhetők a digitális technológiák használata során felmerülő, az egészségre, illetve a fizikai és pszichológiai jóllétre veszélyt jelentő

kockázatok. – Adaptálja a legmegfelelőbb módszereket, amelyekkel megvédheti önmagát és másokat digitális környezetben. – Részt vesz a feladatköréhez kapcsolódó problémakezelési/incidenskezelési folyamatban, a károk enyhítése érdekében mindent megtesz, ami tőle az adott helyzetben elvárható. – Megkülönbözteti a kockázatokat és veszélyeket digitális környezetben. – Biztonsági intézkedéseket alkalmaz. – Feladatköréhez kapcsolódóan együttműködik az ellenőrzések során az ellenőrzést végző belső szervezeti egységgel vagy külső szervezettel/céggel, részt vesz az ellenőrzések során készült dokumentumok előállításában, véleményezésében. – Részt vesz a kiberbiztonság tárgyú vagy kapcsolódású jelentések, dokumentumok, feladatkörét érintő előállításában. – Egyszerű vizsgálatokat végez a részletes utasítások szigorú betartásával. – Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, valamint az IBF-vel együttműködve biztosítja a legmegfelelőbb információs struktúrát. – A célnak megfelelően kiválasztja a társadalmi jóllétet és befogadást elősegítő digitális technológiákat. – Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.) – Számot ad saját tevékenységéről.

23. táblázat: Közszolgálati „szerepprofil” (forrás: saját szerkesztés)

5.6. BIZONYÍTÁSI KÍSÉRLET: KÉRDŐÍVES VIZSGÁLAT

A következő részben bemutatott kérdőíves vizsgálat segítségével bizonyítási kísérletet tettem a közszolgálati „szerepprofil” elemeivel kapcsolatos szakértői attitűdök mérésére, valamint a kutatási eredményeim árnyalására, esetleges módosítására. A kérdőíves vizsgálatra az Ibtv.-ben foglalt feladatok címzettjei körében került sor.

A kutatás célja annak megállapítása volt, hogy a szakértők véleménye szerint egy közigazgatásban dolgozó átlagfelhasználónak az Ibtv.-ben meghatározott feladatok végrehajtása érdekében valóban a közszolgálati „szerepprofil” részeként megállapított kiberbiztonsági feladatokat kell-e végrehajtania a mindennapi munkavégzése során, és ehhez a „szerepprofilban” bemutatott készségekre, ismeretekre valamint kompetenciákra van-e szüksége.

A kérdőív lehetőséget teremt a kidolgozott „szerepprofil” egyes elemei kapcsán a szakértői vélemények mérésére, melynek segítségével megállapíthatom a „szerepprofil” egyes elemeinek megfelelőségét és alkalmazhatóságát, az eredmények figyelembevételével módosíthatom a „szerepprofil” elemeit, illetve azonosíthatom, hogy mely elemek kívánnak meg esetleg további vizsgálatokat.

5.6.1. A kérdőíves vizsgálat bemutatása

A kérdőív felépítése

Az általam szerkesztett kérdőív (Függelék – 3. sz. melléklet) bevezető részében kerül bemutatásra a kérdőív címe, a vizsgálat célja, valamint a kutatás háttere. A kérdőív érdemi része öt egységből áll:

I. Általános kérdések
II. Fő feladatok
III. Kulcs készségek
IV. Kulcs ismeretek
V. Kulcs kompetenciák

Az „I. Általános kérdések” rész nyílt, feleltválasztós zárt, illetve félig zárt kérdéseket foglal magában, mely a kitöltő által képviselt szervezetről, a kitöltő Ibtv.-ben foglalt feladatokhoz kapcsolódó szerepköréről, illetve a közszolgálati „szerepprofillal” kapcsolatos attitűdjéről nyújt információkat.

A II.-V. egységek a „szerepprofil” részek (feladatok, készségek, ismeretek, kompetenciák) egyes elemeivel kapcsolatos attitűdöt mérik Likert-skála segítségével.

A Likert-skála Rensis Likert amerikai pszichológus és szociológus nevéhez fűződik, aki 1932-ben a doktori értekezéséhez kapcsolódóan fejlesztette ki a két szélsőséges érték közötti mérési skálát, mely attitűd mérésére szolgál. A módszer lényege, hogy a kérdőívben szereplő állításokat „két szélsőséges végpont között kialakított skálán értékelnek”, melyek egyik végpontja az abszolút egyetértés, míg a másik a teljes elutasítása az állításnak. (Zerényi, 2016)

Annak érdekében, hogy meg tudjam állapítani, hogy a szakértők hogyan viszonyulnak a kidolgozott „szerepprofil” egyes elemeihez, azaz hogy egy közszolgálatban dolgozó átlagfelhasználó kiberbiztonsági „szerepprofiljának” mely feladatokat, készségeket,

ismereteket és kompetenciákat kell tartalmaznia, a vizsgálat során alkalmazott kérdőívben ötfokozatú skálát alkalmaztam, az alábbi megjelölésekkel: „rendkívüli mértékben egyetértek”, „eléggé egyetértek”, „közepes mértékben értek egyet”, „alig értek egyet” és „egyáltalán nem értek egyet”.

Próba

A kérdőív összeállítását követően, az esetleges hibák kiszűrése érdekében próbát végeztem, mely során a vizsgálandó populáció szempontjából releváns személyt kértem fel a kitöltésre. Az ő javaslatainak figyelembevételével, a kérdések felülvizsgálatával alakult ki a kérdőív végleges változata.

Az alapsokaság és a mintavételi eljárás meghatározása

Az alapsokaság (populáció)[188] meghatározása:

Az Ibtv.-ben foglalt feladatok címzettjei:

- a szervezet vezetője (Ibtv. 11.§),
- az elektronikus információs rendszer biztonságáért felelős személy (Ibtv. 13.§),
- az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (Ibtv. 13.§ (11)),
- egyéb, az Ibtv.-ben nevesített feladat ellátásában résztvevő személy.

Minta: „Mintának nevezzük a mérni, megkérdezni kívánt alapsokaságból kiválasztott egyedeket, akiket bevonunk a vizsgálatba.” (Hornyacsek 2014., p. 98.)

Az alapsokaságból a megfelelő minta biztosítása az alábbi mintavételi eljárással történt:

Az Ibtv. hatálya alá tartozó szervezetekről, valamint a szervezetek vezetője által kinevezett vagy megbízott elektronikus információs rendszer biztonságáért felelős személyről nyilvántartást az Ibtv. 15.§ (1) c) pontja alapján kijelölt hatóság, jelenleg a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet vezet. Az Ibtv. 15.§ 1) bekezdésben meghatározott nyilvántartásból - ha jogszabály eltérően nem rendelkezik - adattovábbítás kizárólag a 19. § (1) és (2) bekezdésében meghatározott eseménykezelő központok részére végezhető.

[188] Populáció: „Azon egyedek összessége, akikre vonatkozóan általánosításokat akarunk megfogalmazni a kutatás során.” In: Lengyelné Molnár Tünde–Tóvári Judit: Kutatásmódszertan, Eszterházy Károly Főiskola Médiainformatika Intézet Eger, 2001., p. 87. http://publikacio.uni-eszterhazy.hu/147/1/kutatasmodszertan_lengyeln%C3%A9_t%C3%B3v%C3%A1ri.pdf (Letöltve: 2023.09.25.)

Reprezentatív csak abban az esetben lesz a minta, „vagyis akkor fedi le a sokaság minden jellemzőjét, ha az eloszlása, rétegződése, főbb ismérvei stb. megegyeznek az alapsokaságéval” (Hornyacsek 2014., p. 98.). Mivel jelen vizsgálat során az alapsokaság minden jellemzője megismerését a törvény eleve kizárta, ezért a reprezentatív mintavétel és a véletlen mintavételi eljárás megvalósítása nem volt lehetséges.

Az alkalmazott nem véletlenszerű mintavétel során először koncentrált kiválasztást alkalmaztam annak érdekében, hogy a sokaságra legjellemzőbb egyedek kerüljenek a mintába. A sokaság tipikus és egyben legjellemzőbb eleme az elektronikus információs rendszer biztonságáért felelős személy (IBF), mivel az Ibtv.-ben, illetve a végrehajtási rendeleteiben foglalt feladatok jelentős, operatív részét ő látja el, neki van a legnagyobb tapasztalata a jogszabályban megfogalmazott információbiztonsági követelmények szervezeti szintű megvalósításában. E célcsoport elérése érdekében többnyire IBF-ket tömörítő levelező listán került továbbításra a kérdőív:

- EIVOK (Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztálya) levelező lista (több, mint 200 fő),
- ISACA Magyarországi Egyesület (a nemzetközi ISACA -Information Systems Audit and Control Association- magyarországi szakmai szervezete) levelező listája.

Emellett személyes megkeresés útján kértem fel IBF-ket, illetve a szervezet vezetőjeként jegyzőket a kérdőív kitöltésére.

Második lépésként hólabda-mintavételt alkalmaztam, így a megkérdezettek javaslatai alapján újabb személyek kerültek kiválasztásra.

A mintavétel kivitelezése

A mintavételre 2023. április 11. és 2023. május 12. között került sor.

A kérdőívet 27 fő töltötte ki, ebből az adattisztítást követően 26 db kérdőív került kiértékelésre.

Az adattisztítás során 1 db kérdőív került törlésre, mely esetében megállapítható volt, hogy a kitöltő szándéka nem a valós válaszadásra irányult.

Adatfeldolgozás

Az adattisztítást követően a válaszadóknak az egyes kérdésekre adott válaszát, kérdés csoportonként külön-külön táblázatban rögzítettem, melynek segítségével adatbázist hoztam létre, mely az összes válaszadó valamennyi válaszát magában foglalja.

Az adatok rendezését követően az adatelemzés következett leíró statisztikai eljárások segítségével Excel táblázatban.

Az **„I. Általános kérdések”** esetében a kérdésekre adott válaszok relatív gyakoriságának meghatározásával kerül bemutatásra, hogy a mintához, azaz az összelemszámhoz, mint száz százalékhoz képest, hogyan oszlanak meg az egyes csoportok között a minta elemei (mintára vetített hányad).

A **II-V. rész** esetében az alábbi eljárások kerültek alkalmazásra:

1. **Relatív gyakoriság**

Megállapításra került az **egyes kérdésekre adott válaszok gyakorisága és relatív gyakorisága**, tehát, hogy a vizsgált kérdésre adott válaszokhoz, mint százszázalékhoz képest, hány fő, illetve a válaszadók hány százaléka értett egyet rendkívüli mértékben, eléggé, közepes mértékben, alig, vagy egyáltalán nem a feltett kérdéssel.

2. **Medián**

Ahhoz, hogy felállítsak egy kritériumrendszert, amely szerint azonosítható, hogy mely elemet fogadunk el a „szerepprofil” részeként, illetve melyik az, amelyik esetében további vizsgálatok elvégzése szükséges, vagy teljesen mértékben elhagyható a profilból, először csoportokat képeztem a válaszadókból az alábbiak szerint:

1. **fenntartások nélkül egyetértők**: rendkívüli mértékben egyetért + eléggé egyetért,
2. **bizonytalan válaszadók:** közepes mértékben ért egyet,
3. **elutasítók:** alig ért egyet + egyáltalán nem ért egyet.

Ezt követően a II-V. rész tekintetében, a feladatok, a készségek, az ismeretek és a kompetenciák részterületek esetében külön-külön kiszámításra került az adott részterület valamennyi eleme figyelembevételével, összességében **a fenntartások nélkül egyetértők és a bizonytalan válaszadók mediánértéke** az alábbi képlet (Kövesi et al., 2013., pp. 54-55) segítségével:

$$\hat{Me} = X_{Me,0} + \frac{\frac{N}{2} - f'_{Me-1}}{f_{Me}} \cdot h_{Me},$$

ahol Me annak a legelső osztályköznek a sorszáma, melyre igaz hogy $f_{ME} \geq N/2$ és $X_{Me,0}$ az Me sorszámú osztályköz alsó határa, és a h_{Me} pedig ennek az osztálynak az osztályköz hosszúsága, ami egyszerűen a felső és alsó osztályhatár értékének a különbsége.
A medián a változó azon számértéke, amelynél az összes előforduló számérték fele kisebb, fele pedig nagyobb, tehát a rangsorba állított sokasági számértékeket két egyenlő gyakoriságú osztályra bontja.
A medián előnye, hogy mindig egyértelműen meghatározható, és mivel valódi középérték, így érzéketlen az adathalmazunkban szereplő szélsőértékekre, amely szélsőségesen nagy vagy kicsi értékeket általában a véletlen szeszélyei alakítják, és nem függ a többi ismérvértéktől sem. (Kövesi et al., 2013., p. 55)

A statisztikai módszer kiválasztása során átlagpróbát is végeztem a fenntartások nélkül egyetértők és a bizonytalan válaszadók viszonylatában. Az átlagpróbánál megállapításra került, hogy a szélsőértékeket rosszul kezeli, mivel olyan feladatelemek is elutasításra kerültek, melyek esetében a válaszadók összességében több mint a fele egyetértő és bizonytalan volt.

Ugyanakkor abban az esetben ha az adott állítással (szerepprofil elemmel) a válaszadók több, mint fele egyáltalán nem vagy alig éretett egyet, tehát **a relatív gyakorisága az elutasítóknak nagyobb, mint 50% volt**, melyből következik, hogy a fenntartások nélküliek és a bizonytalanok kumulatív relatív gyakorisága alacsonyabb volt, mint 50%, **az elem törlésre kerül a „szerepprofilból”**.

A bemutatott statisztikai módszerek segítségével az alábbi, kutatói döntéseket megalapozó kritériumrendszer került felállításra, ahol Me a medián érték, R pedig a relatív gyakoriság:

Kritériumok	Értelmezés	Kutatói döntés
Fenntartások nélkül ≥ Me	elfogadjuk	elfogadjuk a „szerepprofil” részeként
Bizonytalan < Me		
Elutasító < R 50%		
Fenntartások nélkül ≥ Me	elfogadjuk	elfogadjuk a „szerepprofil” részeként
Bizonytalan ≥ Me	vizsgáljuk	
Elutasító < R 50%		
Fenntartások nélkül < Me		további statisztikai vizsgálat szükséges
Bizonytalan ≥ Me	vizsgáljuk	
Elutasító < R50%		
Fenntartások nélkül < Me		nem fogadjuk el a „szerepprofil” részeként
Bizonytalan < Me		
Elutasító > R 50%	nem fogadjuk el	
Fenntartások nélkül < Me		további statisztikai vizsgálat szükséges
Bizonytalan < Me		
Elutasító < R 50%		

24. táblázat: Kérdőíves vizsgálat - kutatói döntéseket megalapozó kritériumrendszer (forrás: saját szerkesztés)

3. További statisztikai vizsgálatok

Azon profilelem esetében, ahol a fenntartások nélkül elfogadók, illetve a bizonytalanok mediánja, valamint az elutasítók relatív többsége alapján nem lehetett egyértelműen megállapítani, hogy elfogadható, vagy kizárható a „szerepprofilból” az adott elem, további statisztikai vizsgálatokat végeztem, mely során a fenntartások nélkül elfogadók, a bizonytalanok és az elutasítók arányait (kumulatív gyakoriságukat) vizsgáltam.

Ha a fenntartások nélkül elfogadók (rendkívüli mértékben egyet ért, eléggé egyet ért) és a bizonytalanok (közepes mértékben ért egyet) száma meghaladja a válaszadók 2/3-át, és az elutasítók (alig ért egyet, egyáltalán nem ért egyet) száma kevesebb, mint a válaszadók 1/3-a, a vizsgált elem a „szerepprofil” részét fogja képezni, ellenkező esetben további, későbbi vizsgálatok szükségesek. (Jelen disszertáció nem vizsgálja tovább a kérdéses elemeket, ez egy későbbi kutatási irányt jelenthet.)

A vizsgálat nehézségei

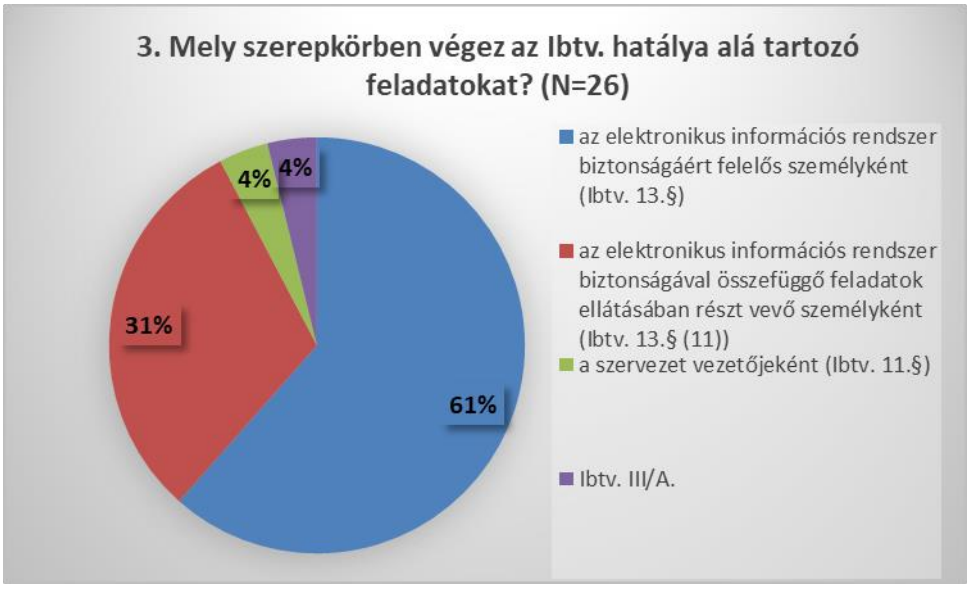
A kérdőíves vizsgálat kritikus pontja a mintavétel során az alacsony válaszadási hajlandóság volt. A levelező listákra elküldött kérdőív kitöltésében minimális számú fő vett részt, ehelyett a személyes megkeresések bizonyultak hatékonynak. A kérdőív első kérdésére adott válaszokból megállapítható, hogy a kitöltők jelentős hányada az államigazgatáshoz kapcsolódik, önkormányzatok részéről kisebb kitöltési hajlandóság mutatkozott, a válaszadók mindösszesen 23,08%-a nyilatkozott úgy, hogy az általa képviselt szerv az Ibtv. 2. § (1) k) pontja (a helyi önkormányzatok képviselő-testületének hivatalai, a hatósági igazgatási társulások) hatálya alá tartozik. E jelenség hátterének vizsgálata nem képzi a disszertáció részét, ugyanakkor további kutatási célként azonosítottam a jövőben.

5.6.2. Adatelemzés

5.6.2.1. Általános kérdések

Az adatelemzés szempontjából minden olyan kitöltő személy válaszadása relevánsnak számít, aki az Ibtv. hatálya alá tartozó feladatokat lát el a törvény meghatározott pontja alapján.

Az adatelemzés során figyelembe vett kitöltő személyek szerepköre az alábbiak szerint alakult:



37. ábra: Általános kérdések: Mely szerepkörben végez az Ibtv. hatálya alá tartozó feladatokat? (forrás: saját szerkesztés)

A kitöltő személyek közül csupán egy személy van (4%), aki a szervezeteknek az elektronikus információs rendszereik védelmét biztosító, Ibtv.-ben meghatározott kötelezettségeinek nem közvetlen címzettje, hanem az Ibtv. III/A szakasz alapján kapcsolódik a feladatellátása az Ibtv.-hez. A megjelölt szakasz a kiberbiztonsági tanúsítást ellátó hatósággal kapcsolatos szabályozást foglalta magában, azonban a kérdőíves vizsgálat lezárását követően, a jogszabályi változásoknak következtében e szakasz már hatályát vesztette, a terület a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényben került újra szabályozásra. A jogszabályi változásoktól függetlenül a kérdőív kitöltőjének véleménye releváns a vizsgálat szempontjából, mivel a kiberbiztonság területének szakértőjeként és a kitöltés időpontjában az Ibtv.-ben megfogalmazott feladatokat látott el.

A kitöltő személyek által képviselt szervezetek százalékos eloszlását a következő táblázat mutatja be részletesen.

Válaszok	Az Ibtv. hatálya alá tartozószerv megnevezése		Mintára (26) vetített hányad
Igen		1	3,85%
2.§		1	3,85%
2.§ (1)		1	3,85%
2.§ (1) a)	**központi államigazgatási szervek**	**9**	34,62%
2.§. (1) c)	Országgyűlés Hivatala	1	3,85%
2.§. (1) j)	fővárosi és vármegyei kormányhivatalok	1	3,85%
2. § (1) k)	**a helyi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulások**	**6**	23,08%
2. § (1) a), (2) a)	központi államigazgatási szervek, az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők	1	3,85%
2.§ (2)	2.§ (2)a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők, b) a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, c) az európai vagy nemzeti létfontosságú rendszerelemmé - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján - kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő, d) az alapvető szolgáltatást nyújtó szereplőknek az alapvető szolgáltatás nyújtásában közreműködő, e) az elektronikus információs rendszert működtető, a központi államigazgatási és kormányzati tevékenység szempontjából fontos, nemzetbiztonsági védelem alá eső szervek	1	3,85%
2.§. (2) c)	az európai vagy nemzeti létfontosságú rendszerelemmé - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján - kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő	1	3,85%
23.§	Nemzeti Közszolgálati Egyetem	1	3,85%
háttérintézményként egyik sem, maximum best practice-ként, továbbiakban így értelmezem a kérdéseket		1	3,85%
Nem tartozik a hatálya alá		1	3,85%
Összesen		**26**	**100,00%**

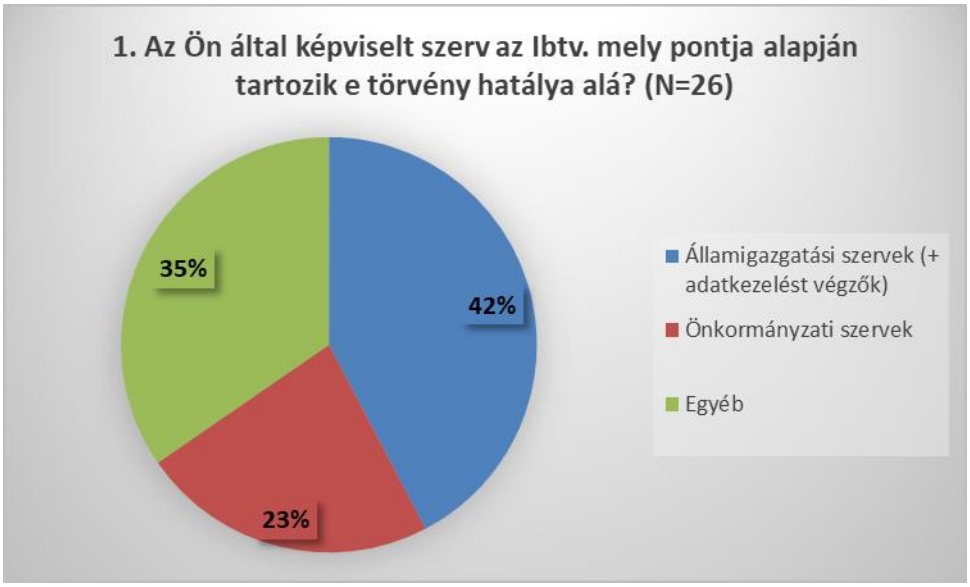
25. táblázat: Általános kérdések: Az Ön által képviselt szerv az Ibtv. mely pontja alapján tartozik e törvény hatálya alá? (forrás: saját szerkesztés)

A kérdőív első kérdése, tekintettel a válaszok lehetséges számára és azok kombinációjára, nyílt kérdésként szerepelt a kérdőívben, azonban az adatelemzés során a válaszok

feldolgozása, csoportosítása és elemzése nem volt könnyű feladat. Sajnos a válaszadók egy része nem határozta meg pontosan a jogalapot, vagy egyszerűen válaszként „Igen”-t írt, de nehézséget okozott azon válaszok kategorizálása is, amelyek ugyan megjelölték az Ibtv. egy bizonyos szakaszát, azonban azon belül a vonatkozó pontot már nem. Ennek tükrében a feldolgozás során a válaszokból kizárólag az egyértelműen levonható következtetéseket fogalmaztam meg.

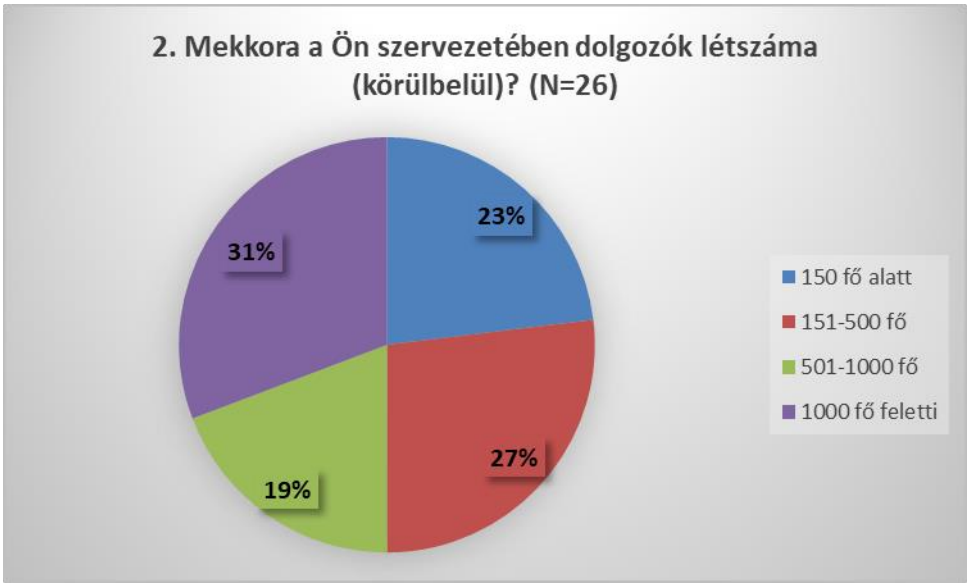
A visszajelzésekből megállapítható, hogy a válaszadók által képviselt szervezetek 92,31%-a tartozik az Ibtv. hatálya alá, míg 7,69%-a nem, amely 2 főt jelent. Az egyik válaszadó háttérintézményként lát el Ibtv.-ben foglalt feladatokat, míg a másik kitöltő válaszában jelölte, hogy „Nem tartozik a hatálya alá.” Válaszaikat mégis relevánsnak tekinthetjük, hiszen szerepkörük alapján figyelembe kell venni a „szerepprofil” egyes elemeivel kapcsolatos attitűdjüket.

Amennyiben az államigazgatási és az önkormányzati szervek százalékos eloszlását vizsgáljuk, megállapíthatjuk, hogy a kitöltők között majdnem kétszer annyian dolgoznak államigazgatási szervnél, mint önkormányzati szervnél. Az elemzés során azokat a szerveket, amelyeknél nem volt egyértelműen megállapítható, hogy az Ibtv. mely pontjához tartozik, az „Egyéb” kategóriában szerepeltettem.



38. ábra: Általános kérdések: 1. Az Ön által képviselt szerv az Ibtv. mely pontja alapján tartozik e törvény hatálya alá? (forrás: saját szerkesztés)

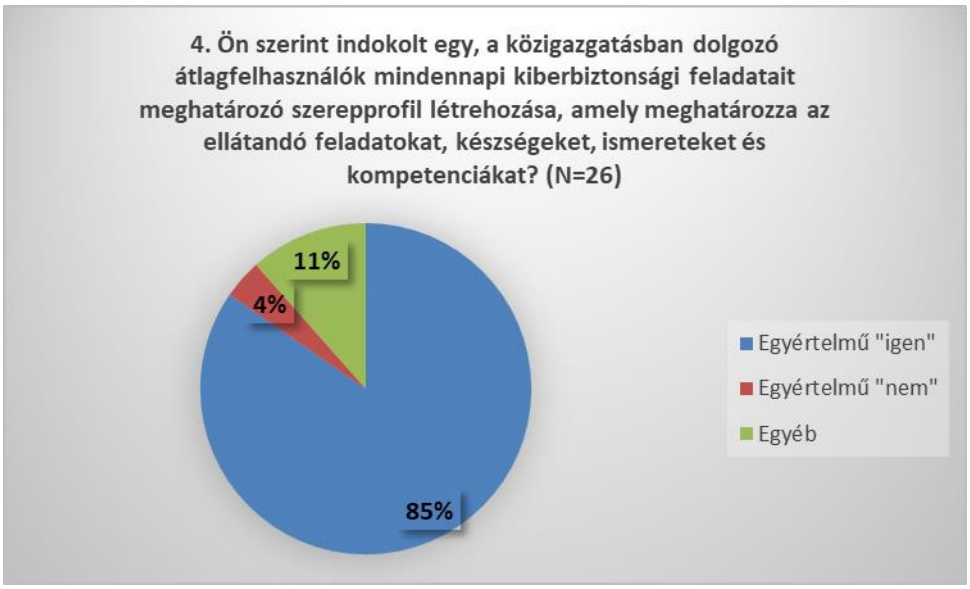
A kitöltők által képviselt szervezetek fele 500 főnél, közel egyharmada pedig 1000 főnél több főt foglalkoztató szervezet.



39. ábra: Általános kérdések: 2. Mekkora a Ön szervezetében dolgozók létszáma (körülbelül)? (forrás: saját szerkesztés)

Az általános kérdések között kaptak helyet a közszolgálati „szerepprofillal” kapcsolatos általános attitűdöt mérő kérdések is.

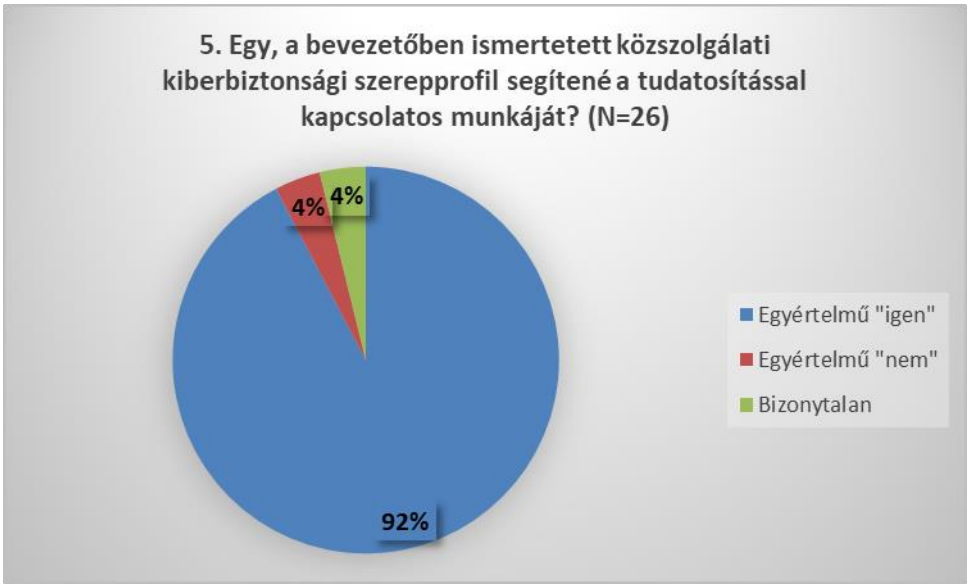
Arra a kérdésre, hogy indokolt-e a közigazgatásban dolgozó átlagfelhasználók mindennapi kiberbiztonsági feladatait meghatározó „szerepprofil” létrehozása a válaszadók 85%-a egyértelmű igennel válaszolt és csupán 1 fő (4%) jelölte meg a „Nem” választ.



40. ábra: Általános kérdések: 4. Ön szerint indokolt egy, a közigazgatásban dolgozó átlagfelhasználók mindennapi kiberbiztonsági feladatait meghatározó szerepprofil létrehozása, amely meghatározza az ellátandó feladatokat, készségeket, ismereteket és kompetenciákat? (forrás: saját szerkesztés)

Az „Egyéb" válaszok között egy fő (4%) kifejtette, hogy „Ez komplex kérdés. A szerepkör alapú megkülönböztetés szerintem jó, de nehéz téma, de jó példa is van", egy másik válaszadó (4%) jelezte, hogy az indokoltságát látja a szerepprofilnak, „de követelményszintű megkövetelését nem látom kivitelezhetőnek. Ajánlás szinten tudja segíteni a szervezetek munkáját.". Pusztán egy fő (4%) válaszolta azt, hogy nem biztos, hogy indokolt a szerepprofil létrehozása.

Arra a kérdésre, hogy az ismertetett közszolgálati kiberbiztonsági szerepprofil segítené-e a tudatosítással kapcsolatos munkáját, a válaszadók 92%-a igennel válaszolt, míg egy fő egyértelmű nemmel válaszolt, illetve egy további fő bizonytalan volt a válasz kapcsán.



41. ábra: Általános kérdések: 5. Egy, a bevezetőben ismertetett közszolgálati kiberbiztonsági szerepprofil segítené a tudatosítással kapcsolatos munkáját? (forrás: saját szerkesztés)

5.6.2.2. Fő feladatok

A közszolgálati „szerepprofil" részeként 17 db fő feladat került azonosításra. A kérdőív az egyes feladatokkal kapcsolatos szakértői attitűd vizsgálatára alkalmazott Likert-skálás mérés bevezetéseként az alábbi kérdést fogalmazza meg: *„Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben meghatározott*

feladatok végrehajtása érdekében az alábbi, kiberbiztonsággal kapcsolatos feladatot kell a mindennapi munkavégzése során végrehajtania?" Az egyes feladatok kapcsán a válaszadók *„a rendkívüli mértékben egyetértek"* és az *„egyáltalán nem értek"* között elhelyezkedő ötfokozatú skálán tudták megjelölni válaszaikat.

Az adatfeldolgozás korábban ismertetett lépéseit, az egyes leíró statisztikai eljárások eredményeit és értelmezéseit a Függelék 4. sz. mellékletében bemutatott táblázat részletesen ismerteti. A táblázat jobb szélső oszlopa mutatja be a „szerepprofil" egyes elemeire vonatkozó végső kutatói döntést: amennyiben a vizsgálatok alapján az adott elem a „szerepprofil" részét képezi, egy ✓ kerül a sor végére. Amennyiben egyértelműen nem utasítható el az adott elem, ugyanakkor a „szerepprofil" részének sem lehet tekinteni, abban az esetben további, jövőbeni vizsgálat javasolt, melyet egy ? jellel jelölök. Amennyiben a mediánértékek figyelembe vételével azonosított, további arányszámítást igénylő elemek esetében mind az egyetértők és a bizonytalanok száma, mind pedig az elutasítók száma éppen hogy eléri a validitás küszöbértékét, a „szerepprofil része (határeset)" elnevezés, illetve ✓! jelek kerültek az adott sor végére. A táblázatok jelölésrendszere minden egyes részterület (fő feladatok, kulcs készségek, kulcs ismeretek, kulcs kompetenciák) esetén megegyezik.

Minden részterület esetében, azon elemek esetében, ahol az arányszámítás során határérték került megállapításra, így éppen hogy a „szerepprofil" részének lehetne tekinteni az adott elemet, egyéni kutatói döntés alapján, a jövőben további vizsgálatok elvégzését javaslom, így jelen disszertációban ezeket az elemeket nem tekintem a „szerepprofil" részének.

Az egyes kérdéscsoportok végleges elemei a kérdéscsoportra vonatkozó, valamennyi elem figyelembevételével meghatározott mediánértékek (a fenntartások nélkül egyetértők és a bizonytalan válaszadók mediánértéke) kiszámítását követően, a korábban bemutatott kutatói döntést megalapozó kritériumrendszer segítségével, valamint a további vizsgálatot igénylő elemek esetében az arányszámítás elvégzését követően alakultak ki.

A vizsgálat eredményeképpen megállapításra került, hogy a „Fő feladatok" csoportját az alábbi elemek képzik:

	Fő feladatok
1	Biztosítja a munkaköréhez kapcsolódóan a kiberbiztonsággal kapcsolatos szabványoknak, törvényeknek és rendeleteknek, illetve a szervezetszabályozó eszközöknek való megfelelést.
2	Részt vesz a feladatköréhez kapcsolódóan a szervezet kiberbiztonsága jövőképét, stratégiáját és politikáját meghatározó dokumentumok végrehajtásában.
3	Részt vesz az Informatikai Biztonsági Szabályzat végrehajtásában.
4	Részt vesz a kiberbiztonsággal kapcsolatos tudatosságnövelő programokon, az előírt követelményeket teljesíti.
5	Részt vesz a feladatköréhez kapcsolódóan a kockázatkezelés folyamatában.
6	Részt vesz a szervezet belső szervezetszabályozó eszközeiben rögzített incidenskezelési eljárásban a feladatköréhez kapcsolódóan.
7	Azonosítja és jelenti az IBF-nek a kiberbiztonsági eseményeket vagy annak gyanúját, részt vesz az esetleges károk enyhítésében.
8	Kapcsolatot tart, bejelentést tesz, tájékoztatja az IBF-et az esetleges biztonsági eseményről vagy annak gyanújáról, a felmerülő kockázatokról, továbbá bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába.
9	A kiberbiztonsággal kapcsolatos intézkedések során szorosan együttműködik az IBF-fel, illetve az üzemeltetést végző informatikusokkal.
10	Együttműködik a kiberbiztonsági ellenőrzésekben.
11	Együttműködik az ellenőrzések során a szükséges információk, adatok, dokumentumok átadásában.
12	Integrálja a feladatkörhöz kapcsolódó kiberbiztonsági megoldásokat és biztosítja megfelelő működésüket

26. táblázat: Közszolgálati „szerepprofil” – Fő feladatok (forrás: saját szerkesztés)

További vizsgálatok elvégzése javasolt a jövőben a következő elemek tekintetében:

- Részt vesz a feladatkörét érintő kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.
- Részt vesz az IBF által azonosított kockázatok értékelésében, valamint a kockázatkezelésben (a kockázatra adott válaszlépések meghatározásában, a kockázatcsökkentő intézkedések végrehajtásában)
- Indokolt esetben (pl. egy információbiztonsági incidens esetén) együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel.
- Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát.
- Alkalmazza a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.

5.6.2.3. Kulcs készségek

A közszolgálati „szerepprofil” részeként 28 db kulcs készség került azonosításra. A kérdőív az egyes készségekkel kapcsolatos szakértői attitűd vizsgálatára alkalmazott Likert-skálás mérés bevezetéseként az alábbi kérdést fogalmazza meg: *„Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs készségekkel kell rendelkeznie?”* Az egyes feladatok kapcsán a válaszadók *„a rendkívüli mértékben egyetértek”* és az *„egyáltalán nem értek”* között elhelyezkedő ötfokozatú skálán tudták megjelölni válaszaikat.

A vizsgálatok elvégzését követően megállapításra került, hogy a „Kulcs Készségek” csoportját az alábbi elemek képzik:

	Kulcs készségek
1	Képes a feladatai ellátása során alkalmazni a kiberbiztonságra vonatkozó jogi követelményeket, szervezetszabályozó eszközöket, valamint a vonatkozó ajánlásokat és a bevált gyakorlatokat.
2	Képes megérteni és feladatai ellátása során figyelembe venni a szervezeti célokat, jövőképet, a biztonsággal kapcsolatos politikát és stratégiát, a jogi, szabályozási és szabvány követelményeket.
3	Képes részt venni a szervezet kiberbiztonsági jövőképének, stratégiájának, politikájának, valamint az Informatikai Biztonsági Szabályzatnak a feladatköréhez kapcsolódó végrehajtásában.
4	Képes részt venni a feladatköréhez kapcsolódó, a szervezetszabályozó eszközöket és egyéb jogi követelményeket kiegészítő, megfelelő kiberbiztonsági irányelvek, eljárások és szabályok kidolgozásában és végrehajtásában.
5	Képes az üzleti igények kiberbiztonsági vonatkozásai kommunikálására a felső vezetés és az IBF felé.
6	Képes a biztonságtudatosító programokon való aktív részvételre, a tananyag elsajátítására és alkalmazására.
7	Képes megfogalmazni az elsajátítandó ismeretekre, készségekre vonatkozó igényét.
8	Képes a feladatköréhez kapcsolódóan a kiberbiztonsági problémák azonosítására, a kockázatok értékelésére, valamint a kockázatcsökkentő intézkedések megértésére és végrehajtására.
9	Képes gyakorolni az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatokat.
10	Képes a social engineering típusú támadásokat felismerni.
11	Képes a problémák és hibák segítséggel történő elhárítására.
12	Képes kommunikálni és kapcsolatot építeni az IBF-el, illetve az érdekelt felekkel, a feladatkörét érintő kiberbiztonsági kockázatok kezelése, illetve az incidensek megelőzése és kezelése érdekében.
13	Képes jelentéseket kidolgozni, vagy az elkészítésükben közreműködni, valamint a jelentéseket megfelelően kommunikálni.

14	Képes részt venni és együttműködni a kiberbiztonsági tárgyú ellenőrzésekben.
15	Képes az auditálási és megfelelőség-értékelési módszertanok, eszközök és technikák – feladatköréhez kapcsolódó – alkalmazására (kizárólag vezetői szerepben).
16	Képes a feladatköréhez kapcsolódóan az etikai követelmények és szabványok megértésére, gyakorlására és betartására.
17	Képes a szervezet kiberbiztonsági kultúrájának befolyásolására, a munkatársak motiválására és ösztönzésére.
18	Képes a nyomás alatti munkavégzésre.
19	Képes együttműködni más csapattagokkal és kollégákkal.
20	Képes a belső és külső érdekelt felekkel történő kommunikációra, koordinációra és együttműködésre.

27. táblázat: Közszolgálati „szerepprofil” – Kulcs készségek (forrás: saját szerkesztés)

További vizsgálatok elvégzése javasolt a jövőben a következő elemek tekintetében:

- Képes részt venni a feladatkörét érintő, kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.
- Képes a jogi és szabályozási környezet, valamint a műszaki üzleti igények alapszintű megértésére és kommunikációjára.
- Képes a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozni.
- Képes kommunikálni, koordinálni és együttműködni a belső és külső érintettekkel (pl. hatóságok, auditorok, alvállalkozók) a feladatkörét érintő, kiberbiztonság tárgyú vagy azzal kapcsolatos feladatok ellátása során.
- Képes részt venni az ellenőrzési jelentések elkészítésben.
- Képes a feladatköréhez kapcsolódóan a kiberbiztonsági ajánlások és legjobb gyakorlatok implementálására, valamint a kiberbiztonsági megoldások integrálására a szervezet infrastruktúrájába.
- Képes az érdekelt felek számára történő megfelelő kommunikációra, prezentációra és jelentéstételre.
- Képes az összetett problémák és biztonsági kihívások alapszintű elemzésére és megoldására.

5.6.2.4. Kulcs ismeretek

A közszolgálati „szerepprofil” részeként 10 db kulcs ismeret került azonosításra. A kérdőív az egyes ismeretekkel kapcsolatos szakértői attitűd vizsgálatára alkalmazott Likert-skálás mérés bevezetéseként az alábbi kérdést fogalmazza meg: *„Egyetért-e Ön azzal, hogy egy*

közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs ismeretekkel kell rendelkeznie?" Az egyes ismeretek kapcsán a válaszadók *„a rendkívüli mértékben egyetértek"* és az *„egyáltalán nem értek"* között elhelyezkedő ötfokozatú skálán tudták megjelölni válaszaikat.

A vizsgálatok elvégzését követően megállapításra került, hogy a „Kulcs Ismeretek" csoportját az alábbi elemek képzik:

	Kulcs ismeretek
1	Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete.
2	Általános kiberbiztonsági ismeretek, szervezeti szinten az információbiztonsági előírások és stratégiák feladatkörhöz kapcsolódó ismerete.
3	Az elektronikus információs rendszerek biztonságának felügyelete rendszerének, valamint az incidens-, illetve kockázatkezelésnek alapszintű ismerete.
4	A kockázatkezelés folyamatának és abban betöltött szerepének az alapszintű ismerete.
5	A megfelelő biztonsági eljárások, követelmények, technikák, valamint ajánlások és szabványok feladatkörhöz kapcsolódó, a lehetséges támadási és védekezési alternatívák alapszintű ismerete.
6	A potenciális kiberfenyegetések, kibertámadási formák és a számítógépes rendszerek sebezhetőségeinek alapszintű ismerete.
7	A kiberbiztonsági ellenőrzések, auditálási szabványok, módszertanok és keretrendszerek feladatkörhöz kapcsolódó alapszintű ismerete (kizárólag vezetői szerepben).
8	Kiberbiztonsággal kapcsolatos technológiák, megoldások és kontrollok feladatkörhöz kapcsolódó ismerete.

28. táblázat: Közszolgálati „szerepprofil„– Kulcs ismeretek (forrás: saját szerkesztés)

További vizsgálatok elvégzése javasolt a jövőben a következő elemek tekintetében:

- Az auditálással és a kiberbiztonsággal kapcsolatos tanúsítások feladatkörhöz kapcsolódó, alapszintű ismerete.
- Etikus kiberbiztonsági szervezeti követelmények.

5.6.2.5. Kulcs kompetenciák

A közszolgálati „szerepprofil" részeként 22 db kulcs kompetencia került azonosításra. A kérdőív az egyes kompetenciákkal kapcsolatos szakértői attitűd vizsgálatára alkalmazott Likert-skálás mérés bevezetéseként az alábbi kérdést fogalmazza meg: *„Egyetért-e Ön*

azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs kompetenciákkal kell rendelkeznie?”. Az egyes feladatok kapcsán a válaszadók *„a rendkívüli mértékben egyetértek”* és az *„egyáltalán nem értek”* között elhelyezkedő ötfokozatú skálán tudták megjelölni válaszaikat.

A vizsgálatok elvégzését követően megállapításra került, hogy a „Kulcs Kompetenciák” csoportját az alábbi elemek képzik:

	Kulcs kompetenciák
1	Részt vesz az információs rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, valamint a vonatkozó jogi követelménynek való megfelelésben.
2	Részt vesz az Információbiztonsági Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában.
3	Részt vesz az információbiztonságnak a szervezet kultúrájába való beillesztése folyamatában.
4	Részt vesz a tudatosító képzések során elsajátított ismeretek, készségek segítségével a biztonságtudatos szervezeti kultúra kialakításában, fenntartásában és kommunikálásában.
5	Megérti és alkalmazza a kockázatkezelés elveit, részt vesz az IBSZ-ben meghatározott kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében a feladatköréhez kapcsolódóan.
6	A kockázatokra vonatkozó információkkal alátámasztott megalapozott döntéseket hoz a feladatköréhez kapcsolódó kockázatok kezelése és mérséklése érdekében (kizárólag vezetői szerepben).
7	Különböző módszereket alkalmaz eszközei és digitális tartalmai megóvására.
8	Értékeli a legmegfelelőbb módszereket, amelyekkel kellő mértékben figyelembe lehet venni a megbízhatósági és adatvédelemi szempontokat.
9	Kiválasztja a megfelelőbb módszereket a személyes adatok és a magánélet megóvására digitális környezetben.
10	Értékeli a legmegfelelőbb módszereket arra, hogyan lehet felhasználni és megosztani személyazonosításra alkalmas adatokat úgy, hogy közben megvédje önmagát és másokat a nem megfelelő adatkezeléssel kapcsolatos, lehetséges károktól.
11	Értékeli az adatvédelmi nyilatkozatok megfelelőségét a személyes adatok felhasználásával kapcsolatban.
12	Megkülönbözteti a legmegfelelőbb módszereket, amelyekkel elkerülhetők a digitális technológiák használata során felmerülő, az egészségre, illetve a fizikai és pszichológiai jóllétre veszélyt jelentő kockázatok.
13	Adaptálja a legmegfelelőbb módszereket, amelyekkel megvédheti önmagát és másokat digitális környezetben.
14	Részt vesz a feladatköréhez kapcsolódó problémakezelési/incidenskezelési folyamatban, a károk

	enyhítése érdekében mindent megtesz, ami tőle az adott helyzetben elvárható.
15	Megkülönbözteti a kockázatokat és veszélyeket digitális környezetben.
16	Biztonsági intézkedéseket alkalmaz.
17	Feladatköréhez kapcsolódóan együttműködik az ellenőrzések során az ellenőrzést végző belső szervezeti egységgel vagy külső szervezettel/céggel, részt vesz az ellenőrzések során készült dokumentumok előállításában, véleményezésében.
18	Részt vesz a kiberbiztonság tárgyú vagy kapcsolódású jelentések, dokumentumok, feladatkörét érintő előállításában.
19	Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.).

29. táblázat: Közszolgálati „szerepprofil" – Kulcs kompetenciák (forrás: saját szerkesztés)

További vizsgálatok elvégzése javasolt a jövőben a következő elemek tekintetében:

- Egyszerű vizsgálatokat végez a részletes utasítások szigorú betartásával.
- Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és az IBF-vel együttműködve biztosítja a legmegfelelőbb információs struktúrát.
- A célnak megfelelően kiválasztja a társadalmi jóllétet és befogadást elősegítő digitális technológiákat.

5.6.3. A vizsgálat következtetései

A kérdőíves vizsgálat során alkalmazott statisztikai eljárás, a nem véletlenszerű mintavétel, valamint az alacsony kitöltési szám kizárja a vizsgálat reprezentativitását. A kidolgozott kérdőív a dokumentumelemzés módszerével meghatározott közszolgálati kiberbiztonsági „szerepprofil" egyes elemeivel kapcsolatos szakértői attitűdök mérésére alkalmas, ugyanakkor ennek segítségével –tekintettel a feldolgozott kérdőívek számára- korlátozott módon vonható le következtetés az egyes elemek megfelelőségéről és alkalmazhatóságáról.

Az adatok többszempontú elemzését követően megállapítottam, hogy mely elemek azok, amelyek részei lehetnek a közszolgálati „szerepprofilnak", illetve mely elemek, amelyek esetében további vizsgálatok elvégzése javasolt. A kutatás során egyetlen elem sem került kizárásra a „szerepprofilból".

Összességében a kérdőíves vizsgálat bizonyítási kísérletnek tekinthető, azonban a tudományos eredmény igazolására nem alkalmas. Éppen ezért a disszertáció lezárását

követően jövőbeni kutatási irányként egy nagymintás vizsgálat keretében szeretném alátámasztani az eredményeket, melynek részeként megvizsgálni tervezem a kismintás kutatás alapján további vizsgálatot igénylő elemek megfelelőségét és alkalmazhatóságát, illetve szeretném feltárni az alacsony kitöltési hajlandóság okait és annak esetleges szektorális hátterét.

5.7. KÖVETKEZTETÉSEK

Jelen vizsgálat keretében azzal a feltételezéssel éltem, hogy azonosíthatók a közszolgálatban dolgozók mindennapi munkavégzése során ellátandó kiberbiztonsági feladatok, valamint a szükséges ismeretek, képességek és kompetenciák. Az előző fejezetekben bemutatott kutatási lépések bizonyításai voltak a hipotézis megválaszolásának.

A feltételezésem igazolására az alábbi lépéseket hajtottam végre:

1. Az IBF, Európai Kiberbiztonsági Készség-keretrendszer segítségével azonosított feladataiból kiválasztottam a közszolgálati dolgozók mindennapi munkavégzése során releváns, a szervezeti kiberbiztonság megteremtése szempontjából nélkülözhetetlen feladatokat, és meghatároztam az ellátásukhoz szükséges készségeket, ismereteket és kompetenciákat. A kapott eredményt, a hazai jogszabályi megfelelés érdekében kiegészítettem további profil elemekkel.
2. Annak érdekében, hogy a közszolgálati dolgozók kompetenciakészlete megfelelően részletezett legyen, megvizsgáltam néhány, korábbi tanulmányomban elemzett nemzetközi és hazai keretrendszer alkalmazhatóságát, melynek eredményeként a „szerepprofil” kiegészítésre került az Állampolgári digitális kompetencia-keret (DigComp 2.1.) releváns elemeivel.
3. Kutatási eredményeim összefoglalásaként meghatároztam a közszolgálati „szerepprofilt”, melynek részeként azonosítottam a bizonyítási célban szereplő feladatokat, készségeket, ismereteket és kompetenciákat.

A közszolgálati „szerepprofil” elemeivel kapcsolatos szakértői attitűdök mérésére, valamint a kutatási eredményeim árnyalására, esetleges módosítására bizonyítási kísérletet végeztem egy kismintás kérdőív segítségével.

A bemutatott lépések segítségével, a bizonyítási folyamat eredményeként azonosítottam a közszolgálati dolgozók (átlagfelhasználók) számára a mindennapi munkavégzéshez szükséges kiberbiztonsággal kapcsolatos feladatokat, és e feladatok ellátásához nélkülözhetetlen ismereteket, képességeket és kompetenciákat, így az általam felállított hipotézis igaznak bizonyult.

Az Európai Kiberbiztonsági Készség-keretrendszer (ECSF) és az általa alkalmazott Európai e-Kompetencia Keretrendszer (e-CF) segítségével, az Állampolgári digitális kompetencia-kerettel (DigComp 2.1.) kiegészítve kidolgoztam egy közszolgálati „szerepprofilt", amely meghatározza, hogy a közszolgálatban dolgozóknak milyen kiberbiztonsággal kapcsolatos feladatokat kell ellátniuk az Ibtv.-ben megfogalmazott követelmények, a nemzeti elektronikus adatvagyon és az azt kezelő elektronikus információs rendszerek és rendszerelemek védelme érdekében. A „szerepprofil" részeként azonosítottam azok a speciális készségeket, ismereteket és kompetenciákat, amelyekkel egy nem kiberbiztonsági munkakört ellátó közszolgálati dolgozónak rendelkeznie kell e feladatok ellátásához. A „szerepprofil" támogatja az egyéni biztonságtudatosság fejlesztését és ezen keresztül a biztonságtudatos szervezeti kultúra kialakítását, megfelelő alapot szolgáltat a képzési programok kidolgozásához és folyamatos fejlesztéséhez, valamint segítséget nyújt a humánerőforrás menedzsment számára a jelöltekkel, illetve a foglalkoztatott közszolgálati dolgozókkal szembeni kiberbiztonsági követelmények megfogalmazásában, felelősségük megalapozásában. A „szerepprofil" megfelelő tájékoztatást nyújt a felső vezetés számára is a nem kiberbiztonsági munkakörben foglalkoztatott közszolgálati dolgozók szervezeti környezetben értelmezhető feladatairól is.

A „szerepprofilban" meghatározott elemek biztosítják a napi szintű, egyéni és szervezeti szinten értelemezhető kiberbiztonsági kihívások kezelését a közszolgálati dolgozók számára. Amennyiben a felhasználók ismerik a megfelelő biztonsági eljárásokat, követelményeket és technikákat, a lehetséges támadási és védekezési alternatívákat és azokat képesek alkalmazni is, akkor a különféle bizalmas információk megszerzésére irányuló támadások bekövetkezésének valószínűsége is csökkenthető, mely összességében növeli a közigazgatási szervek működésének stabilitását, valamint a nemzeti adatvagyon biztonságát.

A „szerepprofil” segítségével pontosan meghatározhatók azok a humánerőforrás-fejlesztési irányok, amelyek a nem kiberbiztonsági feladatokat ellátó munkatársak képzése segítségével hozzájárulnak a kibertámadások elleni fokozott védelem eléréséhez és az elektronikus információs rendszerek biztonságához.

6. ÖSSZEGZETT KÖVETKEZTETÉSEK

A globális világ digitalizációjának köszönhetően megnőtt a társadalom sebezhetősége a kibertér felől érkező támadásokkal szemben, mely hatással van a közigazgatás működésére is.

Az elmúlt években a hazánkban elfogadott jogszabályok és stratégia szintű dokumentumok is a digitális állam kialakítása irányába mutatnak. A Digitális Jólét Program a teljes közigazgatás digitális átalakítását tűzte ki célul, melynek részeként alapvető célként határozta meg a biztonságos kibertér megteremtését, ugyanakkor az egyik legnagyobb kihívásként tekintett a kapcsolódó internetbiztonság megteremtésére és fenntartására. A digitális állam önálló pillérként jelenik meg a Nemzeti Digitalizációs Stratégiában (2022-2030), amely kiemeli, hogy „ágazati és központi szinten kiemelten szükséges az információbiztonsági elemek és a kibervédelmi kapacitások bővítése, összhangban a hazai és az EU-s szintű törekvésekkel”[189]. A közigazgatás teljes digitalizációja felé vezető úton a következő lépés a 2022. decemberében elfogadott Digitális Állampolgárság Program, amely egységesen magas szintű digitális környezetet teremt, és egyszerűbb alapokra helyezi az állampolgárok és a kormányzat különböző szervei közötti kommunikációt. A program eredményeképpen már okostelefonon a Digitális Állampolgár mobilalkalmazás segítségével állami szolgáltatások válnak elérhetővé, egyszerűen –igazolványok nélkül- igazolhatjuk magunk a telefonunk használatával, a következő években pedig már személyes megjelenés nélkül, digitálisan fogjuk tudni intézni a közigazgatást érintő legfontosabb ügyeket.

Az e-közigazgatás „a közszféra kapcsolatrendszerének tudás alapú átalakítását és racionalizált, szolgáltató jellegű újra szervezését jelenti, az infokommunikációs technológiai alkalmazások közműszerű használata révén”. (Budai, 2014., 47.) Azonban minél szélesebb körben valósul meg az e-közigazgatás, annál fontosabbá és sürgetőbbé válik, hogy az elektronikus információs rendszerek révén a kibertérben hozzáférhető adatokat, információkat, tehát a nemzeti adatvagyon részét képző nemzeti elektronikus adatvagyont megfelelően védjük, amely kiemelt feladat valamennyi közigazgatási szerv és intézmény számára.

[189] Nemzeti Digitalizációs Stratégia 2022-2030, p. 68.

A közigazgatás digitalizációjának, a digitális állam megvalósítása sikerességéhez elengedhetetlen, hogy az érintett szervek hatékony védelmi képességgel rendelkezzenek a kibertér felől érkező fenyegetésekkel szemben, melyhez többek között azonosítani szükséges az őket fenyegető támadás típusokat, valamint biztosítani kell a vezetők és a munkatársak megfelelő felkészültségét.

A disszertáció az Ibtv. -2025. január 1-től a Kibertv.- hatálya alá tartozó szervek kiberbiztonsági feladatai megvalósítását kívánja elősegíteni, és a vonatkozó tudományos ismereteket szeretné bővíteni a közigazgatást érintő kiberbiztonsági incidenstrendek azonosítására, valamint az elektronikus információs rendszer biztonságáért felelős személy, illetve a közszolgálati dolgozók kiberbiztonsági feladatai, készségei, ismeretei és kompetenciái meghatározására irányuló vizsgálatok segítségével.

Bár az értekezésben megfogalmazott kutatási kérdések és hipotézisek, illetve bemutatott vizsgálatok 2023. őszén zárultak le, így az Ibtv.-ben és végrehajtási rendeleteiben megfogalmazott szabályozást vették alapul, ugyanakkor az Ibtv.-t felváltó Kibertv. szellemiségékben nem jelent gyökeres változást. Az új szabályozás minden eleme –az Ibtv.-vel megegyező módon- arra irányul, hogy „az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét”[190] biztosítsa. Az Ibtv. és a Kibertv. hatálya alá tartozó közigazgatási szervezetek tekintetében sincs jelentős eltérés, ezért a disszertációban „az Ibtv. hatálya alá eső szervek” alanyi kör számára tett megállapítások a Kibertv. közigazgatási ágazathoz tartozó szerveire is érvényesek. A Kibertv.-ben, az IBF szerepe és feladatai vonatkozásában sem állapítható meg számottevő eltérés, a jogszabály az elektronikus információs rendszerek védelméhez kapcsolódó feladatok ellátását, a kockázatmenedzsment keretrendszer működtetését, a kiberbiztonsági incidensek bejelentését és kezelését, valamint a tudatosítást határozza meg, mint legfontosabb kötelezettségeket. Az IBF feladataiból kiindulva pedig megállapítható, hogy a kutatás fókuszát képező szervek esetében, a nem kiberbiztonsági feladatokat ellátó, átlagfelhasználónak tekinthető közszolgálati állomány vonatkozásában, az értekezésben azonosított kiberbiztonsági feladatok helytállóak az új szabályozás esetében is, így a

[190] Kibertv. tervezete preambulum

feladatellátást biztosító készségekre, ismeretekre és kompetenciákra vonatkozó megállapítások a Kibertv. esetén is érvényesek.

Jelen fejezet célja a kutatási célok kapcsán megfogalmazott hipotézisek, valamint a kapcsolódó vizsgálatok és az összegzett következtetések rövid bemutatása.

Az első hipotézis vizsgálata

H1	**A magyar közigazgatást érő kiberbiztonsági incidensek megfelelnek az európai incidenstrendeknek, melyekben meghatározó szerepe van a pszichológiai manipuláción alapuló, úgynevezett social engineering típusú támadási formának.**

30. táblázat: H1 hipotézis (forrás: saját szerkesztés)

Az első hipotézis bizonyítása érdekében, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által 2019 és 2021 között detektált incidensekre vonatkozó adatok statisztikai elemzése segítségével azonosítottam a hazai kiberbiztonsági incidenstrendeket incidens típusok és szektorális eloszlás szerint, évenkénti bontásban és a három évet összesítve, külön megvizsgálva a pszichológiai manipuláción alapuló támadási forma, a social engineering előfordulási arányát. Következő lépésként megvizsgáltam az európai kiberbiztonsági incidenstrendekre vonatkozó dokumentumokat (ENISA Threat Landscape 2020, 2021, 2022; IOCTA 2019, 2020, 2021; SOCTA 2021) és dokumentumelemzés segítségével meghatároztam a vizsgált időszak incidenstrendjeit. Végül az incidensek típusaira, a fenyegetett szektorokra, valamint a social engineeringre vonatkozó összehasonlító elemzés segítségével megállapítottam, hogy a magyar közigazgatást érő incidenstrendek megfelelnek az európai trendeknek.

A kutatás eredménye alapján egyértelműen kimondható, hogy a hazai közigazgatási szervek számára a megfelelő védelmi képességek kialakításában, valamint a fenyegetésekkel szembeni felkészülésben nem csak a hazai, hanem az európai incidenstrendek ismerete, és azok figyelemmel kísérése is megfelelő segítséget nyújthat.

A második hipotézis vizsgálata

H2	**Meghatározható az elektronikus információs rendszer biztonságáért felelős személy számára egy olyan szerepprofil, amely azonosítja a mindennapi munkavégzés részét képező feladatokat, illetve a végrehajtáshoz szükséges készségeket, ismereteket és kompetenciákat.**

31. táblázat: H2 hipotézis (forrás: saját szerkesztés)

A kutatási cél elérése érdekében az alábbi három alhipotézist állítottam fel:

H2-1.	Azonosíthatók a kiberbiztonsággal kapcsolatos ismeretekkel, tudással, készségekkel és kompetenciákkal foglalkozó nemzetközi keretrendszerek segítségével olyan jó gyakorlatok, amelyek átültethetők a magyar közigazgatási környezetbe.
H2-2.	Az elektronikus információs rendszer biztonságáért felelős személy jogszabályokban meghatározott feladatai, és e feladatok ellátásához szükséges készségek, ismeretek és kompetenciák azonosíthatók a jó gyakorlatként bemutatott nemzetközi keretrendszerekben.
H2-3.	Kidolgozható az elektronikus információs rendszer biztonságáért felelős személy számára egy olyan szerepprofil, amely meghatározza a mindennapi munkavégzés részét képző feladatokat, illetve a végrehajtáshoz szükséges készségeket, ismereteket és kompetenciákat.

32. táblázat: H2 hipotézis alhipotézisei (forrás: saját szerkesztés)

A második hipotézis vizsgálata során, első lépésként előre meghatározott kritériumrendszer alapján azonosítottam a téma szempontjából releváns nemzetközi és hazai keretrendszereket, majd ezek közül összehasonlító elemzés segítségével meghatároztam az IBF szerepprofil kidolgozásában jó gyakorlatként alkalmazható rendszereket, valamint a magyar közigazgatási környezetbe átültethető elemeket. Következő lépésként a vonatkozó hazai jogszabályi környezet elemzését követően felsoroltam az IBF kötelező feladatait, majd e feladatokat és a hozzá kapcsolódó készségeket, ismeretek és kompetenciákat azonosítottam a jó gyakorlatként meghatározott keretrendszerekben. Végezetül az előző lépésben azonosított keretrendszerek és elemei segítségével meghatároztam azokat az Ibtv. hatálya alá tartozó szerveknél értelmezhető feladatokat és az ellátásukhoz szükséges készségeket, ismeretek és kompetenciákat, amelyek elengedhetetlenek az IBF szervezeti

szinten értelmezhető kiberbiztonsági feladatai ellátásához, majd megalkottam az IBF szerepprofilját és annak tartalmi elemeit.

A harmadik hipotézis vizsgálata

H3	**Azonosíthatók a közszolgálatban dolgozók mindennapi munkavégzése során ellátandó kiberbiztonsági feladatok, valamint a feladatellátást biztosító ismeretek, képességek és kompetenciák.**

33. táblázat: H3 hipotézis (forrás: saját szerkesztés)

A kutatási cél elérése érdekében az alábbi két alhipotézist állítottam fel:

H3-1.	A közszolgálatban dolgozók szervezeti szinten értelmezhető kiberbiztonsági feladatai, valamint az ellátásukhoz szükséges készségek, ismeretek és kompetenciák levezethetők az IBF Európai Kiberbiztonsági Készség-keretrendszer (ECSF)[191] segítségével azonosított feladataiból.
H3-2.	Az ECSF segítségével meghatározott ismerethalmazok kiegészítése szükséges további, átlagfelhasználó-specifikus elemekkel annak érdekében, hogy pontosan definiálni tudjuk a nem kiberbiztonsági munkakörökhöz kapcsolódó kiberbiztonsági feladatokat, és a biztonságtudatosság kialakításához nélkülözhetetlen ismereteket, készségeket és kompetenciákat.

34. táblázat: H3 hipotézis alhipotézisei (forrás: saját szerkesztés)

A harmadik hipotézis vizsgálata során abból a feltételezésből indultam ki, hogy a közszolgálatban dolgozók kiberbiztonsági feladatai a hazai jogszabályokban megfogalmazott, IBF számára előírt feladatokból eredeztethetők. Első lépésként az IBF szerepprofilhoz kapcsolódó kutatás eredményei segítségével meghatároztam azokat az ECSF-ben az IBF számára azonosított feladatokat (H2-2), amelyek végrehajtása igényli a közszolgálatban dolgozók közreműködését, majd meghatároztam a közszolgálati dolgozók -magyar jogszabályi környezet figyelembevételével módosított- feladatait, készségeit, ismereteit és kompetenciáit. Következő lépésként áttekintettem a korábbi kutatások alkalmával azonosított keretrendszereket (H2-1), és dokumentumelemzést követően

[191] European Cybersecurity Skills Framework Role Profiles : https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.11.20.); European Cybersecurity Skills Framework (ECSF) - User Manual: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

további elemekkel egészítettem ki a közszolgálati szerepprofilt. Utolsó lépésként létrehoztam egy kiberbiztonsági feladatokat, készségeket, ismereteket és kompetenciákat tartalmazó közszolgálati kiberbiztonsági „szerepprofilt", melyek hozzájárulnak a közigazgatásban dolgozó átlagfelhasználók kiberbiztonsági képességei növeléséhez és ezáltal a biztonságtudatos szervezeti kultúra kialakításához.
Végül bizonyítási kísérletet tettem a közszolgálati „szerepprofil" elemeivel kapcsolatos szakértői attitűdök mérésére, valamint a kutatási eredményeim árnyalására, esetleges módosítására egy kismintás kérdőíves vizsgálat segítségével.

6.1. ÚJ TUDOMÁNYOS EREDMÉNYEK

A H1 hipotézis kapcsán megfogalmazott új tudományos eredmény:
Azonosítottam a hazai és az európai kiberbiztonsági incidenstrendeket, majd ezek összehasonlítása segítségével bizonyítottam, hogy a hazai trendek -incidens típusok, szektorális eloszlás, valamint a pszichológiai manipuláción alapuló, social engineering támadások tekintetében is- megfelelnek az európai incidenstrendeknek.

A H2 hipotézis kapcsán megfogalmazott új tudományos eredmény:
Nemzetközi és hazai keretrendszerek segítségével kidolgoztam egy, a magyar jogszabályi környezethez igazodó szerepprofilt az elektronikus információs rendszer biztonságáért felelős személy részére, melyben meghatároztam a mindennapi munkavégzés részét képző feladatokat, valamint a végrehajtáshoz szükséges készségeket, ismereteket, és kompetenciákat.

A H3 hipotézis kapcsán megfogalmazott új tudományos eredmény:
Meghatároztam a közszolgálatban, nem kiberbiztonsági munkakörben foglalkoztatott átlagfelhasználók szervezeti szintű és egyéni kiberbiztonsági feladatait, valamint az ellátásukhoz nélkülözhetetlen speciális készségeket, ismereteket és kompetenciákat.

6.2. AJÁNLÁSOK A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGÁRA

Kutatásom során részletesen meghatároztam a hazai kiberbiztonsági incidenstrendeket, egyenként vizsgálva az egyes incidens típusok eloszlását, valamint az állami és önkormányzati szerveket érő leggyakoribb támadási formákat. A bemutatott eredmények gyakorlati felhasználást az alábbi területeken javaslom:

- az Ibtv. hatálya alá tartozó szervek felső vezetőinek, IBF-jének, az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyeknek a szervezeti szintű kibervédelmi képességek tervezése, kialakítása és fejlesztése céljából;
- az Ibtv. hatálya alá tartozó szervek munkatársainak, a megfelelő szintű biztonságtudatosság kialakítása és fejlesztése érdekében;
- az incidenskezelésben résztvevő intézmények számára;
- a kiberbiztonsági/információbiztonsági oktatásban részt vevő intézményeknek (például: Nemzeti Közszolgálati Egyetemen a kiberbiztonsági mesterszakon, az elektronikus információs rendszer biztonságáért felelős személy képzésében, továbbképzésében)
- a kiberbiztonsági/információbiztonsági tudatosításban résztvevő intézmények számára a megfelelő képzési program kidolgozása érdekében.

Vizsgálataim eredményeképpen meghatároztam az IBF, valamint a közszolgálatban dolgozók kiberbiztonsági szerepprofilja részeként az ellátandó feladatokat, valamint a szükséges készségeket, ismereteket és kompetenciákat. Az eredmények gyakorlati felhasználást javaslom:

- az egyéni fejlesztési lehetőségek támogatására: az IBF szerepprofilt az IBF-k, valamint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyeknek, a közszolgálati „szerepprofilt” pedig a közszolgálatban dolgozó átlagfelhasználóknak ajánlom;
- a képzési szolgáltatóknak a megfelelő képzési program kidolgozásához és fejlesztéséhez;
- az Ibtv. hatálya alá eső szervek számára a közszolgálati szerepprofil egyes elemeit a tudatosítási program kidolgozásához és fejlesztéséhez;

- a humánerőforrás menedzsment számára a jelölt vagy foglalkoztatott IBF-vel szembeni követelmények megfogalmazásában, felelősségük megalapozásában, valamint a közszolgálatban dolgozók kiberbiztonsági feladatai áttekintésében;
- a felső vezetés számára az IBF, valamint a közszolgálatban dolgozók szervezeti szinten értelmezhető feladatai áttekintésére.

6.3. JÖVŐBELI TERVEK

Az értekezésben bemutatott vizsgálatok során megértettem, hogy a doktori kutatásra is igaz az a mára szállóigévé vált mondás, mi szerint „Minden vég valaminek a kezdete.”. A disszertáció terjedelmi és időbeni korlátai nem tették lehetővé, hogy az általam tervezett valamennyi kutatási elem megvalósuljon, ezért már a kutatás során pontosan meghatároztam magamnak azokat a területeket, amelyeket a jövőben további vizsgálatok tárgyává szeretném tenni.

A kiberbiztonsági incidenstrendek többszempontú elemzése és meghatározása véleményem szerint állandó kihívás a kutatók számára, mivel egy nagyon gyorsan fejlődő és dinamikusan változó területről van szó, amelyben az összefüggések vizsgálata folyamatosan indokolt.

Az IBF szerepprofilban meghatározott egyes elemek esetleges változáskövetése nem feltétlenül igényel tudományos kutatást, míg a közszolgálati szerepprofil egyes elemei tekintetében számos tudományos vizsgálat elvégzését tervezem. Egyrészt a kidolgozott kérdőív segítségével szeretnék egy nagymintás vizsgálatot végezni az eddigi eredmények alátámasztására, másrészt önálló kutatásként kívánom megvizsgálni a kérdőíves vizsgálat során tapasztalt alacsony kitöltési hajlandóság okait.
További kutatási irányként szeretném a tudatosítás néhány aspektusát részletesen megvizsgálni, úgy mint a tématerületeket, a tudatosítási módszereket, valamint a gamifikációs lehetőségeket a programok kidolgozásában.

7. PUBLIKÁCIÓS JEGYZÉK

Az értekezésben bemutatott vizsgálatok és megfogalmazott tudományos eredmények az alábbi tanulmányokban kerültek publikálásra:

- LEGÁRD Ildikó (2020b): *A humán faktor szerepe a kiberbiztonság megteremtésében* - In: Tick, József; Kokas, Károly; Holl, András (szerk.) Networkshop 2020. Országos Online Konferencia. 2020. szeptember 2-4., Budapest, Magyarország : Hungarnet, 2020, pp. 124-132.

- LEGÁRD Ildikó (2023b): *A közigazgatást érő hazai és európai incidenstrendek összehasonlítása*- In. Jegyző és közigazgatás XXV. évfolyam, 2. szám, 2023., p. 34-42.

- LEGÁRD Ildikó (2022a): *A nemzetközi keretrendszerek összehasonlítása és a jó gyakorlatok azonosítása az IBF szerepprofil definiálása érdekében* - In. Jegyző és közigazgatás XXIV. évfolyam, 6. szám, 2022. november-december, p. 43-55.

- LEGÁRD Ildikó (2023c): *Az elektronikus információs rendszer biztonságáért felelős személy szerepprofilja* – In. Jegyző és Közigazgatás XXV. évfolyam, 1. szám, 2023., 25 : 1 p. 39-48.

- LEGÁRD Ildikó (2020d): *Building An Effective Information Security Awareness Program*. - In: Thomas, Hemker; Robert, Müller-Török; Alexander, Prosser; Dona, Scola; Tamás, Szádeczky; Nicolae, Urs (szerk.) Central and Eastern European e|Dem and e|Gov Days 2020, Wien, Ausztria : Österreichische Computer Gesellschaft (ÖCG) (2020) - p. 189-200.

- LEGÁRD Ildikó (2020e): *Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre,* - In. Hadmérnök, 2020. 15. évf., 1. szám, p. 91-105.

- LEGÁRD Ildikó (2023d): *Információbiztonsági incidenstrendek a közigazgatásban* - In. Nemzetbiztonsági Szemle (online) 11 : 1,2023., p. 78-107.

- LEGÁRD Ildikó (2023e): *Közszolgálati kiberbiztonsági szerepprofil* – In. Új Magyar Közigazgatás 2023.

A témában megjelent, de a disszertációban bemutatott kutatáshoz csak érintőlegesen kapcsolódó publikációk:

- LEGÁRD Ildikó (2020a): *A barát és ellenség megkülönböztetése a kibertérben* – In. Jog Állam Politika: Jog- És Politikatudományi Folyóirat 2020, 12 : 3 pp. 125-140.

- LEGÁRD Ildikó (2023a): *A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintés* - In: Krasznay, Csaba (szerk.) Taktikák és stratégiák a kiberhadviselésben, Budapest, Magyarország : Ludovika Egyetemi Kiadó, 2023, pp. 11-40.

- LEGÁRD Ildikó (2020c): *Az államok új típusú kihívásai a kibertér felől érkező fenyegetések formájában: A lehetséges válaszlépések nemzetközi jogi megítélése, a szükséges védekezési képességek kialakítása és működtetése Magyarországon* - In: Jámborné, Róth Erika (szerk.) Doktoranduszok fóruma, Miskolc, Magyarország : Miskolci Egyetem, Állam- és Jogtudományi Kar 2020, pp. 37-41.

- LEGÁRD Ildikó (2021a): *Effective methods for successful information security awareness* – In. Pro Publico Bono: Magyar Közigazgatás; A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi szakmai folyóirata 9 : 1, 2021 pp. 108-127.

- LEGÁRD Ildikó (2021b): *Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével*, Polgári Szemle: Gazdasági És Társadalmi Folyóirat 2021. 17 : 1-3 p. 358-373.

8. IRODALOMJEGYZÉK

8.1. Irodalomjegyzék

ALBININÉ Budavári, Edina; RAJNAI, Zoltán: *The Energy Impact of Social Engineering* – In. Transactions On Advanced Research, 2021. 17 : 2 - p. 37-40.

ALBININÉ Budavári, Edina; RAJNAI, Zoltán: *Social Engineering—The Hidden Control* – In. Proceedings, 2020. 63 : 1

ALDAWOOD, Hussain – SKINNER, Geoffrey: *A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications*. Conference paper: 2018. 26th International Conference on Systems Engineering (ICSEng) https://www.researchgate.net/publication/330661441_A_Critical_Appraisal_of_Contemporary_Cyber_Security_Social_Engineering_Solutions_Measures_Policies_Tools_and_Applications/link/5d9ae3b392851c2f70f21bf6/download (Letöltve: 2021.11.13.)

ALDAWOOD, H. - SKINNER, G. (2019a): *Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal*. – In. International Journal of Security (IJS), 2019. Volume (10) : Issue (1) https://www.researchgate.net/publication/333531483_Contemporary_Cyber_Security_Social_Engineering_Solutions_Measures_Policies_Tools_and_Applications_A_Critical_Appraisal (Letöltve: 2023.09.14.)

ALDAWOOD, Hussain – SKINNER, Geoffrey (2019b): *Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues*. In. Future Internet, 2019. vol. 11, no. 3. https://www.researchgate.net/publication/331848369_Reviewing_Cyber_Security_Social_Engineering_Training_and_Awareness_Programs-Pitfalls_and_Ongoing_Issues (Letöltve: 2023.09.14.)

BÁNYÁSZ Péter: *A közösségi média, mint a nyílt forrású információszerzés fontos területe* – In. Nemzetbiztonsági Szemle (Online), 2015. 3. évf. 2. szám, - p. 21-36., http://real.mtak.hu/72506/ (Letöltve: 2022.04.26.)

BÁNYÁSZ Péter: *Social engineering and social media* – In. Nemzetbiztonsági Szemle, 2018. 6. évf. 1. szám - p. 59-77. http://real.mtak.hu/94335/1/EPA02538_nemzetbiztonsagi_szemle_2018_01_059-077.pdf (Letöltve: 2022.04.26.)

BÁNYÁSZ Péter – KRASZNAY Csaba: *Kiberbiztonsági incidensek a magyar közigazgatásban* – In: Kaiser Tamás (szerk.): A jó állam mérhetősége III. - Budapest 2019. - p. 249-270.

BARNA, Bianka Rita ; KOLLÁR, Csaba ; OROSZI, Eszter Diána: *A social engineering helye az információbiztonsági auditban* – In. Biztonságtudományi Szemle, 2023. 5 : 1. - p. 25-41.

BELÁZ Annamária: *A közigazgatás információbiztonsága: megjósolhatók az incidensek?* - In. Hadtudomány : A Magyar Hadtudományi Társaság Folyóirata, 2019. 29:3. - p. 92-104.

BERZSENYI Dániel, BODÓ Attila Pál, KAPITÁNY Sándor, SÁGI Gábor, SEBŐK Viktória: *Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára*, - Budapest: Nemzeti Közszolgálati Egyetem, 2022

BERZSENYI Dániel, GYARAKI Réka, HÁMORNIK Balázs Péter, HIRSCH Gábor, KISS Attila, MARSI Tamás ,ORBÓK Ákos, SIMON Béla, SOLYMOS Ákos, TIKOS Anita, ZSÍROS Péter: *Incidensmenedzsment - Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017*. Budapest: Dialóg Campus, 2018.

BODÓ Attila Pál, MARSI Tamás, SEBŐK Viktória, ZÁMBÓ Nóra: *Célzott Kibertámadások - Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* – Budapest: Nemzeti Közszolgálati Egyetem, 2022

BOR Olivér: *Egységesen magas kiberbiztonság az Európai Unióban*. - In: Szakmai Szemle XXII. évfolyam 1. szám 2024. április, Katonai Nemzetbiztonsági Szolgálat – p. 177-196. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2024_1_szam.pdf

BUDAI Balázs Benjámin: *Az e-közigazgatás elmélete* (második, átdolgozott kiadás). - Budapest, Akadémiai Kiadó, 2014.

BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. - In. MIS Quarterly, 2010. vol. 34, no. 3, - p. 523–548, DOI: https:// doi.org/10.2307/25750690.

CARRETERO, S., Vuorikari, R., Punie, Y.: DigComp 2.1: *Állampolgári digitáliskompetencia-keret nyolc jártassági szinttel és gyakorlati példákkal*, EUR 28558 EN, doi: 10.2760/38842

CHEN, C. C., MEDLIN, D. B.: *A cross-cultural investigation of situational information security awareness programs*. - In. Information Management & Computer Security, 2008. 16(4) – p. 360-376.

CONTEH, Nabie Y., SCHMICK Paul J.: *Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks* – In. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention 2021. - p. 19-31.

CULOT, G., NASSIMBENI, G., PODRECCA, M., SARTOR, M.: *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda* – In. The TQM Journal, 2021. Vol. 33 No. 7 - p. 76-105. https://doi.org/10.1108/TQM-09-2020-0202

DEÁK Veronika: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során*. - In. Hadmérnök, 2018. XIII. Évfolyam 3. szám – p. 391-402.

DEÁK Veronika (2017a): *A social engineering humán alapú támadási technikái*. – In. Biztonságpolitika, 2017. április 10. https://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (Letöltve: 2021.11.13.)

DEÁK Veronika (2017b): *A számítógép alapú social engineer támadási technikák.* – In. Biztonságpolitika, 2017. április. https://biztonsagpolitika.hu/wp-content/uploads/2017/04/biztpol_IT_Deak_Veronika.pdf (Letöltve: 2021.11.13.)

DEÁK Veronika: *Kártékony programok terjedése social engineering technikákon keresztül*. – In. Hadmérnök, 2019. XIV. Évfolyam 2. szám - p. 256-271.

FONSECA-HERRERA, Omar A. – ROJAS, Alix E. – FLOREZ, Hector: *A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard* – In. IAENG International Journal of Computer Science, 2021. 48:2

GRAGG, David: *A Multi-Level Defense Against Social Engineering*. SANS Institute 2003.

HAIG Zsolt: *Az információbiztonság szabályzói és szervezeti keretei* – In. Hadmérnök:(Különszám) p. online. 2007. - 12 p. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/2055/haig_rw7.pdf?sequence=2&isAllowed=y (Letöltve: 2023.09.25.)

HANSCHE, S. (2001): *Designing a Security Awareness Program: Part I.* – In. Information Systems Security, 2001. 9(6), - p. 14-23.

HATFIELD, Joseph M.: *Social engineering in cybersecurity: The evolution of a concept* – In. Computers & Security Volume 2018. 73.sz. - p. 102-113

HORNYACSEK Júlia: *A tudományos kutatás elmélete és módszertana.* - Budapest, NKE, 2014

HORVÁTH Gergely Krisztián: *Közérthetően (nem csak) az IT biztonságról* - Budapest, 2013. https://kifu.gov.hu/sites/default/files/IT_brosura_v7.pdf (Letöltve: 2021.03.22.)

ILLÉSSY Miklós, NEMESLAKI András, SOM Zoltán: *Elektronikus információbiztonság-tudatosság a magyar közigazgatásban*. - In. Információs Társadalom 2014/1. - p. 52–73.

JAGODICS, Ibolya ; KOLLÁR, Csaba: *21. századi social engineering támadások, védekezés és szervezeti hatások Európában* – In. KISS György (Szerk.): Közszolgálati életpályák jogi szabályozása, Budapest, Dialóg Campus, 2019

KISS György (szerk.): *Közszolgálati életpályák jogi szabályozása*. Budapest, Dialóg Campus, 2019

KOLLÁR Csaba: *Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében*.- In: Magyar Coachszemle, 2016. V. évfolyam 3. szám - p. 35-50.

KOLLÁR, Csaba ; ZAKAR, Ákos (2020a)*: A social engineering és a manipulációs technikák és módszerek* - In. Biztonságtudományi Szemle, 2020. 2 : 2. - p. 23-38.

KOLLÁR, Csaba ; ZAKAR, Ákos (2020b)*: A social engineering és a manipulációs technikák és módszerek - kutatási jelentés* – In. Biztonságtudományi Szemle 2020. 2 : 3 pp. 31-46.

KÖVESI János – ERDEI János – TÓTH Zsuzsanna Eszter – JÓNÁS Tamás: *Kvantitatív módszerek*. Budapest, BME 2013

KRASZNAY Csaba, DOBOS Gergely, POLLNER Péter: *Információbiztonsági incidensek a közigazgatásban.* In: Auer, Ádám; Joó, Tamás (szerk.): Hálózatok a közszolgálatban. Budapest: Ludovika Egyetemi Kiadó 2019. - 54-59.

LEGÁRD Ildikó (2020a): *A barát és ellenség megkülönböztetése a kibertérben* – In. Jog Állam Politika: Jog- És Politikatudományi Folyóirat 2020, 12 : 3. - p. 125-140.

LEGÁRD Ildikó (2020b): *A humán faktor szerepe a kiberbiztonság megteremtésében* - In: Tick, József; Kokas, Károly; Holl, András (szerk.) Networkshop 2020. Országos Online Konferencia. 2020. szeptember 2-4., Budapest, Magyarország : Hungarnet, 2020. - p. 124-132.

LEGÁRD Ildikó (2023a): *A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintés* - In: Krasznay, Csaba (szerk.) Taktikák és stratégiák a kiberhadviselésben, Budapest, Magyarország : Ludovika Egyetemi Kiadó, 2023. - p. 11-40.

LEGÁRD Ildikó (2023b): *A közigazgatást érő hazai és európai incidenstrendek összehasonlítása*- In. Jegyző és közigazgatás XXV. évfolyam, 2. szám, 2023. - p. 34-42.

LEGÁRD Ildikó (2022a): *A nemzetközi keretrendszerek összehasonlítása és a jó gyakorlatok azonosítása az IBF szerepprofil definiálása érdekében* - In. Jegyző és közigazgatás XXIV. évfolyam, 6. szám, 2022. november-december - p. 43-55.

LEGÁRD Ildikó (2020c): *Az államok új típusú kihívásai a kibertér felől érkező fenyegetések formájában: A lehetséges válaszlépések nemzetközi jogi megítélése, a szükséges védekezési képességek kialakítása és működtetése Magyarországon* - In: Jámborné, Róth Erika (szerk.) Doktoranduszok fóruma, Miskolc, Magyarország : Miskolci Egyetem, Állam- és Jogtudományi Kar 2020. - p. 37-41.

LEGÁRD Ildikó (2023c): *Az elektronikus információs rendszer biztonságáért felelős személy szerepprofilja* – In. Jegyző és Közigazgatás 2023. XXV. évfolyam, 1. sz. - p. 39-48.

LEGÁRD Ildikó (2020d): *Building An Effective Information Security Awareness Program*. - In: Thomas, Hemker; Robert, Müller-Török; Alexander, Prosser; Dona, Scola; Tamás, Szádeczky; Nicolae, Urs (szerk.) Central and Eastern European e|Dem and e|Gov Days 2020, Wien, Ausztria : Österreichische Computer Gesellschaft (ÖCG) 2020. - p. 189-200.

LEGÁRD Ildikó (2020e): *Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre,* - In. Hadmérnök, 2020. 15. évf., 1. sz. - p. 91-105.

LEGÁRD Ildikó (2021a): *Effective methods for successful information security awareness* – In. Pro Publico Bono: Magyar Közigazgatás; A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi szakmai folyóirata 2021: 9 : 1. - p. 108-127.

LEGÁRD Ildikó (2023d): *Információbiztonsági incidenstrendek a közigazgatásban* - In. Nemzetbiztonsági Szemle (online), 2023: 11 : 1 - p. 78-107.

LEGÁRD Ildikó (2021b): *Játék a jövőért: Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével*, Polgári Szemle: Gazdasági És Társadalmi Folyóirat 2021. 17 : 1-3 - p. 358-373.

LEGÁRD Ildikó (2023e): *Közszolgálati kiberbiztonsági szerepprofil* – In. Új Magyar Közigazgatás 2023. (megjelenés alatt)

LENGYELNÉ MOLNÁR Tünde–TÓVÁRI Judit: *Kutatásmódszertan*. - Eszterházy Károly Főiskola Médiainformatika Intézet, Eger, 2001. http://publikacio.uni-eszterhazy.hu/147/1/kutatasmodszertan_lengyeln%C3%A9_t%C3%B3v%C3%A1ri.pdf

MAEYER, D. D.: *Setting up an Effective Information Security Awareness Programme*. - In: ISSE/SECURE 2007 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/SECURE 2007 Conference (part 1), 2007.

MARSI Tamás: *A Nemzeti Kibervédelmi Intézet szerepe az eseménykezelésben*. – In. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Budapest, Nemzeti Közszolgálati Egyetem, 2018, 49-84.

MICHELBERGER Pál: *Információ-, folyamat- és vállalatbiztonság*. - Budapest Óbudai Egyetem Keleti Károly Gazdasági Kar, 2018.

MITNICK, Kevin– SIMON, William L.: *A legendás hacker. A behatolás művészete*; ford. Lénárt Szabolcs – Budapest, Perfact-Pro Kft. 2006

MITNICK, Kevin– SIMON, William L.: *A legendás hacker. A megtévesztés művészete*; ford. Lénárt Szabolcs – Budapest, Perfact-Pro Kft., Bp., 2003

MITNICK, Kevin– SIMON, William L.: *A legkeresettebb hacker. Az emberi hiszékenység sötét oldala*; ford. Takács Zoltán – Budapest: HVG Könyvek,. 2012

MOLNÁR László, SASVÁRI Péter, TARPAI Zoltán Tamás: *Közigazgatási informatikai alkalmazások* – Budapest, NKE 2017.

MONORI Zsuzsanna Éva: *Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái* – In. In Medias Res 2016/2. - p. 246–261. https://media-tudomany.hu/2016/12/22/zaklatas-e-a-cyberbullying/ (Letöltve: 2023.09.25.)

MOUTON Francois, LEENEN Louise, VENTER H.S.: Social engineering attack examples, templates and scenarios – In. Computers & Security, 2016. Volume 59. - p. 186-209.

MUHA Lajos: *Az informatikai biztonság egy lehetséges rendszertana* – In. Bolyai Szemle, 2008. XVII. 4. szám, Budapest - p. 137-156.

MUHA Lajos: *Az Informatikai Biztonsági Irányítási Rendszer* - In: Cserny, László (szerk.) Informatika Korszerű Technikái Konferencia 2010, Dunaújváros, Magyarország: Dunaújvárosi Főiskola (DF) (2010) - p. 156-164.

MUHA Lajos, KRASZNAY Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése* – Budapest, NKE 2019.

MUHA Lajos, KRASZNAY Csaba: *Az elektronikus információsrendszerek biztonságáról vezetőknek* – Budapest, NKE 2014.

MUHA Lajos, SZÁDECZKY Tamás: *Irányítási rendszerek* (egyetemi jegyzet) – Budapest, NKE 2014.

NAGY László: *Az informatikai kultúra – különös tekintettel a felhasználói tudatosságra – a Magyar Honvédség szervezetében a generációk viszonyrendszerében*. – In. Hadtudományi Szemle, 2015. VIII. évfolyam 4. szám - p. 393-431.

NEMESLAKI András: *Elektronikus információbiztonság tudatosság és képzési igények a magyar közigazgatásban*. –Budapest, NKE, 2014.

NEMESLAKI András, SASVÁRI Péter: *Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában*. – In. Háttér, 2014./4. - p. 169-177.

OPPLIGER R.: *Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale*. – In. IEEE Security and Privacy. 13:6. (18-21). Online publication 2015.

OROSZI, Eszter: *Exploitable Traits as Vulnerabilities: The Human Element in Security* – In: ISACA Journal: Source Of I T Governance Professionals 2021. - p. 16-21.

OROSZI, Eszter: Információbiztonsági stratégia és vezetés, Budapest, NKE 2014.

PELTIER, T. R.: *Implementing an Information Security Awareness Program*. – In. Information Systems Security, 2005. 14 (2) - p. 37- 48.

PRAH, A. N. W. - OTCHERE, A. A. - OPAN, K. E.: *The Perceived Effectiveness of Information Security Awareness*. – In. Information and Knowledge Management, 2016.Vol.6, No.7. - 62-73.

SHAW, R. S., CHEN, C. C., HARRIS, A. L., HUANG, H.-J. (2009): *The impact of information richness on information security awareness training effectiveness*. - Computers & Education, 2009. 52., - p. 92-100.

SIPONEN, M.: *A conceptual foundation for organizational information security awareness*. In. Information Management & Computer Security, 2000. 8 (1) - p. 31-41.

SOM Zoltán - PAPP Gergely: *Hungarian Trends in Password Usage, in an International Comparison*, 2015. Budapest http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10844/SOM_PAPP_Hungarian%20Trends%20in%20Password%20Usage.pdf?sequence=1&isAllowed=y (Letöltve: 2021.11.12.)

SOM Zoltán — PAPP Gergely Zoltán: *Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban* - Nemzeti Közszolgálati Egyetem; Hírvillám-Signal Badge 2016/1., - p. 47-59.

SZARVÁK Anikó, PÓSER Valéria: *Information Technology Safety Awareness – a review of regularly used terms and methods* – In. Orosz, Gábor Tamás; Petőné Csuka, Ildikó (szerk.) 15th International Symposiumon Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020: AIS 2020, Székesfehérvár, Magyarország : Óbudai Egyetem, 2020. - p. 107-111.

SZARVÁK Anikó, PÓSER Valéria: *Review of knowledge base according to Information Technology Safety Awareness* – In. Csuka, Ildikó; Simon, Gyula (szerk.) AIS 2021-16th International Symposium on Applied Informatics and Related Areas – Proceedings, Székesfehérvár, Magyarország : Óbudai Egyetem, 2021. - p. 25-29.

TETRI, Pekka; VUORINEN, Jukka: *Dissecting social engineering* – In. Behaviour & Information Technology, 2013. Volume 32. - p. 1014-1023.

ŢIGĂNOAIA, Bogdan: *Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard,* Stud. Informatics Control, 2015

TSOHOU, A., KARYDA, M., EL-HADDADEH, R.: *Implementation challenges for information security awareness initiatives in e-government*. In. European Conference on Information Systems, 2012.

VESELI, Ilirjana: *Measuring the Effectiveness of Information Security Awereness Program*. - M. S. thesis, Gjøvik University College, Gjøvik, 2011, https://www.semanticscholar.org/paper/Measuring-the-Effectiveness-of-Information-Security-Veseli/4105e146d3e0d13afe62960db6f1157722d824c9 (Letöltve: 2023.09.12.)

ZERÉNYI, Károly: *A Likert-skála adta lehetőségek és korlátok* - Opus et Educatio 3. évfolyam 4. szám, 2016. - 470-478. http://opuseteducatio.hu/index.php/opusHU/article/view/39 (Letöltve: 2023.06.05.)

8.2. Jogszabályok jegyzéke

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

2012. évi CLXVI. törvény A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

271/2018. (XII. 20.) Korm. Rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

214/2020. (V. 18.) Korm. Rendelet az elektronikus információbiztonsági korai figyelmeztető rendszerről

7/2024. (VI.24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

1341/2019. (VI. 11.) Korm. határozat a Digitális Kompetencia Keretrendszer fejlesztéséről és bevezetésének lépéseiről

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Magyarország kiberbiztonságáról szóló törvény, tervezet T/9716 https://www.parlament.hu/web/guest/folyamatban-levo-torvenyjavaslatok?p_p_id=hu_parlament_cms_pair_portlet_PairProxy_INSTANCE_9xd2Wc9jP4z8&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_auth=VgTOrFwf&_hu_parlament_cms_pair_portlet_PairProxy_INSTANCE_9xd2Wc9jP4z8_pairAction=%2Finternet%2Fcplsql%2Fogy_irom.irom_adat%3Fp_ckl%3D42%26p_izon%3D9716

8.3. Európai uniós jogszabályok és egyéb dokumentumok

Az **Európai Parlament és a Tanács (EU) (EU) 2016/679 rendelete** (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az **Európai Parlament és a Tanács 2013/40/EU irányelve** (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

Az **Európai Parlament és a Tanács (EU) 2016/1148 irányelve** (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Az **Európai Parlament és a Tanács (EU) (EU) 2022/2555 irányelve** (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító

intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

A **Tanács 2005/222/IB kerethatározata** (2005. február 24.) az információs rendszerek elleni támadásokról

Az **Európai Gazdasági és Szociális Bizottság (2021/c 286/14) véleménye** közös közleményéről az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre (JOIN(2020) 18 final)

Az **Európai Parlament és a Tanács ajánlása** (2006. december 18.) az egész életen át tartó tanuláshoz szükséges kulcskompetenciákról

Az **Európai Gazdasági és Szociális Bizottság (2021/C 286/14) véleménye** közös közleményéről az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre (JOIN(2020) 18 final)

Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér

CyberSec4Europe https://cybersec4europe.eu/ (Letöltve: 2022.10.12.)

Digital Economy and Society Index 2022, https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (Letöltve: 2023.09.25.)

Digitális Kompetencia Keretrendszer (DIGCOMP) https://dpmk.hu/wp-content/uploads/2019/07/DigComp2.1_forditas_6_20200130.pdf (Letöltve: 2022.04.20.)

DigKomp Állampolgári Digitáliskompetencia-keret - The Digital Competence Framework for Citizens: DigComp 2.2. https://dpmk.hu/2019/07/25/a-digitalis-kompetencia-unios-referenciakerete-magyarul/ (Letöltve: 2022.10.11.) https://joint-research-centre.ec.europa.eu/digcomp_hu (Letöltve: 2022.04.20.)

CONCORDIA (Cyber Security Competence for Research and Innovation) http://www.concordia-h2020.eu/press_release/CONCORDIA_Press_release_FInal_1_Page.pdf (Letöltve: 2022.10.12.)

ECHO (The European network of Cybersecurity centres and competence Hub for innovation and Operations) https://echonetwork.eu/project-summary/ (Letöltve: 2022.10.12.)

ENISA fenyegetések 2021-ben https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf p. 7-8. (Letöltve: 2022.11.11.)

ENISA Threat Landscape 2020 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020 (Letöltve: 2022.11.11.)

ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis (Letöltve: 2022.11.11.)

ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (Letöltve: 2022.11.11.); https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_hu.pdf (Letöltve: 2022.11.11.)

ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Letöltve: 2023.09.25.)

ESCO (European Skills, Competences, Qualifications and Occupations) https://ec.europa.eu/esco/portal/howtouse/21da6a9a-02d1-4533-8057-dea0a824a17a (Letöltve: 2022.04.22.)

Európai Uniós Kiberbiztonsági Ügynökség, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees (A kiberbiztonsági készségek fejlesztése az EU-ban: a kiberbiztonsági diplomák tanúsítása) https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (Letöltve: 2022.04.21.)

European Cybersecurity Skills Framework - ECSF (Európai Kiberbiztonsági Készség-keretrendszer) https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (Letöltve: 2022.11.20.)

European Cybersecurity Taxonomy https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy (Letöltve: 2022.04.21.)

European e-Competence Framework (e-CF) https://itprofessionalism.org/ (Letöltve: 2022.03.25.)

EUROPOL (2021), European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Internet Organised Crime Threat Assessment (IOCTA) 2019, Europol https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (Letöltve: 2022.11.11.)

Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf (Letöltve: 2022.11.11.)

Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 (Letöltve: 2022.11.11.); https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (Letöltve: 2022.11.11.)

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján készült Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégia https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf (Letöltve: 2021.11.12.)

Magyary Zoltán Közigazgatási-fejlesztési Program (MP 12.0); https://www.uni-nke.hu/document/uni-nke-hu/gal_1_1modul.pdf (Letöltve: 2023.09.21.)

National Initiative for Cybersecurity Education (NICE) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (Letöltve: 2022.03.10.)

Nemzeti Digitalizációs Stratégia 2022-2030, p.88. https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf (Letöltve: 2023.03.20.)

NTT Security Global Threat Intelligence Report 2020," [Online]: https://de.nttdata.com/-/media/NTTDataGermany/Files/2020-EN-Study-NTT-Ltd-Global-Threat-Intelligence-Report-2020.pdf (Letöltve: 2023. 09. 25.)

Reference Incident Classification Taxonomy (2018) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Letöltve: 2023.09.21.)

SPARTA (Strategic programs for advanced research and technology in Europe) https://www.sparta.eu/ (Letöltve: 2022.10.12.)

The Cyber Security Body of Knowledge (CyBOK) https://www.cybok.org/ (Letöltve: 2022.03.10.)

9. ÁBRAJEGYZÉK

10. TÁBLÁZATJEGYZÉK

11. FÜGGELÉK

1. sz. melléklet: Az IBF ECSF-ben meghatározott feladatai (forrás: saját szerkesztés)

Az IBF jogszabályban meghatározott feladatai szerint, az ECSF-ben beazonosított feladatokat és a hozzá kapcsolódó készségeket, ismereteket, kompetenciákat az alábbi táblázatok mutatják be (zárójelben jelezve, hogy az adott elem, mely szerepprofilból került azonosításra):

1. Jogszabályokkal való összhang megteremtése és fenntartása	
Fő feladatok	• Biztosítja az (adatvédelmi és) adatbiztonsági szabványoknak, törvényeknek és rendeleteknek való megfelelést jogi tanácsadás és iránymutatás nyújtása segítségével *(Legal, Policy and Compliance Officer)* • Irányítja az Információbiztonsági Irányítási Rendszer alkalmazását és fejlesztését. *(Legal, Policy and Compliance Officer)*
Kulcs készségek	• A kiberbiztonsággal kapcsolatos törvények, rendeletek és jogszabályok elemzése és betartása. *(CISO)* • Kiberbiztonsági irányelvek, tanúsítványok, szabványok, módszertanok és keretrendszerek elemzése és végrehajtása. *(CISO)* • Az üzleti stratégia, modellek és termékek átfogó megértése, valamint a jogi, szabályozási és szabványkövetelmények figyelembevételének képessége. *(Legal, Policy and Compliance Officer)* • Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása. *(CISO)*
Kulcs ismeretek	• Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok *(CISO)* • Kiberbiztonsággal kapcsolatos tanúsítványok *(CISO)* • Kiberbiztonsági szabványok, módszertanok és keretrendszerek *(CISO)* • Kiberbiztonsági politikák *(CISO)*
E-kompetenciák	• **D.10. Információ- és tudásmenedzsment** 3. szint Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és ennek megfelelően biztosítja a legmegfelelőbb információs struktúrát. *(Cybersec. Researcher)* • **E.8. Információbiztonsági irányítás** 4. szint Vezeti az információs

	rendszerekben tárolt adatok integritásának, bizalmasságának és rendelkezésre állásának biztosítását, és megfelel az összes jogi követelménynek. *(CISO)* • **E.9. Információs rendszerek irányítása** 4. szint Az információs rendszerek irányítási stratégiájának vezetése a vonatkozó folyamatok kommunikálásával, terjesztésével és ellenőrzésével a teljes IKT-infrastruktúrában. *(CISO)*

2. Szabályozás / Véleményezés	
Fő feladatok	• Előkészíti és bemutatja a szervezet felső vezetése jóváhagyása céljából a kiberbiztonság jövőképét, stratégiáját és politikáját, valamint biztosítja ezek megvalósítását. *(CISO)* • Meghatározza, végrehajtja, kommunikálja és fenntartja a kiberbiztonsághoz kapcsolódó célokat, követelményeket, stratégiákat, politikákat beleértve az erőforrás tervezést is az üzleti stratégiával összehangolva a szervezeti célok támogatása érdekében. *(CISO)* • Kidolgozza a kiberbiztonsági terveket *(CISO),* többek között az Incidenkezelési Tervet is. *(Incident Responser)*
Kulcs készségek	• A kiberbiztonsági stratégia kidolgozása, támogatása és végrehajtásának irányítása. *(CISO)* • Információbiztonsági irányítási rendszer (IBIR) kialakítása, alkalmazása, ellenőrzése és felülvizsgálata közvetlen irányítással, vagy kiszervezés révén. *(CISO)* • Kiberbiztonsági terv kidolgozása. *(CISO)* • A szervezet információbiztonsági stratégiája szükséges módosításainak előrejelzése és új tervek kidolgozása. *(CISO)* • A jogi keretrendszer módosításainak megértése, a változások átvezetése a kiberbiztonsági és adatvédelmi stratégiába és politikákba. *(Legal, Policy and Compliance Officer)* • Az üzleti igényeket és a jogi követelményeket kiegészítő, megfelelő kiberbiztonsági és adatvédelmi irányelvek és eljárások kidolgozásának irányítása. *(Legal, Policy and Compliance Officer)*
Kulcs ismeretek	• Kiberbiztonsági szabványok, módszertanok és keretrendszerek *(CISO)* • Kiberbiztonsági ajánlások és legjobb gyakorlatok *(CISO)* • Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok *(CISO)* • Kiberbiztonsággal kapcsolatos tanúsítványok *(CISO)* • Etikus kiberbiztonsági szervezeti követelmények *(CISO)* • Kiberbiztonsági érettségi modellek *(CISO)*

	• Kiberbiztonsági eljárások *(CISO)* • Erőforrás-gazdálkodás *(CISO)* • Irányítási gyakorlatok *(CISO)* • Kockázatkezelési szabványok, módszertanok és keretrendszerek *(CISO)*
E-kompetenciák	• **A.1. Az információs rendszerek és az üzleti stratégia összehangolása 4. szint** Vezető szerepet vállal a hosszú távú innovatív informatikai megoldások kialakításában és végrehajtásában. *(Legal, Policy and Compliance Officer)* • **B.5. Dokumentumok előállítása - 3. szint** A részletesség szintjét a célcsoport igényeihez igazítja. *(Incident Responder)* • **D.1. Információbiztonsági stratégia kidolgozása 5. szint** Stratégiai vezetést biztosít az információbiztonságnak a szervezet kultúrájába való beillesztése érdekében. *(CISO)* • **E.8. Információbiztonsági irányítás - 3. szint** Értékeli a biztonságirányítási intézkedéseket és mutatókat, dönt ezek információbiztonsági politikának való megfelelőségéről. Vizsgálatot és korrekciós intézkedéseket kezdeményez a biztonsági előírások megsértése esetén. *(Educator)*

3. Tudatosítás	
Fő feladatok	• A kiberbiztonsággal és adatvédelemmel kapcsolatos tantervek és oktatási anyagok kidolgozása, frissítése és azok átadása a képzés során a tudatosság növelése érdekében, a tartalom, a módszer, az eszközök, valamint a képzésben résztvevők igényei figyelembevételével. *(Educator)* • A kiberbiztonsággal és adatvédelemmel kapcsolatos tudatosságnövelő tevékenységek, szemináriumok, tanfolyamok, gyakorlati képzések szervezése, tervezése és lebonyolítása. *(Educator)* • A képzés hatékonyságának nyomon követése, értékelése és jelentése. *(Educator)* • A képzésben részt vevők teljesítményének értékelése és jelentése. *(Educator)* • Új megközelítések keresése az oktatás, képzés és tudatosságnövelés számára. *(Educator)* • A kiberbiztonság fejlődési irányainak nyomonkövetése. *(CISO)*
Kulcs készségek	• A kiberbiztonsági tudatossággal, képzéssel és oktatással kapcsolatos igények azonosítása. *(Educator)* • A kiberbiztonsági igények lefedésére irányuló tanulási programok

	tervezése, fejlesztése és megvalósítása. *(Educator)* • Kiberbiztonsági gyakorlatok kidolgozása, beleértve a kibertér tágabb értelemben vett környezetét alkalmazó szimulációkat is. *(Educator)* • A meglévő, kiberbiztonsággal kapcsolatos képzési források felhasználása. *(Educator)* • Értékelési programok kidolgozása a tudatosságnövelő, képzési és oktatási tevékenységekhez. *(Educator)* • A célközönségnek megfelelő pedagógiai megközelítések azonosítása és kiválasztása. *(Educator)* • Az emberek motiválása és bátorítása. *(Educator)*
Kulcs ismeretek	• Kiberbiztonsági tudatosítás, oktatás és képzési programok fejlesztése. *(Educator)* • Kiberbiztonsággal kapcsolatos tanúsítványok. *(Educator)* • Kiberbiztonsági oktatási és képzési szabványok, módszertanok és keretrendszerek. *(Educator)*
E-kompetenciák	• **D.3. Oktatási és képzési szolgáltatás 3. szint** Kreatívan jár el a készséghiányok elemzése érdekében; konkrét követelményeket dolgoz ki és azonosítja a képzési kínálat lehetséges forrásait. Szakterületi ismeretekkel rendelkezik a képzési piacról, és visszajelzési mechanizmust hoz létre az alternatív képzési programok hozzáadott értékének értékelésére. *(Educator)* • **D.9. Humánerőforrás-fejlesztés 3. szint** Figyelemmel kíséri és kezeli az egyének és csoportok fejlesztési igényeit. *(Educator)*

4. Kockázatkezelés	
Fő feladatok	• Kidolgozza a szervezet kiberbiztonsági kockázatkezelési stratégiáját. *(Risk Manager)* • Kidolgozza, fenntartja, jelenti és kommunikálja a teljes kockázatkezelési ciklust. *(Risk Manager)* • Értékeli a kiberbiztonsági kockázatokat és javaslatot tesz a legmegfelelőbb kockázatkezelési lehetőségekre, beleértve a biztonsági kontrollokat, valamint azokat a kockázatcsökkentő és a kockázatok elkerülését segítő intézkedéseket, amelyek a legjobban illeszkednek a szervezet stratégiájába. *(Risk Manager)* • Azonosítja és értékeli az IKT-rendszerek kiberbiztonsággal kapcsolatos fenyegetéseit és sebezhetőségeit. *(Risk Manager)* • Azonosítja a fenyegetettségi környezetet, beleértve a támadók profilját és a támadási potenciál becslését. *(Risk Manager)* • Nyomon követi a kiberbiztonsági ellenőrzések hatékonyságát és a

	kockázati szinteket. *(Risk Manager)* • Biztosítja hogy valamennyi kiberbiztonsági kockázat a szervezet számára elfogadható szinten maradjon. *(Risk Manager)* • Biztosítja, hogy a felső vezetés jóváhagyja a szervezet kiberbiztonsági kockázatait. *(CISO)* • Közvetíti a megfelelő biztonsági fokozatot a nem szakértő érdekeltek számára a kockázati kitettség és annak következményei kommunikálásával. *(Cyber Threat Intelligence Specialist)* • Nyomon követi a kockázatjavításra irányuló tevékenységeket. *(Auditor)*
Kulcs készségek	• Kiberbiztonsági kockázatkezelési keretrendszerek, módszertanok és iránymutatások átültetése, valamint a szabályozásoknak és szabványoknak való megfelelés biztosítása. *(Risk Manager)* • A szervezet minőségirányítási és kockázatkezelési gyakorlatának elemzése és megerősítése. *(Risk Manager)* • Képessé teszi az üzleti rendszerek tulajdonosait, a vezetőket és más érdekelt feleket arra, hogy a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozzanak. *(Risk Manager)* • Kiberbiztonsági kockázattudatos környezet kialakítása. *(Risk Manager)* • Kockázatmegosztási lehetőségek tervezése és kezelése. *(Risk Manager)* • A szervezet kiberbiztonsági helyzetének értékelése és javítása *(CISO)* • A kiberbiztonsággal kapcsolatos problémák azonosítása és megoldása. *(CISO)* • A rendszerek részekre bontása és elemzése a gyenge pontok és a nem hatékony ellenőrzések azonosítása érdekében. *(Researcher)*
Kulcs ismeretek	• Kockázatkezelési szabványok, módszertanok és keretrendszerek (*Risk Manager)* • Kockázatkezelési eszközök *(Risk Manager)* • Kockázatkezelési ajánlások és legjobb gyakorlatok *(Risk Manager)* • Kiberfenyegetések *(Risk Manager)* • Számítógépes rendszerek sebezhetőségei *(Risk Manager)* • Kiberbiztonsági kockázatok *(Risk Manager)*
E-kompetenciák	• **C.4. Problémakezelés 3. szint** Az IKT-infrastruktúra és a problémakezelési folyamat speciális ismereteit használja fel a hibák azonosítása és a minimális kieséssel történő megoldása érdekében. Nyomás alatt is megalapozott döntéseket hoz az üzleti hatás minimalizálása érdekében szükséges megfelelő intézkedésekről. *(Researcher)* • **E.3. Kockázatkezelés 4. szint** Vezető szerepet vállal a

	kockázatkezelési politika meghatározásában és annak alkalmazásban, figyelembe véve az összes lehetséges korlátozó tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál. *(Risk Manager)*

5. Biztonsági események kezelése	
Fő feladatok	• Kidolgozza, végrehajtja és értékeli az incidensek kezelésével kapcsolatos eljárásokat. *(Incident Responder)* • Biztosítja a szervezet ellenálló képességét a kiberbiztonsági incidensekkel szemben. *(CISO)* • Azonosítja, elemzi, mérsékli és kommunikálja a kiberbiztonsági incidenseket. *(Incident Responder)* • Értékeli és kezeli a technikai sebezhetőségeket. *(Incident Responder)* • Méri a kiberbiztonsági incidensek észlelése és a válaszadás hatékonyságát. *(Incident Responder)* • Értékeli a kiberbiztonsági ellenőrzéseket és a kiberbiztonsági incidenst követően hozott intézkedések ellenálló képességét. *(Incident Responder)* • Eljárásokat dolgoz ki az incidensek következményeinek elemzésére és az incidenskezelési jelentésre vonatkozó eljárásokra. *(Incident Responder)* • Dokumentálja az incidensek következményeinek elemzését és az incidenskezelési intézkedéseket. *(Incident Responder)* • Együttműködik a biztonsági műveleti központokkal (SOC) és a számítógépes biztonsági eseményelhárítási csoportokkal (CSIRT). *(Incident Responder)* • Azonosítja és értékeli a szervezetet érintő kiberfenyegetések szereplőit. (*Cyber Threat Intelligence S.)* • Azonosítja, nyomon követi és értékeli a kiberfenyegetést jelentő szereplők által alkalmazott taktikákat, technikákat és eljárásokat, a nyílt forráskódú, a védett adatok, információk és a hírszerzési adatok elemzésével. *(Cyber Threat Intelligence S.)*
Kulcs készségek	• Az eseménykezelés és válaszadás során a feladatok valamennyi technikai, funkcionális és operatív aspektusának gyakorlása. *(Incident Responder)* • A kiberfenyegetésről szóló, többféle forrásból származó információk összegyűjtése, elemzése és összefüggéseinek feltárása. *(Incident Responder, Cyber Threat Intelligence S.)* • (Naplófájlok kezelése és elemzése. *(Incident Responder))*

	• A kiberbiztonsági fenyegetések, igények és közelgő kihívások előrejelzése. *(CISO)*
Kulcs ismeretek	• Incidenskezelési szabványok, módszertanok és keretrendszerek. *(Incident Responder)* • Eseménykezelési ajánlások és legjobb gyakorlatok. *(Incident Responder)* • Incidenskezelési eszközök (*Incident Responder)* • Operációs rendszerek biztonsága (*Incident Responder)* • Számítógépes hálózatok biztonsága *(Incident Responder)* • Kiberfenyegetések *(Incident Responder)* • Kibertámadási formák *(Incident Responder)* • Számítógépes rendszerek sebezhetőségei *(Incident Responder)* • Biztonsági műveleti központok (SOC) működése *(Incident Responder)* • Számítógépes biztonsági eseményelhárítási csoportok (CSIRT) működése *(Incident Responder)*
E-kompetenciák	• **C.4. Problémakezelés 4. szint** Vezető szerepet tölt be és felelős a teljes problémakezelési folyamatért. Beosztja és biztosítja, hogy jól képzett emberi erőforrások, eszközök és diagnosztikai berendezések álljanak rendelkezésre a vészhelyzeti események kezelésére. Mély szakértelemmel rendelkezik a kritikus komponensek meghibásodásának előrejelzéséről és a minimális leállási idővel történő helyreállításról. Kialakítja az eszkalációs folyamatokat annak érdekében, hogy minden egyes incidenshez megfelelő erőforrásokat lehessen alkalmazni. *(Incident Responder)*

6. Ellenőrzés / Audit	
Fő feladatok	• Kiberbiztonsági ellenőrzéseket hajt végre. *(Implementer)* • Dokumentálja és jelentést készít a rendszerek, szolgáltatások és termékek biztonságáról. *(Implementer)* • Kidolgozza az ellenőrzési tervet, melyben megfogalmazza az alkalmazni kívánt keretrendszereket, szabványokat, módszertant és ellenőrzési teszteket. *(Auditor)* • Végrehajtja az ellenőrzési tervet, illetve összegyűjti a bizonyítékokat és dokumentálja a méréseket. *(Auditor)* • Meghatározza a rendszerek auditálásához használt módszertanokat és gyakorlatokat. *(Auditor)* • Meghatározza a célterületet és irányítja az auditálási tevékenységeket. *(Auditor)* • Meghatározza az audit hatókörét, célkitűzéseit és az audittal szemben

	támasztott követelményeket. *(Auditor)* • Ellenőrzi a kiberbiztonsággal kapcsolatos alkalmazandó törvényeknek és rendeleteknek való megfelelést. *(Auditor)* • Ellenőrzi a kiberbiztonsággal kapcsolatos alkalmazandó szabványoknak való megfelelést. *(Auditor)*
Kulcs készségek	• Auditálási eszközök és technikák alkalmazása. *(Auditor)* • Üzleti folyamatok elemzése, a szoftver- vagy hardverbiztonság értékelése és felülvizsgálata, technikai és szervezeti ellenőrzések. *(Auditor)* • A rendszerek elemeire bontása és elemzése a gyenge pontok és a nem hatékony ellenőrzések azonosítása érdekében. *(Auditor)* • Az auditálási információk összegyűjtése, értékelése, megőrzése és védelme. *(Auditor)* • Az ellenőrzés integránsan, pártatlanul és függetlenül történő elvégzése. *(Auditor)*
Kulcs ismeretek	• Kiberbiztonsági ellenőrzések és megoldások *(Auditor)* • Auditálási szabványok, módszertanok és keretrendszerek *(Auditor)* • Kiberbiztonsági szabványok, módszertanok és keretrendszerek *(Auditor)* • Az auditálással kapcsolatos tanúsítás *(Auditor)* • Kiberbiztonsággal kapcsolatos tanúsítások *(Auditor)*
E-kompetenciák	• **B.3. Tesztelés – 4. szint** Széleskörű szaktudást használ a teljes tesztelési tevékenység folyamatának kialakítására, beleértve a belső gyakorlati szabályok kialakítását is. Szakértői útmutatást és tanácsadást nyújt a tesztelési csoportnak. *(Auditor)* • **E.6. IKT minőségbiztosítás– 4. szint** Értékeli és megállapítja a minőségi követelmények teljesítésének mértékét, és irányítja a minőségpolitika végrehajtását. Gyakorlati vezetést biztosít a minőségi szabványok meghatározásához és teljesítéséhez. *(Auditor)* • **E.8. Információbiztonsági irányítás - 3. szint** Értékeli a biztonságirányítási intézkedéseket és mutatókat, dönt ezek információbiztonsági politikának való megfelelőségéről. Vizsgálatot és korrekciós intézkedéseket kezdeményez a biztonsági előírások megsértése esetén. *(Legal, Policy and Compliance Officer)* • **E.9. Információs rendszerek irányítása - 4. szint** Az információs rendszerek irányítási stratégiájának vezetése a vonatkozó folyamatok kommunikálásával, terjesztésével és ellenőrzésével a teljes IKT-infrastruktúrában. *(CISO)*

7. Tájékoztatás / Jelentés (vezetés, érintettek)	
Fő feladatok	• Tájékoztatja a felső vezetést a kiberbiztonsági kockázatokról, fenyegetésekről és azok hatásáról a szervezetre. *(CISO)* • Jelentést tesz a felső vezetésnek a kiberbiztonsági incidensekről, kockázatokról és megállapításokról. *(CISO)* • Egyeztet a felső vezetéssel a kiberbiztonsággal kapcsolatos költségvetésről. *(CISO)* • Támogatást nyújt a kiberbiztonsággal kapcsolatos kérdésekben a felhasználók és/vagy ügyfelek számára. *(Implementer)* • Szorosan együttműködik az informatikusokkal[192] a kiberbiztonsággal kapcsolatos intézkedéseken. *(Implementer)*
Kulcs készségek	• A jogi és szabályozási követelmények, valamint az üzleti igények kommunikálása, magyarázata és adaptálása. *(Auditor)* • A biztonsági dokumentumok, jelentések, SLA-k felülvizsgálata és javítása, valamint a biztonsági célkitűzések elérésének biztosítása. *(CISO)* • Kommunikáció, bemutatás és jelentés az érintett érdekeltek számára. *(Threat Intelligence Specialist)*
Kulcs ismeretek	
E-kompetenciák	• **A.7. Technology Trend Monitoring – 5. szint** Megtervezi és vezeti a szisztematikus technológiai megfigyelés szervezeti struktúráját és támogatási rendszerét. Tanácsot ad és befolyásolja a stratégiai döntéseket a jövőbeli IKT-megoldások megtervezésében és megfogalmazásában. *(Researcher)* • **B.5. Dokumentumok előállítása 3. szint** A részletesség szintjét a célcsoport igényeihez igazítja *(Incident Responder)* • **E.4. Kapcsolatmenedzsment 3. szint** Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. *(Threat Intelligence Specialist)* • **E.9. Információs rendszerek irányítása 4. szint** Az információs rendszerek irányítási stratégiájának vezetése a vonatkozó folyamatok kommunikálásával, terjesztésével és ellenőrzésével a teljes IKT-infrastruktúrában. *(Legal, Policy and Compliance Officer)*

8. Kapcsolattartás	
Fő feladatok	• Kapcsolatot alakít ki a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel. *(CISO)* • Együttműködik és információkat oszt meg a hatóságokkal és szakmai

[192] szerzői megjegyzés: üzemeltetőkkel

	csoportokkal. *(Legal, Policy and Compliance Officer)* • Kiberbiztonsággal kapcsolatos támogatást nyújt a felhasználók és az ügyfelek számára. *(Implementer)*
Kulcs készségek	• Kommunikálás, koordinálás és együttműködés a belső és külső érdekelt felekkel. *(CISO)* • Az üzleti igényeket és a jogi követelményeket kiegészítő, megfelelő kiberbiztonsági és adatvédelmi irányelvek és eljárások kidolgozásának irányítása; továbbá az érintett felek közötti elfogadás, megértés, végrehajtás és kommunikáció biztosítása. *(Legal, Policy and Compliance Officer)*
Kulcs ismeretek	
E-kompetenciák	• **E.4. Kapcsolatmenedzsment 3. szint** Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. *(Threat Intelligence Specialist)*

9. Egyéb feladatok	
Fő feladatok	• Nyomon követi a kiberbiztonság fejlődési irányait. *(CISO)* • Biztosítja a kiberbiztonsági stratégia végrehajtásához szükséges erőforrásokat. *(CISO)* • Irányítja a szervezeten belüli folyamatos kapacitásépítést. *(CISO)* • Biztosítja a megfelelő kiberbiztonsági erőforrások felülvizsgálatát, tervezését és elosztását. *(CISO)* • Elvégzi a kiberbiztonsági megoldások integrálását és biztosítja megfelelő működésüket. *(Implementer)* • Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát. *(Implementer)* • Alkalmazza és irányítja a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat. *(Implementer)* • Elemzi és értékeli a kiberbiztonsági technológiákat, megoldásokat, fejlesztéseket és eljárásokat. *(Researcher)*
Kulcs készségek	• Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása. *(CISO)* • A kiberbiztonsági erőforrások vezetése. *(CISO)* • A szervezet kiberbiztonsági kultúrájának befolyásolása. *(CISO)* • A kiberbiztonsági irányítás érettségi modelljeinek meghatározása és alkalmazása. *(CISO)* • A munkatársak motiválása és ösztönzése. *(CISO)* • Az etikai követelmények és szabványok megértése, gyakorlása és betartása. *(Legal, Policy and Compliance Officer)*

	• Kiberbiztonsági megoldások integrálása a szervezet infrastruktúrájába. *(Implementer)* • A megoldások értékelése azok biztonságossága és teljesítménye alapján. *(Implementer)* • Új ötletek megfogalmazása és az elmélet átültetése a gyakorlatba. *(Researcher)* • A kiberbiztonsággal kapcsolatos technológiák új fejlesztéseinek nyomon követése. *(Researcher)*
Kulcs ismeretek	• Kiberbiztonsági trendek *(Architect)* • Kiberbiztonsággal kapcsolatos technológiák *(Architect)* • Kiberbiztonsági megoldások és kontrollok *(Architect)*
E-kompetenciák	• **D.10. Információ- és tudásmenedzsment – 3. szint** Elemzi az üzleti folyamatokat, illetve a kapcsolódó információs követelményeket, és biztosítja a legmegfelelőbb információs struktúrát. *(Researcher)*

Egyéb általános készségek	
Kulcs készségek	• A munkatársak motiválása és ösztönzése. • Nyomás alatti munkavégzés. • Kommunikáció, prezentáció és jelentéstétel az érdekelt felek számára. • Az etikai követelmények és szabványok megértése, gyakorlása és betartása. • Együttműködés más csapattagokkal és kollégákkal. • Kommunikáció, koordináció és együttműködés a belső és külső érdekelt felekkel.

2. sz. melléklet: A közszolgálati dolgozók, ECSF-ben azonosítható kiberbiztonsági feladatai, és az ellátást támogató ismeretek, készségek és kompetenciák (forrás: saját szerkesztés)

Az IBF ECSF-ben azonosított feladatai közül a táblázatban kizárólag azokat szerepeltetem („IBF" oszlop), amelyek a közszolgálati dolgozók mindennapi feladatellátása szempontjából relevánsnak számítanak. A táblázat harmadik, „közszolgálati dolgozó" oszlopában azok a feladatok, készégek, ismeretek és kompetenciák kerülnek meghatározásra, amelyek az IBF feladatai szervezeti szintű végrehajtásához kapcsolódnak, ugyanakkor értelmezhetők és figyelembe veendők a közszolgálati dolgozók munkavégzése során. Ez utóbbi oszlopban piros színnel jelölve szerepelnek azon elemek, amelyek a hazai jogszabályokkal, elsősorban az Ibtv.-vel, valamint annak végrehajtási rendeleteivel való összhang megteremtését célozzák, és a közszolgálati dolgozók számára nélkülözhetetlenek a kiberbiztonsággal kapcsolatos feladatok ellátása, valamint a szervezeti szintű kiberbiztonság megteremtése szempontjából.

A ECSF-ben több feladat esetében meghatározott „adatvédelem" fogalma a magyar jogszabályi környezetben egyértelműen a GDPR[193], valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) fogalomkörébe tartozik, így ez nem képezi a vizsgálat részét.

A közszolgálati dolgozók feladatellátása szempontjából releváns kiberbiztonsági feladatok, ismeretek, készségek és kompetenciák meghatározása, az IBF számára az ECSF profilokban beazonosított szerepprofil elemek alapján:

1. Jogszabályokkal való összhang megteremtése

	IBF	Közszolgálati dolgozó
ECSF-ben azonosított feladatok	Biztosítja az (adatvédelmi és) adatbiztonsági szabványoknak, törvényeknek és rendeleteknek való megfelelést jogi tanácsadás és iránymutatás nyújtása segítségével	Biztosítja a munkaköréhez kapcsolódóan a kiberbiztonsággal kapcsolatos szabványoknak, törvényeknek, rendeleteknek, illetve a szervezetszabályozó eszközöknek[194] való megfelelést.
Kulcs készségek	A kiberbiztonsággal kapcsolatos törvények, rendeletek és jogszabályok elemzése és betartása.	Képes a feladatai ellátása során alkalmazni a kiberbiztonságra vonatkozó jogi követelményeket, szervezetszabályozó

[193] Az Európai Parlament és a Tanács (Eu) 2016/679 rendelete „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről" (általános adatvédelmi rendelet)

[194] A szervezet elektronikus információs rendszereire vonatkozó, szervezeti szintű informatikai biztosági szabályokat az Ibtv. 11.§ (1) f) és 13.§ (2) c) pontjai szerint az informatikai biztonsági szabályzatban kell rögzíteni, melyet a kijelölt hatóság részére megküldeni szükséges.

	Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása.	eszközöket, valamint a vonatkozó ajánlásokat és a bevált gyakorlatokat.
	Az üzleti stratégia, modellek és termékek átfogó megértése, valamint a jogi, szabályozási és szabványkövetelmények figyelembevételének képessége.	Képes megérteni és feladatai ellátása során figyelembe venni a szervezeti célokat, a jövő képet, a biztonsággal kapcsolatos politikát és stratégiát, a jogi, szabályozási és szabvány követelményeket.
Kulcs ismeretek	Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok.	Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete.
E-kompetenciák	E.8. Információbiztonsági irányítás 4. szint Vezeti az információs rendszerekben tárolt adatok integritásának, bizalmasságának és rendelkezésre állásának biztosítását, és megfelel az összes jogi követelménynek.	Részt vesz az információs rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, és a vonatkozó jogi követelménynek való megfelelésben.

35. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Jogszabályokkal való összhang megteremtése és fenntartása (forrás: saját szerkesztés)

2. Szabályozás / Véleményezés

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	Előkészíti és bemutatja a szervezet felső vezetése jóváhagyása céljából a kiberbiztonság jövőképét, stratégiáját és politikáját, valamint biztosítja ezek megvalósítását.	Részt vesz a feladatköréhez kapcsolódóan a szervezet kiberbiztonsága jövőképét, stratégiáját és politikáját meghatározó dokumentumok végrehajtásában. Részt vesz az Informatikai Biztonsági Szabályzat végrehajtásában.[195] Részt vesz a feladatkörét érintő kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.[196]
Kulcs készségek	A kiberbiztonsági stratégia kidolgozása, támogatása és végrehajtásának irányítása.	Képes részt venni a szervezet kiberbiztonsági jövőképének, stratégiájának, politikájának, valamint az Informatikai Biztonsági szabályzatnak a feladatköréhez kapcsolódó végrehajtásában.
	Az üzleti igényeket és a jogi követelményeket kiegészítő, megfelelő kiberbiztonsági és adatvédelmi irányelvek, valamint eljárások kidolgozásának irányítása.	Képes részt venni a feladatköréhez kapcsolódó, a szervezetszabályozó eszközöket és egyéb jogi követelményeket kiegészítő, megfelelő kiberbiztonsági irányelvek, eljárások és szabályok kidolgozásában és végrehajtásában. Képes részt venni a feladatkörét érintő, kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök, szerződések véleményezésében.[197]
Kulcs ismeretek	Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok.	Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete.
	Etikus kiberbiztonsági szervezeti	Etikus kiberbiztonsági szervezeti követelmények.

[195] Ld. 169. lj.
[196] Alapvetően az Ibtv, 13. § (2) e) pontja szerint az IBF feladata, azonban végrehajtása az adott elektronikus információs rendszer tekintetében elképzelhetetlen a szakterület (adatgazda) közreműködése nélkül.
[197] Ld. 171. lj.

	követelmények.	
E-kompetenciák	D1 Információbiztonsági stratégia kidolgozása 5. szint Stratégiai vezetést biztosít az információbiztonságnak a szervezet kultúrájába való beillesztése érdekében.	Részt vesz az információbiztonságnak a szervezet kultúrájába való beillesztése folyamatában.

36. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Szabályozás / Véleményezés (forrás: saját szerkesztés)

3. Tudatosítás

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	A kiberbiztonsággal és adatvédelemmel kapcsolatos tudatosságnövelő tevékenységek, szemináriumok, tanfolyamok, gyakorlati képzések szervezése, tervezése és lebonyolítása.	Részt vesz a kiberbiztonsággal kapcsolatos tudatosságnövelő programokon, az előírt követelményeket teljesíti.
Kulcs készségek		Képes a biztonságtudatosító programokon való aktív részvételre, a tananyag elsajátítására és alkalmazására.[198] Képes megfogalmazni az elsajátítandó ismeretekre, készségekre vonatkozó igényét.[199]
Kulcs ismeretek		Kiberbiztonsággal kapcsolatos jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete. Általános kiberbiztonsági ismeretek, szervezeti szinten az információbiztonsági előírások és stratégiák feladatkörhöz kapcsolódó ismerete. A megfelelő kiberbiztonsági eljárások, követelmények, technikák, ajánlások és szabványok feladatkörhöz kapcsolódó ismerete, a lehetséges támadási és védekezési alternatívák alapszintű ismerete.
E-kompetenciák		Részt vesz a tudatosító képzések során elsajátított ismeretek, készségek segítségével a biztonságtudatos szervezeti kultúra kialakításában, fenntartásában és kommunikálásában.

37. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai -Tudatosítás (forrás: saját szerkesztés)

4. Kockázatkezelés

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	Kidolgozza, fenntartja, jelenti és kommunikálja a teljes kockázatkezelési ciklust. Kidolgozza a szervezet kiberbiztonsági kockázatkezelési stratégiáját.	Részt vesz a feladatköréhez kapcsolódóan a kockázatkezelés folyamatában.
	Biztosítja hogy valamennyi kiberbiztonsági kockázat a szervezet számára elfogadható	Részt vesz az IBF által azonosított kockázatok értékelésében, valamint a

[198] Az Ibtv. 11.§ (1) g) pontja szerint a szervezet vezetőjének felelősségi körébe tartozik a biztonságtudatosítás, azonban ez a feladat kizárólag a munkatársak együttműködésével valósítható meg, a„Tudatosítás” részeként azonosított feladatok, készségek, ismeretek és kompetenciák segítségével.
[199] Ld. 173. lj.

	szinten maradjon. Értékeli a kiberbiztonsági kockázatokat és javaslatot tesz a legmegfelelőbb kockázatkezelési lehetőségekre, beleértve a biztonsági kontrollokat, valamint azokat a kockázatcsökkentő és a kockázatok elkerülését segítő intézkedéseket, amelyek a legjobban illeszkednek a szervezet stratégiájába.	kockázatkezelésben (a kockázatra adott válaszlépések meghatározásában, a kockázatcsökkentő intézkedések végrehajtásában).
Kulcs készségek	A szervezet kiberbiztonsági helyzetének értékelése és javítása. A kiberbiztonsággal kapcsolatos problémák azonosítása és megoldása. Képessé teszi az üzleti rendszerek tulajdonosait, a vezetőket és más érdekelt feleket arra, hogy a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozzanak.	Képes a feladatköréhez kapcsolódóan a kiberbiztonsági problémák azonosítására, a kockázatok értékelésére, valamint a kockázatcsökkentő intézkedések megértésére és végrehajtására. Képes a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozni. (Kizárólag vezetői szerepben.)
Kulcs ismeretek	Kiberfenyegetések Számítógépes rendszerek sebezhetőségei Kiberbiztonsági kockázatok	A kiberbiztonsági kockázatok, a kiberfenyegetések valamint a számítógépes rendszerek sebezhetőségei alapszintű ismerete. A kockázatkezelés folyamatának és abban betöltött szerepének alapszintű ismerete.[200]
E-kompetenciák	E.3. Kockázatkezelés 4. szint Vezető szerepet vállal a kockázatkezelési politika meghatározásában és annak alkalmazásban, figyelembe véve az összes lehetséges korlátozó tényezőt, beleértve a műszaki, gazdasági és politikai kérdéseket is. Feladatokat delegál. C.4. Problémakezelés 3. szint Az IKT-infrastruktúra és a problémakezelési folyamat speciális ismereteit használja fel a hibák azonosítása és minimális kieséssel történő megoldása érdekében. Nyomás alatt is megalapozott döntéseket hoz az üzleti hatás minimalizálása érdekében szükséges megfelelő intézkedésekről.	Megérti és alkalmazza a kockázatkezelés elveit, részt vesz az IBSZ-ben meghatározott kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében a feladatköréhez kapcsolódóan. A kockázatokra vonatkozó információkkal alátámasztott, megalapozott döntéseket hoz a feladatköréhez kapcsolódó kockázatok értékelése, kezelése és mérséklése érdekében. (Kizárólag vezetői szerepben.)

38. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai -Kockázatkezelés (forrás: saját szerkesztés)

5. Biztonsági események kezelése

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	Kidolgozza, végrehajtja és értékeli az incidensek kezelésével kapcsolatos eljárásokat. Azonosítja, elemzi, mérsékli és kommunikálja a kiberbiztonsági incidenseket.	Részt vesz a szervezet belső szervezetszabályozó eszközeiben rögzített incidenskezelési eljárásban a feladatköréhez kapcsolódóan. Azonosítja és jelenti az IBF-nek a kiberbiztonsági eseményeket vagy annak gyanúját, részt vesz az esetleges károk

[200] Az Ibtv. 11.§ (1) h) pontja alapján a rendszeresen végrehajtott biztonsági kockázatelemzések a szervezet vezetője feladatát képzik, azonban a kockázatok felmérése, értékelése valamint a megfelelő információk birtokában hozott, kockázatokra vonatkozó döntések meghozatala az adatgazda felelősségi körébe tartoznak.

		enyhítésében.
Kulcs készségek	Az eseménykezelés és válaszadás során a feladatok valamennyi technikai, funkcionális és operatív aspektusának gyakorlása.	Képes gyakorolni az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatokat. Képes a problémák és hibák segítséggel történő elhárítására. Képes a social engineering típusú támadásokat felismerni.
Kulcs ismeretek	Kiberfenyegetések Kibertámadási formák Számítógépes rendszerek sebezhetőségei	A potenciális kiberfenyegetések, kibertámadási formák és a számítógépes rendszerek sebezhetőségeinek alapszintű ismerete.
E-kompetenciák	C.4. Problémakezelés 4. szint Vezető szerepet tölt be és felelős a teljes problémakezelési folyamatért. Beosztja és biztosítja, hogy jól képzett emberi erőforrások, eszközök és diagnosztikai berendezések álljanak rendelkezésre a vészhelyzeti események kezelésére. Mély szakértelemmel rendelkezik a kritikus komponensek meghibásodásának előre jelzéséről és a minimális leállási idővel történő helyreállításról. Kialakítja az eszkalációs folyamatokat annak érdekében, hogy minden egyes incidenshez megfelelő erőforrásokat lehessen alkalmazni.	Részt vesz a feladatköréhez kapcsolódó problémakezelési/incidenskezelési folyamatban, a károk enyhítése érdekében mindent megtesz, ami tőle az adott helyzetben elvárható.

39. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Biztonsági események kezelése (forrás: saját szerkesztés)

6. Ellenőrzés / Audit

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	Kiberbiztonsági eljárásokat és ellenőrzéseket hajt végre. Végrehajtja az ellenőrzési tervet, illetve összegyűjti a bizonyítékokat és dokumentálja a méréseket.	Részt vesz és/vagy együttműködik a kiberbiztonsági ellenőrzésekben. Együttműködik az ellenőrzések során a szükséges információk, adatok, dokumentumok átadásában.
Kulcs készségek		Képes az auditálási és megfelelőségértékelési módszertanok, eszközök és technikák –feladatköréhez kapcsolódó- alkalmazására. (Kizárólag vezetői szerepben.)[201] Képes részt venni az ellenőrzési jelentések elkészítésben. Képes a jogi és szabályozási környezet, valamint a műszaki üzleti igények alapszintű megértésére és kommunikációjára.

[201] Az Ibtv. 11.§ (1) h) pontja szerint a szervezet vezetőjének feladata, hogy rendszeres ellenőrzések, auditok révén meggyőződjön arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak, azonban a munkatársaknak, illetve kiemelten az adatgazda szervezeti egységeknek együtt kell működniük az ellenőrzést során az ellenőrzést végző személyekkel, melyekhez megfelelő készségek, ismeretek és kompetenciák szükségesek.

Kulcs ismeretek	Kiberbiztonsági ellenőrzések és megoldások Auditálási szabványok, módszertanok és keretrendszerek Az auditálással kapcsolatos tanúsítás Kiberbiztonsággal kapcsolatos tanúsítások	A kiberbiztonsági ellenőrzések, auditálási szabványok, módszertanok és keretrendszerek feladatkörhöz kapcsolódó alapszintű ismerete. (Kizárólag vezetői szerepben.) Az auditálással és a kiberbiztonsággal kapcsolatos tanúsítások feladatkörhöz kapcsolódó, alapszintű ismerete.
E-kompetenciák		Feladatköréhez kapcsolódóan együttműködik az ellenőrzések során az ellenőrzést végző belső szervezeti egységgel vagy külső szervezettel/céggel, részt vesz az ellenőrzések során készült dokumentumok előállításában, véleményezésében. Egyszerű vizsgálatokat végez a részletes utasítások szigorú betartásával.

40. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Ellenőrzés / Audit (forrás: saját szerkesztés)

7. Tájékoztatás / Jelentés (vezetés, érintettek)

	IBF	**Közszolgálati dolgozó**
ECSF-ben azonosított feladatok	Támogatást nyújt kiberbiztonsággal kapcsolatos kérdésekben a felhasználók és/vagy ügyfelek számára.	Bejelentést tesz, tájékoztatja az IBF-et az esetleges biztonsági eseményről, kockázatokról, továbbá bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába.
	Szorosan együttműködik az informatikusokkal a kiberbiztonsággal kapcsolatos intézkedések során.	A kiberbiztonsággal kapcsolatos intézkedések során szorosan együttműködik az IBF-fel, illetve az üzemeltetést végző informatikusokkal.
Kulcs készségek	A jogi és szabályozási követelmények, valamint az üzleti igények kommunikálása, magyarázata és adaptálása. Kommunikáció, bemutatás és jelentés az érintett érdekeltek számára.	Képes az üzleti igények kiberbiztonsági vonatkozásai kommunikálására a felső vezetés és az IBF felé. Képes kommunikálni és kapcsolatot építeni az IBF-el, illetve az érdekelt felekkel, a feladatkörét érintő kiberbiztonsági kockázatok kezelése, illetve az incidensek megelőzése és kezelése érdekében.[202] Képes jelentéseket kidolgozni, vagy az elkészítésükben közreműködni, valamint a jelentéseket megfelelően kommunikálni.[203]
Kulcs ismeretek		
E-kompetenciák	E.4. Kapcsolatmenedzsment 3. szint Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során.	Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.) Számot ad saját tevékenységéről.[204]

[202] Ibtv. 13.§ (2) bekezdéshez kapcsolódó feladatok ellátása.
[203] Ibtv. 13.§ (2) bekezdéshez kapcsolódó feladatok ellátása, kiemelten ellenőrzések, incidenskezelés, kockázatkezelés.

	E.9. Információs rendszerek irányítása 4. szint Az információs rendszerek irányítási stratégiájának vezetése a vonatkozó folyamatok kommunikálásával, terjesztésével és ellenőrzésével a teljes IKT-infrastruktúrában.	Részt vesz az Információbiztonsági Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában.
	B.5. Dokumentumok előállítása 3. szint A részletesség szintjét a célcsoport igényeihez igazítja	Részt vesz a kiberbiztonság tárgyú vagy kapcsolódású jelentések, dokumentumok, feladatkörét érintő előállításában.

41. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Tájékoztatás / Jelentés (vezetés, érintettek) (forrás: saját szerkesztés)

8. Kapcsolattartás

	IBF	Közszolgálati dolgozó
ECSF-ben azonosított feladatok	Kapcsolatot alakít ki a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel. Együttműködik és információkat oszt meg a hatóságokkal és szakmai csoportokkal. Kiberbiztonsággal kapcsolatos támogatást nyújt a felhasználók és az ügyfelek számára.	Szükség –különösen információbiztonsági incidens- esetén együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel. Kapcsolatot tart az IBF-vel, melynek keretében bejelentést tesz, tájékoztatja az IBF-et az esetleges kiberbiztonsági eseményről, vagy annak gyanújáról, bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába.[205]
Kulcs készségek	Kommunikálás, koordinálás és együttműködés a belső és külső érdekelt felekkel.	Képes kommunikálni, koordinálni és együttműködni a belső és külső érintettekkel (pl. hatóságok, auditorok, alvállalkozók) a feladatkörét érintő, kiberbiztonság tárgyú vagy azzal kapcsolatos feladatok ellátása során.
Kulcs ismeretek		Az elektronikus információs rendszerek biztonságának felügyelete rendszerének, valamint az incidens-, illetve kockázatkezelésnek az alapszintű ismerete.[206]
E-kompetenciák	E.4. Kapcsolatmenedzsment 3. szint Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során.	Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.) Számot ad saját tevékenységéről.

42. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Kapcsolattartás (forrás: saját szerkesztés)

9. Egyéb feladatok és a hozzá kapcsolódó ismeretek, képességek, kompetenciák

	IBF	Közszolgálati dolgozó
ECSF-ben azonosított feladatok	Elvégzi a kiberbiztonsági megoldások integrálását és biztosítja megfelelő működésüket.	Elvégzi a feladatkörhöz kapcsolódó kiberbiztonsági megoldások integrálását és biztosítja a megfelelő működésüket.

[204] Az Ibtv.-ben meghatározott, bármely, a munkatárs munkaköréhez kapcsolódó feladat kapcsán.
[205] Az Ibtv. 11.§ (1) j) pontja, valamint a 13.§ (2) bekezdés, és annak e) pontja alapján.
[206] Az Ibtv. 11.§ (1) j) pontja végrehajtásához nélkülözhetetlen egyes esetekben a munkatárs közvetlen együttműködése a hatóságokkal.

	Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát. Alkalmazza és irányítja a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.	Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát. Alkalmazza a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.
Kulcs készségek	Kiberbiztonsági ajánlások és legjobb gyakorlatok implementálása. Kiberbiztonsági megoldások integrálása a szervezet infrastruktúrájába. Az etikai követelmények és szabványok megértése, gyakorlása és betartása. A szervezet kiberbiztonsági kultúrájának befolyásolása. A munkatársak motiválása és ösztönzése.	Képes a feladatköréhez kapcsolódóan a kiberbiztonsági ajánlások és legjobb gyakorlatok implementálására, valamint a kiberbiztonsági megoldások integrálására a szervezet infrastruktúrájába. Képes a feladatköréhez kapcsolódóan az etikai követelmények és szabványok megértésére, gyakorlására és betartására. Képes a szervezet kiberbiztonsági kultúrájának befolyásolására, a munkatársak motiválására és ösztönzésére.
Kulcs ismeretek	Kiberbiztonsággal kapcsolatos technológiák. Kiberbiztonsági megoldások és kontrollok .	Kiberbiztonsággal kapcsolatos technológiák, megoldások és kontrollok feladatkörhöz kapcsolódó ismerete.
E-kompetenciák	D.10. Információ- és tudásmenedzsment – 3. szint Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, valamint biztosítja a legmegfelelőbb információs struktúrát.	Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és az IBF-vel együttműködve biztosítja a legmegfelelőbb információs struktúrát.

43. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Egyéb feladatok és a hozzá kapcsolódó ismeretek, képességek, kompetenciák (forrás: saját szerkesztés)

Egyéb általános készségek	
Kulcs készségek	• Képes a munkatársak motiválására és ösztönzésére. • Képes a nyomás alatti munkavégzésre. • Képes az érdekelt felek számára történő megfelelő kommunikációra, prezentációra és jelentéstételre. • Képes az etikai követelmények és szabványok megértésére, gyakorlására és betartására. • Képes együttműködni más csapattagokkal és kollégákkal. • Képes a belső és külső érdekelt felekkel történő kommunikációra, koordinációra és együttműködésre. • Képes az összetett problémák és biztonsági kihívások alapszintű elemzésére és megoldására.

44. táblázat: A közszolgálati dolgozó ECSF-ben meghatározott feladatai - Egyéb általános készségek (forrás: saját szerkesztés)

3. sz. mellékelt: Közszolgálati kiberbiztonsági szerepprofil – Kérdőív

Közszolgálati kiberbiztonsági szerepprofil

Tisztelt Kitöltő!

Legárd Ildikó, a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolájának negyedéves hallgatója vagyok.
A kutatásom témája: Az e-közigazgatás: Kibervédelmi kihívások a közszolgálat személyi állományában. Kutatásomat Dr. habil Budai Balázs Benjámin és Dr. Krasznay Csaba vezetésével folytatom.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.) és a végrehajtási rendeleteiben meghatározott feladatok közvetlen címzettjei bár a hatálya alá tartozó szervezetek vezetői, illetve az általa kinevezett/megbízott elektronikus információs rendszer biztonságáért felelős személy (továbbiakban: IBF), **az elektronikus információk rendszerek védelméhez kapcsolódó feladatok végrehajtása elképzelhetetlen az érintett szerveknél dolgozó munkatársak közreműködése nélkül. A közszolgálatban dolgozó átlagfelhasználók a mindennapi munkájuk során számos, kiberbiztonsággal szorosan összefüggő feladattal találkoznak, melyek ellátásához elengedhetetlen meghatározni a szükséges ismereteket, készségeket és kompetenciákat**.
A közszolgálatban dolgozók kiberbiztonsági feladatai meghatározása érdekében megvizsgáltam az elektronikus információs rendszer biztonságáért felelős személy Európai Kiberbiztonsági Készség-keretrendszerben (European Cybersecurity Skills Framework, ECSF) azonosítható feladatait, melyek közül kiválasztottam a közszolgálati dolgozók számára értelmezhető, releváns feladatokat, majd a szükséges módosításokkal, kiegészítésekkel alkalmaztam őket a közszolgálati szerepprofil részeként, az ellátásukhoz szükséges készségekkel, ismeretekkel és kompetenciákkal együtt. A szerepprofil kiegészítésre került a DigKomp Állampolgári Digitáliskompetencia-keret 2.2. releváns elemeivel.
A szerepprofil nem a közszolgálatban dolgozók jelenlegi ismereteire vonatkoznak, hanem egyfajta jövőben elérendő célként határozza meg a szükséges fejlesztési irányokat!

A kérdőív a közszolgálati kiberbiztonsági szerepprofil részeként azonosított feladatokkal, készséggel, ismeretekkel és kompetenciákkal kapcsolatos kérdéseket fogalmaz meg. A kitöltés célja, hogy az Ön szakértelme segítségével árnyalni tudjam kutatásom eredményét, a szerepprofil egyes elemeit, ezáltal minél hitelesebb képet kapjak a munkatársak általános, szervezeti keretek között értelmezhető kiberbiztonsági szerepéről.

A kérdőív kitöltése **önkéntes**. A kapott adatokat **bizalmasan** kezelem, kizárólag a tudományos kutatásomhoz és az abból készült publikációhoz, illetve előadásokhoz használom fel **anonim módon**.
Az adatvédelmi elveket illetően a Google szabályzata a releváns: https://policies.google.com/privacy?hl=hu

A kérdőív 5 kérdés csoportot tartalmaz és kitöltése hozzávetőlegesen 15 percet vesz igénybe!

Köszönöm, hogy a kitöltéssel segíti kutatásomat!

Budapest, 2023. április

Tisztelettel,
Legárd Ildikó

Általános kérdések

1. Az Ön által képviselt szerv az Ibtv. mely pontja alapján tartozik e törvény hatálya alá?

……

2. Mekkora a Ön szervezetében dolgozók létszáma (körülbelül)?

- 150 fő alatt
- 151-500 fő
- 501-1000 fő
- 1000 fő felett

3. Mely szerepkörben végez az Ibtv. hatálya alá tartozó feladatokat?

- a szervezet vezetőjeként (Ibtv. 11.§)
- az elektronikus információs rendszer biztonságáért felelős személyként (Ibtv. 13.§)
- az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyként (Ibtv. 13.§ (11))
- Egyéb:

4. Ön szerint indokolt egy, a közigazgatásban dolgozó átlagfelhasználók mindennapi kiberbiztonsági feladatait meghatározó szerepprofil létrehozása, amely meghatározza az ellátandó feladatokat, készségeket, ismereteket és kompetenciákat?

- igen
- nem
- Egyéb:

5. Egy, a bevezetőben ismertetett közszolgálati kiberbiztonsági szerepprofil segítené a tudatosítással kapcsolatos munkáját?

- igen
- nem
- Egyéb:

II. Fő feladatok

Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben meghatározott feladatok végrehajtása érdekében az alábbi, kiberbiztonsággal kapcsolatos feladatot kell a mindennapi munkavégzése során végrehajtania?

Kérem, az Ön véleményéhez leginkább közelálló választ szíveskedjen megjelölni!

Feladatok	**Rendkívüli mértékben egyetértek**	**Eléggé egyetértek**	**Közepes mértékben értek egyet**	**Alig értek egyet**	**Egyáltalán nem értek egyet**
Biztosítja a munkaköréhez kapcsolódóan a kiberbiztonsággal kapcsolatos szabványoknak, törvényeknek és rendeleteknek, illetve a szervezetszabályozó eszközöknek való megfelelést.					
Részt vesz a feladatköréhez kapcsolódóan a szervezet kiberbiztonsága jövőképét, stratégiáját és politikáját meghatározó dokumentumok végrehajtásában.					
Részt vesz az Informatikai Biztonsági Szabályzat végrehajtásában.					
Részt vesz a feladatkörét érintő kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.					
Részt vesz a kiberbiztonsággal kapcsolatos tudatosságnövelő programokon, az előírt követelményeket teljesíti.					
Részt vesz a feladatköréhez kapcsolódóan a kockázatkezelés folyamatában.					
Részt vesz az IBF által azonosított kockázatok értékelésében, valamint a kockázatkezelésben (a kockázatra adott válaszlépések meghatározásában, a					

kockázatcsökkentő intézkedések végrehajtásában).					
Részt vesz a szervezet belső szervezetszabályozó eszközeiben rögzített incidenskezelési eljárásban a feladatköréhez kapcsolódóan.					
Azonosítja és jelenti az IBF-nek a kiberbiztonsági eseményeket vagy annak gyanúját, részt vesz az esetleges károk enyhítésében.					
Kapcsolatot tart, bejelentést tesz, tájékoztatja az IBF-et az esetleges biztonsági eseményről vagy annak gyanújáról, a felmerülő kockázatokról, továbbá bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába.					
A kiberbiztonsággal kapcsolatos intézkedések során szorosan együttműködik az IBF-fel, illetve az üzemeltetést végző informatikusokkal.					
Indokolt esetben (pl. egy információbiztonsági incidens esetén) együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel.					
Együttműködik a kiberbiztonsági ellenőrzésekben.					
Együttműködik az ellenőrzések során a szükséges információk, adatok, dokumentumok átadásában.					
Integrálja a feladatkörhöz kapcsolódó kiberbiztonsági megoldásokat és biztosítja megfelelő működésüket.					
Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát.					
Alkalmazza a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat.					

III. Kulcs készségek

Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs készségekkel kell rendelkeznie?

Kérem, az Ön véleményéhez leginkább közelálló választ szíveskedjen megjelölni

Kulcs készségek	**Rendkívüli mértékben egyetértek**	**Eléggé egyetértek**	**Közepes mértékben értek egyet**	**Alig értek egyet**	**Egyáltalán nem értek egyet**
Képes a feladatai ellátása során alkalmazni a kiberbiztonságra vonatkozó jogi követelményeket, szervezetszabályozó eszközöket, valamint a vonatkozó ajánlásokat és a bevált gyakorlatokat.					
Képes megérteni és feladatai ellátása során figyelembe venni a szervezeti célokat, jövő képet, a biztonsággal kapcsolatos politikát és stratégiát, a jogi, szabályozási és szabvány követelményeket.					
Képes részt venni a szervezet kiberbiztonsági jövőképének, stratégiájának, politikájának, valamint az Informatikai Biztonsági Szabályzatnak a feladatköréhez kapcsolódó végrehajtásában.					
Képes részt venni a feladatköréhez kapcsolódó, a szervezetszabályozó eszközöket és egyéb jogi követelményeket kiegészítő, megfelelő kiberbiztonsági irányelvek, eljárások és szabályok kidolgozásában és végrehajtásában.					
Képes részt venni a feladatkörét érintő, kiberbiztonság tárgyú jogszabályok, szervzetszabályozó eszközök és					

szerződések véleményezésében.					
Képes a jogi és szabályozási környezet, valamint a műszaki üzleti igények alapszintű megértésére és kommunikációjára.					
Képes az üzleti igények kiberbiztonsági vonatkozásai kommunikálására a felső vezetés és az IBF felé.					
Képes a biztonságtudatosító programokon való aktív részvételre, a tananyag elsajátítására és alkalmazására.					
Képes megfogalmazni az elsajátítandó ismeretekre, készségekre vonatkozó igényét.					
Képes a feladatköréhez kapcsolódóan a kiberbiztonsági problémák azonosítására, a kockázatok értékelésére, valamint a kockázatcsökkentő intézkedések megértésére és végrehajtására.					
Képes a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozni.					
Képes gyakorolni az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatokat.					
Képes a social engineering típusú támadásokat felismerni.					
Képes a problémák és hibák segítséggel történő elhárítására.					
Képes kommunikálni és kapcsolatot építeni az IBF-el, illetve az érdekelt felekkel, a feladatkörét érintő kiberbiztonsági kockázatok kezelése, illetve incidensek megelőzése és kezelése érdekében.					
Képes jelentéseket kidolgozni, vagy az elkészítésükben közreműködni, valamint					

a jelentéseket megfelelően kommunikálni.					
Képes kommunikálni, koordinálni és együttműködni a belső és külső érintettekkel (pl. hatóságok, auditorok, alvállalkozók) a feladatkörét érintő, kiberbiztonság tárgyú vagy azzal kapcsolatos feladatok ellátása során.					
Képes részt venni és együttműködni a kiberbiztonsági tárgyú ellenőrzésekben.					
Képes részt venni az ellenőrzési jelentések elkészítésben.					
Képes az auditálási és megfelelőségértékelési módszertanok, eszközök és technikák –feladatköréhez kapcsolódó- alkalmazására. (Kizárólag vezetői szerepben.)					
Képes a feladatköréhez kapcsolódóan a kiberbiztonsági ajánlások és legjobb gyakorlatok implementálására, valamint a kiberbiztonsági megoldások integrálására a szervezet infrastruktúrájába.					
Képes a feladatköréhez kapcsolódóan az etikai követelmények és szabványok megértésére, gyakorlására és betartására.					
Képes a szervezet kiberbiztonsági kultúrájának befolyásolására, a munkatársak motiválására és ösztönzésére.					
Képes a nyomás alatti munkavégzésre.					
Képes az érdekelt felek számára történő megfelelő kommunikációra, prezentációra és jelentéstételre.					
Képes együttműködni más csapattagokkal és kollégákkal.					
Képes a belső és külső érdekelt felekkel történő kommunikációra, koordinációra és együttműködésre.					
Képes az összetett problémák és					

biztonsági kihívások alapszintű elemzésére és megoldására.					

IV. Kulcs ismeretek

Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs ismeretekkel kell rendelkeznie?

Kérem, az Ön véleményéhez leginkább közelálló választ szíveskedjen megjelölni

Kulcs ismeretek	**Rendkívüli mértékben egyetértek**	**Eléggé egyetértek**	**Közepes mértékben értek egyet**	**Alig értek egyet**	**Egyáltalán nem értek egyet**
Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete.					
Általános kiberbiztonsági ismeretek, szervezeti szinten az információbiztonsági előírások és stratégiák feladatkörhöz kapcsolódó ismerete.					
Az elektronikus információs rendszerek biztonságának felügyelete rendszerének, valamint az incidens-, illetve kockázatkezelésnek az alapszintű ismerete.					
A kockázatkezelés folyamatának és abban betöltött szerepének alapszintű ismerete.					
A megfelelő biztonsági eljárások, követelmények, technikák, valamint ajánlások és szabványok feladatkörhöz kapcsolódó, a lehetséges támadási és védekezési alternatívák alapszintű					

ismerete.					
A potenciális kiberfenyegetések, kibertámadási formák és a számítógépes rendszerek sebezhetőségeinek alapszintű ismerete.					
A kiberbiztonsági ellenőrzések, auditálási szabványok, módszertanok és keretrendszerek feladatkörhöz kapcsolódó alapszintű ismerete. (Kizárólag vezetői szerepben.)					
Az auditálással és a kiberbiztonsággal kapcsolatos tanúsítások feladatkörhöz kapcsolódó, alapszintű ismerete.					
Kiberbiztonsággal kapcsolatos technológiák, megoldások és kontrollok feladatkörhöz kapcsolódó ismerete.					
Etikus kiberbiztonsági szervezeti követelmények.					

V. Kulcs kompetenciák

Egyetért-e Ön azzal, hogy egy közigazgatásban dolgozó átlagfelhasználónak, elsősorban az Ibtv.-ben nevesített elektronikus információs rendszerek védelme érdekében az alábbi, kiberbiztonsággal kapcsolatos kulcs kompetenciákkal kell rendelkeznie?

Kérem, az Ön véleményéhez leginkább közelálló választ szíveskedjen megjelölni!

Kulcs kompetenciák	**Rendkívüli mértékben egyetértek**	**Eléggé egyetértek**	**Közepes mértékben értek egyet**	**Alig értek egyet**	**Egyáltalán nem értek egyet**
Részt vesz az információs rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, valamint a vonatkozó jogi követelménynek való megfelelésben.					
Részt vesz az Információbiztonsági					

Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában.					
Részt vesz az információbiztonságnak a szervezet kultúrájába való beillesztése folyamatában.					
Részt vesz a tudatosító képzések során elsajátított ismeretek, készségek segítségével a biztonságtudatos szervezeti kultúra kialakításában, fenntartásában és kommunikálásában.					
Megérti és alkalmazza a kockázatkezelés elveit, részt vesz az IBSZ-ben meghatározott kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében a feladatköréhez kapcsolódóan.					
A kockázatokra vonatkozó információkkal alátámasztott megalapozott döntéseket hoz a feladatköréhez kapcsolódó kockázatok kezelése és mérséklése érdekében. (Kizárólag vezetői szerepben.)					
Különböző módszereket alkalmaz eszközei és digitális tartalmai megóvására.					
Értékeli a legmegfelelőbb módszereket, amelyekkel kellő mértékben figyelembe lehet venni a megbízhatósági és adatvédelemi szempontokat.					
Kiválasztja a megfelelőbb módszereket a személyes adatok és a magánélet megóvására digitális környezetben.					
Értékeli a legmegfelelőbb módszereket arra, hogyan lehet felhasználni és megosztani személyazonosításra alkalmas adatokat úgy, hogy közben megvédje önmagát és másokat a nem megfelelő adatkezeléssel kapcsolatos, lehetséges károktól.					

Értékeli az adatvédelmi nyilatkozatok megfelelőségét a személyes adatok felhasználásával kapcsolatban.					
Megkülönbözteti a legmegfelelőbb módszereket, amelyekkel elkerülhetők a digitális technológiák használata során felmerülő, az egészségre, illetve a fizikai és pszichológiai jóllétre veszélyt jelentő kockázatok.					
Adaptálja a legmegfelelőbb módszereket, amelyekkel megvédheti önmagát és másokat digitális környezetben.					
Részt vesz a feladatköréhez kapcsolódó problémakezelési/incidenskezelési folyamatban, a károk enyhítése érdekében mindent megtesz, ami tőle az adott helyzetben elvárható.					
Megkülönbözteti a kockázatokat és veszélyeket digitális környezetben.					
Biztonsági intézkedéseket alkalmaz.					
Feladatköréhez kapcsolódóan együttműködik az ellenőrzések során az ellenőrzést végző belső szervezeti egységgel vagy külső szervezettel/céggel, részt vesz az ellenőrzések során készült dokumentumok előállításában, véleményezésében.					
Részt vesz a kiberbiztonság tárgyú vagy kapcsolódású jelentések, dokumentumok, feladatkörét érintő előállításában.					
Egyszerű vizsgálatokat végez a részletes utasítások szigorú betartásával.					
Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és az IBF-vel együttműködve biztosítja a legmegfelelőbb információs struktúrát.					
A célnak megfelelően kiválasztja a társadalmi jóllétet és befogadást elősegítő digitális technológiákat.					
Számot ad saját és mások tevékenységéről					

korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.)					

Segítő közreműködését még egyszer nagyon szépen köszönöm!

4. sz. melléklet: Közszolgálati szerepprofil kérdőíves vizsgálat eredményei (forrás: saját szerkesztés)

A kérdőív az egyes feladatokkal/készségekkel/ismeretekkel/e-kompetenciákkal kapcsolatos szakértői attitűd vizsgálatára likert skálás mérés alkalmaz. A válaszadók „a rendkívüli mértékben egyetértek” és az „egyáltalán nem értek” között elhelyezkedő ötfokozatú skálán tudták megjelölni válaszaikat.

Az adatfeldolgozás 5.6.1. pontban ismertetett lépéseit, az egyes leíró statisztikai eljárások eredményeit és értelmezéseit jelen, 4. sz. mellékletben bemutatott táblázatok részletesen ismertetik. A táblázatok jobb szélső oszlopa mutatja be a szerepprofil egyes elemeire vonatkozó végső kutatói döntést: amennyiben a vizsgálatok alapján az adott elem a szerepprofil részét képzi, egy ✓ kerül a sor végére. Amennyiben egyértelműen nem utasítható el az adott elem, ugyanakkor a szerepprofil részének sem lehet tekinteni, abban az esetben további, jövőbeni vizsgálat javasolt, melyet egy ? jellel jelölök. Amennyiben a mediánértékek figyelembe vételével azonosított, további arányszámítást igénylő elemek esetében mind az egyetértők és a bizonytalanok száma, mind pedig az elutasítók száma éppen hogy eléri a validitás küszöbértékét, a „szerepprofil része (határeset)” elnevezés, illetve ✓! jelek kerültek az adott sor végére. A táblázatok jelölésrendszere minden egyes részterület (fő feladatok, kulcs készségek, kulcs ismeretek, kulcs kompetenciák) esetén megegyezik.

Feladatalapú értékelés I: ***FELADATOK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 69,23% Bizonytalan válaszadók mediánértéke (M_B): 15,38% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
1. Biztosítja a munkaköréhez kapcsolódóan a kiberbiztonsággal kapcsolatos szabványoknak, törvényeknek és rendeleteknek, illetve a szervezetszabályozó eszközöknek való megfelelést								
Fenntartások nélküli egyetértő	65,38%	$< M_{FNE}$		22 fő	4 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
2. Részt vesz a feladatköréhez kapcsolódóan a szervezet kiberbiztonsága jövőképét, stratégiáját és politikáját meghatározó dokumentumok végrehajtásában								
Fenntartások nélküli egyetértő	57,69%	$< M_{FNE}$		21 fő	5 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	19,23%	$< R_E$						
3. Részt vesz az Informatikai Biztonsági Szabályzat végrehajtásában.								
Fenntartások nélküli egyetértő	92,31%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	3,85%	$< M_B$						
Elutasító	3,82%	$< R_E$						
4. Részt vesz a feladatkörét érintő kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében								
Fenntartások nélküli egyetértő	30,77%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	38,46%	$\geq M_B$	további vizsgálatok					
Elutasító	30,77%	$< R_E$						
5. Részt vesz a kiberbiztonsággal kapcsolatos tudatosságnövelő programokon, az előírt követelményeket teljesíti								
Fenntartások nélküli egyetértő	96,15%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	0,00%	$< M_B$						
Elutasító	3,85%	$< R_E$						
6. Részt vesz a feladatköréhez kapcsolódóan a kockázatkezelés folyamatában								
Fenntartások nélküli egyetértő	65,38%	$< M_{FNE}$		22 fő	4 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
7. Részt vesz az IBF által azonosított kockázatok értékelésében, valamint a kockázatkezelésben (a kockázatra adott válaszlépések meghatározásában, a kockázatcsökkentő intézkedések végrehajtásában)								
Fenntartások nélküli egyetértő	53,85%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	15,38%	$\geq M_B$	további vizsgálatok					
Elutasító	30,77%	$< R_E$						
8. Részt vesz a szervezet belső szervezetszabályozó eszközeiben rögzített incidenskezelési eljárásban a feladatköréhez kapcsolódóan								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	3,85%	$< R_E$						
9. Azonosítja és jelenti az IBF-nek a kiberbiztonsági eseményeket vagy annak gyanúját, részt vesz az esetleges károk enyhítésében								
Fenntartások nélküli egyetértő	88,46%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						
Elutasító	0,00%	$< R_E$						
10. Kapcsolatot tart, bejelentést tesz, tájékoztatja az IBF-et az esetleges biztonsági eseményről vagy annak gyanújáról, a felmerülő kockázatokról, továbbá bevonja az IBF-et a kiberbiztonsági tárgyú szerződések, beszerzések, fejlesztések véleményezésébe, folyamatába								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓

Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	7,69%	$< R_E$						

Feladatalapú értékelés II: ***FELADATOK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 69,23% Bizonytalan válaszadók mediánértéke (M_B): 15,38% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**		**Értelmezés**	**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
11. A kiberbiztonsággal kapcsolatos intézkedések során szorosan együttműködik az IBF-fel, illetve az üzemeltetést végző informatikusokkal								
Fenntartások nélküli egyetértő	84,62%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	3,85%	$< M_B$						
Elutasító	11,54%	$< R_E$						
12. Indokolt esetben (pl. egy információbiztonsági incidens esetén) együttműködik és információkat oszt meg a kiberbiztonsággal kapcsolatos hatóságokkal és szervezetekkel								
Fenntartások nélküli egyetértő	46,15%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	15,38%	$\geq M_B$	további vizsgálatok					
Elutasító	38,46%	$< R_E$						
13. Együttműködik a kiberbiztonsági ellenőrzésekben								
Fenntartások nélküli egyetértő	73,08%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$\geq M_B$	további vizsgálatok					
Elutasító	11,54%	$< R_E$						
14. Együttműködik az ellenőrzések során a szükséges információk, adatok, dokumentumok átadásában								
Fenntartások nélküli egyetértő	92,31%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	3,85%	$< M_B$						
Elutasító	3,85%	$< R_E$						
15. Integrálja a feladatkörhöz kapcsolódó kiberbiztonsági megoldásokat és biztosítja megfelelő működésüket								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						
Elutasító	19,23%	$< R_E$						
16. Fenntartja és frissíti a rendszerek, szolgáltatások és termékek biztonságát								
Fenntartások nélküli egyetértő	26,92%	$< M_{FNE}$		14 fő	12 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	46,15%	$< R_E$						
17. Alkalmazza a technikai sebezhetőségek kezelése érdekében a termékekhez kapcsolódó programjavításokat								
Fenntartások nélküli egyetértő	46,15%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	15,38%	$\geq M_B$	további vizsgálatok					
Elutasító	38,46%	$< R_E$						

5. táblázat: Közszolgálati szerepprofil – Feladatok értékelése (forrás: saját szerkesztés)

Medián: 17 feladat közül 8,5 feladattal a válaszadók több, mint 69,23%-a fenntartások nélkül egyetért, ill. 8,5 feladattal a válaszadók kevesebb, mint 69,23%-a ért egyet fenntartások nélkül

Fenntartások nélkül ért egyet (rendkívüli mértékben egyetért és eléggé egyetért)
Bizonytalan (közepes mértékben ért egyet)
Elutasító (alig ért egyet és egyáltalán nem ért egyet)

Feladatalapú értékelés I: ***KÉSZSÉGEK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 63,46% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
1. Képes a feladatai ellátása során alkalmazni a kiberbiztonságra vonatkozó jogi követelményeket, szervezetszabályozó eszközöket, valamint a vonatkozó ajánlásokat és a bevált gyakorlatokat								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	11,54%	$< R_E$						
2. Képes megérteni és feladatai ellátása során figyelembe venni a szervezeti célokat, jövő képet, a biztonsággal kapcsolatos politikát és stratégiát, a jogi, szabályozási és szabvány követelményeket								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	3,85%							
3. Képes részt venni a szervezet kiberbiztonsági jövőképének, stratégiájának, politikájának, valamint az Informatikai Biztonsági Szabályzatnak a feladatköréhez kapcsolódó végrehajtásában								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	7,69%	$< R_E$						
4. Képes részt venni a feladatköréhez kapcsolódó, a szervezetszabályozó eszközöket és egyéb jogi követelményeket kiegészítő, megfelelő kiberbiztonsági irányelvek, eljárások és szabályok kidolgozásában és végrehajtásában								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	23,08%	$< R_E$						
5. Képes részt venni a feladatkörét érintő, kiberbiztonság tárgyú jogszabályok, szervezetszabályozó eszközök és szerződések véleményezésében.								
Fenntartások nélküli egyetértő	42,31%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	38,46%	$< R_E$						
6. Képes a jogi és szabályozási környezet, valamint a műszaki üzleti igények alapszintű megértésére és kommunikációjára								
Fenntartások nélküli egyetértő	53,85%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	15,38%	$< M_B$						
Elutasító	30,77%	$< R_E$						
7. Képes az üzleti igények kiberbiztonsági vonatkozásai kommunikálására a felső vezetés és az IBF felé								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		21 fő	5 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	30,77%	$\geq M_B$	további vizsgálatok					
Elutasító	19,23%	$< R_E$						
8. Képes a biztonságtudatosító programokon való aktív részvételre, a tananyag elsajátítására és alkalmazására								
Fenntartások nélküli egyetértő	96,15%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	3,85%	$< M_B$						
Elutasító	0,00%	$< R_E$						
9. Képes megfogalmazni az elsajátítandó ismeretekre, készségekre vonatkozó igényét								
Fenntartások nélküli egyetértő	80,77%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	0,00%	$< R_E$						
10. Képes a feladatköréhez kapcsolódóan a kiberbiztonsági problémák azonosítására, a kockázatok értékelésére, valamint a kockázatcsökkentő intézkedések megértésére és végrehajtására.								
Fenntartások nélküli egyetértő	73,08%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						

Elutasító	15,38%	$< R_E$						

Feladatalapú értékelés II: ***KÉSZSÉGEK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 63,46% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
11. Képes a kockázatok kezelése és mérséklése érdekében a kockázatokra vonatkozó információkkal alátámasztott döntéseket hozni.								
Fenntartások nélküli egyetértő	46,15%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓!
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	30,77%	$< R_E$						
12. Képes gyakorolni az eseménykezelés és válaszadás során a feladatköréhez kapcsolódó, az IBF által meghatározott technikai, funkcionális és operatív feladatokat								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	15,38%	$< R_E$						
13. Képes a social engineering típusú támadásokat felismerni								
Fenntartások nélküli egyetértő	84,62%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	3,85%	$< M_B$						
Elutasító	11,54%	$< R_E$						
14. Képes a problémák és hibák segítséggel történő elhárítására								
Fenntartások nélküli egyetértő	73,08%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						
Elutasító	15,38%	$< R_E$						
15. Képes kommunikálni és kapcsolatot építeni az IBF-el, illetve az érdekelt felekkel, a feladatkörét érintő kiberbiztonsági kockázatok kezelése, illetve incidensek megelőzése és kezelése érdekében								
Fenntartások nélküli egyetértő	80,77%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	11,54%	$< R_E$						
16. Képes jelentéseket kidolgozni, vagy az elkészítésükben közreműködni, valamint a jelentéseket megfelelően kommunikálni								
Fenntartások nélküli egyetértő	42,31%	$< M_{FNE}$		19 fő	7 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	30,77%	$\geq M_B$	további vizsgálatok					
Elutasító	26,92%	$< R_E$						
17. Képes kommunikálni, koordinálni és együttműködni a belső és külső érintettekkel (pl. hatóságok, auditorok, alvállalkozók) a feladatkörét érintő, kiberbiztonság tárgyú vagy azzal kapcsolatos feladatok ellátása során								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		17 fő	9 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	15,38%	$< M_B$						
Elutasító	34,62%	$< R_E$						
18. Képes részt venni és együttműködni a kiberbiztonsági tárgyú ellenőrzésekben								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	7,69%	$< R_E$						
19. Képes részt venni az ellenőrzési jelentések elkészítésben								
Fenntartások nélküli egyetértő	53,85%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓!
Bizonytalan	15,38%	$< M_B$						
Elutasító	30,77%	$< R_E$						
20. Képes az auditálási és megfelelőségértékelési módszertanok, eszközök és technikák – feladatköréhez kapcsolódó – alkalmazására (kizárólag vezetői szerepben)								

Fenntartások nélküli egyetértő	65,38%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						

Feladatalapú értékelés III: ***KÉSZSÉGEK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 63,46% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
21. Képes a feladatköréhez kapcsolódóan a kiberbiztonsági ajánlások és legjobb gyakorlatok implementálására, valamint a kiberbiztonsági megoldások integrálására a szervezet infrastruktúrájába								
Fenntartások nélküli egyetértő	42,31%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	30,77%	$< R_E$						
22. Képes a feladatköréhez kapcsolódóan az etikai követelmények és szabványok megértésére, gyakorlására és betartására								
Fenntartások nélküli egyetértő	84,62%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	7,69%	$< R_E$						
23. Képes a szervezet kiberbiztonsági kultúrájának befolyásolására, a munkatársak motiválására és ösztönzésére								
Fenntartások nélküli egyetértő	61,54%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	23,08%	$< R_E$						
24. Képes a nyomás alatti munkavégzésre								
Fenntartások nélküli egyetértő	57,69%	$< M_{FNE}$		22 fő	4 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
25. Képes az érdekelt felek számára történő megfelelő kommunikációra, prezentációra és jelentéstételre								
Fenntartások nélküli egyetértő	46,15%	$< M_{FNE}$		17 fő	9 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	34,62%	$< R_E$						
26. Képes együttműködni más csapattagokkal és kollégákkal								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	0,00%	$< R_E$						
27. Képes a belső és külső érdekelt felekkel történő kommunikációra, koordinációra és együttműködésre								
Fenntartások nélküli egyetértő	61,54%	$< M_{FNE}$		22 fő	4 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
28. Képes az összetett problémák és biztonsági kihívások alapszintű elemzésére és megoldására								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	11,54%	$< M_B$						
Elutasító	38,46%	$< R_E$						

5. táblázat: Közszolgálati szerepprofil – Készségek értékelése (forrás: saját szerkesztés)

Medián: 28 készség közül 14 készséggel a válaszadók több, mint 63,46%-a fenntartások nélkül egyetért, ill. 14 készséggel a válaszadók kevesebb, mint 63,46%-a ért egyet fenntartások nélkül

Feladatalapú értékelés: ***ISMERETEK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 59,62% Bizonytalan válaszadók mediánértéke (M_B): 17,31% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
1. Kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok, illetve szervezetszabályozó eszközök munkakörhöz kapcsolódó, alapszintű ismerete								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		23 fő	3 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	38,46%	$\geq M_B$	további vizsgálatok					
Elutasító	11,54%	$< R_E$						
2. Általános kiberbiztonsági ismeretek, szervezeti szinten az információbiztonsági előírások és stratégiák feladatkörhöz kapcsolódó ismerete								
Fenntartások nélküli egyetértő	80,77%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						
Elutasító	7,69%	$< R_E$						
3. Az elektronikus információs rendszerek biztonságának felügyelete rendszerének, valamint az incidens-, illetve kockázatkezelésnek az alapszintű ismerete								
Fenntartások nélküli egyetértő	57,69%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	23,08%	$< R_E$						
4. A kockázatkezelés folyamatának és abban betöltött szerepének alapszintű ismerete								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	15,38%	$< R_E$						
5. A megfelelő biztonsági eljárások, követelmények, technikák, valamint ajánlások és szabványok feladatkörhöz kapcsolódó, a lehetséges támadási és védekezési alternatívák alapszintű ismerete								
Fenntartások nélküli egyetértő	61,54%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	34,62%	$\geq M_B$	további vizsgálatok					
Elutasító	3,85%	$< R_E$						
6. A potenciális kiberfenyegetések, kibertámadási formák és a számítógépes rendszerek sebezhetőségeinek alapszintű ismerete								
Fenntartások nélküli egyetértő	80,77%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	11,54%	$< M_B$						
Elutasító	7,69%	$< R_E$						
7. A kiberbiztonsági ellenőrzések, auditálási szabványok, módszertanok és keretrendszerek feladatkörhöz kapcsolódó alapszintű ismerete (kizárólag vezetői szerepben)								
Fenntartások nélküli egyetértő	61,54%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	23,08%	$< R_E$						
8. Az auditálással és a kiberbiztonsággal kapcsolatos tanúsítások feladatkörhöz kapcsolódó, alapszintű ismerete								
Fenntartások nélküli egyetértő	42,31%	$< M_{FNE}$		17 fő	9 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	34,62%	$< R_E$						
9. Kiberbiztonsággal kapcsolatos technológiák, megoldások és kontrollok feladatkörhöz kapcsolódó ismerete								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		19 fő	7 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	26,92%	$< R_E$						
10. Etikus kiberbiztonsági szervezeti követelmények								
Fenntartások nélküli egyetértő	53,85%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	15,38%	$< M_B$						

Elutasító	30,77%	$< R_E$						

5. táblázat: Közszolgálati szerepprofil – Ismeretek értékelése (forrás: saját szerkesztés)

Feladatalapú értékelés I: ***KOMPETENCIÁK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 65,38% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
1. Részt vesz az információs rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításában, valamint a vonatkozó jogi követelménynek való megfelelésben								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	7,69%	$< R_E$						
2. Részt vesz az Információbiztonsági Irányítási Rendszer működésével kapcsolatos, feladatkörét érintő feladatok végrehajtásában, a biztonságtudatos viselkedés munkatársak felé történő kommunikálásában								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	7,69%	$< R_E$						
3. Részt vesz az információbiztonságnak a szervezet kultúrájába való beillesztése folyamatában								
Fenntartások nélküli egyetértő	65,38%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	19,23%	$< R_E$						
4. Részt vesz a tudatosító képzések során elsajátított ismeretek, készségek segítségével a biztonságtudatos szervezeti kultúra kialakításában, fenntartásában és kommunikálásában								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	3,85%	$< R_E$						
5. Megérti és alkalmazza a kockázatkezelés elveit, részt vesz az IBSZ-ben meghatározott kockázatkezeléssel kapcsolatos feladatok ellátásában, az azonosított kockázatok mérséklésében a feladatköréhez kapcsolódóan								
Fenntartások nélküli egyetértő	65,38%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
6. A kockázatokra vonatkozó információkkal alátámasztott megalapozott döntéseket hoz a feladatköréhez kapcsolódó kockázatok kezelése és mérséklése érdekében (kizárólag vezetői szerepben)								
Fenntartások nélküli egyetértő	65,38%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	19,23%	$< R_E$						
7. Különböző módszereket alkalmaz eszközei és digitális tartalmai megóvására								
Fenntartások nélküli egyetértő	73,08%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	11,54%	$< R_E$						
8. Értékeli a legmegfelelőbb módszereket, amelyekkel kellő mértékben figyelembe lehet venni a megbízhatósági és adatvédelemi szempontokat								
Fenntartások nélküli egyetértő	38,46%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	38,46%	$\geq M_B$	további vizsgálatok					
Elutasító	23,08%	$< R_E$						
9. Kiválasztja a megfelelőbb módszereket a személyes adatok és a magánélet megóvására digitális környezetben								
Fenntartások nélküli egyetértő	57,69%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	23,08%	$< R_E$						

Feladatalapú értékelés II: ***KOMPETENCIÁK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 65,38% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
10. Értékeli a legmegfelelőbb módszereket arra, hogyan lehet felhasználni és megosztani személyazonosításra alkalmas adatokat úgy, hogy közben megvédje önmagát és másokat a nem megfelelő adatkezeléssel kapcsolatos, lehetséges károktól								
Fenntartások nélküli egyetértő	57,69%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	23,08%	$< R_E$						
11. Értékeli az adatvédelmi nyilatkozatok megfelelőségét a személyes adatok felhasználásával kapcsolatban								
Fenntartások nélküli egyetértő	42,31%	$< M_{FNE}$		19 fő	7 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	30,77%	$\geq M_B$	további vizsgálatok					
Elutasító	26,92%	$< R_E$						
12. Megkülönbözteti a legmegfelelőbb módszereket, amelyekkel elkerülhetők a digitális technológiák használata során felmerülő, az egészségre, illetve a fizikai és pszichológiai jóllétre veszélyt jelentő kockázatok								
Fenntartások nélküli egyetértő	53,85%	$< M_{FNE}$		21 fő	5 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	19,23%	$< R_E$						
13. Adaptálja a legmegfelelőbb módszereket, amelyekkel megvédheti önmagát és másokat digitális környezetben								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	23,08%	$< R_E$						
14. Részt vesz a feladatköréhez kapcsolódó problémakezelési/incidenskezelési folyamatban, a károk enyhítése érdekében mindent megtesz, ami tőle az adott helyzetben elvárható								
Fenntartások nélküli egyetértő	76,92%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	15,38%	$< R_E$						
15. Megkülönbözteti a kockázatokat és veszélyeket digitális környezetben								
Fenntartások nélküli egyetértő	61,54%	$< M_{FNE}$		22 fő	4 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	15,38%	$< R_E$						
16. Biztonsági intézkedéseket alkalmaz								
Fenntartások nélküli egyetértő	65,38%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	23,08%	$\geq M_B$	további vizsgálatok					
Elutasító	11,54%	$< R_E$						
17. Feladatköréhez kapcsolódóan együttműködik az ellenőrzések során az ellenőrzést végző belső szervezeti egységgel vagy külső szervezettel/céggel, részt vesz az ellenőrzések során készült dokumentumok előállításában, véleményezésében								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	26,92%	$\geq M_B$	további vizsgálatok					
Elutasító	3,85%	$< R_E$						
18. Részt vesz a kiberbiztonság tárgyú vagy kapcsolódású jelentések, dokumentumok, feladatkörét érintő előállításában								
Fenntartások nélküli egyetértő	61,54%	$< M_{FNE}$		20 fő	6 fő	teljesül	**a szerepprofil része**	✓
Bizonytalan	15,38%	$< M_B$						
Elutasító	23,08%	$< R_E$						

Feladatalapú értékelés III: ***KOMPETENCIÁK***

Fenntartások nélküli egyetértők mediánértéke (M_{FNE}): 65,38% Bizonytalan válaszadók mediánértéke (M_B): 19,23% Elutasítók aránya (R_E) > 50%	**Relatív gyakoriság (válaszadók aránya)**	**Értelmezés**		**További vizsgálatok**			**Kutatói döntés**	
				Egyetértő (*FNE*) és bizonytalan (*B*)	Elutasító (*E*)	Feltétel: $FNE + B > 17 \wedge E < 9$		
19. Egyszerű vizsgálatokat végez a részletes utasítások szigorú betartásával								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	11,54%	$< M_B$						
Elutasító	38,46%	$< R_E$						
20. Elemzi az üzleti folyamatokat és a kapcsolódó információs követelményeket, és az IBF-vel együttműködve biztosítja a legmegfelelőbb információs struktúrát								
Fenntartások nélküli egyetértő	50,00%	$< M_{FNE}$		18 fő	8 fő	teljesül	**a szerepprofil része** (határeset)	✓ !
Bizonytalan	19,23%	$\geq M_B$	további vizsgálatok					
Elutasító	30,77%	$< R_E$						
21. A célnak megfelelően kiválasztja a társadalmi jóllétet és befogadást elősegítő digitális technológiákat								
Fenntartások nélküli egyetértő	30,77%	$< M_{FNE}$		16 fő	10 fő	nem teljesül	**tovább vizsgáljuk**	?
Bizonytalan	30,77%	$\geq M_B$	további vizsgálatok					
Elutasító	38,46%	$< R_E$						
22. Számot ad saját és mások tevékenységéről korlátozott számú érintett irányítása során. (Kizárólag vezetői szerepben.)								
Fenntartások nélküli egyetértő	69,23%	$\geq M_{FNE}$	elfogadjuk	–	–	–	**a szerepprofil része**	✓
Bizonytalan	7,69%	$< M_B$						
Elutasító	23,08%	$< R_E$						

5. táblázat: Közszolgálati szerepprofil – Kompetenciák értékelése (forrás: saját szerkesztés)

Medián: 22 kompetencia közül 11 kompetenciával a válaszadók több, mint 65,38%-a fenntartások nélkül egyetért, ill. 11 kompetenciával a válaszadók kevesebb, mint 65,38%-a ért egyet fenntartások nélkül.