Kapcsolattartó Bizottság

Az EU Legfőbb Ellenőrző intézményeinek Kapcsolattartó Bizottsága

Ellenőrzési kompendium

Kiberbiztonság az Európai Unióban és tagállamaiban

A kritikus információs rendszerek és a digitális infrastruktúrák kibertámadásokkal szembeni rezilienciájának ellenőrzése

2014 és 2020 között közzétett ellenőrzési jelentések

HU

2020. december

Az Európai Unió Legfőbb Ellenőrző Intézményeinek Kapcsolattartó Bizottsága fórumot biztosít a közpénzellenőrzéssel kapcsolatos uniós kérdéskörök megvitatásához és kezeléséhez. A bizottság a tagjai közötti párbeszéd és együttműködés fokozásával elősegíti az uniós szakpolitikák és programok külső ellenőrzésének hatékonyabbá tételét. Emellett segít erősíteni az elszámoltathatóságot, javítani az uniós pénzgazdálkodást és megszilárdítani a jó kormányzást, valamennyi uniós polgár javát szolgálva.

Kapcsolat: www.contactcommittee.eu

Tartalomjegyzék

Tartalomjegyzék

Előszó

Kedves Olvasó!

A digitalizáció révén, valamint azáltal, hogy mindennapi életünk összes területén egyre inkább használjuk az információtechnológiát, a lehetőségek új világa nyílik meg előttünk. Ugyanakkor megnőtt annak kockázata, hogy egyének, vállalkozások és állami hatóságok kiberbűnözés vagy kibertámadás áldozatává válnak, és ennek társadalmi és gazdasági hatása is jelentősebbé vált.

Az Unióban a kiberbiztonság a tagállamok hatáskörébe tartozik. Az Unió abban játszik szerepet, hogy közös keretszabályozást hoz létre az uniós egységes piacon belül, és megteremti a feltételeket a tagállamok kölcsönös bizalmon alapuló együttműködéséhez.

A kiberbiztonság és digitális autonómiánk stratégiai jelentőségű kérdéssé vált az Unió és tagállamai számára. Bár eltérő szinten, de továbbra is valamennyi tagállamban hiányosságok tapasztalhatók a kiberbiztonság irányítása terén, a köz- és a magánszférában egyaránt. Ez gyengíti arra való képességünket, hogy korlátozzuk a kibertámadásokat, és szükség esetén reagáljunk rájuk. A dezinformáció – amelyet gyakran az Unión kívülről vezényelnek – egyre erősödik, amint az az idei COVID-19 világjárvány során is megmutatkozott. Ez olyan fenyegetést jelent a társadalmi kohézióra és a polgárok demokratikus rendszereinkbe vetett bizalmára nézve, amelyet nem hagyhatunk figyelmen kívül.

Az Unión belüli legfőbb ellenőrző intézmények körében 2018-ban végzett felmérés megállapította, hogy mindaddig az intézmények mintegy fele nem készített ellenőrzést a kiberbiztonság témájában. Azóta legfőbb ellenőrző intézményeink fokozták a kiberbiztonsággal kapcsolatos ellenőrzési tevékenységüket, különös figyelmet fordítva az adatvédelemre, a rendszerek kibertámadásokkal szembeni felkészültségére, valamint az alapvető közszolgáltatási rendszerek védelmére. Érthető módon ezek közül nem minden ellenőrzést lehet nyilvánosságra hozni, mivel némelyek érzékeny (nemzetbiztonsági) információkat érinthetnek.

Az idei év során a COVID-19 válság alaposan próbára tette gazdaságainkat és társadalmainkat. Mára már annyira függővé váltunk az információs technológiáktól, hogy hatását tekintve egy kiberválság is felérne egy világjárvánnyal. Fel kell készülnünk, és fokoznunk kell a kritikus információs rendszerek és a digitális infrastruktúrák kibertámadásokkal szembeni ellenálló képességét.

Reméljük, hogy az e kompendiumban nyújtott áttekintés Unió-szerte még inkább fokozni fogja a közszférabeli auditorok érdeklődését e kritikus terület iránt.

Klaus-Heiner Lehne

az Európai Számvevőszék elnöke
a Kapcsolattartó Bizottság elnöke
és a projekt vezetője

Összefoglaló

I A kiberbiztonság és digitális autonómiánk **stratégiai jelentőségű kérdéssé vált az Unió és tagállamai számára**, és a fenyegetés szintjének emelkedésével fokozni kell erőfeszítéseinket a kritikus információs rendszerek és a digitális infrastruktúrák kibertámadásokkal szembeni védelmében. A kiberbiztonság nemcsak a közműveket, védelmi és egészségügyi rendszereinket érinti, hanem személyes adataink, üzleti modelljeink és szellemi tulajdonunk védelmét is jelenti. Végső soron a kiberbiztonság arról szól, hogy megvédjük demokratikus társadalmainkat, európaiként fennálló függetlenségünket és azt, ahogy eddig együtt éltünk.

II A Kapcsolattartó Bizottság e harmadik kompendiumának első része azt fejti ki, **mit foglal magában a kiberbiztonság**. Felvázolja, miért jelent kihívást a kiberbiztonság az állami hatóságok, a vállalatok és a magánszemélyek számára, és kiemelten foglalkozik a dezinformációval, ezzel az új jelenséggel, amely egyre nagyobb fenyegetést jelent társadalmaink és demokratikus rendszereink társadalmi kohéziójára. Ismerteti továbbá az Unió kiberbiztonsággal kapcsolatos hatásköreit és szereplőit, stratégiáját és jogszabályait, valamint az e területen rendelkezésre álló uniós forrásokat.

III A kompendium második része összefoglalást ad **tizenkét közreműködő tagállam legfőbb ellenőrző intézményei és az Európai Számvevőszék által végzett**, 2014 és 2020 között közzétett, **kiválasztott ellenőrzések eredményeiről**. Ezek az ellenőrzések a kiberbiztonság olyan fontos szempontjaival foglalkoztak, mint a személyes adatok védelme, a nemzeti adatközpontok integritása, a közműlétesítmények biztonsága, valamint a tágabb értelemben vett nemzeti kiberbiztonsági stratégiák végrehajtása.

IV A kompendium harmadik része **részletes tájékoztatókat tartalmaz a kiválasztott ellenőrzésekről**, valamint röviden ismerteti a legfőbb ellenőrző intézmények által a kiberbiztonság témaköréhez kapcsolódóan közzétett egyéb ellenőrzéseket.

I. RÉSZ. A kiberbiztonság európai összefüggésben

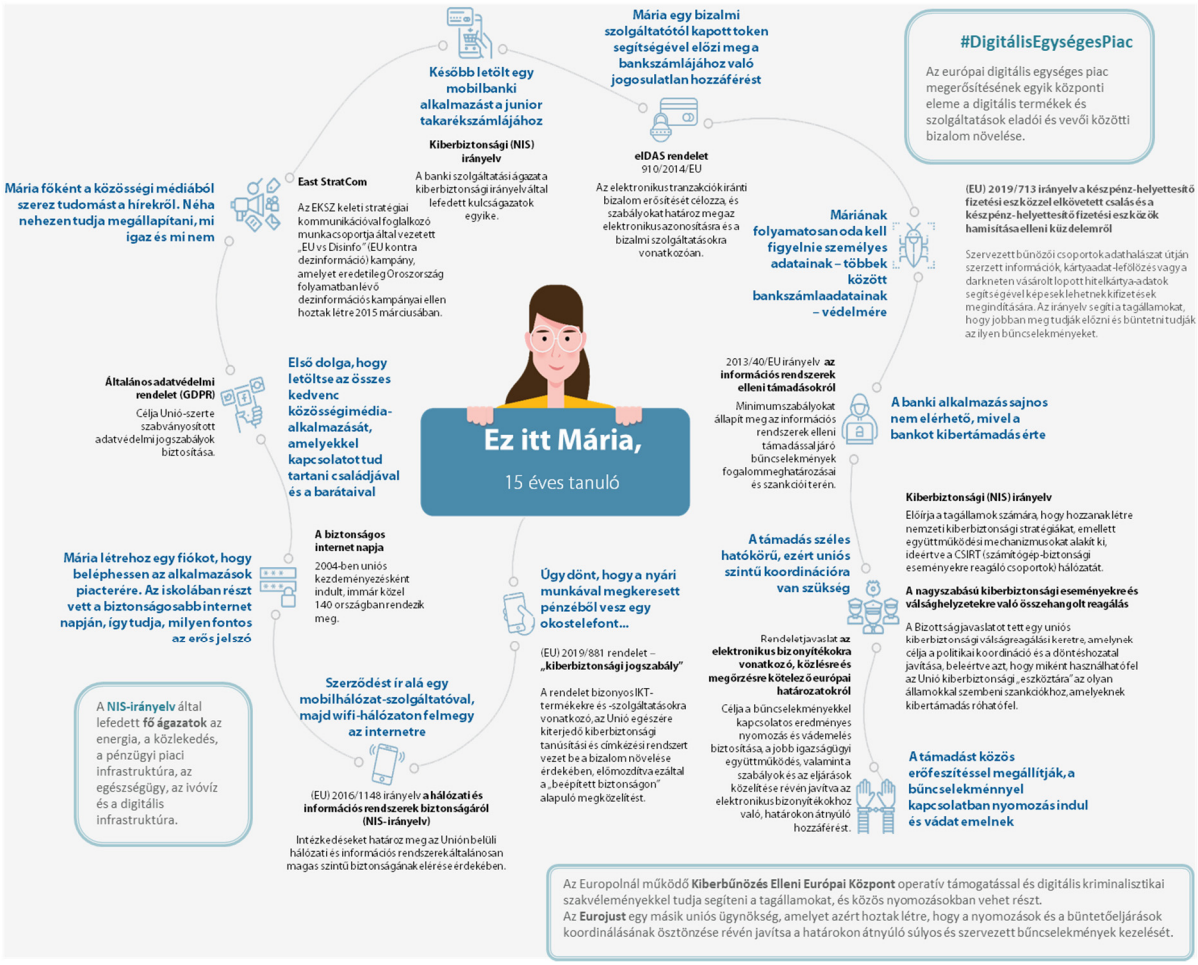
Mi a kiberbiztonság?

1 A **kiberbiztonságnak** nincsen szabványos, egyetemes **definíciója**. Jelen dokumentumban a kiberbiztonság azokra a **tevékenységekre** utal, amelyek **a kiberfenyegetésekkel érintett hálózati és információs rendszerek, felhasználóik és más személyek védelméhez szükségesek.** A kiberbiztonság csakúgy magában foglalja a kiberbiztonsági események megelőzését és felderítését, mint az azokra való reagálást és a következményeik elhárítását. Ilyen incidensek szándékosan vagy véletlenül is bekövetkezhetnek: az információk véletlen nyilvánosságra hozatala ugyanúgy e fogalom körébe tartozik, mint a vállalkozások és kritikus infrastruktúrák elleni támadások, a személyes adatok eltulajdonítása, vagy akár a demokratikus folyamatokba (például a választásokba) való beavatkozás és a nyilvános viták befolyásolására törekvő általános félretájékoztatási kampányok.

A kiberbiztonság minden uniós polgár mindennapi életét érinti

2 A kiberbiztonság minden uniós polgár mindennapi életét érinti, valahányszor személyes információtechnológiai eszközöket használunk, ideértve az okostelefonokat, a wifi-hálózatokat, a közösségi médiát, illetve az elektronikus bankolást. 2020-ban a kérdés már nem az, lesz-e kibertámadás, inkább az, hogy mikor és milyen módon következik be. Ez mindannyiunkat érint: **egyéneket, vállalkozásokat és állami hatóságokat** egyaránt. Az ***1. kép*** bemutatja, miként támogatja az Unió a kiberbiztonságot, és milyen keretrendszert hozott létre az emberek mindennapos elektronikus tevékenységeinek a kibertámadásokkal szembeni védelmére. A kritikus információs rendszerek és a digitális infrastruktúrák kibertámadások elleni védelme ma már stratégiai kihívást jelent.

1. kép. Hogyan támogatja az Unió a kiberbiztonságot az uniós polgárok mindennapi életében?

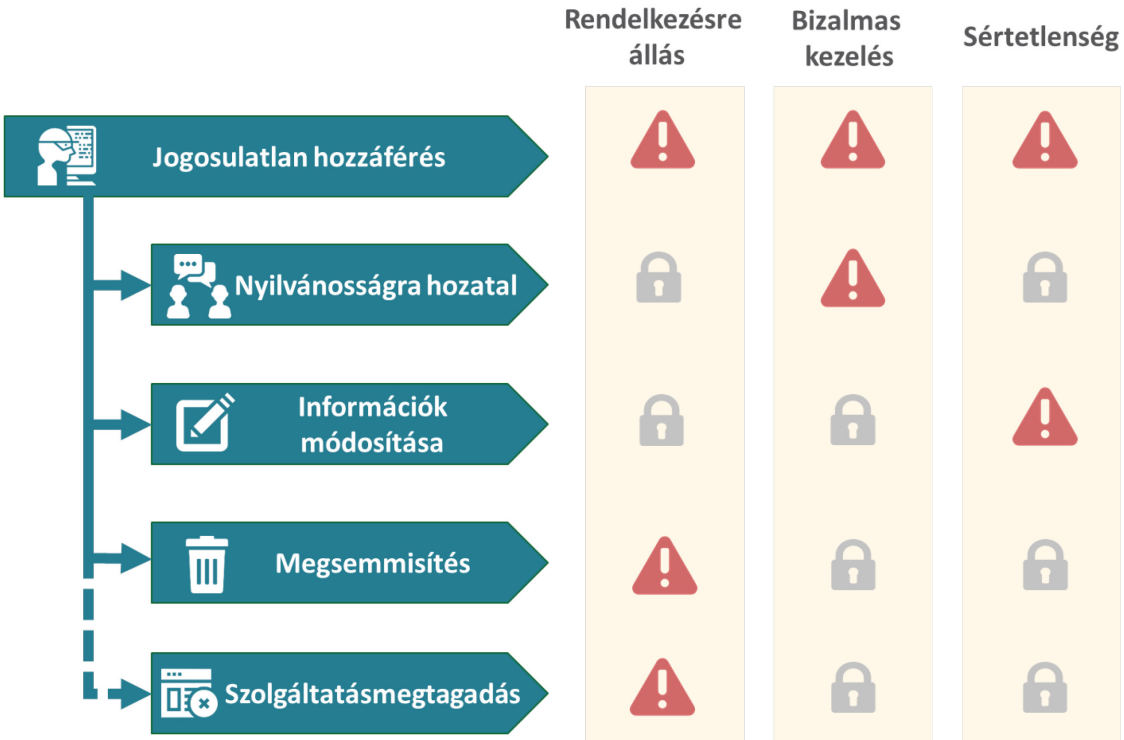


Forrás: Európai Számvevőszék, ikonok: Pixel perfect, www.flaticon.com.

Számos különféle kiberfenyegetés létezik

3 A társadalmunkat érő sokféle kiberbiztonsági fenyegetés aszerint csoportosítható, hogy **mi történik az adatokkal (nyilvánosságra hozatal, módosítás, megsemmisítés vagy a hozzáférés megtagadása)**, illetve hogy milyen információbiztonsági alapelveket sértenek meg (lásd: ***1. ábra***).

1. ábra. A fenyegetések típusai és az általuk veszélyeztetett információbiztonsági elvek



Lakat = nincs hatással a biztonságra; felkiáltójel = biztonsági kockázat

Forrás: Európai Számvevőszék, egy európai parlamenti tanulmány nyomán[1].

4 Valahányszor egy eszköz felcsatlakozik az internetre vagy összekapcsolódik más eszközökkel, nő az úgynevezett kiberbiztonsági „támadási felület”. A dolgok internetének (IoT), a számítási felhőnek, a nagy adathalmazoknak és az ipar digitalizációjának exponenciális növekedése együtt jár a sebezhetőség növekedésével, lehetővé téve a támadók számára, hogy egyre több áldozatot célozzanak meg. A támadástípusok sokfélesége és egyre kifinomultabb volta miatt nehéz tartani a lépést[2]. Az ***1. háttérmagyarázat*** példákkal szolgál a **lehetséges kibertámadásokra**.

[1] Európai Parlament: *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, a LIBE bizottság számára készült tanulmány, 2015. szeptember.

[2] ENISA: *ENISA Threat Landscape Report 2017*, 2018. január 18.

1. háttérmagyarázat.

A kibertámadások típusai

A **rosszindulatú szoftverek** („malicious software”, röviden „malware”) az eszközök vagy hálózatok károsítására szolgálnak. Ilyen szoftverek többek között a vírusok, a trójai programok, a zsarolóvírusok, a férgek, a reklámprogramok és a kémprogramok (például a NotPetya).

A **zsarolóvírusok** titkosítják az adatokat, így a felhasználók csak akkor juthatnak hozzá fájljaikhoz, ha váltságdíjat fizetnek (rendszerint kriptopénzben) vagy ha megteszik, amit a zsaroló kér tőlük. Az Europol szerint az elmúlt néhány évben robbanásszerűen megsokszorozódtak a zsarolóvírusok típusai, és jelenleg ezek jelentik a leggyakoribb problémát (például a Wannacry[3]).

Az **elosztott szolgáltatásmegtagadással járó támadás** (Distributed Denial of Service, DDoS, másik magyar nevén elosztott túlterheléses támadás) azáltal tesz elérhetetlenné bizonyos szolgáltatásokat vagy erőforrásokat, hogy kezelhetetlen mennyiségű kéréssel árasztja el őket. E támadástípus gyakorisága szintén egyre nő, 2017-ben a szervezetek egyharmada szembesült ilyen típusú támadással[4].

A **webalapú támadások** vonzó módszert jelentenek, amelynek révén a szereplők a fenyegetés vektoraként webes rendszereket és szolgáltatásokat használva téveszthetik meg az áldozatokat. Ez hatalmas támadási felületre terjed ki, ideértve annak elősegítését, hogy rosszindulatú webcímek vagy szkriptek egy kívánt weboldalra irányítsák a felhasználót vagy az áldozatot, vagy rosszindulatú tartalmat töltessenek le vele („watering hole” támadás, drive-by támadás), illetve rosszindulatú kódot **építsenek be** egy jogszerű, de feltört honlapba („formjacking”), és ezáltal pénzügyi haszonszerzés vagy adatlopás céljából információkat tulajdonítsanak el[5].

A felhasználók bizonyos manipulációk útján csalárd módon rávehetők egy cselekvés végrehajtására vagy bizalmas információk kiadására. Ez a **„pszichológiai manipuláció”** néven ismert trükk adatlopásra vagy kiberkémkedésre adhat alkalmat. Több módszer is létezik erre, a leggyakoribbak egyike az **adathalászat**, ahol látszólag megbízható forrásból érkező e-mailek révén veszik rá a felhasználókat adataik felfedésére vagy arra, hogy olyan hiperhivatkozásokra (linkekre) kattintsanak rá, amelyek rosszindulatú szoftvereket töltenek le és azokkal megfertőzik a készülékeket. A tagállamok több mint fele számolt be ilyen hálózati támadásokra irányuló vizsgálatokról[6].

A fenyegetéstípusok közül talán a legkártékonyabb a **fejlett tartós fenyegetés** (advanced persistent threat, APT). Az ennek hátterében álló kifinomult támadók hosszú távon figyelik és lopják az adatokat, olykor destruktív célokkal. Ennek során

arra törekszenek, hogy a lehető leghosszabb ideig észrevétlenek maradjanak. Az APT-k gyakran kötődnek különböző államokhoz, és előszeretettel célozzák meg a különösen érzékeny ágazatokat, például a technológiát, a védelmet és a kritikus infrastruktúrát. Információk szerint ez a típusú **kiberkémkedés** teszi ki az összes kiberbiztonsági esemény legalább egynegyedét[7].

A kibertámadások jelentős gazdasági hatással járnak

5 Az elmúlt években jelentős problémává váltak **a kibertámadások és a kiberbűnözés**. Már 2016-ban az uniós vállalkozások 80%-a tapasztalt meg legalább egy kiberbiztonsági eseményt[8]. 2018-ban egy robotikát vagy automatizálást használó szervezetek körében végzett felmérés válaszadóinak 40%-a számolt be arról, hogy kibertámadás esetén a rendszereikre gyakorolt legkritikusabb következményt a működés zavara jelentené. Ennek ellenére a vállalatok – bár tudatában vannak a zavart okozó kiberkockázatoknak – gyakran nem rendelkeznek rendszerrel ezek kezeléséhez[9].

---

[3] A *WannaCry* zsarolóvírus a Microsoft Windows protokoll sebezhetőségeit kihasználva tette lehetővé a számítógépek feletti irányítás távolról történő átvételét. A Microsoft a sebezhetőség felfedezését követően javítócsomagot adott ki annak orvoslására. Több százezer számítógépen azonban nem végezték el a frissítést, és ezek közül sok megfertőződött. *Forrás*: A. Greenberg: *Hold North Korea Accountable for Wannacry – and the NSA, too*, WIRED, 2017. december 19.

[4] Europol: *Internet Organised Crime Threat Assessment 2018*.

[5] ENISA: *ENISA Threat Landscape 2020 – Web-based attacks*, 2020. október 20.

[6] Europol, lásd fent, 2018.

[7] European Centre for International Political Economy: *Stealing Thunder:Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, 2/18. sz. eseti kiadvány, 2018. február.

[8] Europol: *Internet Organised Crime Threat Assessment 2017*.

[9] PWC, Globális információbiztonsági felmérés (GSISS): *Strengthening digital society against cyber shocks*, 2017.

6 Azóta a kibertámadások száma, súlyossága és pénzügyi költségei tovább növekedtek. Amennyire a **pénzügyi hatást** meg lehet becsülni, a kiberbűnözés **2021-re évi 6 billió USA-dollárba** fog kerülni a világgazdaság számára, szemben a 2015-ben becsült 3 billió USA-dollárral[10], miközben a globális GDP becsült összege 2020-ban 138 billió USA-dollár. A kiberbűnözés költségei közé tartozik az adatok károsodása és megsemmisülése, az ellopott pénz, a kieső termelékenység, a szellemi tulajdon ellopása, a személyes és pénzügyi adatok eltulajdonítása, a rendes üzletmenet támadást követő zavara, a hírnév károsodása. Az Európai Rendszerkockázati Testület (ERKT) becslése szerint 2015 és 2020 között 72%-kal nőtt a kiberbiztonsági események átlagos költsége[11].

7 A kiberbűnözés **eltérő módon érinti a különféle gazdasági ágazatokat**, amint azt egy 2020-ban készült friss tanulmány kimutatta[12]: ez volt a legnagyobb zavart okozó csalásos jelenség a kormányzat és a közigazgatás területén, valamint a technológia, a média, a távközlés és az egészségügy ágazatában (lásd: ***2. háttérmagyarázat***); emellett ez volt a második legnagyobb zavart okozó csalásos jelenség a pénzügyi ágazatban, valamint az iparban és a feldolgozóiparban.

[10] Cybersecurity Ventures: *2019 Official Annual Cybercrime Report*, a Herjavec Csoport szponzorálásával, 2019.

[11] ERKT (Európai Rendszerkockázati Testület): *Systemic cyber risk*, 2020. február.

[12] PWC: *Fighting fraud: A never-ending battle – PwC's Global Economic Crime and Fraud Survey*, 2020.

2. háttérmagyarázat.

Pszichoterápiában részesült finnországi betegek zsarolása a 2018 és 2019 között ellopott személyes egészségügyi adataikkal

Egy nagy – az egész országban kirendeltségekkel rendelkező – finnországi pszichoterápiás klinika betegeivel 2020-ban egyenként kapcsolatba lépett egy zsaroló, miután 2018 novemberében ellopta személyes adataikat, majd 2019 márciusában potenciálisan újabb adatsértést követett el. A jelek szerint az adatok között voltak személyazonosító adatok és a terápiás ülések során lezajlott beszélgetésekről készült feljegyzések.

A klinikát és a betegeket egyaránt arra szólították fel, hogy bitcoinban fizessenek váltságdíjat a zsarolónak, hogy az adatok ne kerüljenek nyilvánosságra. Az incidens nyomán a finn kormány rendkívüli ülést tartott[13].

8 2019-ben az Europol[14] ismét rámutatott arra, hogy **továbbra is tartósan fennáll több alapvető fenyegetés a kiberbűnözés terén**:

- a legfőbb fenyegetést még mindig a zsarolóvírusos támadások jelentik; ezek egyre célzottabbak, egyre jövedelmezőbbek és egyre nagyobb gazdasági kárt okoznak. Mindaddig, amíg a zsarolóvírus viszonylag könnyű bevételt biztosít a kiberbűnözők számára, és továbbra is jelentős kárt és pénzügyi veszteségeket okoz, valószínűleg ez marad a legfőbb fenyegetés a kiberbűnözés terén;
- a rosszindulatú szoftverek első számú vektorai az adathalászat és a sérülékeny távoli asztali protokollok (RDP-k); ezenkívül
- a kiberbűnözés fő célpontját, árucikkét és előmozdítóját továbbra is az adatok jelentik.

9 Hasonlóképpen az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) ***„Main incidents in the EU and worldwide”*** **című 2020. évi jelentésében**[15] több példát említ a kiberbiztonsági eseményekre (lásd: ***3. háttérmagyarázat***).

---

[13] BBC News: *Therapy patients blackmailed for cash after clinic data breach*, 2020. október 26.

[14] Europol: *INTERNET organised crime threat assessment (IOCTA)*, 2019.

[15] ENISA: *Main incidents in the EU and worldwide – January 2019 to April 2020*, 2020. október.

3. háttérmagyarázat.

Európai Uniós Kiberbiztonsági Ügynökség (ENISA): Kiberbiztonsági események 2019–2020 folyamán

A „verifications.io” e-mail-platform jelentős adatvédelmi incidenst szenvedett el egy védelem nélküli MongoDB adatbázis miatt. Több mint 800 millió e-mail adatai kerültek ki, amelyek érzékeny információkat, köztük személyazonosító adatokat is tartalmaztak.

Egy, a MEGA1 felhőszolgáltató által tárolt népszerű hekkerfórumon több mint 770 millió e-mail-cím és 21 millió egyedi jelszó került nyilvánosságra. „Collection #1” néven ez lett minden idők legjelentősebb, feltört személyazonosítókat tartalmazó gyűjteménye.

A Citrix nevű virtualizációs és felhőszolgáltató célzott kibertámadás áldozatává vált. A Citrix rendszereihez való hozzáférés érdekében a támadók a szoftver több kritikus sebezhetőségét használták ki, ideértve a CVE-2019–19781-et, és az úgynevezett „jelszó-szórás” technikáját alkalmazták.

Az iNSYNQ19 felhőalapú tárhelyszolgáltatót zsarolóvírusos támadás érte, amelynek nyomán az ügyfelek több mint egy hétig nem tudtak hozzáférni adataikhoz, így helyi biztonsági mentésekre kellett támaszkodniuk.

10 Az Europol szerint 2019 első hat hónapjában kétszeresére nőtt azon kibertámadások száma, amelyek **tartós kár** okozását célozták, főként a feldolgozóiparban. A hagyományos zsarolóvírusos támadásokkal szemben ezek szabotázs jellegű cselekedetek, amelyek véglegesen törlik vagy más módon visszafordíthatatlanul károsítják a vállalat adatait (lásd: ***4. háttérmagyarázat***).

4. háttérmagyarázat.

Romboló zsarolóvírus: a 2019. évi „GermanWiper” támadások

2019-ben egy sor zsarolóvírusos támadást azonosítottak, amelyek Németországban működő vállalatokat vettek célba. A *GermanWiper* elnevezésű zsarolóvírus képes arra, hogy nullákkal és egyesekkel írja felül a megfertőzött fájlokat, lehetetlenné téve ezáltal a fájlok helyreállítását. A zsarolóvírus e-mailes adathalász kampányokkal terjedt, és különösen vezető vállalatok humánerőforrás-ügyi munkatársait vette célba, mivel hamis álláspályázatokba volt beágyazva[16].

A kiberfenyegetések gyakoribbá válásával egyre nő a velük kapcsolatos tudatosság

11 A legutóbbi időkig azonban még mindig meglehetősen alacsony volt az efféle kockázatok ismertsége és elismertsége. 2017-ben az uniós vállalkozások 69%-a egyáltalán nem tudott vagy csak alapvető ismeretekkel rendelkezett a **kiberfenyegetésekkel szembeni kitettségéről**[17], és 60%-uk soha nem becsülte fel a **lehetséges pénzügyi veszteségeket**[18]. Ezenfelül egy 2018. évi globális felmérés szerint a szervezetek egyharmada inkább megfizetné a hekkerek által kért váltságdíjat, mintsem beruházzon az információbiztonságba[19].

---

[16] Cybersecurity Insiders: *GermanWiper Ransomware attack warning for Germany*, dátummegjelölés nélkül.

[17] Európai Bizottság: *Tájékoztató a kiberbiztonságról*, 2017. szeptember.

[18] Ilyen veszteségek lehetnek többek között a bevételkiesés, a károsodott rendszerek helyreállítási költségei, az ellopott vagyonért vagy információkért való esetleges felelősség, az ügyfelek megtartását célzó ösztönzők, a magasabb biztosítási díjak, a védelmi költségek növekedése (új rendszerek, alkalmazottak, képzések), valamint az esetleges jogszabályi megfelelési és perköltségek.

[19] NTT Security: *Risk: Value 2018 Report*.

12 **Az európaiak kiberbiztonsághoz való hozzáállásáról készített 2020. évi Eurobarométer-felmérés**[20] kimutatta, hogy az uniós polgárok tudatossága nő és aggályaik erősödnek:

- Az internetet használó válaszadók leginkább amiatt aggódnak, hogy valaki visszaél személyes adataikkal (46%), hogy mennyire biztonságos az internetes fizetés (41%), illetve hogy nem tudják megnézni az árukat vagy nem tudnak tanácsot kérni egy valóságos személytől, továbbá hogy esetleg nem kapják meg az interneten rendelt árut vagy szolgáltatást (22–22%).
- A válaszadók több mint háromnegyede (76%) úgy véli, egyre nagyobb a veszélye annak, hogy kiberbűnözés áldozatává válik. Ugyanakkor jóval kevesebben (52%) gondolják azt, hogy kellően meg tudják védeni magukat ezzel szemben – ez az arány pedig kilenc százalékpontos csökkenést jelent 2018-hoz képest.
- Mindazonáltal a válaszadók valamivel több mint fele (52%) úgy véli, jól tájékozott a kiberbűnözéssel kapcsolatban, ugyanakkor csupán 11% érzi magát nagyon jól tájékozottnak.

A kiberbiztonság fontos a társadalmi kohézióhoz és a politikai stabilitáshoz

Újfajta fenyegetés: a kiberbiztonság és a dezinformáció

13 A szándékosan és szisztematikusan terjesztett **dezinformáció akut stratégiai kihívást jelent demokráciáinkban**[21]. A dezinformáció és az álhírek képesek a társadalmak megosztására, bizalmatlanság keltésére, sőt akár a társadalmi kohézió és a demokratikus folyamatokba vetett bizalom aláásására is (lásd: ***5. háttérmagyarázat***).

[20] Európai Bizottság: *499. számú Eurobarométer tematikus felmérés – „Europeans' attitudes towards cyber security"*, 2020. január.

[21] Az Oxfordi Egyetem *The Global Disinformation Order* című tanulmánya szerint (2019. szeptember) az utóbbi két évben több mint kétszeresére, 70-re nőtt azon országok száma, ahol politikai dezinformációs kampányok zajlottak.

5. háttérmagyarázat.

Dezinformáció

Az Európai Bizottság fogalommeghatározása szerint a dezinformáció olyan igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy szándékos megtévesztés céljából hoznak létre, hoznak nyilvánosságra és terjesztenek, és amely kárt okozhat a közérdeknek[22]. A közérdeknek okozott károk magukban foglalják a demokratikus folyamatok aláásását, valamint a közjavak – például az egészségügy, a környezet vagy a biztonság – veszélyeztetését.

A jogellenes tartalommal szemben (ilyen például a gyűlöletbeszéd, a terrorista tartalom vagy a gyermekpornográfia) a dezinformáció jogszerű tartalmakat fed le, ezért összefügg a véleménynyilvánítás szabadságának és a tömegtájékoztatás szabadságának alapvető uniós értékeivel. A Bizottság fogalommeghatározása értelmében nem tartoznak a dezinformáció körébe a megtévesztő reklámok, a jelentéstételi hibák, a szatírák és paródiák, illetve az egyértelműen azonosítható módon pártokhoz köthető hírek és kommentárok.

14 Új technológiák és szoftverek lehetővé teszik a dezinformáció **közösségi és egyéb online médián** keresztül történő gyors és viszonylag olcsó terjesztését.
A dezinformáció jellemzően olyan érzékeny témakörökre összpontosul, amelyek valószínűsíthetően polarizálhatják a véleményeket és felszíthatják az érzelmeket, amiből adódóan nagyobb valószínűséggel osztják meg őket. Ilyen témakörök például az egészségügyi kérdések (például oltásellenes kampányok), a migráció, az éghajlatváltozás vagy a társadalmi igazságossággal kapcsolatos kérdések.

Harmadik országok által a demokratikus folyamatok befolyásolása érdekében folytatott dezinformációs kampányok

15 A dezinformáció célja a demokratikus vita kiélezése, feszültség előidézése vagy fokozása a társadalmon belül, valamint a választási rendszerek aláásása, ami szélesebb körben kihat az európai társadalmakra és biztonságra, végső soron pedig veszélyezteti a véleményalkotás és a véleménynyilvánítás szabadságát. A dezinformációt gyakran **harmadik országbeli szereplők támogatják**, akik destabilizálni kívánják társadalmainkat és demokratikus rendszereinket. Ebben az összefüggésben a nagyszabású dezinformációs kampányok magukban foglalhatják hálózatok feltörését is.

[22] Európai Bizottság: *Közlemény az online félretájékoztatás kezeléséről*, COM(2018) 236.

Példa erre az Egyesült Királyságban folytatott, az Európai Unióból történő kilépésről szóló népszavazás befolyásolását célzó orosz kampány (lásd: ***6. háttérmagyarázat***).

6. háttérmagyarázat.

Demokratikus döntéshozatali folyamatokat megcélzó orosz dezinformációs kampányok[23]

2016 közepén oroszországi szereplők kampányt indítottak annak érdekében, hogy befolyásolják az Egyesült Királyságban 2016 júniusában megtartott, az Unióból történő kilépésről szóló szavazást. Egy tweetelemzésből kiderült, hogy a szavazást megelőző 48 órában több mint 150 000 orosz fiókról tweeteltek a *#Brexit* témában, és több mint 45 000 üzenetet tettek közzé a szavazásról. A népszavazás napján orosz fiókok 1102 Twitter-üzenetet osztottak meg a *#ReasonsToLeaveEU* hashtaggel.

16 A dezinformációval szembeni küzdelem jelentős kihívás, mivel megfelelő egyensúlyt kell teremteni a biztonság, valamint alapvető jogaink és szabadságaink között, ösztönözve az innovációt és a nyitott piacot. Az Unió számos intézkedést hozott **a dezinformáció kezelése** érdekében.

- 2015-ben létrehozták az EKSZ-nél működő, **keleti stratégiai kommunikációval foglalkozó munkacsoportot** (East StratCom Task Force) az orosz dezinformációs kampányok ellen[24]. A szakértők dicsérik azt a munkát, amelyet a csoport az uniós politikák előmozdítása, az európai szomszédságpolitikában részt vevő országok független médiájának támogatása, valamint a dezinformáció előrejelzése, nyomon követése és kezelése terén végzett[25].

---

[23] Park Advisors: *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr és William Gangware, 2019.

[24] Az Európai Tanács 2015. március 20-i következtetései (EUCO 11/15). Azóta két további munkacsoport jött létre a Nyugat-Balkán és a déli szomszédság vonatkozásában.

[25] Az Atlanti Tanács egyik jelentésében felszólította az Uniót, hogy valamennyi tagállamot kötelezze arra, hogy küldjenek nemzeti szakértőket a munkacsoportba. Lásd: D. Fried és A. Polyakova: *Democratic Offense Against Disinformation*, 2018. március 5.

- Az ENISA 2018-ban **közleményt adott ki az online félretájékoztatás kezeléséről**[26]. A fellépés többek között segíti a tartalmak megbízhatóbbá tételét, valamint támogatja a média- és hírműveltség növelésére irányuló erőfeszítéseket.
- A Bizottság Közös Kutatóközpontja meglévő szakpolitikai eszközök alapján kidolgozott egy önkéntes jellegű, **önszabályozó gyakorlati kódexet**, amelyet a reklámipar és online platformok elfogadtak[27].
- Emellett létrejött egy **tényellenőrzéssel foglalkozó** független európai **hálózat**.

Dezinformáció a COVID-19 idején és az arra adott uniós válasz

17 A dezinformáció a **COVID-19 egészségügyi válság**[28] vonatkozásában is problémát jelent (az efféle dezinformációra példákért lásd: ***7. háttérmagyarázat***).

[26] ENISA: *Strengthening Network & Information Security & Protecting against Online Disinformation („Fake News”)*, 2018. április.

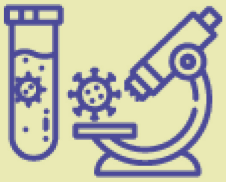
[27] JRC: *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018–02, 2018. április.

[28] Reuters Institute és Oxfordi Egyetem: *Types, Sources, and Claims of Covid-19 Misinformation*, 2020. április.

7. háttérmagyarázat.

Példák a Bizottság által jelentett, COVID-19 világjárvánnyal kapcsolatos dezinformációra[29]

Hamis állítások, mint például „a koronavírusos fertőzés fehérítő vagy tiszta szesz fogyasztásával gyógyítható”: épp ellenkezőleg, a fehérítő vagy a tiszta szesz fogyasztása nagyon káros lehet. **Belgium mérgezésvédelmi központja 15%-kal nagyobb számban regisztrált fehérítővel kapcsolatos eseteket.**



Összeesküvés-elméletek, mint például az az állítás, miszerint a koronavírus „a globális elit által okozott fertőzés, amelynek célja a népességnövekedés visszaszorítása”. A tudományos bizonyítékok egyértelműek: a vírus egy állati eredetű víruscsaládból származik, amelybe más vírusok is beletartoznak, köztük a SARS és a MERS.

Nem tudományos állítások, mint például „az 5G létesítmények terjesztik a vírust”. Ezekre az elméletekre ugyan nincs semmilyen konkrét bizonyíték, mégis antennatornyok megrongálását eredményezték.

[29] Európai Bizottság: *Tackling coronavirus disinformation*, dátummegjelölés nélkül.

18 A Bizottság, az ENISA, a CERT-EU és az Europol 2020 márciusában kiadott egy **közös nyilatkozatot a COVID-19-cel kapcsolatos fenyegetésekről**[30], rámutatva arra, hogy rosszindulatú szereplők aktívan kihasználják a közegészségügyi válság alatti nehéz körülményeket, hogy célba vegyék a távmunkázókat, vállalatokat és magánszemélyeket egyaránt. Ezenkívül az ENISA külön tájékoztató kampányokat dolgozott ki azon ágazatok számára, amelyeket a COVID-19 világjárvány alatt érintett a dezinformáció[31].

A dezinformáció leküzdéséhez nélkülözhetetlen a tényellenőrzés

19 Az Unió emellett fokozta az európai tényellenőrzők és dezinformációval foglalkozó kutatók támogatására irányuló erőfeszítéseit. Létrehozta **a digitális média európai megfigyelőközpontját**, hogy megvizsgálja és jobban megértse a dezinformáció jelenségét, ideértve az olyan tényezőket, mint az érintett szereplők, a vektorok, az eszközök, a módszerek, a terjedés dinamikája, az elsődlegesen megcélzott csoportok, valamint a társadalomra gyakorolt hatás. A dezinformáció kezelésére irányuló, uniós finanszírozású projektekre példa továbbá a PROVENANCE, a SocialTruth, a EUNOMIA és a WeVerify.

20 2018-ban az Unió **a dezinformáció visszaszorítását célzó gyakorlati kódexével**[32] világszerte elsőként terjesztett elő önszabályozó jellegű előírásokat a dezinformációval szembeni fellépés érdekében. Ezt az önkéntes kódexet 2018 októberében platformok, vezető közösségi hálózatok, hirdetők és a reklámipar is aláírták. Az aláírók között megtalálhatók a Facebook, a Twitter, a Mozilla, a Google, valamint a reklámipar szervezetei és tagjai. A Microsoft 2019 májusában írta alá a gyakorlati kódexet, a TikTok pedig 2020 júniusában.

---

[30] Az Európai Bizottság, a ENISA, a CERT-EU és az Europol közös nyilatkozata: *Coronavirus outbreak*, 2020. március 20.

[31] ENISA: *Information sheets relating to Covid-19*, 2020.

[32] *A dezinformáció visszaszorítását célzó uniós gyakorlati kódex*, 2018. szeptember.

A 2019. évi európai parlamenti választások biztosítása

21 Az európai demokratikus rendszerek legitimitásának alapja az, hogy tájékozott választók **szabad és tisztességes választások** keretében kinyilvánítják demokratikus akaratukat. Ezért a közvélemény rosszindulatú és szándékos befolyásolására és manipulálására irányuló valamennyi kísérlet súlyos fenyegetést jelent társadalmainkra nézve. A választásokba és a választási infrastruktúrába való beavatkozásnak célja lehet a választói preferenciák, a részvételi arány vagy maga a választási folyamat befolyásolása, ideértve a tényleges szavazást, valamint a szavazatösszesítést és a kommunikációt. Az Egyesült Királyságban tartott népszavazás nyomán a 2019. évi európai parlamenti választások során került sor első ízben a tagállamok összehangolt fellépésére **a demokratikus választások integritásának védelme** érdekében, ideértve az európai parlamenti és a nemzeti parlamenti választásokat egyaránt.

22 Amint azt fentebb már említettük, a Bizottság 2018 áprilisában kiadott egy **közleményt az online félretájékoztatás kezelését célzó európai megközelítésről**[33]. Ezt követte 2018 szeptemberében a **választási csomag**[34], amely az uniós és a tagállami választások dezinformációval és kibertámadásokkal szembeni védelmét hivatott szolgálni. A csomag középpontjában az adatvédelem, a politikai hirdetések és a finanszírozás átláthatósága, a kiberbiztonság és a választások kérdése, valamint az adatvédelmi szabályok politikai pártok általi megsértése esetén alkalmazandó szankciók álltak. Ezenkívül sor került egy **közös gyakorlatra** annak tesztelése céljából, mennyire eredményesek a tagállamok és az Unió reagálási gyakorlatai és válságkezelési tervei az európai parlamenti választások védelme tekintetében (lásd: ***8. háttérmagyarázat***).

[33] Európai Bizottság: *Európai megközelítés az online félretájékoztatás kezelésére*, COM(2018) 236 final.

[34] Európai Bizottság: *Az Unió helyzete (2018)*, 2018. szeptember.

8. háttérmagyarázat.

ELEx19: a 2019. évi európai parlamenti választások védelme[35]

A közelgő európai parlamenti választások rezilienciájára irányuló ELEx19 gyakorlat azt volt hivatott azonosítani, hogy miként lehet megelőzni, feltárni és enyhíteni a 2019. évi választások eredményét esetlegesen befolyásoló kiberbiztonsági eseményeket.

A gyakorlat lehetővé tette a résztvevők számára, hogy különféle – számítógépes fenyegetéseket és eseményeket magukban foglaló – forgatókönyvek alapján:

— áttekintést kapjanak az Unió-szerte meglévő választási rendszerek rezilienciájának szintjéről (az elfogadott szabályok, illetve a rendelkezésre álló képességek és készségek tekintetében);

— fokozzák az érintett hatóságok közötti nemzeti szintű együttműködést (beleértve a választási hatóságokat és más releváns szerveket és hivatalokat);

— teszteljék a válságkezelési terveiket, valamint a kiberbiztonsági támadások és a hibrid fenyegetések (köztük a dezinformációs kampányok) megelőzésére, felderítésére, kezelésére és a reagálásra irányuló eljárásaikat;

— javítsák a határokon átnyúló együttműködést és erősítsék a vonatkozó uniós szintű együttműködési csoportokkal fennálló kapcsolatokat (például választási együttműködési hálózat, NIS együttműködési csoport, CSIRT-hálózat); valamint

— azonosítsák az összes egyéb lehetséges hiányosságot és a megfelelő kockázatcsökkentő intézkedéseket, amelyeket az európai parlamenti választások előtt végre kell hajtani.

Ezen a gyakorlaton az uniós tagállamok több mint 80 képviselője vett részt, az Európai Parlament, a Bizottság, valamint az Európai Uniós Kiberbiztonsági Ügynökség megfigyelői mellett.

[35] ENISA: *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 2019. április 5.

23 Végezetül, 2018 decemberében az Európai Tanács elfogadta a **félretájékoztatással szembeni cselekvési tervet**[36], amelynek célja az összehangolt reagálás és a tagállami intézkedések kiegészítése volt. A cselekvési terv konkrét fellépéseket tartalmazott, amelyek a következő négy pillérre épültek: a félretájékoztatás felderítésére, elemzésére és nyilvánosság elé tárására irányuló uniós intézményi képességek javítása, a félretájékoztatásra történő összehangolt és közös reagálás megerősítése, a magánszektornak a félretájékoztatás kezelése érdekében történő mozgósítása, valamint a tudatosság növelése és a társadalmi reziliencia javítása.

Kiberbiztonság az Európai Unióban: hatáskörök, szereplők, stratégiák és jogszabályok

A kiberbiztonság elsődlegesen tagállami hatáskör

24 Az Unióban a kiberbiztonság elsődlegesen **a tagállamok felelőssége**. Különösen igaz ez a nemzetbiztonságot érintő érzékeny információk védelmére. Minden tagállam rendelkezik egy **nemzeti kiberbiztonsági stratégiával** (NCSS), amely segíti őket azon kockázatok kezelésében, amelyek akadályozhatják a kibertérből származó gazdasági és társadalmi előnyök elérését. Ugyanakkor a tagállamok között még mindig vannak különbségek a kiberbiztonsággal kapcsolatos kapacitásuk és kötelezettségvállalásuk tekintetében.

25 Az Uniónak szerepet kell vállalnia az uniós egységes piacon belüli **közös keretszabályozás** kiépítésében és az ahhoz szükséges feltételek megteremtésében, hogy a tagállamok eredményesen működjenek együtt a kiberbiztonságot érintő különböző szakpolitikai területeken, mint a bel- és igazságügy, az egységes piac, a közlekedés, a népegészségügy, a fogyasztóvédelmi politika és a kutatás.

---

[36] Európai Bizottság, az Unió külügyi és biztonságpolitikai főképviselője: *Cselekvési terv a félretájékoztatással szemben*, JOIN(2018) 36 final. A terv az uniós intézményeknek a félretájékoztatás felderítésére, elemzésére és nyilvánosság elé tárására irányuló képességei javítására, az összehangolt és közös reagálás megerősítésére, a magánszektor mozgósítására, valamint a tudatosság növelésére és a társadalmi reziliencia javítására összpontosít.

A külpolitikában a kiberbiztonság szervesen beépül a diplomáciába, és egyre fontosabb részét képezi az Unió kialakulóban lévő védelmi és biztonságpolitikájának.

26 Az **uniós szinten** legjelentősebb kiberbiztonsági **szereplőket** az alábbi ***9. háttérmagyarázat*** mutatja be.

9. háttérmagyarázat.

Az uniós szinten legjelentősebb kiberbiztonsági szereplők

Az **Európai Bizottság** törekszik arra, hogy növelje a kiberbiztonsági kapacitásokat és együttműködést, megerősítse az Unió szerepét a kiberbiztonság biztosításában, és a többi uniós szakpolitikába is beépítse a kiberbiztonság szempontját.

Ebben több uniós ügynökség is segíti a Bizottságot, nevezetesen az **ENISA**, az **EC3** és a **CERT-EU**. Az **Európai Uniós Kiberbiztonsági Ügynökség** (eredeti neve – Európai Hálózat- és Információbiztonsági Ügynökség – alapján röviden **ENISA**) elsősorban tanácsadó szerv, amely támogatja a szakpolitikák kidolgozását, a kapacitásépítést és a tudatosságnövelést. Az Europolon belül működő **Kiberbűnözés Elleni Európai Központot (EC3)** azzal a céllal hozták létre, hogy eredményesebbé tegye a kiberbűncselekmények nyomán hozott uniós bűnüldözési válaszintézkedéseket. A Bizottság biztosít működési keretet az összes uniós intézményt, szervet és ügynökséget segítő, **hálózatbiztonsági vészhelyzeteket elhárító csoportnak (CERT-EU)**.

Az **Európai Külügyi Szolgálat (EKSZ)** irányítja a kibervédelmet, a kiberdiplomáciát és a stratégiai kommunikációt, továbbá hírszerzési és elemzőközpontoknak ad otthont. Az **Európai Védelmi Ügynökség (EDA)** célja a kibervédelmi kapacitások fejlesztése.

Uniós szinten a tagállamok a **Tanács** keretében járnak el, amely számos koordinációs és információmegosztó testülettel rendelkezik (beleértve a kiberkérdésekkel foglalkozó horizontális munkacsoportot). Az **Európai Parlament** társjogalkotóként jár el.

A **magánszektorbeli szervezetek**, köztük az ipar, az internetirányítási szervek és a tudományos körök hozzájáruló partnerként – többek között egy szerződéses köz-magán társulás (**cPPP**) révén – vesznek részt a szakpolitikák kidolgozásában és végrehajtásában.

Az uniós kiberstratégia: a kiberbiztonság 2013 óta fontos kérdéskör

27 A kiberbiztonság legalább 2013 óta fontos politikai kérdéskör; akkor fogadta el a Bizottság a **kiberbiztonsági stratégiáját**[37]. A stratégia öt fő célkitűzést követ:

- a kibertámadásokkal szembeni reziliencia fokozása;
- a kiberbűnözés csökkentése;
- kibervédelmi politikák és képességek kifejlesztése;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- nemzetközi szakpolitika létrehozása a kibertér vonatkozásában, az Unió alapértékeihez igazítva.

Az ezt követő években a kiberbiztonság kérdésével más uniós stratégiák is foglalkoztak (lásd: ***10. háttérmagyarázat***).

[37] Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér*, JOIN(2013) 1 final, 2013. február 7.

10. háttérmagyarázat.

A kiberbiztonság kérdésével foglalkozó további uniós stratégiák

- Az **európai biztonsági stratégia** (2015)[38] a kiberbűncselekmények üldözésének és igazságügyi kezelésének javítását célozta, elsősorban a meglévő politikák és jogszabályok megújítása és aktualizálása révén.
- A **digitális egységes piaci stratégia** (2015)[39] a digitális árukhoz és szolgáltatásokhoz való jobb hozzáférést célozta: ehhez elengedhetetlen az online biztonság, a bizalom és a befogadás erősítése.
- **Az EU globális stratégiája**(2016)[40] több kezdeményezést határozott meg az Unió globális szerepének erősítése érdekében. Ennek egyik alapvető pillére volt a kiberbiztonság, valamint a dezinformáció stratégiai kommunikáció segítségével történő megcáfolása.

28 Ezenkívül az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselője 2017-ben kiadott egy, az Európai Parlamentnek és a Tanácsnak címzett **közös közleményt az Unió kiberbiztonságáról**[41]: ebben szilárdabb és eredményesebb struktúrákat szorgalmaztak, amelyek elősegítik a kiberbiztonságot és a tagállamokban, illetve az Unió saját intézményei, ügynökségei és szervezetei ellen elkövetett kibertámadásokra való reagálást.

29 2020 júliusában az Európai Bizottság aktualizálta 2015. évi stratégiáját, és a 2020 és 2025 közötti időszakra elfogadta **a biztonsági unióra vonatkozó uniós stratégiát**[42], amely stratégiai jelentőségű kérdésként határozza meg a kiberbiztonságot. Ebben a stratégiában a Bizottság különös hangsúlyt helyez az úgynevezett hibrid

---

[38] Európai Bizottság: *Az európai biztonsági stratégia*, COM(2015) 185 final, 2015. április 28.

[39] Európai Bizottság: *Európai digitális egységes piaci stratégia*, COM(2015) 192 final, 2015. május 6.

[40] EKSZ: *Közös jövőkép, közös fellépés: erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*, 2016. június.

[41] Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselője: *Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése*, JOIN(2017) 450, 2017. szeptember 13.

[42] Európai Bizottság: *Közlemény a biztonsági unióra vonatkozó uniós stratégiáról*, COM(2020) 605 final, 2020. július 24.

fenyegetésekre, amelyek kibertámadásokat és dezinformációs kampányokat is magukban foglalnak, amelyek során harmadik országbeli állami és nem állami szereplők összehangoltan lépnek fel azzal a szándékkal, hogy manipulálják az információs környezetet, és támadást intézzenek az alapvető infrastruktúra ellen.

A kiberbiztonságra vonatkozó uniós jogszabályok: a hálózati és információs rendszerek biztonságáról szóló irányelv, az általános adatvédelmi rendelet, a kiberbiztonsági jogszabály, valamint egy új szankciós mechanizmus

30 A jogszabályi rendszer alapkövét az első uniós szintű kiberbiztonsági jogszabály, a 2016. évi **hálózat- és információbiztonsági (NIS) irányelv**[43] jelenti, amely a 2013. évi kiberbiztonsági stratégia fő pillére. Az irányelv célja a képességek bizonyos szintű összehangolása azáltal, hogy nemzeti hálózat- és információbiztonsági stratégiák elfogadására, valamint integrált kapcsolattartó pontok és számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) létrehozására kötelezi a tagállamokat[44]. Az irányelv ezenfelül biztonsági és bejelentési követelményeket állapít meg a kritikus ágazatokban alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára.

31 A tagállamoknak 2018 májusáig kellett átültetniük **nemzeti jogukba a NIS-irányelvet**. Emellett 2018 novemberéig azonosítaniuk kellett az úgynevezett „alapvető szolgáltatásokat nyújtó szereplőket”. Az Európai Bizottságnak rendszeresen felül kell vizsgálnia az irányelv működését. A Bizottság – „a digitális korra felkészült Európa” alapvető szakpolitikai célkitűzésének részeként, és összhangban a biztonsági unió céljaival – 2020. júliustól októberig konzultációt tartott, amelynek eredményeit felhasználják a NIS-irányelv első értékeléséhez és utólagos hatásvizsgálatához.

---

[43] 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.

[44] Ezek a csoportok az irányelv által létrehozott együttműködési struktúrákba – a CSIRT-hálózatba (az uniós tagállamok által kinevezett CSIRT csoportokból és a CERT-EU-ból álló hálózat, amely titkárságának az ENISA ad otthont) és az együttműködési csoportba (a tagállamok közötti stratégiai együttműködést és információcserét támogató és elősegítő csoport, amely titkárságának a Bizottság ad otthont) – illeszkednek.

32 Ezzel párhuzamosan 2016-ban hatályba lépett az **általános adatvédelmi rendelet**[45] (GDPR), amely 2018 májusa óta alkalmazandó. E rendelet azáltal kívánja biztosítani az európai polgárok személyes adatainak védelmét, hogy előírja az azok kezelésére és továbbadására irányadó szabályokat. Bizonyos jogokat biztosít az érintettek számára, valamint kötelezettségeket ró az adatkezelőkre (digitális szolgáltatók) az információk felhasználása és átadása tekintetében.

33 Emellett az uniós **kiberbiztonsági jogszabály**[46] első ízben vezet be az Unió egészére kiterjedő kiberbiztonsági tanúsítási keretrendszert az IKT-termékek, -szolgáltatások és -folyamatok vonatkozásában. Ez azt jelenti, hogy az Unióban működő vállalatoknak csupán egyszer kell tanúsíttatniuk IKT-termékeiket, -folyamataikat és -szolgáltatásaikat, és tanúsítványaikat Unió-szerte elismerik. Az uniós kiberbiztonsági jogszabály emellett létrehozta az **Európai Uniós Kiberbiztonsági Ügynökséget** (az ENISA rövidítés a korábbi Európai Uniós Hálózat- és Információbiztonsági Ügynökség nevéből származik). A jogszabály megbízza az ügynökséget azzal, hogy fokozza az uniós szintű operatív együttműködést, segítve az uniós tagállamokat – azok kérésére – a kiberbiztonsági események kezelésében, valamint támogatva az uniós koordinációt a nagy kiterjedésű, határokon átnyúló kibertámadások és válságok esetén.

[45] 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

[46] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról.

34 Végezetül a Tanács 2019 májusában létrehozott egy olyan jogi eszközt, amely lehetővé teszi az Unió számára, hogy célzott korlátozó **intézkedéseket** vezessen be az Unióra vagy tagállamaira nézve külső fenyegetést jelentő **kibertámadásoktól való elrettentés és az azokra való reagálás érdekében**[47]. Ennek eredményeképpen az Unió jogi hatáskörrel rendelkezik az olyan személyek vagy szervezetek szankcionálására, akik, illetve amelyek:

- kibertámadásokért vagy megkísérelt kibertámadásokért felelősek; vagy
- pénzügyi, technikai vagy anyagi támogatást nyújtanak ilyen támadásokhoz vagy azokban más módon közreműködnek.

A Tanács első alkalommal 2020 júliusában élt ezekkel az új előjogokkal (lásd: ***11. háttérmagyarázat***).

11. háttérmagyarázat.

Működésben a rendszer: az Unió legelső alkalommal ró ki kibertámadásokkal szembeni szankciókat[48]

A Tanács 2020 júliusában korlátozó intézkedéseket foganatosított hat olyan személlyel és három olyan szervezettel szemben, akik, illetve amelyek különböző kibertámadásokért felelősek vagy részt vettek azokban. A szóban forgó támadások egyike a Vegyifegyver-tilalmi Szervezet ellen irányult, de köztük voltak például a „WannaCry”, a „NotPetya” és az „Operation Cloud Hopper” néven ismert támadások is.

A szankciók utazási tilalomból és pénzeszközök befagyasztásából álltak. Emellett uniós személyek és szervezetek nem bocsáthatnak pénzeszközöket a jegyzékbe vett személyek és szervezetek rendelkezésére.

---

[47] A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.

[48] A Tanács (KKBP) 2020/1127 határozata (2020. július 30.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról.

Kiberbiztonság és kibervédelem

35 A kibertér az elmúlt években egyre inkább militarizálódott[49], és egyre inkább katonai színtérként szolgál[50]. A szárazföld, a tenger, a levegő és az űr mellett immár az ötödik hadviselési területnek minősül. 2014-ben elfogadták, majd 2018-ban aktualizálták az **uniós kibervédelmi szakpolitikai keretet**[51]. A 2018-as verzió prioritásként jelöli meg többek között a kibervédelmi kapacitás fejlesztését, valamint az Unió közös biztonság- és védelempolitikai (KBVP) kommunikációs és információs hálózatainak védelmét. A kibervédelem az állandó strukturált együttműködés (PESCO) keretének és az EU–NATO együttműködésnek is részét képezi.

36 Általánossá váltak az olyan esetek, amikor politikai célokra használják a kiberteret, és agresszívan tesztelik és megsértik az Unió és a tagállamok kiberbiztonságát. Ezek a kiberkémkedési és feltörési tevékenységek – amelyek nemzeti kormányokat, politikai szervezeteket és uniós intézményeket vesznek célba bizalmas információk kinyerése és gyűjtése céljából – arra utalnak, hogy kifinomult kiberkémkedés és adatmanipulálás zajlik az Unió és tagállamai ellen. **A hibrid fenyegetésekkel szembeni fellépés közös uniós kerete** (2016) mind a kritikus infrastruktúrákat, mind a magánfelhasználókat fenyegető kiberfenyegetésekkel foglalkozik, kiemelve, hogy kibertámadások a közösségi médiában folytatott félretájékoztatási kampányok révén is végrehajthatók[52]. Megállapítja továbbá, hogy

---

[49] Európai Politikai Tanulmányok Központja: *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, 2018. november.

[50] Az Egyesült Államok, az Egyesült Királyság és Ausztrália által Észak-Koreának tulajdonított WannaCry zsarolóvírusos támadás mögötti rosszindulatú szoftvert eredetileg az Egyesült llamok Nemzetbiztonsági gynöksége fejlesztette ki saját célra a Windows sebezhetőségeinek kihasználása érdekében.
Forrás: A. Greenberg, WIRED, 2017. december 19. A támadások után a Microsoft elítélte azt a gyakorlatot, hogy egyes kormányok megtartják maguknak a szoftversebezhetőségekhez kapcsolódó információkat, és megismételte a Digitális Genfi Egyezmény létrehozására irányuló felhívását.

[51] *Az Unió kibervédelmi szakpolitikai kerete (2018. évi frissített változat)*, 14413/18, 2018. november 19.

[52] Európai Bizottság/Európai Külügyi Szolgálat: *A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz*, JOIN(2016) 18 final, 2016. április 6.

javítani kell a tudatosságot és fokozni kell az Unió és a NATO közötti, a 2016. és 2018. évi EU–NATO együttes nyilatkozatban[53] lefektetett együttműködést.

Kiberbiztonsággal kapcsolatos kiadások az Unióban: széttagoltak és elégtelenek

A 27 tagú EU kevesebbet költ kiberbiztonságra, mint az USA

37 A kiberbiztonságra fordított közkiadásokat nehéz megbecsülni, tekintettel annak horizontális jellegére, és mivel a kiberbiztonsággal kapcsolatos és az általános információtechnológiai kiadások gyakran nem választhatók szét egymástól[54]. Ezzel együtt a rendelkezésre álló adatok azt mutatják, hogy az Unión belül **kiberbiztonságra fordított közkiadások** szintje viszonylag alacsony:

- 2020-ban az USA szövetségi kormányzatának kizárólag kiberbiztonságra elkülönített költségvetése **17,4 milliárd USA-dollár** körül alakult[55].
- Ezzel szemben a Bizottság becslése szerint a kiberbiztonságra fordított közkiadások az összes uniós tagállamot tekintve (amelyek együttvéve közel akkora GDP-vel rendelkeznek, mint az USA) évi **egy és kétmillió euró** között mozognak[56].
- A kiberbiztonságra irányuló állami kiadások GDP-arányos szintje számos tagállam esetében **az USA szintjének egytizede** körül alakul vagy még azt sem éri el[57].

---

[53] Az Európai Tanács elnökének, az Európai Bizottság elnökének és az Észak-atlanti Szerződés Szervezete főtitkárának közös nyilatkozata, 2016. július 8. és 2018. július 10.

[54] Európai Bizottság: COM(2018) 630 final, 2018. szeptember 12.

[55] Fehér Ház: *Cybersecurity budget fiscal year 2020*.

[56] Európai Bizottság: *A Bizottsági szolgálatainak munkadokumentuma: Hatásvizsgálat, amely a következő dokumentumot kíséri: „Javaslat európai parlamenti és tanácsi rendeletre a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról”*, SWD(2018) 305 final, 2018. június 6.

[57] Hágai Stratégiai Tanulmányi Központ: *Dutch investments in ICT and cybersecurity: putting it in perspective*, 2016. december.

2014–2020: A kiberbiztonságra fordított uniós finanszírozás több különböző eszköz között oszlik meg

38 A Bizottság szerint[58] az Unió általános költségvetésén belül legalább **tíz különböző eszköz** létezik, amelyekből kiberbiztonsághoz kapcsolódó célokra finanszírozás nyújtható (a főbb programok pénzügyi keretfeltételeit lásd: ***12. háttérmagyarázat***). Összességében a nem katonai vonatkozású kiberbiztonságra fordított teljes uniós finanszírozás a 2014 és 2020 közötti időszakban **nem érte el az évi 200 millió eurót**. Emellett nem létezik az Unió egészére kiterjedő finanszírozási eszköz, amely támogatná a tagállamokat kiberbiztonsági tevékenységeik összehangolásában.

[58] Európai Bizottság: Hatásvizsgálat, amely a következő dokumentumot kíséri*: Javaslat az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendeletre*, SWD(2018) 403 final, 2018. szeptember 12.

12. háttérmagyarázat.

Kiberbiztonsági projekteket támogató uniós programok (2014–2020)

- Az Unió **Horizont 2020 kutatási programjai** a 2014 és 2020 közötti időszakra mintegy 600 millió eurót különítettek el kiberbiztonsággal és kiberbűnözéssel kapcsolatos projektekre. Ezen belül 2017 és 2020 között 450 millió eurót szántak a kiberbiztonsággal kapcsolatos szerződéses köz-magán társulásra (cPPP) azzal a céllal, hogy további 1,8 milliárd eurót vonzzanak be a magánszektorból.

- Az **európai strukturális és beruházási alapok** 400 millió euróig terjedő összegű hozzájárulást irányoztak elő a tagállamok kiberbiztonsági beruházásaihoz 2020 végéig.

- Az **Európai Hálózatfinanszírozási Eszköz (CEF)** évente mintegy 30 millió euró összegben finanszírozott beruházásokat. Ez magában foglalja a NIS-irányelv értelmében a tagállamok által felállítandó, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) társfinanszírozását évi mintegy 13 millió euró összegben, 2016 és 2018 között[59].

- **A Belső Biztonsági Alap rendőrségi együttműködést támogató eszköze (ISF-P)** tanulmányokat, szakértői találkozókat és kommunikációs tevékenységeket támogat; ezek összege 2014 és 2017 között közel 62 millió eurót tett ki. A tagállamok emellett támogatást kaphatnak a megosztott irányítás keretében vásárolt felszerelésekhez, illetve végrehajtott képzéshez, kutatáshoz és adatgyűjtéshez. Ilyen támogatást 19 tagállam vett igénybe összesen 42 millió euró értékben.

- A **Jogérvényesülés program** 9 millió eurós támogatást nyújtott az igazságügyi együttműködésről és a kölcsönös jogsegélyről szóló megállapodásokhoz, különös tekintettel az elektronikus adatok és a pénzügyi információk cseréjére.

[59] A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv (kiberbiztonsági (NIS) irányelv) 9. cikkének (2) bekezdése.

39 Ezenfelül 2019-ben és 2020-ban 500 millió eurót irányoztak elő az uniós költségvetésből az **európai védelmi ipari fejlesztési programra**[60]. A program célja, hogy a közös fejlesztés ösztönzése révén javítsa a tagállamok védelmi kiadásainak koordinációját és hatékonyságát. A program a tervek szerint összesen 13 milliárd euró értékű védelmi kapacitási beruházást generál a 2020 utáni időszakban az Európai Védelmi Alapon keresztül, és ez a beruházás részben a kibervédelemre fog irányulni. Végezetül az **európai biztonsági kezdeményezés** keretében az Európai Beruházási Bank 2018 és 2020 között 6 milliárd eurót biztosít kettős felhasználású finanszírozás formájában (kutatás-fejlesztés/kiberbiztonság és polgári biztonság)[61].

2021–2027: az új Digitális Európa program

40 A 2021–2027-es időszakra vonatkozó új többéves pénzügyi keretről (TPK) szóló 2020. júliusi következtetéseiben a Tanács úgy határozott, hogy a **Digitális Európa program (DEP)**[62] olyan kulcsfontosságú stratégiai digitális képességekbe ruház majd be, mint az uniós nagy teljesítményű számítástechnika, mesterséges intelligencia és kiberbiztonság. A program más eszközöket – nevezetesen az Európai Horizont programot és az Európai Hálózatfinanszírozási Eszközt – kiegészítve támogatja majd Európa digitális transzformációját.

41 A Tanács arról is döntött, hogy a 2021 és 2027 közötti időszakra 6,8 milliárd eurót – azaz körülbelül **évi 970 millió eurót** – különít el a Digitális Európa programra. Ez jelentős növekedés a 2014–2020-as időszakhoz képest, de még mindig alatta marad a Bizottság eredeti javaslatának (8,2 milliárd euró ugyanazon időszakra, amiből 2 milliárd eurót az uniós kiberbiztonsági ágazat erősítésére és általában véve a társadalom védelmére szánnának, például a NIS-irányelv végrehajtásának támogatása révén).

---

[60] Európai Bizottság: Az Európai Parlament és a Tanács (EU) 2018/1092 rendelete (2018. július 18.) az Unió védelmi iparának versenyképességét és innovációs képességét támogató európai védelmi ipari fejlesztési program létrehozásáról (HL L 200., 2018.8.7., 30. o.).

[61] Európai Beruházási Bank: *The EIB Group Operating Framework and Operational Plan 2018*, 2017. december 12.

[62] Európai Bizottság: *Europe investing in digital: the Digital Europe Programme*, 2020. szeptember.

II. RÉSZ. Áttekintés a legfőbb ellenőrző intézmények munkájáról

II. RÉSZ. Áttekintés a legfőbb ellenőrző intézmények munkájáról

Bevezetés

42 A kiberbiztonság és digitális autonómiánk stratégiai jelentőségű kérdéssé vált az Unió és tagállamai számára. Bár eltérő szinten, de továbbra is valamennyi tagállamban hiányosságok tapasztalhatók a kiberbiztonság irányítása terén, a köz- és a magánszférában egyaránt. Emiatt kevésbé vagyunk képesek arra, hogy korlátozzuk a kibertámadásokat, és szükség esetén reagáljunk rájuk.

43 Ennek ellenére 2018-ban az Unión belüli legfőbb ellenőrző intézmények körében végzett felmérés megállapította, hogy az intézmények mintegy fele még soha nem végzett ellenőrzést a kiberbiztonság területére vonatkozóan. Azóta a legfőbb ellenőrző intézmények fokozták ellenőrzési tevékenységüket a kiberbiztonsággal kapcsolatban, különös figyelmet fordítva az adatvédelemre, a rendszerek kibertámadásokkal szembeni felkészültségére, valamint az alapvető közszolgáltatási rendszerek védelmére. Emellett más rendkívül fontos kérdésköröket is vizsgáltak. Érthető módon ezek közül nem minden ellenőrzést lehet nyilvánosságra hozni, mivel némelyek érzékeny (nemzetbiztonsági) információkat érinthetnek.

44 Tekintettel arra, hogy milyen fontos a kiberbiztonság társadalmaink és a politikai intézmények működéséhez, a Kapcsolattartó Bizottság úgy határozott, hogy az idei ellenőrzési kompendiumot ennek a témának szenteli. A második rész 12 közreműködő tagállam legfőbb ellenőrző intézményei és az Európai Számvevőszék által elvégzett, válogatott kiberbiztonsági ellenőrzések eredményeiről ad összefoglalást. Minden részt vevő legfőbb ellenőrző intézmény egy-egy kiválasztott ellenőrzési jelentéssel működött közre, amelyeket a III. rész összegez alaposabban. A témában számos egyéb ellenőrzésre is sor került, amint az a részt vevő legfőbb ellenőrző intézmények által felsorolt további jelentésekből is kitűnik.

Ellenőrzési módszertan és a vizsgált témakörök

45 Ami az e kompendiumban összefoglalt ellenőrzési jelentések kapcsán végrehajtott ellenőrzések típusát illeti, a közreműködő legfőbb ellenőrző intézmények többsége teljesítmény-ellenőrzéseket végzett a kiberbiztonsággal kapcsolatos témákban, míg kettő (a lengyel és a magyar számvevőszék) szabályszerűségi ellenőrzést hajtott végre, egy pedig (az Európai Számvevőszék) szakpolitikai áttekintést készített.

46 Az ellenőrzés módszerének meghatározásakor a legfőbb ellenőrző intézmények többsége úgy alakította ki ellenőrzését, hogy az legalább kétféle módon értékelje az ellenőrzés tárgyát. Ez állhatott magas szintű (például nemzeti) stratégiai dokumentumok vagy meghatározott szakpolitikák áttekintéséből, az eljárások felülvizsgálatából a bevett COBIT módszertannak való megfelelés értékelése érdekében (lásd: ***13. háttérmagyarázat***), illetve a meglévő informatikai irányítási rendszerek eredményességének felülvizsgálatából. Egy legfőbb ellenőrző intézmény (a holland számvevőszék) még etikus hekkereket is igénybe vett a határellenőrzéshez és a kritikus vízi létesítményekhez kapcsolódó kiberbiztonsági rendszerek eredményességének tesztelése céljából. A ***14. háttérmagyarázatban*** vázlatosan összefoglaljuk a különböző legfőbb ellenőrző intézmények által ellenőrzési munkájuk elvégzéséhez alkalmazott módszereket és technikákat.

13. háttérmagyarázat.

A COBIT

Az informatikára és a kapcsolódó technológiára vonatkozó ellenőrzési célkitűzések (COBIT) az informatikai irányítás és kormányzás elismert helyes gyakorlatainak és eljárásainak keretrendszere, amelyet az Információrendszer-ellenőrök Egyesülete (ISACA) határozott meg. Segíti a szervezeteket abban, hogy a rendelkezésre álló erőforrások eredményes felhasználása és az információtechnológiai kockázatok minimalizálása révén elérjék stratégiai céljaikat. A COBIT összeköti egymással a vállalatirányítást és az informatikai kormányzást. Ez a kapcsolat azáltal jön létre, hogy összekapcsolják egymással az üzleti és az információtechnológiai célokat, mérőszámokat és érettségi modelleket határozva meg a célok elérésének méréséhez, valamint meghatározva az üzleti és az információtechnológiai folyamatokért felelős személyek felelősségi köreit.

47 A kiberbiztonság ellenőrzése során vizsgált témakörök változatosak voltak. Egyes legfőbb ellenőrző intézmények nagyon specifikus közérdekű területeket ellenőriztek; a holland legfőbb ellenőrző intézmény például a létfontosságú tengeri védelmének és vízgazdálkodási rendszereinek kiberbiztonságát ellenőrizte. Mások, köztük az ír és a magyar legfőbb ellenőrző intézmény horizontálisabb jellegű kérdéseket tárgyaltak, ideértve a nemzeti kiberbiztonsági stratégia végrehajtását, valamint a személyes adatok és a nemzeti adatvagyon védelmét. Ugyanakkor valamennyi legfőbb ellenőrző intézmény foglalkozott olyan kérdésekkel, amelyek negatívan hathatnak a közszolgáltatásokra vagy az infrastruktúrára.

48 Az észt és a litván legfőbb ellenőrző intézmény felismerte a nemzetbiztonság szempontjából létfontosságú nemzeti adatvagyon stratégiai jelentőségét és integritásuk külső kibertámadásokkal szembeni védelmének fontosságát. A dán legfőbb ellenőrző intézmény kifejezetten annak értékelésére szánt egy ellenőrzést, hogy mennyire van biztonságban négy közjogi szerv a zsarolóvírusos támadásokkal szemben. A holland, a lengyel és a portugál legfőbb ellenőrző intézmény a határellenőrzéseket támogató különféle informatikai rendszerek eredményességét ellenőrizte (a Schiphol repülőtéren, a lengyel határőrség főparancsnokságán és a lengyel belügyi és közigazgatási minisztériumban, illetve Portugáliai határain), aminek keretében így az Unión belüli biztonság kérdését is érintették.

Ellenőrzött időszak

49 Az e kompendiumban megtalálható kiválasztott ellenőrzési jelentéseket 2014 és 2020 között tették közzé. A legtöbb esetben az ellenőrzött időszak két vagy több évre terjedt ki, bár négy esetben (Dánia, Észtország, Franciaország és Portugália) egyéves időszakokat ellenőriztek.

Az ellenőrzések céljai

50 Az e kompendiumban közreműködő különböző legfőbb ellenőrző intézmények különféle kockázatokkal foglalkoztak ellenőrzési munkájuk során. A kompendiumba bevont jelentéseikben tárgyalt kockázatok közé tartoztak a következők: a személyes adatokkal való visszaélés révén az egyes uniós polgárok jogait érintő fenyegetések, annak kockázata, hogy az adott intézmények nem képesek fontos közszolgáltatás nyújtására vagy korlátozott teljesítményt nyújtanak, továbbá a tagállam közbiztonságára, jólétére és gazdaságára, valamint az Unión belüli kiberbiztonságra gyakorolt súlyos következmények. Legalább négy legfőbb ellenőrző intézmény (az észt, a magyar, a holland és a portugál) az említettek közül három vagy több témakört tárgyalt az e kompendiumban szereplő ellenőrzési jelentésében.

51 A kiberbiztonság továbbra is tagállami hatáskör. Ugyanakkor az uniós jogszabályok idővel egyre szélesebb körűvé és egyre konkrétabbá váltak, és a legfőbb ellenőrző intézmények által ellenőrzött intézmények és szervek nagy része már hozzájárul az EU kiberbiztonsági stratégiai céljainak eléréséhez, még ha eltérő

mértékben is. Így például az írországi *Office of the Comptroller and Auditor General* (A Számvevőszék Elnökének Hivatala) ellenőrizte a hálózati és információs rendszerekről szóló uniós irányelv végrehajtását, amelynek célja a kulcsfontosságú hálózati és információs rendszerek ellenálló képességének javítása, és tanácsokkal szolgált ennek tökéletesítésére irányulóan. Hasonlóképpen a magyar Állami Számvevőszék ellenőrzése a meglévő uniós irányelveknek való megfelelés szempontjával foglalkozott.

52 A ***14. háttérmagyarázat*** azt is bemutatja, hogy mely esetekben járult hozzá az ellenőrzés kimenetele az auditálás alatti szervezet kibertámadásokkal szembeni rezilienciájának erősödéséhez vagy a kiberbűnözés csökkenéséhez, vagy segítette a kibervédelmi politikák kidolgozását és a hatáskörök erősítését, a technológiák fejlesztésének javítását, valamint a nemzetközi szintű együttműködés terén történő előrelépést; ezek ugyanis az uniós kiberbiztonsági stratégia fő célkitűzései. A legfőbb ellenőrző intézmények által tett ajánlások a legtöbb esetben több mint két olyan stratégiai célt érintettek, amelyet az Unió el kíván érni.

53 Ezenkívül a legfőbb ellenőrző intézmények az ellenőrzési tevékenységük során azonosították a biztonsági vagy végrehajtási hiányosságokat, ami további erőfeszítések megtételére indította az ellenőrzött intézményeket. Így például Dániában négy ellenőrzött intézmény már az ellenőrzési munka során megkezdte több előretekintő biztonsági ellenőrzés bevezetését annak érdekében, hogy jelentősen növeljék a zsarolóvírusos támadások elleni védelem szintjét, fejlesztve a védelmi képességeket és növelve a kibertámadásokkal szembeni rezilienciát, ezáltal pedig csökkentve a jövőbeni kibertámadásoknak való kitettségüket.

54 Emellett az is látszik, hogy ellenőrzési ajánlások különböző irányítási és felelősségi szinteket céloztak meg, köztük a központi kormányzatot, az operatív szintet – minisztériumokat és hivatalokat –, illetve az információtechnológiai rendszerek felelőseit.

14. háttérmagyarázat.

Áttekintés a legfőbb ellenőrző intézmények ellenőrzési tevékenységéről a kompendiumhoz nyújtott hozzájárulásaik tekintetében (1. rész)

A legfontosabb kiemelt terület		Dánia	Észtország	Írország	Franciaország	Lettország	Litvánia	Magyarország	Hollandia	Lengyelország	Portugália	Finnország	Svédország	EU (Európai Számvevőszék)
Ellenőrzés típusa	Teljesítmény-ellenőrzés	✓	✓	✓	✓		✓	✓		✓		✓	✓	✓	
	Szabályszerűségi ellenőrzés								✓		✓				
	Áttekintés														✓
Ellenőrzési koncepció	Szakpolitikák áttekintése	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
	Eljárások felülvizsgálata	✓	✓		✓		✓	✓		✓	✓	✓			
	Rendszerek felülvizsgálata	✓			✓		✓	✓	✓	✓	✓		✓		
	A robusztusság értékelése közvetlen teszteléssel								✓		✓				
Kezelt fenyegetések	A személyhez fűződő jogokra gyakorolt hatás		✓		✓			✓			✓			✓	
	Az állami infrastruktúrára vagy szolgáltatásokra gyakorolt hatás	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
	A nemzetbiztonságra gyakorolt hatás		✓	✓			✓	✓	✓		✓				
	Az Unión belüli biztonságra gyakorolt hatás	✓							✓		✓			✓	

Áttekintés a legfőbb ellenőrző intézmények ellenőrzési tevékenységéről a kompendiumhoz nyújtott hozzájárulásaik tekintetében (2. rész)

A legfontosabb kiemelt terület		Dánia	Észtország	Írország	Franciaország	Lettország	Litvánia	Magyarország	Hollandia	Lengyelország	Portugália	Finnország	Svédország	EU (Európai Számvevőszék)
A tárgyalt uniós kiberbiztonsági stratégiai célok	A kibertámadásokkal szembeni reziliencia fokozása	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	A kiberbűnözés csökkentése	✓					✓							✓
	Kibervédelmi politikák és képességek kifejlesztése	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Technológiai erőforrások kifejlesztése				✓	✓			✓				✓	
	A nemzetközi együttműködés fejlesztése (szakpolitikák)			✓				✓						✓
Az ajánlások címzettjének szintje	Központi kormányzat	✓	✓				✓					✓	✓	✓
	Operatív szint (minisztériumok és hivatalok)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Információtechnológiai rendszerfelelősök	✓			✓			✓	✓	✓				

Főbb ellenőrzési észrevételek

55 A legfőbb ellenőrző intézmények legfontosabb ellenőrzési megfigyeléseit az alábbi szakaszok foglalják össze.

Teljesítmény-ellenőrzések

56 A **dán *Rigsrevisionen*** azt értékelte, hogy kielégítően védve vannak-e a kiválasztott alapvető kormányzati intézmények a zsarolóvírusokkal szemben. A kormányzati szervezetek a kibertámadások gyakori célpontjai, és a zsarolóvírus jelenleg egyike a legnagyobb kiberbiztonsági fenyegetéseknek. Az ellenőrzés az egészségügyi adatokkal foglalkozó dán hatóságot, a Külügyminisztériumot, a dán vasúti hálózatot (Banedanmark) és a dán vészhelyzet-kezelési hivatalt érintette. Ezt a négy intézményt azért választották ki, mert alapvető szolgáltatások nyújtásáért felelősek az egészségügy, a külügyek, a közlekedés és a veszélyhelyzetekre való felkészültség területén, ahol az adatokhoz való hozzáférés biztosítása kritikus jelentőséggel bírhat. Az ellenőrzés során megállapítást nyert, hogy a négy intézmény nem rendelkezik kielégítő védelemmel a zsarolóvírusokkal szemben. Az ellenőrzési munka során kiderült, hogy a négy intézmény nem hajtott végre számos általános biztonsági ellenőrzést, amelyek a támadások mérséklését szolgálják. Az ellenőrzés ahhoz a következtetéshez vezetett, hogy az intézményeknek fontos mérlegelniük előretekintő biztonsági ellenőrzések bevezetését a zsarolóvírusos támadásokkal szembeni ellenálló képességük fokozása érdekében.

57 Az **észt *Riigikontroll*** felismerte, hogy Észtország függetlenségének megőrzéséhez nemcsak az ország területének fizikai védelmére van szükség, hanem az állam számára elsőrendű fontosságú digitális vagyon védelmére is. A leginkább védelemre szoruló digitális vagyontárgyak az állampolgárokat, az ország területét és a jogalkotást érintő adatok. Emellett gondoskodni kell a tulajdonnal, az ingatlan javakkal és az Észtország lakosainak jogaival kapcsolatos adatok biztonságáról is. Az észt számvevőszék mérlegelte azt a lehetőséget, hogy bizonyos biztonsági problémák eszkalálódása esetén kiberfenyegetésekre kerülhet sor. Az ilyen kockázati forgatókönyvek, valamint az információbiztonsági incidensek – például a kibertámadások és az adatszivárgások – számának növekedése veszélyeztethetik az állam számára legnagyobb jelentőséggel bíró adatokat és adatbázisokat. Az ellenőrzés ezért azt vizsgálta, hogyan határozta meg az állam, hogy mely adatok és adatbázisok kritikus fontosságúak a nemzetbiztonság szavatolásához. Az ellenőrzés során megállapítást nyert, hogy az állami hivatalok

számára kötelező ISKE háromszintű biztonsági alaprendszer[63] alkalmazása ellenére jelentős hiányosságok vannak számos kritikus adatbázis információbiztonságának szavatolása terén.

58 Az **ír *Office of the Comptroller and Auditor General*** áttekintette az ír Nemzeti Kiberbiztonsági Központ létrejötte óta a kiberbiztonsági intézkedések tekintetében elért előrehaladást. A központot 2011-ben hozták létre, és a Kommunikációs, Éghajlat-politikai és Környezetvédelmi Minisztérium működteti. Elsődleges feladata a kormányzati hálózatok biztonságának szavatolása, az ipar és a magánszemélyek segítése saját rendszereik védelmében, valamint a kritikus nemzeti infrastruktúra megóvása. Az ellenőrzés során megállapítást nyert, hogy bár a Nemzeti Kiberbiztonsági Központ kritikus funkciót töltött be, működésének első négy évében erőforrásainak szintje lényegesen alatta maradt az eredetileg tervezettnek, és a központ átfogó stratégiai irányításához hiányzott a stratégiai terv. Tisztázni kellett a kiberbűnözés és a nemzetbiztonsági incidensek kivizsgálásában részt vevő szervek szerepköreit is. Emellett a hálózati és információs rendszerek biztonságáról szóló uniós irányelv nemzeti stratégia kidolgozásával kapcsolatos követelményei még végrehajtásra vártak.

59 A **francia *Cour des comptes*** megvizsgálta a „*Parcoursup*” elnevezésű új digitális platformot, amely információforrásként szolgál az elérhető egyetemi kurzusokra és bemeneti követelményekre vonatkozóan, hogy a középiskolás diákok könnyebben megtalálják a képességeikhez és tanulmányi eredményeikhez illeszkedő felsőoktatási kurzusokat. Az ellenőrzés során megállapítást nyert, hogy a kormányzat az egyre bővülő felsőoktatási kínálat összefogása érdekében a digitális platformon keresztül sikeresen központosította az összes posztszekunder képzéshez való hozzáférést. A korábbi rendszert azonban sietősen, lényegi strukturális változtatások nélkül dolgozták át az új „*Parcoursup*” platformmá. Így az információs rendszer biztonsággal, teljesítménnyel és robusztussággal kapcsolatos sebezhetőségeit nem orvosolták. A platform továbbra is jelentős kockázatoknak van kitéve a közszolgáltatás minősége és folyamatossága, valamint a személyes adatok biztonsága tekintetében.

[63] Az ISKE egy információbiztonsági szabvány, amelyet az észt közszféra számára fejlesztettek ki; kötelező azon állami és helyi önkormányzati szervezetek számára, amelyek adatbázisokat/nyilvántartásokat kezelnek.

60 A **lett *Valsts Kontrole*** teljesítmény-ellenőrzést végzett az állami információs és kommunikációs technológiai (IKT) infrastruktúra hatékonyságára vonatkozóan. Az ellenőrzés azt vizsgálta, hogy egységes megközelítést alkalmaz-e a közigazgatás az IKT-infrastruktúra hatékony irányítása tekintetében, és értékelték-e az intézmények a központosítás előnyeit. Az ellenőrzés során megállapítást nyert, hogy mivel a hatóságok vonakodtak az IKT-infrastruktúra központi irányításától, számos szervertermet hoztak létre, ami jelentősen növeli a karbantartási költségeket. A legtöbb szerverteremben voltak biztonsági fenyegetések, miközben az adatközpontok nem voltak kellően védve a fizikai hozzáféréstől és a környezeti kockázatoktól. Emellett az intézményekben nem tették gyakorlattá annak rendszeres értékelését, hogy mi lenne olcsóbb: házon belül végezni az IKT-infrastruktúra karbantartását, együttműködni más intézménnyel, vagy kiszervezni azt. Az ellenőrzés rendszeres monitoringon alapuló rendszert javasolt, amely lehetővé tenné a teljes közigazgatás egyetlen rendszerként történő értékelését.

61 A **litván *Valstybės kontrolė*** felismerte a kritikus elektronikus állami információs erőforrások alkalmazásának jelentőségét, ideértve a kormányzati pénzügyek, az adóhatóság és az egészségügyi ellátás igazgatását. A kritikus információk elvesztése és a vonatkozó információs rendszerek elérhetetlensége súlyos következményekkel járhat a közbiztonság, a jólét és a gazdaság tekintetében. Az ellenőrzés annak értékelését célozta, hogy milyen az irányítás (általános irányítás), és mennyire érettek a kritikus állami információs erőforrások. Rendszerszintű problémákra derített fényt mind az állami információs erőforrásokra irányuló politika kialakítása és végrehajtása, mind pedig azok irányítási mechanizmusa tekintetében. Az ellenőrzés során megállapítást nyert, hogy a kritikus állami információs erőforrások alacsony szintű érettsége az állami információs erőforrásokra irányuló politika kialakításának és végrehajtásának hiányosságait jelzi, ami sebezhetőbbé teszi ezeket az erőforrásokat. Az állami információs erőforrások biztonságának fokozása érdekében fejleszteni kellene az irányítási mechanizmust.

62 2018-ban a **holland *Algemene Rekenkamer*** úgy döntött, ellenőrzéseket végez a társadalom számára kritikus fontosságú ágazatokon belüli kiberbiztonságra vonatkozóan. Az első két ellenőrzött ágazat a vízgazdálkodás és az automatizált határellenőrzés volt, amelyek közül az első azért létfontosságú, mert az ország jelentős részben a tengerszint alatt fekszik, a második pedig azért, mert az amszterdami Schiphol repülőtér nemzetközi csomópont és bejárat az országba. Az infrastruktúráért és vízgazdálkodásért felelős miniszter több, az építési beruházásokért és a

vízgazdálkodásért felelős főigazgatóság (az ellenőrzött szerv) által kezelt vízi létesítményt jelölt meg a vízgazdálkodási ágazat „kritikus” részeiként. A kritikus vízi létesítmények működtetéséhez használt számítógépes rendszerek közül sok az 1980-as és az 1990-es évekből származik, amikor a kiberbiztonságot rendszerint még nem tartották szem előtt. A védelmi miniszter, valamint az igazságügyi és biztonsági miniszter közösen felel a holland határőrök által a Schiphol repülőtéren végzett határellenőrzésekért. Mindkét minisztérium rendelkezik információtechnológiai rendszerekkel, amelyekre a határőrök támaszkodnak. Ezek a rendszerek kritikus jelentőségűek a repülőtéri műveletek szempontjából, és igen érzékeny adatok feldolgozására használják őket. Ezáltal vonzó célpontjai lehetnek az olyan kibertámadásoknak, amelyek célja a szabotázs, a kémkedés vagy a határellenőrzések manipulálása. Az ellenőrzés azt vizsgálta, hogy az ellenőrzött szervek fel voltak-e készülve a kiberfenyegetések kezelésére, és eredményesen végezték-e ezt a munkát. A vízi létesítmények esetében az ellenőrzött szervnek többet kell még tennie a felderítés és a reagálás tekintetében ahhoz, hogy eleget tegyen saját kiberbiztonsági célkitűzéseinek. Ami a határellenőrzést illeti, a kiberbiztonsági intézkedések nem bizonyultak megfelelőnek, sem pedig időtállónak.

63 A **portugál *Tribunal de Contas*** azokat az információs rendszereket ellenőrizte, amelyek támogatják a portugál elektronikus útlevél (PEP) odaítélését, kibocsátását és használatát, különösen az utasok automatizált szűrése során, a biometrikus adatok portugál határokon történő leolvasásánál. Az ellenőrzés vizsgálta az uniós és a nemzeti jognak, a nemzetközi szabványoknak, valamint a PEP megadására, kibocsátására és használatára vonatkozó iránymutatásoknak való megfelelést, beleértve a nemzeti jogi keret megfelelőségét. Elemezte továbbá a PEP életciklusához kapcsolódó alapvető folyamatok eredményességét, különös tekintettel azokra, amelyek a PEP odaítéléséhez, kibocsátásához és használatához kapcsolódnak. Az ellenőrzés során emellett felülvizsgálták az információs rendszerek teljesítőképességének kritikus elemeit, különösen a PEP információs rendszereivel (SIPEP) kapcsolatos biztonsági követelmények teljesítését.

64 A **finn *Valtiontalouden tarkastusvirasto*** azt vizsgálta, hogy a lehető legeredményesebb és legköltséghatékonyabb-e a központi kormányzat kibervédelme. Az ellenőrzés középpontjában a központi kormányzat kiberbiztonságának irányítási módja állt. Az ellenőrzött szervezetek közé tartoztak a központi kormányzat kibervédelmét irányító hatóságok (a Miniszterelnöki Hivatal, a Pénzügyminisztérium, valamint a Közlekedési és Kommunikációs Minisztérium), továbbá a központi kormányzaton belüli központosított kibervédelmi feladatokért és központosított információtechnológiai szolgáltatásokért felelős hatóságok. A finn kormányon belül a kibervédelemért viselt felelősség decentralizált, minden egyes szerv a saját kiberbiztonságáért felel. Az ellenőrzés javasolta, hogy a Pénzügyminisztérium határozzon meg és hajtson végre egy kiterjedt operatív irányítási modellt arra az esetre, ha kiberbiztonsági események következnének be a központi kormányzat információtechnológiai szolgálatainál. A Pénzügyminisztériumnak emellett választ kell találnia arra a kérdésre, hogy a szolgáltatások egész életciklusuk alatti finanszírozása tekintetében hogyan kell figyelembe venni a kiberbiztonsági szempontokat, valamint javítania kell operatív helyzetismeretét azáltal, hogy utasítja a hatóságokat a számítógépes visszaélések Kiberbiztonsági Központ felé történő jelentésére.

65 A **svéd *Riksrevisionen*** az elavult információtechnológiai rendszerek központi kormányzati igazgatáson belüli előfordulását vizsgálta, értékelve, hogy megfelelő intézkedéseket hoztak-e a kormány és a hatóságok annak megelőzése érdekében, hogy az informatikai rendszerek akadályozzák az eredményes digitalizációt. Az ellenőrzés sok kormányzati hivatalnál tárt fel elavult információtechnológiai rendszereket. Számos ellenőrzött hivatalnál egy vagy több, az ügymenet szempontjából kritikus jelentőségű informatikai rendszer elavult volt, és a vizsgált hivatalok jelentős része nem alkalmazott megfelelő megközelítést az információtechnológiai támogatás fejlesztése és igazgatása tekintetében. A hivatalok nagy része nem rendelkezett arra vonatkozó általános leírással, hogy miként kapcsolódnak egymáshoz a stratégiák, az operatív folyamatok és a rendszerek. Az általános következtetés az volt, hogy a legtöbb hivatalnak még nem sikerült eredményesen kezelnie az elavult informatikai rendszerekkel összefüggő problémákat. A svéd számvevőszék véleménye szerint a probléma olyan súlyos és olyan kiterjedt, hogy akadályozza az államigazgatás további eredményes digitalizálását.

A kiberbiztonság kapcsán végzett szabályszerűségi ellenőrzések

66 A **magyar *Állami Számvevőszék*** felismerte, hogy a nemzeti adatvagyon biztonsága alapvető társadalmi érdek a nemzeti értékek megőrzése és védelme szempontjából. A nemzeti adatvagyon körébe tartozó személyes és közérdekű adatok fokozott biztonságáról való gondoskodás elengedhetetlen az állampolgárok államba vetett bizalmának erősítése, valamint a közigazgatás folyamatos és zavartalan működése érdekében. Az adatvédelemre vonatkozó szabályszerűségi ellenőrzés annak értékelését célozta, hogy megvalósult-e Magyarországon az adatvédelem szabályozási és operatív keretrendszere, és a jelentős adatkezelő szervezetek megfelelően alkalmazták-e a biztonságos adatkezelésre, valamint az adatfeldolgozás kiszervezésére vonatkozó előírásokat. Az ellenőrzés megállapította, hogy az adatkezelő szervezetek adatkezelési tevékenységre vonatkozó belső szabályai a 2011 és 2015 között hatályos jogszabályi előírásoknak megfelelően biztosították a nemzeti vagyon részét képező nemzeti adatvagyon védelmét. Az adatkezelők megfelelően alkalmazták a követelményeket, és az adatok harmadik feleknek történő továbbítását megfelelően hajtották végre.

67 A **lengyel *Najwyższa Izba Kontroli*** azt értékelte, hogy a fontos közfeladatok végrehajtására szolgáló rendszerekben gyűjtött adatok biztonságban vannak-e.
Az ellenőrzés hat kiválasztott intézményre terjedt ki, amelyek jelentős közfeladatokat látnak el. Az információbiztonsági rendszer készültségi foka és végrehajtása nem szavatolta megfelelő szinten a fontos közfeladatok végrehajtására használt informatikai rendszerekben gyűjtött adatok biztonságát. Az információbiztonsági folyamatokat rendezetlenül, eljárások hiányában intuitív módon hajtották végre. A hat ellenőrzött egység közül mindössze egy vezetett be információbiztonsági rendszert, noha meg kell jegyezni, hogy annak működésénél is jelentős hibák fordultak elő.
Az ellenőrzés során megállapítást nyert, hogy központi szinten általános ajánlásokat és követelményeket kell kidolgozni és végrehajtani az információtechnológiai biztonsággal kapcsolatban, amelyek valamennyi közigazgatási intézményre alkalmazandók.

A kiberbiztonsággal kapcsolatos áttekintések

68 Az ***Európai Számvevőszék*** áttekintette az Unió kiberbiztonsággal kapcsolatos szakpolitikai környezetét, és meghatározta a szakpolitika eredményes megvalósítása tekintetében fennálló fő kihívásokat. Tárgyalta többek között a hálózat- és információbiztonság, a kiberbűnözés, a kibervédelem és a félretájékoztatás témáját. Az áttekintés több hiányosságot is feltárt az uniós kiberbiztonsági jogszabályok tekintetében, és megjegyezte, hogy a meglévő jogszabályokat a tagállamok nem ültették át következetesen. Végezetül az áttekintés ráirányította a figyelmet arra, hogy uniós szinten nem állnak rendelkezésre megbízható adatok a kiberbiztonsági eseményekre vonatkozóan, és nincs átfogó kép az Unió és a tagállamok kiberbiztonsági kiadásairól. Az áttekintés emellett megállapította, hogy a kibervédelemhez kapcsolódó tevékenységet folytató uniós ügynökségek erőforrásai szűkösek, többek között nehézségekkel küzdenek a tehetséges munkaerő megnyerése és megtartása terén. További kihívást jelent, hogy a kiberbiztonság finanszírozása nincs megfelelően összehangolva az Unió stratégiai céljaival.

III. RÉSZ. Összefoglaló a legfőbb ellenőrző intézmények jelentéseiről

Dánia
Rigsrevisionen

A zsarolóvírusos támadások elleni védelem

Közzététel időpontja: 2017

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2017. április–szeptember

A jelentés összefoglalása

Az ellenőrzés tárgya

A jelentés azt vizsgálta, hogy kielégítően védve vannak-e kiválasztott alapvető kormányzati intézmények a zsarolóvírusokkal szemben.

A kormányzati szervezetek a kibertámadások gyakori célpontjai, és a zsarolóvírus jelenleg egyike a legnagyobb kiberbiztonsági fenyegetéseknek. A zsarolóvírus olyan kártékony szoftver, amely blokkolja az adatokhoz való hozzáférést. A zsarolóvírus általában titkosítja az adatokat, és megakadályozza, hogy a támadás alatt álló intézmények használják azokat. A hekkerek váltságdíjat kérnek az adatok visszafejtéséért és az intézmények újbóli hozzáférésének lehetővé tételéért. Ebből következően a zsarolóvírus különös veszélyt jelent az adatok hozzáférhetősége tekintetében.

Ha az adatokhoz hirtelen megszűnik a hozzáférés, az megnehezítheti az intézmények számára fontos szolgáltatások nyújtását, vagy teljesen meggátolhatja őket a szolgáltatás nyújtásában. A zsarolóvírusos támadás által érintett intézmények rendszerint kénytelenek leállítani informatikai hálózatuk egyes részeit vagy annak egészét, hogy megvizsgálják, mennyire kiterjedt a támadás. A zsarolóvírusos

támadások jelentős gazdasági hatással járhatnak, mivel fennáll a veszély, hogy az intézmények termeléskiesést szenvednek el, például ha nem tudnak hozzáférni informatikai hálózatukhoz, vagy ha hosszabb időszakon át gyűjtött és feldolgozott adatok vesznek el. 2017-ben a brit nemzeti egészségügyi szolgálatot ért zsarolóvírusos támadás miatt 19 000 műtétet és konzultációt kellett törölni. Az intézmények vezetésének ezért kiemelt figyelmet kell fordítaniuk a zsarolóvírusos támadások kockázatára, és végre kell hajtaniuk a szükséges biztonsági ellenőrzéseket a zsarolóvírussal szembeni védelem és az esetleges támadások hatásának csökkentése érdekében.

A vizsgálat az egészségügyi adatokkal foglalkozó dán hatóságra, a Külügyminisztériumra, a dán vasúti hálózatra (Banedanmark) és a dán vészhelyzet-kezelési hivatalra terjedt ki. Ezt a négy intézményt azért választották ki, mert alapvető szolgáltatások nyújtásáért felelősek az egészségügy, a külügyek, a közlekedés és a veszélyhelyzetekre való felkészültség területén, ahol az adatokhoz való hozzáférés kritikus jelentőséggel bírhat. Az egészségügyi adatokkal foglalkozó hatóság emellett központosított információtechnológiai szolgáltatásokat nyújt az Egészségügyi Minisztérium alá tartozó kormányzati szervek többsége számára.

A vizsgálat azt volt hivatott értékelni, hogy kielégítő védelemmel rendelkezik-e a négy intézmény az e-mail-alapú zsarolóvírusos támadásokkal szemben. A *Rigsrevisionen* ezért 20 általános biztonsági ellenőrzést vizsgált meg, amelyek alapvető védelmet nyújtanak a zsarolóvírussal szemben. Ezenkívül a legfőbb ellenőrző intézmény felülvizsgált öt biztonsági ellenőrzést, amelyeket az intézményeknek mérlegelniük kellene a jövőbeni kockázatértékeléseikkel összefüggésben. Az előremutató ellenőrzések magukban foglalják például az olyan új technológiát, amely csökkentheti az intézményhez beérkező hamis e-mailek számát, vagy felderítheti a számítógépeken zajló szokatlan tevékenységet és figyelmeztetéseket küldhet róluk. A vizsgálatot a *Rigsrevisionen* kezdeményezte négy, 2017 áprilisa és szeptembere között elvégzett információtechnológiai audit megállapításai alapján. A vizsgálat pillanatképet nyújt arról, hogy mennyire vannak megfelelően védve az intézmények a zsarolóvírusokkal szemben. Az intézményeknek lehetőségük nyílt arra, hogy az információtechnológiai auditok elvégzését követően végrehajtsák a 20 általános biztonsági ellenőrzést.
A vizsgálat eredményei ezért csak arra vonatkoznak, hogy a négy információtechnológiai audit idején mennyire voltak védve az intézmények a zsarolóvírusokkal szemben. A vizsgálat áttekintést ad a négy intézmény teljesítményéről, de nem tartalmaz összehasonlító elemzést és nem rangsorolja teljesítményüket.

Megállapítások és következtetések

A *Rigsrevisionen* megállapította, hogy a négy intézmény nem rendelkezik kielégítő védelemmel a zsarolóvírusokkal szemben. A vizsgálat alapján a négy intézmény nem hajtott végre számos általános biztonsági ellenőrzést, amelyek a támadások mérséklését szolgálják. Különösen az egészségügyi adatokkal foglalkozó hatóság és a Banedanmark esetében mutatkoztak jelentős biztonsági hiányosságok. Ez azt jelentette, hogy mind a négy intézmény fokozottan ki van kitéve az e-mail-alapú zsarolóvírusos támadások kockázatának, amelyek nyomán különböző ideig képtelenek lennének szolgáltatásaik nyújtására. Mind a négy intézmény arról tájékoztatta a *Rigsrevisionen*-t, hogy a vizsgálat lezárása óta dolgoznak több biztonsági ellenőrzés bevezetésén, erősítve ezáltal a zsarolóvírussal szembeni védelem szintjét.

Az intézményeknél nem volt megfelelő a zsarolóvírusos támadások megelőzése, legyen szó belső vagy külső fenyegetésekről. Különösen aggályos, hogy egyik intézmény sem gondoskodott arról, hogy a szoftverek biztonsági javítócsomagjai naprakészek legyenek, valamint hogy három intézmény nem alkalmazott fehérlistát, megelőzendő, hogy a személyzet kártékony szoftvert futtasson. Ez növeli annak kockázatát, hogy zsarolóvírus fertőzze meg az informatikai hálózat egy részét vagy egészét, és szétterjedjen.

Az intézmények közül háromnak a vezetése nem figyelt oda kellőképpen a zsarolóvírus jelentette fenyegetésre, emellett az egészségügyi adatokért felelős hatóság és a Banedanmark esetében a vezetés által elvégzett kockázatértékelések nem terjedtek ki minden releváns szempontra. Emiatt az intézmények nem rendelkeztek naprakész értékeléssel a zsarolóvírus jelentette fenyegetésre vonatkozóan, és ezért gyenge pozícióban voltak az új támadások megelőzését és a jövőbeni támadások hatásának csökkentését illetően. Az egészségügyi adatokért felelős hatóság és a Banedanmark vezetése nem összpontosított kellően a kockázatértékelésre, és ezért e két intézmény informatikai biztonsága nem a vezetőség által meghatározott prioritásokon alapult.

Három intézmény nem rendelkezett megfelelő tervvel a biztonsági eseményekre történő reagáláshoz, amely egy zsarolóvírusos támadás után segítené őket műveleteik helyreállításában. Különösen jelentős probléma, hogy három intézmény nem tesztelte rendszeresen, képesek lennének-e helyreállítani az esetleges zsarolóvírusos támadással érintett adatokat és rendszereket. Ez növeli annak kockázatát, hogy egy zsarolóvírusos támadással összefüggésben elveszhetnek az ezen intézmények birtokában lévő adatok, és az intézmények hosszabb ideig nem lennének képesek szolgáltatásaik nyújtására.

Mivel a kockázati forgatókönyvek folyamatosan változnak, fontos, hogy az intézmények mérlegeljék olyan előremutató biztonsági ellenőrzések elvégzését, amelyek fokozzák a zsarolóvírusos támadásokkal szembeni ellenálló képességüket, ideértve az olyan ellenőrzéseket, amelyek segítségével könnyebben ellenőrizhető az e-mailek feladóinak kiléte, és amelyek képesek a potenciálisan kártékony e-mailek felderítésére és kiszűrésére. Mind a négy intézmény dolgozik jelenleg olyan előremutató biztonsági ellenőrzéseken, amelyek segíthetik a zsarolóvírusos támadások elleni védelmük javítását.

A területet érintő további jelentések

A jelentés címe:	Jelentés a kutatási adatok dán egyetemeken alkalmazott védelméről
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat)
A közzététel időpontja:	2019
A jelentés címe:	Jelentés az informatikai rendszerek és az egészségügyi adatok védelméről három dán régióban
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat)
A közzététel időpontja:	2017
A jelentés címe:	Jelentés a külső szolgáltatókhoz kiszervezett rendszerek informatikai biztonságának irányításáról
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat)
A közzététel időpontja:	2016
A jelentés címe:	Jelentés a dán társadalom részére alapvető szolgáltatások nyújtását támogató informatikai rendszerekhez való hozzáférésről
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat)
A közzététel időpontja:	2015

Észtország
Riigikontroll

Kritikus állami adatbázisok biztonságának és megőrzésének szavatolása Észtországban

Közzététel időpontja: 2018. május

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)
Jelentés (észt nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2017

A jelentés összefoglalása

Az ellenőrzés tárgya

Észtország függetlenségének megőrzéséhez nemcsak az ország területének fizikai védelmére van szükség, hanem az állam számára elsőrendű fontosságú digitális vagyon védelmére is, tekintettel a legnagyobb fenyegetést jelentő eseményekre. A leginkább védelemre szoruló digitális vagyontárgyak az állampolgárokat, az ország területét és a jogalkotást érintő adatok. Emellett be kell biztosítani a tulajdonnal, az ingatlan javakkal és az Észtország lakosainak jogaival kapcsolatos adatokat is.

A nemzeti számvevőszék azt vizsgálta, hogyan határozta meg az állam, hogy mely adatok és adatbázisok kritikus fontosságúak a nemzetbiztonság szavatolásához. Ellenőrizték ezen adatok és adatbázisok biztonságának és folytonosságának védelmét, beleértve a védelemhez használt eszközök áttekintését.

Mivel Észtország immár a NATO és az Európai Unió tagja, fizikai biztonsága jobban garantált, mint az e hálózatokhoz való csatlakozása előtt. Ugyanakkor Észtországnak mérlegelnie kell azt a lehetőséget, hogy biztonsági problémák eszkalálódása esetén

kiberfenyegetésekre kerül sor. Az ilyen kockázati forgatókönyvek, valamint az információbiztonsági incidensek – például a kibertámadások és az adatszivárgások – számának növekedése veszélyeztethetik az állam számára legnagyobb jelentőséggel bíró adatokat és adatbázisokat. Amennyiben az állam számára elsőrendű fontosságú adatokat engedély nélkül megváltoztatják, kiszivárogtatják, vagy ha azok elvesznek, az állam többé nem lenne képes ellátni a szükséges funkciókat, beleértve az emberek biztonságának szavatolását, a szükségletek biztosítását, a vállalkozások számára szükséges környezet megteremtését és számos egyebet. Észtország kezdetben azt tervezi, hogy mintegy egymillió eurót fordít a kritikus adatok külföldi tárolására.

Az ellenőrzés során vizsgált kérdések

- Azonosították-e a minisztériumok az összes kritikus adatbázist és a kezelési követelményeket?
- Biztosítva vannak-e a kritikus adatbázisok és nyilvántartások?
- Szavatolt-e a kritikus adatok és adatbázisok hosszú távú folytonossága?

Megállapítások

A nemzeti számvevőszék az alábbi megfigyeléseket tette az ellenőrzött kritikus adatbázisokkal kapcsolatban:

- Nem állapítottak meg cselekvési tervet vagy követelményeket a kritikus adatbázisok fogalmának alkalmazásához. A kritikus adatbázisok kiválasztásának feltételeit nem határozták meg, és nem volt bizonyos, hogy az összes szükséges adatbázist belefoglalták a folyamatba. Az adatbázisok kiegészítő védelmét informálisan szervezték meg, és nem volt kötelező az adatbázisok tulajdonosai számára, ami miatt az öt kritikus adatbázisban tárolt adatokból nem állt rendelkezésre biztonsági másolat külföldön.
- Nem állapítottak meg kiegészítő információbiztonsági szabályokat a kritikus adatbázisok tekintetében. Sem az ISKE információbiztonsági rendszer (az észt közszféra számára kifejlesztett információbiztonsági szabvány, amely az adatbázisokat/nyilvántartásokat kezelő állami és helyi önkormányzati szervezetek számára kötelező), sem jogi aktus vagy szabvány nem tartalmazott kiegészítő követelményeket a kritikus adatbázisokra vonatkozóan, értve ez alatt például az

adatok biztonsági másolatainak Észtországon kívüli tárolását. Az ellenőrzött adatbázisok biztonsági másolatait külföldre vitték, az információs rendszerek munkájának azokból történő helyreállítását azonban nem tesztelték.

- Az ISKE végrehajtása és a vonatkozó auditálás problémát jelentett a kritikus adatbázisok tekintetében. Az ellenőrzés idejéig a 10 adatbázis közül kettő esetében nem került sor ISKE-auditra, azokat csak ezen ellenőrzés végére szervezték meg (2017. november 30.). Csupán két kritikus adatbázist auditáltak a jogszabályban előírt gyakorisággal. Emellett előfordultak olyan esetek, amikor az auditor által feltárt problémákat nem oldották meg a két ISKE-audit között eltelt (két-hároméves) időszakban.

- Az ellenőrzés során a nemzeti számvevőszék megállapította, hogy egyes kritikus adatbázisoknál nem hajtottak végre néhány fontos információbiztonsági intézkedést. Így például az információbiztonsági iránymutatásokban nem határozták meg az információs rendszerek sebezhetőségeinek rendszeres értékelésére vonatkozó követelményeket, nem került sor az eseménynaplók rendszeres ellenőrzésére, illetve elemzésére, nem voltak képzési tervek az információbiztonsággal kapcsolatos tudatosságra vonatkozóan, illetve nem álltak rendelkezésre az efféle képzési tervek alapjául szolgáló elemzések a kormányzati területen, egyes esetekben nem vizsgálták a fájlok integritását, és nem végeztek teszteket a külső behatolás tekintetében.

Következtetések és ajánlások

Az ellenőrzés során megállapítást nyert, hogy az állami hivatalok számára kötelező ISKE háromszintű biztonsági alaprendszer alkalmazása és auditjai ellenére jelentős hiányosságok vannak számos kritikus adatbázis információbiztonságának szavatolása terén, ideértve a naplók ellenőrzését, a behatolás tesztelését és a mobil eszközök védelmét. A kritikus adatok védelméhez szükséges speciális követelményeket még nem állapították meg.

A Gazdasági és Kommunikációs Minisztérium elindította a kritikus adatok védelméhez szükséges első tevékenységeket, a kritikus adatbázisokra irányuló projekt azonban olyan szakaszban volt, amely jogilag kötelező szabályokat kívánna meg. Emellett nem létezett részletes kockázatelemzés vagy cselekvési terv a jövőre nézve.

Öt kritikus adatbázisról biztonsági másolatokat őriztek külföldi országok követségein, ugyanakkor az Észtországban található adatközpontok fizikai megsemmisülésének esetén nem lenne garantált a fennmaradó öt adatbázisban megtalálható kritikus adatok védelme.

Két általános ajánlást fogalmaztak meg:

- Meg kell határozni a kritikus adatbázisok kiegészítő védelmének szabályait, beleértve a kritikus adatbázisok kiválasztását, az ezen adatbázisokban lévő adatok kezelését, valamint az állam számára kritikus jelentőséggel bíró adatok biztonsági másolatának rendelkezésre állását, továbbá annak értékelését, hogy miként biztosítható kiegészítő finanszírozás ezekhez a tevékenységekhez.
- Mind a pénzügyi tervezés, mind az információbiztonság tekintetében elemezni kell az adatbázisok létrehozásának különböző szakaszait, és e szakaszok végrehajtásánál alkalmazni kell a projektmenedzsment bevált gyakorlatait.

Írország
Office of the Comptroller and Auditor General

A nemzeti kiberbiztonsággal kapcsolatos intézkedések

Közzététel időpontja: 2018. szeptember

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2011–2018

A jelentés összefoglalása

Az ellenőrzés tárgya

Írországban a Kommunikációs, Éghajlat-politikai és Környezetvédelmi Minisztérium felel a kiberbiztonsági politikáért. A minisztérium felelős továbbá – a Nemzeti Kiberbiztonsági Központon keresztül – a kormányzati veszélyhelyzet-elhárítás koordinálásáért valamennyi országos szintű kiberbiztonsági esemény vonatkozásában.

A Nemzeti Kiberbiztonsági Központ 2011-ben jött létre. Elsődleges feladata a kormányzati hálózatok biztonságának szavatolása, az ipar és a magánszemélyek segítése saját rendszereik védelmében, valamint a kritikus nemzeti infrastruktúra megóvása.

Az ellenőrzés során vizsgált kérdések

Ez a vizsgálat áttekinti a Nemzeti Kiberbiztonsági Központ létrejötte óta a kiberbiztonsági intézkedések tekintetében elért előrehaladást. Konkrétabban az alábbiakkal kapcsolatos kérdésköröket érint:

- a központ megbízatása és erőforrásai;

- a nemzeti kiberbiztonsági stratégia (2015–2017);
- a hálózati és információs rendszerek biztonságáról szóló uniós irányelv végrehajtása;
- irányítási és felügyeleti intézkedések.

Megállapítások és következtetések

Bár a Nemzeti Kiberbiztonsági Központ létrehozásáról szóló kormányhatározat évi 800 000 euró összegű finanszírozást hagyott jóvá, 2012 és 2015 között a kiberbiztonságra fordított tényleges finanszírozás ennek egyharmadát sem érte el. 2017-ben az előirányzat 1,95 millió euróra emelkedett. A központ személyzete 2017 során közel kétszeresére, 14,5 teljes munkaidős egyenértékre nőtt. 2018-ban további 16 munkatárs kinevezését hagyták jóvá.

A nemzeti kiberbiztonsági stratégia (2015–2017) 12 intézkedést határoz meg, amelyeket a stratégia időtartama alatt kell megvalósítani. 2018 májusáig négy intézkedést zártak le, négyet részben hajtottak végre, négyet pedig nem hajtottak végre.

A hálózati és információs rendszerek biztonságáról szóló uniós irányelv célja az alapvető hálózati és információs rendszerek ellenálló képességének javítása.
Az irányelv három pillére tekintetében Írországban elért előrehaladás értékelése alapján a következők nyertek megállapítást:

- *1. pillér. Az uniós tagállamok kiberbiztonsági képességeinek javítása.* Részben végrehajtva – a strukturális követelmények problémáját megoldották, de továbbra is hiányosságok vannak a stratégiai tervezés terén.
- 2. pillér. Az uniós tagállamok közötti, kiberbiztonsággal kapcsolatos együttműködés elősegítése. Végrehajtva.
- *3. pillér. Biztonsági intézkedések és az események jelentésére vonatkozó kötelezettségek bevezetése kulcsfontosságú ágazatok esetében.* Részben végrehajtva – van még tennivaló a kritikus hálózati és információs rendszerek azonosítása, az alapvető szolgáltatásokat nyújtó szereplők hivatalos kijelölése, valamint a digitális szolgáltatók irányítása tekintetében.

A Nemzeti Kiberbiztonsági Központ létrehozását jóváhagyó (2011. júliusi) kormányhatározat jóváhagyta egy minisztériumközi bizottság felállítását is, amelynek feladata a kiberbiztonsággal kapcsolatos írországi kihívások kezelésére irányuló szakpolitika meghatározása és végrehajtása. Miközben a csoport 2013 és 2015 között öt alkalommal ülésezett, csupán egy ülésről állt rendelkezésre jegyzőkönyv felülvizsgálat céljára. 2015 óta a bizottság nem ülésezett.

A nemzeti kiberbiztonsági stratégia végrehajtási terve kötelezettségvállalást tartalmaz arra vonatkozóan, hogy éves jelentést tesznek közzé és 2017 végén hivatalos hatásvizsgálatot végeznek munkájukról. Ezek még nem teljesültek, bár a minisztérium éves jelentése felvázolja a központ munkáját.

A minisztériumot hivatalosan felkérték a központ teljesítményének értékelésére. Nem áll rendelkezésre bizonyíték arra vonatkozóan, hogy elvégezték volna ezt az értékelést. A minisztérium állítása szerint a Nemzeti Kiberbiztonsági Központ munkájának teljesítményértékelése a minisztérium rendes teljesítménymenedzsmentjének és szervezetirányításának részét képezte.

Az ellenőrzés megállapításai a következők:

- Bár a Nemzeti Kiberbiztonsági Központ kritikus funkciót tölt be, működésének első négy évében erőforrásainak szintje lényegesen alatta maradt az eredetileg tervezettnek.
- A központ átfogó stratégiai irányítása nem egyértelmű, és jelenleg nem létezik stratégiai terv.
- Nagyobb egyértelműségre van szükség a kiberbűnözés és a nemzetbiztonsági incidensek kivizsgálásában részt vevő szervek szerepköreit illetően.
- A nemzeti stratégia kidolgozásával kapcsolatban a hálózati és információs rendszerek biztonságáról szóló uniós irányelvben előírt követelmények még végrehajtásra várnak.
- Bár az irányítási struktúrákról születtek előírások, nem egyértelmű, hogy a gyakorlatban miként működnek az irányítási rendszerek.

A kiberbiztonságra szánt erőforrások rendelkezésre állása és költségei tekintetében hiányzik az átláthatóság.

Franciaország
Cour des comptes

A felsőoktatásba történő belépés: a diákok számára nyújtott tanácsadásról és a sikeres tanulmányokról szóló jogszabály kezdeti értékelése

Közzététel időpontja: 2020. február

Link a jelentéshez: Jelentés (francia nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2019–2020

A jelentés összefoglalása

Az ellenőrzés tárgya

A diákok számára nyújtott tanácsadásról és a sikeres tanulmányokról szóló 2018. évi jogszabály (*loi relative à l'orientation et à la réussite des étudiants*, ORE) a felsőoktatásba belépő fiatalok útjának három fő szakaszát volt hivatott javítani: a felső középfokú oktatásban részt vevő diákok számára nyújtott tanácsadás és támogatás, a képzés kiválasztása, valamint a tanulmányok első éveinek sikeres abszolválása. A jogszabály bevezette a „*Parcoursup*" elnevezésű új digitális platformot, amely információforrásként szolgál az elérhető egyetemi kurzusokra és bemeneti követelményekre vonatkozóan, aminek célja, hogy a középiskolás diákok könnyebben megtalálják a képességeikhez és tanulmányi eredményeikhez illeszkedő felsőoktatási kurzusokat.

Az ORE első két évében megtörtént az első lépés a felsőoktatásba történő belépés átalakítása terén. Számos korlát ellenére a „*Parcoursup*" bevezetése zökkenőmentesen haladt, bár továbbra is hiányoztak a biztonsági és fenntarthatósági garanciák, és az adatokat ki lehetett volna jobban használni, tekintettel azok fontosságára.

Az ORE elfogadásával két jelentős oktatáspolitikai problémát kívántak megoldani. Az első az egyetemi hallgatók körében tapasztalható magas lemorzsolódási arány volt; a második pedig az, hogy a régi digitális platformmal kapcsolatban komoly elégedetlenség volt tapasztalható, mivel az utolsó szakaszként véletlenszerű kiválasztást alkalmazott.

Az ORE reformjához 867 millió euró összegű finanszírozást ítéltek meg egy ötéves időszakra. A reform egy „-3/+3” kontinuum koncepción alapult, amelynek alapelve, hogy minél többet tudnak a felső középfokú oktatásban részt vevő diákok a felsőoktatási képzések tartalmáról, annál nagyobb valószínűséggel vizsgáznak sikeresen, mivel így olyan képzéseket választanak, amelyek leginkább megfelelnek képességeiknek és törekvéseiknek. Az ORE törekedett arra, hogy (a korábbi helyzettel ellentétben) tanácsadást biztosítson a felső középfokú oktatásban részt vevő diákok számára, ezáltal pedig csökkentse a képzésváltások gyakoriságát, amely a számvevőszék becslése szerint csak a felsőoktatás első évét tekintve évente közel 550 millió euró költséggel járt.

A számvevők végeztek egy kezdeti értékelést a felsőoktatásba való belépésről az ORE összefüggésében, megvizsgálva a platform által felvetett informatikai biztonsági problémákat.

Az információs rendszert a leterheltség növekedése jellemezte (2020-ban belefoglaltak valamennyi felsőoktatási kurzust, és néhány éven belül rohamosan nőtt a felhasználók száma). Ez összefügg azzal, hogy az előző platformról sietve álltak át a „*Parcoursup*” platformra, anélkül, hogy változtattak volna architektúráján, ami jelentős kockázatokhoz vezetett a szolgáltatás minősége, folyamatossága, alkalmazkodóképessége és továbbfejlesztése tekintetében. A rendszernek a biztonság, a teljesítőképesség és a robusztusság területén tapasztalható gyenge pontjait nem javították ki. A „*Parcoursup*” rendszert azért lehetett gyorsan felállítani, mert béta üzemmódban kezelte néhány magasan képzett és motivált ember, ez a megközelítésmód azonban azt vonta maga után, hogy a rendszerből hiányzott a stratégiai irányítás és a kielégítő kormányzás.

Az ellenőrök értékelték az információs rendszer minőségét és az új „*Parcoursup*” platform teljesítőképességét. A „*Parcoursup*” platformot az ORE értelmében hozták létre azzal a céllal, hogy javuljon a felsőoktatási képzési helyek kiosztásának minősége és ezáltal a képzések elvégzésének aránya.

Megállapítások

Bár a „*Parcoursup*” kielégítően működött, informatikai kockázatoknak volt kitéve, amelyeket csökkenteni kellett. Garanciákra volt szükség a platform biztonságát és fenntarthatóságát illetően, és jobban fel lehetett volna használni az adatokat.

Régi információs rendszer

Kevés új dolog volt a „*Parcoursup*” platformban, amely – számos megoldatlan kockázat mellett – megörökölte a korábbi „*Admission Post-Bac*” (APB) platform nehézkességét és sérülékenységét. A „*Parcoursup*” strukturális alapjául szolgáló információs rendszert közvetlenül a korábbi platformból emelték át. Annak ellenére, hogy új férőhelykiosztási rendszerként hirdetik, az információs rendszer veleje az APB óta csupán kismértékben módosult. Valójában az információs infrastruktúra több mint 72%-a változatlan maradt, mivel az APB kódjainak csupán kevesebb mint 30%-át írták újra.

A platform informatikai alapjait a kétezres évek elején alakították ki annak érdekében, hogy kezelni tudja a körülbelül 100 000 helyre beérkező évi mintegy egymillió jelentkezést, az információs rendszert azonban kibővítették, hogy megbirkózzon a megközelítőleg egymillió helyre beérkező mintegy 10 millió jelentkezéssel. A „*Parcoursup*” így valójában nem volt más, mint egy régi eszköz, amelyre új márkanevet ragasztottak. A teher növekedése nyomán kérdésessé vált, képes-e megvalósítani a platform a kívánt célt.

Rosszul dokumentált információs rendszer

A minisztérium átláthatósággal kapcsolatos törekvései ellenére a „*Parcoursup*” forráskódja továbbra is 99%-ban zárt volt. Az a kevés, amit közreadtak, kevéssé volt érdekes abból a szempontból, hogy meg lehessen érteni és értékelni lehessen a képzési helyek jelentkezők közötti kiosztásának folyamatát.

Elődjéhez hasonlóan a „*Parcoursup*” rosszul dokumentált operatív információs rendszer volt. A kódellenőrzés eredményei azt mutatták, hogy az alkalmazás rossz minőségű és magas kockázatú, emellett az ellenőrzés számos kritikus adatsértést azonosított. A rendszer rosszabb minőségű volt, mint más hasonló korú szoftverek, és nagy volt az összeomlás kockázata.

A „*Parcoursup*” nyilvános és zárt forráskódot is használt. A nyílt kód esetében jóval magasabb volt a kritikus adatsértések aránya, mint a zárt kódnál, ami azt jelenti, hogy fennállt a szolgáltatás zavarának kockázata. Emellett a platform nem volt hekkerbiztos

(a forráskód 2018. júliusi biztonsági auditja szerint). 2019 végén azonban a minisztérium bejelentette, hogy megkezdődött a „*Parcoursup*” kód tanúsítási eljárása.

A forráskód meglévő dokumentációja nem volt koherens, sem teljes körű. A „*Parcoursup*” kódja szokatlanul bonyolult volt. A számvevők úgy ítélték meg, hogy a forráskódot át kell alakítani, csökkentve a bonyolult összetevők számát.

A „*Parcoursup*” információs rendszer architektúrája magas kockázatú volt; az adatbázist – elavult módon – manuálisan kezelték. A rendszer sérülékenysége abból ered, hogy nagymértékben támaszkodik az üzemeltető rendelkezésre állására és odafigyelésére. A minisztérium elismerte, hogy a „*Parcoursup*” architektúrájához nagy kockázatok kapcsolódnak, és ezek nem orvosolhatók az alkalmazás továbbfejlesztése nélkül.

A „*Parcoursup*” információs rendszer rosszul volt dokumentálva, és alapvetően a nemzeti kormányhivatal (*Service à Compétence Nationale,* SCN) személyzetének szakértelmére támaszkodott. Az adatbázisba dokumentációként a rendszer magjába is beírtak megjegyzéseket, ami megnehezíti az információs rendszer karbantartását és fejlesztését, valamint az adatok hasznosítását. A platformban tárolt felhasználói információkat nem lehetett egyszerűen, mélyreható kutatás nélkül kinyerni és értékelni. A strukturált műszaki dokumentáció hiányára tekintettel az SCN stratégiai feladatainak elvégzésére való képessége teljes mértékben az információtechnológiai központ vezetőjén múlott.

Biztonsági stratégia: fejlesztésekre van szükség

A rendszerben tárolt személyes adatok érzékeny jellege miatt a „*Parcoursup*” valódi biztonsági kihívást jelent. Alapvetően minden olyan szervezetnek, amely információs rendszert kezel, rendelkeznie kell egy hivatalos, írásos biztonsági szabályzattal az információs rendszerre vonatkozóan (ISSP). Bár a miniszterelnök kulcsfontosságú szolgáltatóként ismerte el a „*Parcoursup*” platformot, az nem rendelkezett ISSP szabályzattal. Haladéktalanul lépéseket kellett tenni ennek bevezetése érdekében.

A „*Parcoursup*” minden egyes csoportjánál volt egy, az információs rendszerek biztonságáért felelős tisztviselő (ISSO), aki az információtechnológiai központ alá volt rendelve. Helyesebb lett volna, ha az ISSO-kat közvetlenül az SCN igazgatója alá rendelik, szavatolva ezáltal függetlenségüket.

2019 közepén még folyamatban volt a „*Parcoursup*” GDPR szerinti kiigazítása. Néhány intézkedés még függőben volt, különösen az, hogy hivatalosan ki kell alakítani az

adatkezelésnél alkalmazott különböző eljárásokat. A személyes adatok biztonsága továbbra sem volt megfelelő, és még mindig túl sok kimerítő egyedi adatot tároltak.

A „*Parcoursup*" egység egyaránt beszámolással tartozott a „*Parcoursup*" projektmenedzsere felé (akit a miniszter hivatalától jelöltek ki), valamint a Felsőoktatási és Szakmai Integrációs Főigazgatóság képzési stratégiáért és hallgatói ügyekért felelős osztálya felé, ami miatt megoszlott a lojalitás. A „*Parcoursup*" információs rendszerrel kapcsolatos gyakorlati kérdéseket hetenkénti üléseken tárgyalták meg. Bár ennek a szervezési formának előnye a gyors reakcióidő a hallgatók áramlásának mindennapi kezelése tekintetében, stratégiailag irányvesztetté tette a „*Parcoursup*" platformot.

Végezetül, a rendszer nem volt elég átlátható. Nem tette lehetővé a platformon tárolt adatok lehető legjobb felhasználását, a bennük rejlő hatalmas potenciál ellenére. E potenciál kiaknázása szinte bizonyosan teljesítményjavulást eredményezett volna.

Következtetések és ajánlások

A kormányzat a digitális platformon keresztül sikeresen központosította az összes posztszekunder képzéshez való hozzáférést, ötvözve valamennyi oktatási programot annak érdekében, hogy kezelje a felsőoktatás általánossá válását. A korábbi rendszert sietősen, lényegi strukturális változtatások nélkül dolgozták át a „*Parcoursup*" platformmá. Így nem orvosolták az információs rendszer sebezhetőségeit a biztonság, a teljesítőképesség és a robusztusság tekintetében, noha a terhelés szükségszerűen tovább növekedett, tekintettel az összes alapképzés integrálásának végső céljára. A rendszert emellett rosszul dokumentálták, kissé kezdetleges megközelítést alkalmazva az informatikai fejlesztés tekintetében, és annak szokatlan bonyolultsága operatív változás esetén fokozza a hibák kockázatát. A platform ezért jelentős kockázatoknak volt kitéve a közszolgáltatás minősége és folyamatossága, valamint a személyes adatok biztonsága tekintetében.

A *Cour des comptes* az alábbi ajánlásokat fogalmazta meg:

- az SCN informatikai csoportjának több álláshelyet kell biztosítani, és az ORE szerinti finanszírozást át kell csoportosítani az információs rendszerekkel és a statisztikai kutatással foglalkozó aligazgatóság emberi és pénzügyi erőforrásainak erősítése érdekében;

- az információs rendszert hosszú távra kell kialakítani, javítva annak legsürgetőbb hiányosságait, korszerűsítve vagy átalakítva architektúráját, valamint szisztematikus és strukturált módon dokumentálva a régi rendszer és a „*Parcoursup*” elsődleges adatbázisait;
- biztonsági szabályzattal kell ellátni a „*Parcoursup*” információs rendszert;
- közös irányító szervet kell létrehozni az Oktatási és Ifjúsági Minisztérium és a Felsőoktatási, Kutatási és Innovációs Minisztérium számára a „*Parcoursup*” platform felügyelete céljából, az ORE „tanácsadási” tevékenységekre szánt finanszírozásából csoportosítva át erőforrásokat.

Lettország
Valsts Kontrole

Kihasznált-e minden lehetőséget a közigazgatás az IKT-infrastruktúra hatékony igazgatására?

Közzététel időpontja: 2019. június

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2017–2019

A jelentés összefoglalása:

Az ellenőrzés tárgya

A lett számvevőszék teljesítmény-ellenőrzést végzett az állami IKT-infrastruktúra hatékonyságára vonatkozóan. Az ellenőrzés annak vizsgálatára irányult, hogy egységes megközelítést alkalmaz-e a közigazgatás az IKT-infrastruktúra hatékony irányítása tekintetében, és értékelték-e az intézmények a központosítás előnyeit. Ezenkívül a további optimalizálás megtervezésének lehetőségei tekintetében fontos kérdésként azonosították az adatközpontok biztonságát.

Mivel a hatóságok – legalábbis egy minisztérium szintjén – vonakodnak az IKT-infrastruktúra központi igazgatásától, számos szervertermet hoztak létre, jelentősen növelve ezzel a karbantartási költségeket. Az ellenőrzés megállapította, hogy a négy vizsgált minisztérium 22 alegysége 38 adatközpontot használt. Az ellenőrzés során a nemzeti számvevőszék tanúja volt olyan helyzeteknek, ahol akár országos jelentőségű információs rendszerek elégtelen biztonsági szintű helyiségekben voltak megtalálhatók. A szervertermek számának optimalizálása nemcsak az IKT-kiadások csökkentését tenné lehetővé, hanem megfelelő biztonsági szintet is nyújtana

alacsonyabb költséggel. Mindeközben az intézményeknél már léteztek magas biztonságú szervertermek, de ezeket nem használták teljes kapacitáson.

Az ellenőrzés fő témája

Az ellenőrzés azt volt hivatott megállapítani, hogy megteremtették-e és bevezették-e az IKT-infrastruktúra egységes igazgatásának valamennyi előfeltételét, előmozdítva ezáltal az IKT-erőforrások hatékonyabb és biztonságosabb felhasználását.

Megállapítások és következtetések

Az IKT irányítása és optimalizálása

- Sem országos szinten, sem a minisztériumokban nem volt hosszú távú elképzelés az IKT fejlesztésével és optimalizálásával kapcsolatban. A minisztériumok és alegységeik saját értelmezésük és kapacitásaik szerint optimalizálták az IKT-infrastruktúrát.

2011 és 2017 között az ellenőrzött intézmények összes IKT-karbantartási költsége évi 17 millió euróról 20 millió euróra nőtt. Az intézményekben nem tették gyakorlattá annak rendszeres értékelését, hogy mi lenne olcsóbb: maguknak végezni az IKT-infrastruktúra karbantartását, együttműködni más intézménnyel, vagy kiszervezni azt. Sem az IKT központosítása, sem annak decentralizálása nem tekinthető önmagában vett célnak, de szükség van a konkrét helyzet és az alternatívák elemzésére ahhoz, hogy egyértelművé lehessen tenni a meglévő költségeket és a lehetséges alternatívákat.

IKT-biztonság

- A jogi keret nem határozta meg egyértelműen az IKT-infrastruktúra biztonsági követelményeit egy, a feldolgozandó információ relevanciájától függő logikus rendszer alapján. Nem léteztek részletes műszaki követelmények az IKT-adatközpontok védelmére vonatkozóan.

- A biztonsági követelményekkel kapcsolatos hiányosságok költséges védelemhez vezettek, vagy épp ellenkezőleg azt eredményezték, hogy nemzeti jelentőségű információk védelme nem volt biztosítva. Sőt, fontos információs rendszereket alacsony biztonságú adatközpontokban helyeztek el.

- A legtöbb szerverteremben voltak biztonsági fenyegetések – az adatközpontok nem voltak kellően védve a fizikai hozzáféréstől és a környezeti kockázatoktól. A biztonsági fenyegetések megelőzéséhez legalább 247 000–765 000 euróra volt szükség, a választott megközelítéstől függően. A következő opciók álltak rendelkezésre: 1) a több fontos információs rendszert befogadó szervertermek fejlesztése és annak biztosítása, hogy a jelentős IKT-erőforrásokat magasabb biztonságú adatközpontokban tárolják; illetve 2) az összes létező szerverterem fejlesztése. Ehhez azonban – hacsak nem csökkentik a minimumra az adatközpontok számát – olyan összegű beruházásra lenne szükség, amelyet a számvevők nem láttak indokoltnak.

A jogi keret nem volt teljes, mivel nem léteztek részletes biztonsági követelmények az IKT-infrastruktúrára vonatkozóan. Így például voltak követelmények a logikai biztonsággal kapcsolatos különféle kritériumokkal kapcsolatban, de nem léteztek kritériumok az infrastruktúra fizikai és környezeti biztonságát illetően, ami szintén hatással van a rendszerek rendelkezésre állására és az adatvédelemre. Noha közpolitikai tervezési dokumentumok kiemelték az IKT-infrastruktúra biztonságának fontosságát és erősítésének szükségességét, senki nem tervezett meg konkrét fellépéseket ezen a területen. A biztonsági követelmények egyértelmű, nyomon követhető és logikus differenciálásának hiánya azzal a kockázattal járt, hogy az országon belül eltérő biztonsági követelmények lehetnek érvényben az azonos fontosságú és jelentőségű információk kezelésére vonatkozóan.

A digitális téren belüli biztonságot az állam központilag felügyelte, és az állam reagált az ott bekövetkező incidensekre, de az informatikai infrastruktúra biztonságának végrehajtásáért a felelősséget az egyes intézmények vezetői viselték. Így jelentős különbségek voltak a tekintetben, hogy miként értelmezik az intézmények az IKT-biztonsági kérdéseket, hogyan értékelik a kezelt információk fontosságát, és milyen erőforrások állnak az intézmények rendelkezésére az IKT-biztonsággal kapcsolatos kérdések kezeléséhez.

Rendszeres monitoringon alapuló rendszerre volt szükség e folyamatok vonatkozásában, hogy egyetlen rendszerként, függetlenül és standard kritériumok alkalmazásával lehessen értékelni a teljes közigazgatást, azonosítani lehessen a megközelítések közötti eltéréseket és a közös kockázatok azonosítása révén meg lehessen előzni azokat, valamint megelőző intézkedéseket lehessen megtervezni a kockázatok csökkentésére.

Litvánia
Valstybės Kontrolė

A kritikus állami információs források kezelése

Közzététel időpontja: 2018. június

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)
Jelentés (litván nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2014–2017

A jelentés összefoglalása

Az ellenőrzés tárgya

A kritikus állami információs erőforrások – kritikus elektronikus információk – használatakor fontos kormányzati funkciók teljesülnek, ideértve a kormányzati pénzgazdálkodást, az adóügyi igazgatást és az egészségügyi ellátást. A kritikus információk elvesztése, illetve a vonatkozó információs rendszerek elérhetetlensége súlyos következményekkel járhat a közbiztonság, a jólét és a gazdaság tekintetében. Az általános információtechnológiai ellenőrzéssel kapcsolatban a litván állami számvevőszék (NAOL) által 2006 és 2016 között lefolytatott értékelések visszatérő problémákat tártak fel az informatikai irányítás terén (tervezés, az információs architektúra meghatározása, szervezeti felépítés, változások, az üzletmenet-folytonosság biztosítása, adatbiztonság, az informatikai irányítás nyomon követése és értékelése). A NAOL ellenőrzést végzett a kritikus állami információs erőforrásokra vonatkozóan, hogy értékelje ezen erőforrások igazgatását és biztonságát, és javító intézkedésekre tegyen javaslatot.

Az ellenőrzés célja az irányításnak (általános irányítás) és a kritikus állami információs erőforrások érettségének értékelése, továbbá a rendszerszintű problémák azonosítása volt.

A NAOL 12 közszektorbeli szervezet[64] informatikai irányításának érettségét értékelte, amelyek 44 első osztályú állami információs rendszert igazgatnak. Az ellenőrzést az állami ellenőrzésekre vonatkozó követelmények és a legfőbb ellenőrző intézmények nemzetközi szabványai szerint végezték el. Az értékelés a COBIT[65] módszertan szerint zajlott az alábbi, leginkább kockázatos területeken: stratégiai informatikai tervezés, az információs architektúra meghatározása, informatikai kockázatkezelés, változásmenedzsment, a megszakítás nélküli szolgáltatásnyújtás biztosítása, információbiztonság, adatgazdálkodás, az informatikai tevékenységek nyomon követése és értékelése, valamint az informatikai irányítás megbízhatósága.
A folyamatértékelés egyaránt kiterjedt a szervezeti és a nemzeti informatikai irányításra, valamint az ezen irányítási szintek közötti interakciókra.

Ellenőrzési megállapítások

A kritikus állami információs erőforrások kezelése tekintetében az érettség szintjének változása kedvező tendenciát mutatott. Ugyanakkor a kiberfenyegetettség növekvő szintjére tekintettel a megfigyelhető előrehaladás túl lassú volt, és az említett erőforrások biztonságát fokozni kellett. Ez az alábbi hiányosságokból adódott.

- A kritikus állami információs erőforrások azonosításának rendszere nem volt kellően eredményes ahhoz, hogy lehetővé tegye a tényleges szükségleteknek megfelelő biztonsági megoldások alkalmazását:
  - Az állami információs erőforrások kritikus voltának igazolására szolgáló értékelések nem voltak objektívek, az újbóli értékelések során nem mindig elemezték a változásokat, ezt a folyamatot nem követték nyomon nemzeti

[64] Állami adófelügyelet, a nyilvántartások állami központja, információtechnológiai és kommunikációs hivatal, az állami társadalombiztosítási alap igazgatósága, a mezőgazdasági információkkal foglalkozó és a vidéki vállalkozások központjaként működő állami vállalat, a váminformációs rendszer központja, állami élelmiszerügyi és állategészségügyi szolgálat, a Litván Köztársaság parlamentjének hivatala, Pénzügyminisztérium, az információs társadalom fejlesztéséért felelős bizottság, Országos Betegpénztár, állami erdészeti szolgálat.

[65] A COBIT (az informatikára és a kapcsolódó technológiára vonatkozó ellenőrzési célkitűzések) a nemzetközi ISACA szervezet szabványa, amely meghatározza az informatikai irányítás helyes gyakorlatait.

szinten, és a kritikus jelleg meghatározására vonatkozó iránymutatások nem biztosították az eredményes végrehajtást.

— A kritikus állami információs erőforrások és a kritikus információs infrastruktúra azonosításának rendszere nem volt szabványosítva; az erőforrásokat és az infrastruktúrát az információk és a szolgáltatások fontossága alapján különbözőképpen azonosították, ami bonyolulttá tette ezen erőforrások azonosításának folyamatát.

— Nem dolgoztak ki nemzeti információs architektúrát annak érdekében, hogy leképezzék az állami információs rendszereket és a közöttük fennálló kapcsolatokat, kimutassák a kritikus állami információs erőforrások nagyságrendjét, valamint lehetővé tegyék a megalapozott döntéshozatalt az erőforrások jelentőségével kapcsolatban.

o Az állami információs erőforrások kezelésének jobban összhangban kellene állnia a bevált informatikai irányítási gyakorlatokkal és normákkal, hogy meg lehessen valósítani az információtechnológia területének integrált fejlesztését, amely hozzájárulna a kritikus állami információs erőforrások kezelése terén történő jobb előrehaladáshoz:

— Az informatikai tervezés nem volt fenntartható: a tervezett informatikai eszközöket különböző dokumentumokban ismertették, a stratégiai dokumentumok túl nagy száma miatt hiányzott a módszeres megközelítés, ami megnehezítette a legfontosabb prioritások azonosítását és az erőforrások becsatornázását a legnagyobb fenyegetések kezelése érdekében.

— Az informatikai nyomon követés nem biztosította, hogy a szervezetek mérjék az informatikai műveletek hatékonyságát, és hogy a kritikus állami információs erőforrások kezelői által elvégzett ellenőrzések az informatikai irányítás tényleges érettségét mutassák meg. Az állami informatikai irányítást nemzeti szinten nem vizsgálták, és az informatikai irányítással kapcsolatos problémákat nem elemezték szisztematikusan. Létrehoztak egy rendszert annak nyomon követésére, hogy megfelelnek-e az állami információs erőforrások az elektronikus információbiztonság követelményeinek, kizárólag azzal a céllal, hogy megkönnyítsék a biztonsági megfelelőség nyomon követését, de ennek funkcióit nem használták fel kellően.

- A kritikus információs erőforrásoknak a kiberfenyegetettségi szinttel szembeni ellenálló képességét biztosítani hivatott intézkedések nem voltak elég eredményesek, ezért továbbra is fennállt ezen erőforrások sebezhetőségének kockázata:

  — Javítani kellene az informatikai biztonsági kockázatok értékelésének eredményességén, mivel nem azonosítottak minden releváns kockázatot, és értékelési módszertanuk nem felelt meg a legújabb informatikai irányítási gyakorlatoknak; nem volt biztosított az elfogadhatatlan kockázatok időben történő kezelése.

  — Nem alkalmaztak módszeresen olyan szervezeti biztonsági intézkedéseket, amelyek képesek csökkenteni a kiberfenyegetettség kockázatát. Elégtelen volt a biztonság tesztelése, a személyzet nem részesült megfelelő képzésben az információs rendszer fejlesztése, frissítése és módosítása során, figyelmen kívül hagyták a biztonságos szoftverkonfigurációkat és frissítéseket, az informatikai üzletmenet-folytonosság és a tartalékfájlok nem megfelelő kezelése veszélyeztette a működés helyreállítását, a biztonsági teljesítmény mérése pedig elégtelen volt és nem járult hozzá a biztonság megerősítéséhez.

Következtetések

Az elmúlt tíz évben ellenőrzött közszektorbeli intézmények informatikai irányítása átlagosan az ötből az első szintű érettséget érte el[66], a jelentés írásakor pedig 1,7-es szinten állt. A kritikus állami információs erőforrások ilyen alacsony szintű érettsége az állami információs erőforrásokra irányuló politika kialakításának és végrehajtásának hiányosságait jelezte, ami sebezhetőbbé teszi ezeket az erőforrásokat. Az erőforrások biztonságának fokozása érdekében fejleszteni kell az állami információs erőforrások kezelésének mechanizmusát, hogy az a lehető legjobban megfeleljen a bevált gyakorlatoknak. A számvevők megállapították továbbá, hogy a kritikus információs erőforrások kiberfenyegetésekkel szembeni ellenálló képességének szavatolását célzó intézkedések nem voltak kellően eredményesek. Ezért eredményesebbé kell tenni az informatikai biztonsági kockázatok értékelését, nagyobb hangsúlyt helyezve az

[66] A COBIT módszertan szerint.

információs rendszerek létrehozása és korszerűsítése során a biztonsági tesztelésre, valamint a személyzet képzésére.

A területet érintő további jelentések

A jelentés címe:	Hatékony-e a kiberbűnözéssel szembeni fellépés?
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (litván nyelvű változat)
A közzététel időpontja:	2020

A jelentés címe:	A kiberbiztonsági környezet Litvániában
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (litván nyelvű változat)
A közzététel időpontja:	2015

Magyarország
Állami Számvevőszék

Az adatvédelem ellenőrzése – Az adatvédelem hazai keretrendszerének és egyes kiemelt adatnyilvántartások ellenőrzése nemzetközi együttműködés keretében

Közzététel időpontja: 2017. március

Link a jelentéshez: Jelentés (magyar nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Szabályszerűségi ellenőrzés

Ellenőrzött időszak: 2011–2015

A jelentés összefoglalása

Az ellenőrzés tárgya

A nemzeti adatvagyon biztonsága minden országban alapvető társadalmi érdek a nemzeti értékek megőrzése és védelme szempontjából. Ennek megfelelően a nemzeti adatvagyon körébe tartozó személyes és közérdekű adatok fokozott biztonságáról való gondoskodás elengedhetetlen az állampolgárok államba vetett bizalmának erősítése, valamint a közigazgatás folyamatos és zavartalan működése érdekében. Ezért a társadalom számára kiemelt jelentőséggel bír az adatok védelme, valamint az ennek érvényesülését szolgáló jogi keretrendszer révén nyújtott biztonsági háló.

Az adatok védelme területén a közigazgatási szervek kiemelt szerepet töltenek be, hiszen itt kezelik a nemzeti adatvagyon körébe tartozó adatok legnagyobb és legérzékenyebb adatnyilvántartásait. E nyilvántartások adatkezelői a feladatok ellátása érdekében szorosan együttműködnek, rendszeresen nagy mennyiségű adatot tartalmazó nyilvántartásokat továbbítanak, mely során figyelmet kell fordítaniuk az adatok védelmére vonatkozó, jogszabályban foglalt előírásokra. Az elektronikus információs rendszerek adatkezeléshez és -feldolgozáshoz történő alkalmazása ma már

nélkülözhetetlen, ezért megfelelően megtervezett és lefolytatott ellenőrzések révén szavatolni kell a rendszerek megfelelő és megbízható működését.

Ellenőrzései során a magyar Állami Számvevőszék nagy hangsúlyt fektet az adatvédelemre. 2011 és 2015 között átfogó ellenőrzéseket végzett az adatvédelem területén, amelyekről első jelentését 2017 első negyedévében adta ki. Az ellenőrzés az EUROSAI IT munkacsoporttal együttműködésben lefolytatott párhuzamos nemzetközi ellenőrzések szempontjaira is kiterjedt, amelyek elsősorban a meglévő európai uniós irányelveknek való megfelelést vizsgálták.

A magyarországi adatvédelemre vonatkozó szabályszerűségi ellenőrzés annak értékelését célozta, hogy megvalósult-e Magyarországon az adatvédelem szabályozási és operatív keretrendszere, és a jelentős adatkezelő szervezetek megfelelően alkalmazták-e a biztonságos adatkezelésre, valamint az adatfeldolgozás kiszervezésére vonatkozó előírásokat. Az ellenőrzés különösen a személyes adatok és a nemzeti adatvagyon védelmére irányult.

Az ellenőrzés keretében az Állami Számvevőszék értékelte hat adatkezelő szervezet (pl. adóhivatal, államkincstár, egészségbiztosítás, nyugdíjbiztosítás, Oktatási Hivatal, személyes adatok és lakcímek, közlekedési és járműnyilvántartások, valamint a bűnügyi adatok kezelésével foglalkozó közigazgatási szervek) adatkezelési tevékenységét, továbbá az adatvédelmi hatóság és az információbiztonsági hatóság tevékenységeit.

Az ellenőrzés kiemelten foglalkozott az adatkezelő szervezetek felhatalmazásával, különös tekintettel a harmadik felek számára történő adattovábbítás esetére. A belső kontrollrendszer ellenőrzése során értékelték a feladatkörökre, valamint felelősségi és hatáskörökre, a humánerőforrás-kezelésre és a folyamatokra vonatkozó naprakész szabályozások meglétét.

Az adatkezelés keretében használt elektronikus rendszerek vonatkozásában az Állami Számvevőszék értékelte a kapcsolódó védelmi intézkedéseket, ezen belül a fizikai védelem, a hozzáférési jogosultságok, a naplózás, a biztonságértékelési eljárásrend, a rendszer- és kommunikációvédelem területeit, valamint azt, hogy megfelelő-e a szervezet egészének biztonsági besorolása.

Az adatfeldolgozás kiszervezésének ellenőrzése a megkötött szerződések alapján történt, annak vizsgálatával, hogy az adatkezelő szervezetek a jogszabályi előírásoknak megfelelően előírták-e az adatfeldolgozó szervezetek számára az adatfeldolgozási tevékenységgel kapcsolatos követelmények teljesítését.

Megállapítások és következtetések

Az ellenőrzés alapján az Állami Számvevőszék megállapította, hogy az adatkezelő szervezetek adatkezelési tevékenységre vonatkozó belső szabályai a 2011 és 2015 között hatályos jogszabályi előírásoknak megfelelően biztosították a nemzeti vagyon részét képező nemzeti adatvagyon védelmét. Az adatkezelők a gyakorlatban megfelelően alkalmazták a biztonságos adatkezelésre, valamint az adatfeldolgozás kiszervezésére irányuló előírásokat. Az adatok harmadik fél részére történő továbbítását megfelelő felhatalmazással, a felelősségi és hatásköri viszonyok egyértelmű elhatárolása mellett hajtották végre.

Egyes adatkezelők vonatkozásában megállapítást nyert, hogy az elektronikus rendszereknek és a szervezet egészének biztonsági osztály szerinti besorolását nem minden esetben a jogszabályi előírásoknak megfelelően végezték el, a hiányosságok mértéke azonban nem befolyásolta érdemben a feldolgozott adatok biztonságát.
Az ellenőrzési jelentésben foglalt ajánlások alapján az adatkezelő szervezetek az Állami Számvevőszék által jóváhagyott cselekvési tervek keretében orvosolták a hiányosságokat.

Az EUROSAI IT munkacsoporttal együttműködésben végzett párhuzamos nemzetközi ellenőrzés vonatkozásában az Állami Számvevőszék megállapította, hogy a magyar adatvédelmi jogszabályok megfelelnek a hatályos uniós irányelvnek.

Összegezve: a magyar Állami Számvevőszék az adatvédelem ellenőrzésével hozzájárult a jó kormányzáshoz és a nemzeti adatvagyon védelméhez.

A területet érintő további jelentések

A jelentés címe:	Jelentés – Utóellenőrzések – Az adatvédelem ellenőrzése – Az adatvédelem hazai keretrendszerének és egyes kiemelt adatnyilvántartások ellenőrzése nemzetközi együttműködés keretében
Link a jelentéshez:	Jelentés (magyar nyelvű változat)
A közzététel időpontja:	2020

Hollandia
Algemene Rekenkamer

A kritikus vízgazdálkodási létesítmények és a határellenőrzés kiberbiztonsága Hollandiában

Közzététel időpontja: 2019. március és 2020. április

Link a jelentésekhez: A kiberbiztonságról és a kritikus vízgazdálkodási létesítményekről szóló jelentés összefoglalója (angol nyelvű változat)

A kiberbiztonságról és az automatizált határellenőrzésről szóló jelentés összefoglalója (angol nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2018–2020

A jelentés összefoglalása

Az ellenőrzés tárgya

2018-ban a holland Számvevőszék úgy döntött, ellenőrzéseket végez a társadalom számára kritikus fontosságú ágazatokon belüli kiberbiztonságra vonatkozóan.
A központi kormányzaton belüli információbiztonsági megfelelőség ellenőrzése terén szerzett sokéves tapasztalatok alapján a számvevőszék úgy vélte, a szabályzatok és az intézkedések gyakorlati *teljesítményének* ellenőrzése hozzáadott értéket kínál. Az első két ellenőrzött ágazat a vízgazdálkodás és az automatizált határellenőrzés volt, amelyek közül az első azért létfontosságú, mert az ország jelentős részben a tengerszint alatt fekszik, a második pedig azért, mert az amszterdami Schiphol repülőtér nemzetközi csomópont és bejárat az országba.

Az infrastruktúráért és vízgazdálkodásért felelős miniszter több, az építési beruházásokért és a vízgazdálkodásért felelős főigazgatóság (az ellenőrzött szerv) által kezelt vízi létesítményt jelölt meg a vízgazdálkodási ágazat „kritikus” részeiként. A kritikus vízi létesítmények működtetéséhez használt számítógépes rendszerek közül sok az 1980-as és az 1990-es évekből származik, amikor a kiberbiztonságot rendszerint még nem tartották szem előtt. Ezeket a rendszereket eredetileg önálló működésre tervezték, de fokozatosan összekapcsolták őket nagyobb számítógépes hálózatokkal, többek között a távolról történő üzemeltetés megkönnyítése érdekében. Ez a tendencia sebezhetőbbé tette a rendszereket a kiberfenyegetésekkel szemben.

A védelmi miniszter, valamint az igazságügyi és biztonsági miniszter közösen felel a holland határőrök által a Schiphol repülőtéren végzett határellenőrzésekért. Mindkét minisztérium (ellenőrzött szerv) rendelkezik információtechnológiai rendszerekkel, amelyekre a határőrök támaszkodnak. Ezek a rendszerek kritikus jelentőségűek a repülőtéri műveletek szempontjából, és igen érzékeny adatok feldolgozására használják őket. Ezáltal vonzó célpontjai lehetnek az olyan kibertámadásoknak, amelyek célja a szabotázs, a kémkedés vagy a határellenőrzések manipulálása.

Az ellenőrzések azt vizsgálták, hogy az ellenőrzött szervek miként készültek fel a kiberfenyegetések kezelésére, és az eredményesen történt-e.

- Az ellenőrzés során vizsgált kérdések az alábbiak megválaszolására irányultak: Hogyan *védik* az ellenőrzött szervek a rendszereket a kiberfenyegetésekkel szemben, és miként *előzik meg* a kibertámadásokat?
- Hogyan *derítik fel* az ellenőrzött szervek a kiberfenyegetéseket és a támadásokat?
- Hogyan *reagálnak* az ellenőrzött szervek olyan helyzetben, amikor kibertámadásra kerül sor?

Mindkét ellenőrzés külön hangsúlyt helyezett az eredményességre. Az ellenőrzött szervekkel szoros együttműködésben etikus hekkerek dolgoztak a kritikus vízi létesítményeken és az egyik határellenőrzési rendszeren. Magától értetődik, hogy a tesztek valamennyi megállapítása nyomán intézkedésre került sor, mielőtt a jelentéseket közzétették volna, és semmilyen műszaki részletet nem hoztak nyilvánosságra.

A két ellenőrzés között a fő különbség az volt, hogy a vízi létesítményekre irányuló ellenőrzés az ellenőrzött szerv céljainak megvalósulására összpontosított, míg a határellenőrzés auditja a NIST kiberbiztonsági keretrendszerén alapult.

Megállapítások

Mindenekelőtt mindkét ellenőrzés megállapította, hogy az ellenőrzött szervek tudatában voltak a kiberfenyegetettségnek, és azon voltak, hogy professzionális megközelítést alkalmazzanak ebben a kérdésben.

A vízi létesítmények esetében azonban az ellenőrzött szervnek többet kell még tennie a felderítés és a reagálás tekintetében ahhoz, hogy teljesítse saját kiberbiztonsági célkitűzéseit. Az ellenőrzött szerv létrehozott egy biztonsági műveleti központot (SOC) a kibertámadások felderítése és az azokra való reagálás érdekében. 2018 őszéig azonban nem teljesült az a 2017 végére kitűzött cél, hogy a kritikus vízi létesítményekkel szembeni valamennyi kibertámadást azonnal felderítsék. Ebből adódóan fennállt a veszély, hogy egy kritikus vízi létesítmény elleni kibertámadást egyáltalán nem, vagy csak túl későn derítenek fel. Ezenkívül az egyik kritikus vízi létesítménynél elvégzett teszt azt mutatta, hogy abba fizikailag be lehet hatolni. A hekkereknek sikerült bejutniuk a vezérlőterembe, ahol zavartalanul hozzáférhettek a védelem nélküli munkaállomásokhoz. Végezetül az ellenőrzött szerv nem épített ki forgatókönyvet egy kibertámadás által okozott válságra, és a reagálással kapcsolatos információk hiányoztak vagy nem voltak naprakészek. A naprakész információk megléte döntőnek bizonyulhat a válsághelyzetekre való gyors és hathatós reagálás szempontjából.

Ami a határellenőrzést illeti, a kiberbiztonsági intézkedések nem bizonyultak megfelelőnek, sem pedig időtállónak. Először is, a fontos határellenőrzési rendszereket hivatalosan jóvá kellett hagyni, mielőtt megkezdték volna működésüket, amivel azt akarták biztosítani, hogy valamennyi kiberbiztonsági intézkedés végre legyen hajtva. Megállapítottuk, hogy a három rendszerből kettő jóváhagyás nélkül működött, azaz nem volt garantált a szükséges biztonsági intézkedések megléte. Másrészt egy biztonsági műveleti központ működött ugyan, de a rendszerek egyike sem volt közvetlenül összekapcsolva vele. Bár az általános infrastruktúra össze volt kötve a biztonsági műveleti központtal, ettől még fennállt a kockázat, hogy egyes kibertámadások észrevétlenek maradnak, vagy túl későn derítik fel őket. Harmadrészt a biztonsági teszteket nem végezték el rendszeresen. Valójában a három rendszer közül korábban csupán egyet teszteltek, és azt is csak korlátozottan. Végezetül –

miként az első ellenőrzésnél is – nem készült konkrét forgatókönyv egy kibertámadás okozta válságra vonatkozóan.

Az egyik olyan rendszer biztonsági tesztje során, amelyet korábban még sohasem teszteltek, az etikus hekkerek számos sebezhetőségre bukkantak. E sebezhetőségek kihasználásával – egy rosszindulatú, jogosulatlan belső munkatárs közreműködésével – kibertámadást lehet indítani a rendszerben található információkhoz való hozzáférés, azok lemásolása vagy akár azok manipulálása céljából. Ezek az eredmények rámutattak a rendszeres biztonsági tesztelés fontosságára.

A megállapítások a határellenőrzési folyamatok jelenleg zajló automatizálása miatt igen aggasztóak. A közeljövőben egyre több határellenőrzési rendszer fog egyre több adatot kezelni, egyre nagyobb számú kapcsolatot használva. Ez növeli a kibertámadások kockázatát, ezért az alkalmazott megközelítés nem volt időtálló.

Következtetések

A vízi létesítmények esetében bizonyos alapvető elemek miatt az ellenőrzött szerv nem tudta megtenni a végső kiberbiztonsági lépéseket. Így például nem volt egyértelmű a fenyegetettségi szint, ami megnehezítette annak értékelését, hogy elegendőek voltak-e a meghozott intézkedések és az előirányzott költségvetési források. Ezenfelül a kiberbiztonságért felelős központi szervezeti egység nem rendelkezett felhatalmazással a szükséges kiberbiztonsági intézkedések decentralizált vízi létesítményeknél történő végrehajtásához. Az ellenőrzés ajánlásai nyomán lépéseket tettek e tekintetben, ami segítette a szervezetet az előrehaladásban.

A határellenőrzés esetében nem magyarázta egyértelmű ok az elégtelen kiberbiztonsági szintet. Az ellenőrzéshez kapcsolódó vizsgálat során hiánytalan és részletes kiberbiztonsági eljárásokat és szabályzatokat, valamint megfelelő szakértelmet és képzett alkalmazottakat találtak. Az ellenőrzési ajánlások ezért elsősorban annak biztosítását helyezték középpontba, hogy ténylegesen sor kerüljön minden lehetséges lépésre.

A parlament és a média nagy figyelmet szentelt mindkét ellenőrzésnek, amelyek ráirányították a figyelmet a kiberbiztonságra az alapvető infrastruktúra vonatkozásában, és betekintést nyújtottak az ellenőrzött szervek számára abba, hogy miként javíthatják kiberbiztonságukat. Az ellenőrzött szervvel való szoros

együttműködés nélkülözhetetlen volt a helyzetük teljes körű átlátásához és a kiberbiztonság vizsgálatával és tesztelésével kapcsolatos kockázatok kezeléséhez.

Tervbe van véve egy harmadik ellenőrzés is ebben a sorozatban. Emellett a holland kormány információbiztonsági szintje az évenkénti megfelelőség-ellenőrzési ciklus egyik alapvető eleme. Az évek során a holland számvevőszék azt tapasztalta, hogy számos minisztériumnál színvonalon aluliak az információbiztonsági intézkedések. Jelenleg a számvevőszék arra törekszik, hogy a kiberbiztonsági ellenőrzései során szerzett tapasztalatait felhasználva kiszélesítse látókörét az információbiztonság ellenőrzése terén, és ne csak a dokumentumokat és szabályzatokat vizsgálja, hanem az intézkedések tényleges eredményességét is tesztelje.

A területet érintő további jelentések

A jelentés címe:	A „Staat van de rijksverantwoording 2019” 3. fejezete
Link a jelentéshez:	Jelentés (holland nyelvű változat)
A közzététel időpontja:	2020

A jelentés címe:	Középpontban a digitális otthoni munkavégzés
Link a jelentéshez:	Jelentés (holland nyelvű változat)
A közzététel időpontja:	2020

Lengyelország
Najwyższa Izba Kontroli

A közfeladatok ellátásához használt informatikai rendszerek biztonságos működésének biztosítása

A közzététel időpontja: 2016

Link a jelentéshez: Jelentés (lengyel nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Szabályszerűségi ellenőrzés

Ellenőrzött időszak: 2014–2015

A jelentés összefoglalása

Az ellenőrzés tárgya

Az ellenőrzés annak értékelésére irányult, hogy az ellenőrzött egységeknél a fontos közfeladatok végrehajtására szolgáló rendszerekben gyűjtött adatok biztonságban vannak-e. Az ellenőrzés hat kiválasztott intézményre terjedt ki, amelyek jelentős közfeladatokat látnak el. Elemzés nyomán mindegyik intézménynél kiválasztottak egy-egy alapvető informatikai rendszert, amelyet azután részletesen megvizsgáltak.
Az ellenőrzés során a COBIT (az informatikára és a kapcsolódó technológiára vonatkozó ellenőrzési célkitűzések) módszer 4.1 verzióját alkalmazták.

Az ellenőrzésre „Az állami szervek teljesítménye a kiberbiztonsági feladatok ellátása terén Lengyelországban” című 2015. évi ellenőrzést[67] követően került sor, amelynek megállapításai rendszerszintű problémákra mutattak rá. A 2016. évi ellenőrzés egyebek mellett kimutatta, hogy az államigazgatás mindaddig nem tett lépéseket az információtechnológiai biztonság nemzeti szintű szavatolása érdekében. Megállapították, hogy az állami szervek széttagoltan, szisztematikus megközelítés

[67] https://www.nik.gov.pl/kontrole/P/14/043/

nélkül hajtották végre a kibertér védelmével kapcsolatos tevékenységeiket. Mivel nem léteztek központi rendelkezések annak biztosítására, hogy az állam működtetéséhez nélkülözhetetlen specifikus informatikai rendszerekre konkrét biztonsági követelmények vonatkozzanak, az ellenőrzés annak vizsgálatát célozta, vajon a fontos közfeladatok ellátásához használt informatikai rendszereket üzemeltető intézmények gondoskodtak-e arról, hogy ezeket a feladatokat biztonságosan végre lehessen hajtani.

2019-ben jóváhagytak egy másik, kiberbiztonsággal kapcsolatos rendszerellenőrzést, „A kiberbiztonság Lengyelországban” címmel, annak megállapításai azonban bizalmasak.

Az ellenőrzés során vizsgált kérdések

A részcélokat két értékelési területre osztották fel, amelyek konkrét kérdésekre kerestek választ.

Az információtechnológiai biztonság támogatásának területén az ellenőrzés a teljes szervezet szintjén vizsgálta többek között azt, hogy:

- adott-e az informatikai biztonság irányítása;
- végrehajtanak-e terveket az informatikai biztonság szavatolására irányulóan;
- sor kerül-e az informatikai biztonság tesztelésére, felügyeletére és nyomon követésére;
- meghatározzák-e az informatikai biztonsággal kapcsolatos incidenseket;
- titkosítási kulcsokkal igazgatják-e az információtechnológiát;
- alkalmaznak-e a kártékony szoftverekkel szemben, illetve azok felderítéséhez védelmet, valamint patchelést;
- biztosított-e a hálózatbiztonság.

A biztonsági támogatás területén az ellenőrzés a kiválasztott rendszerek szintjén vizsgálta többek között azt, hogy:

- kezelik-e a felhasználók személyazonosságát és fiókjait;
- védve vannak-e a biztonsági technológiák és az érzékeny adatok.

Megállapítások és következtetések

Az információbiztonsági rendszer készültségi foka és végrehajtása nem szavatolta megfelelő szinten a fontos közfeladatok elvégzésére használt informatikai rendszerekben gyűjtött adatok biztonságát. Az információbiztonsági folyamatokat rendezetlenül, eljárások hiányában intuitív módon hajtották végre. A hat ellenőrzött egység közül mindössze egy vezetett be információbiztonsági rendszert, és meg kell jegyezni, hogy annak működésénél is jelentős hibák fordultak elő. Egy kivételével az összes ellenőrzött egységnél azt állapították meg, hogy nem biztosították megfelelően az informatikai rendszerekben kezelt információkra vonatkozó biztonsági feltételeket, mivel a vonatkozó munka csak nemrégiben indult el és még csak az előzetes szakaszban tartott, azaz éppen folyamatban volt a szükséges formális alapok lefektetése. Korábban ugyanis egyszerűsített vagy informális rendelkezésekre támaszkodtak, a bevált gyakorlatokra vagy az informatikai személyzet addigi tapasztalataira építve.

A COBIT 4.1. módszertan szerint az információbiztonság irányítási folyamatának érettsége a különböző ellenőrzött egységek esetében az (1) „kezdeti/*ad hoc*” és a (3) „meghatározott” között mozgott egy nullától ötig terjedő skálán, ahol az ötös a legmagasabb.

Az ellenőrzött egységeknél az informatikai biztonság szavatolásáért a biztonsági koordinátor felel, aki azonban a gyakorlatban nem rendelkezett hatáskörrel a folyamat egészének irányításához. Emellett a vonatkozó feladatokat gyakran egyetlen személy hajtotta végre. Bár kijelöltek szakemberekből álló csoportokat, illetve megállapodásokat kötöttek külső szerződő felekkel, nem végezték el az annak megállapításához szükséges elemzést, hogy a nyújtott szolgáltatások megfeleltek-e az adott egység biztonsági igényeinek. Az ellenőrzött szerv töredékesen és korlátozottan látta át az informatikai biztonság szavatolásának szükségességét. Az adatbiztonságot elsősorban az informatikai osztály felelősségi körének és területének tartották, nem pedig valamennyi, törvény által előírt feladatokat végző szervezeti egységének, ami nagyban akadályozta, hogy koherens informatikai biztonságkezelési rendszereket dolgozzanak ki az intézmény egésze számára.

Ha összehasonlítjuk, milyen minőségben teljesültek az információbiztonság szavatolásával kapcsolatos kötelezettségek a szervezetek egészét, illetve a kiválasztott rendszereket tekintve, egyértelműen kitűnik, hogy a végrehajtás minősége a második esetben jobb volt. Ez adódhat abból, hogy milyen hatással van a biztonság szavatolására a középszintű műszaki személyzet gyakorlati tudása és közreműködése,

valamint abból, hogy a közigazgatásban fokozottabban használtak piaci szabványokon alapuló kereskedelmi informatikai rendszereket és fejlett biztonságbiztosítási megoldásokat. E megoldások, a múltbéli tapasztalatok és a bevált gyakorlatok alkalmazása révén annak ellenére fenn lehetett tartani bizonyos szintű biztonságot a különféle rendszerek működtetésénél, hogy korlátozottan álltak rendelkezésre erőforrások, szervezeti hiányosságok voltak tapasztalhatók, illetve „nem működött” egy-egy rendelkezés. Ez azonban nem lehet a megcélzott megoldás, mivel a fenyegetettségi szint dinamikus növekedésének idején az informatikai rendszerek biztonsága nem alapulhat rendszertelenül irányított és csupán a pillanatnyi nehézségek leküzdésére irányuló intézkedéseken.

Az ellenőrzés során levont következtetések

Központi szinten általános informatikai biztonsági ajánlásokat és követelményeket kell kidolgozni és végrehajtani, amelyek valamennyi állami szervre alkalmazandók. Rendszerszintű megoldásra van szükség, amelynek keretében az informatikai biztonságra irányuló ellenőrzések eredményeit nyilvánosságra hozzák oly módon, hogy a polgárok hozzáférhessenek a közigazgatási intézmények tevékenységeivel kapcsolatos információkhoz, miközben az információk biztonságának szavatolása céljából alkalmazott intézkedésekkel és módszerekkel kapcsolatos ismeretekhez való hozzáférés korlátozott.

A területet érintő további jelentések

A jelentés címe:	Az információbiztonság irányítása a regionális hatóságoknál
Link a jelentéshez:	Jelentés (lengyel nyelvű változat)
A közzététel időpontja:	2019

A jelentés címe:	A kiberbiztonság Lengyelországban (minősített információ)
Link a jelentéshez:	*Nyilvánosan nem hozzáférhető*
Jóváhagyás dátuma:	2019

A jelentés címe:	Az informatikai rendszerek biztonságának szavatolása Podlaskie vajdaság regionális hatóságainál
Link a jelentéshez:	Jelentés (lengyel nyelvű változat)
A közzététel időpontja:	2018

A jelentés címe:	Az internetes megfélemlítés megelőzése és felszámolása a gyermekek és a fiatalok körében
Link a jelentéshez:	Jelentés (lengyel nyelvű változat)
A közzététel időpontja:	2017

A jelentés címe:	Az állami szervek teljesítménye a kiberbiztonsági feladatok ellátása terén Lengyelországban
Link a jelentéshez:	Jelentés (lengyel nyelvű változat)
A közzététel időpontja:	2015

A jelentés címe:	Az információs rendszerekre, az elektronikus információcserére és a nemzeti interoperabilitási keretrendszerre vonatkozó kiválasztott követelmények végrehajtása egyes települési tanácsok és járási jogú városok példája alapján
Link a jelentéshez:	Jelentés (lengyel nyelvű változat)
A közzététel időpontja:	2015

Portugália
Tribunal de Contas

Ellenőrzés a portugál elektronikus útlevélről

Közzététel időpontja: 2014

Link a jelentéshez: Jelentés (portugál nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2013

A jelentés összefoglalása

Az ellenőrzés tárgya

A portugál elektronikus útlevél (PEP) operatív ellenőrzése azon információs rendszerek eredményességére irányult, amelyek támogatják a PEP odaítélését, kibocsátását és használatát, utóbbi esetében különösen az utasok automatizált szűrése során, a biometrikus adatok portugál határokon történő leolvasásánál[68].

A fő ellenőrzési célok a következők voltak:

- az uniós és a nemzeti jognak, a nemzetközi szabványoknak, valamint a PEP megadására, kibocsátására és használatára vonatkozó iránymutatásoknak való megfelelés vizsgálata, beleértve a nemzeti jogi keret megfelelőségét;

[68] Itt a Frontex (az Európai Határ- és Partvédelmi Ügynökség) keretén belüli automatizált határellenőrzési rendszerre utalunk.

- a PEP életciklusához kapcsolódó alapvető folyamatok eredményességének értékelése, különös tekintettel azokra, amelyek a PEP odaítéléséhez, kibocsátásához és használatához kapcsolódnak;
- az információs rendszerek teljesítőképességével kapcsolatos kritikus szempontok vizsgálata, különös tekintettel a PEP információs rendszereivel (SIPEP) kapcsolatos biztonsági követelmények teljesítésére.

Az alapvető kockázati területek közé tartoztak a következők:

- fizikai eszközök és/vagy elektronikus információk elvesztése/ellopása;
- bizalmas adatokkal való visszaélés;
- megfelelési kockázat (a jogi és szabályozási követelményeknek való megfelelés hiánya).

Ellenőrzött időszak: 2013. január 1. – 2013. december 31. (adott esetben kiterjeszthető korábbi és későbbi évekre)

Megállapítások és következtetések

A portugál elektronikus útlevél (PEP) három kategóriát fed le: általános[69], diplomáciai és speciális. Ezenkívül létezik egy útlevél a portugál állampolgársággal nem rendelkezők számára, amely korlátozott privilégiumokat biztosít.

Az útlevél kiadásának rendszere több kérelmet és több adatgyűjtő szervet, valamint az útlevél megadásáról döntő testületet foglal magában, de csupán egy kibocsátót (amely magában foglalja az elkészítést, a személyre szabást és a kézbesítést).

[69] Az összes útlevél mintegy 99%-a.

A folyamatban több szerv (PEP-szerv) vesz részt. Az alábbi szervek gyűjtenek adatokat és ítélnek oda útleveleket:

- Portugália kontinentális területei: a Serviço de Estrangeiros e Fronteiras (SEF)[70], valamint az Instituto dos Registos e do Notariado (IRN) nyilvántartási szolgálatai[71];
- Azori-szigetek[72] és Madeira autonóm régiók: az adott *Vice-Presidência do Governo Regional*[73] alá tartozó szolgálatok; külföldön: a portugál konzulátusok.
- Az útleveleket az Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] adja ki és kézbesíti.

A főbb folyamatokat nagyrészt a SIPEP (a portugál útlevelek kibocsátásához alkalmazott központi igazgatási rendszer) támogatja. A SIPEP lehetővé teszi a PEP megadásához kapcsolódóan szükséges információk nyilvántartásba vételét, tárolását, feldolgozását, validálását és biztosítását, elindítja az INCM által végzett személyreszabási folyamatot, valamint biztosítja az egyéb rendszeralkalmazásokkal való kapcsolatot, koordinálva a gyűjtött adatok fizikai és logisztikai nyilvántartásba vételében közreműködő valamennyi PEP-szervet.

A PEP-szervek olyan szervezeti felépítéssel rendelkeznek, amely lehetővé teszi számukra a PEP-hez kapcsolódó jogi célok megvalósítását. A rendszer a kérelmezés és a gyűjtés szintjén továbbra is nagyban támaszkodik az emberi erőforrásokra. Ugyanakkor a SIPEP számos automatizált feldolgozási funkcióval és validációs ellenőrzéssel rendelkezik.

Mivel az eljárások különféle kontrollfunkciókat és adatkezeléseket tesznek lehetővé, amelyek közül néhányat emberi beavatkozás nélkül, önállóan végre lehet hajtani, a SIPEP-nek jelentős hatása van a szerveződés és az információs rendszer tekintetében,

---

70 Bevándorlási és határvédelmi szolgálat.

71 Nyilvántartó Hatóság és Közjegyzőség (csak fogadás).

72 Valamint az *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – az állampolgároknak nyújtott szolgáltatások korszerűsítéséért és minőségéért felelős hivatal (közintézmény) – ügyfélszolgálati pontjai (csak fogadás).

73 A regionális kormány alelnöki hivatala.

74 Állami nyomda és pénzverde részvénytársaság.

különösen az alábbiakat illetően: i. a standardok, a folyamatok és a szükséges adatok értelmezése és meghatározása; valamint ii. az információs rendszer saját követelményeinek meghatározása.

Az adatgyűjtési folyamat hatékonyságát és eredményességét a SIPEP és más információs rendszerek[75] közötti interakció biztosítja a jogi rendelkezéseknek megfelelően.

Bár nem dokumentálták alaposan, kialakítottak egy keretrendszert az informatikai tevékenységek átfogó ellenőrzéséhez (irányítás, fejlesztés és beszerzés, informatikai műveletek, üzletmenet-folytonosság és katasztrófa utáni helyreállítás, információbiztonság), amely biztosítja a SIPEP rendszer fejlesztését, működését, igazgatását és karbantartását.

Tevékenységi mutatók (2013):

- Mintegy 500 000 PEP odaítélésére került sor, 63%-ban a SEF, 33%-ban a portugál konzulátusok és 4%-ban a regionális kormányok által.
- A PEP kibocsátásából összesen mintegy 37 millió euró bevétel származott, elsősorban az INCM (43%), a SEF (32%) és a *Ministério dos Negócios Estrangeiros (MNE)*[76] (17%) révén.

2013-ra vonatkozóan a SIPEP-ben elvégzett tesztek nem erősítették meg a jogilag meghatározott maximális kézbesítési idő betartását (a kérelmezés időpontjától addig az időpontig terjedő időintervallum, amikor a PEP átvehető a kézbesítőponton), mivel a kézbesítőponton történő tényleges kézbesítés időpontját nem minden esetben vették időben nyilvántartásba.

[75] Nevezetesen: a SEF integrált információs rendszere (SIISEF), a Schengeni Információs Rendszer „nemzeti része” (NSIS), polgári azonosítási adatbázis, bűnügyi nyilvántartások adatbázisa.

[76] Külügyminisztérium.

A biometrikus adatok és az aláírások felvételéhez szükséges berendezések (kioszkok) és az automatizált határellenőrzést (ABC) szolgáló berendezések beszerzésével, valamint az informatikai rendszerek, szolgáltatások és műszaki támogatás megvásárlásával és karbantartásával kapcsolatban a SEF, az MNE, a RIAC és az INCM 11 millió euró összegben hajtott végre beruházásokat; a legtöbbet a SEF költötte.

A PEP előtt a Portugál Köztársaság (nem biometrikus) útlevele 22,44 euróba került; 2006-ban az általános (biometrikus) PEP ára 60 euró volt, ami 2011-ben 65 euróra emelkedett.

A PEP kérelmezése

A PEP iránti kérelmeket személyesen dolgozzák fel az illetékes szolgálatok, amelyek fogadják a kérelmezéshez szükséges dokumentumokat, összegyűjtik a kérelmezők életrajzi és biometrikus adatait, beszedik a díjakat, és később átadják a kiadott elektronikus útleveleket.

Az alapul szolgáló rendszer (SIPEP) virtuális ellenőrzések és más információs rendszerekkel (különösen a polgári azonosítási adatbázissal) való megfeleltetések segítségével validálja az adatok helyességét és minőségét, megbizonyosodva arról, hogy a kérelem megfelelő és alkalmas a PEP odaítélésére és kibocsátására.

A kapcsolódó státuszváltozásokat naplófájlokban feljegyzik, biztosítva a műveletek ellenőrizhetőségét, integritását és letagadhatatlanságát.

Az adatoknak a (portugáliai és külföldi) adatgyűjtő szervek és a SEF közötti átadása virtuális magánhálózaton (VPN) keresztül történik, amelyet a SEF által ellenőrzött hitelesítési adatoknak megfelelően hozzáférés-kezelés alapján hajtanak végre[77].

Az általános PEP iránti kérelmet eltérően dolgozzák fel, ha olyan polgár nyújtja be azt, akinek jogai korlátozva vannak vagy le vannak szűkítve, ideértve: i. azokat, akik nem tudják gyakorolni jogaikat (kiskorúak, cselekvőképtelen vagy kizárt személyek); ii. az igazságszolgáltatás vagy a rendőrség által kizárt személyeket (büntetett előélet, folyamatban lévő eljárás vagy okmányok lefoglalása); valamint azt az esetet, ha egy második PEP-et kérelmező személy nemzeti vagy jogos érdekre hivatkozik.

[77] A SIPEP-hez (az interneten keresztül) nemzeti/regionális és nemzetközi szinten a kontinentális Portugáliában, az Azori-szigetek és Madeira autonóm régiókban, valamint külföldön (a portugál konzulátusokon) működő szolgálatok férnek hozzá.

A PEP odaítélése

Az általános PEP odaítéléséről történő határozathozatal lehet:

- Automatikus – automatikus jóváhagyás a SIPEP kérelemkezelő rendszere által a kérelmező személyazonosságának validálását követően és amennyiben a személy (az IRN polgári azonosítási adatbázisával és a bűnügyi nyilvántartásokkal történő egyeztetés alapján) nem szerepel a bűnügyi nyilvántartásban és nincs folyamatban lévő büntető eljárás ellene. Erre csak a SEF-nél, a kontinentális Portugáliában benyújtott PEP-kérelmek esetében kerül sor[78].

- Egyéb szervek (regionális kormányok és konzuli hivatalok) általi egyedi elfogadás/jóváhagyás tárgya vagy – a SEF esetében – az automatikus odaítélés körébe nem tartozó követelmények függvénye[79].

A PEP kibocsátása

A PEP kibocsátása – ami magában foglalja az elkészítést, a személyre szabást és a kézbesítést – az INCM hatáskörébe tartozik. Amikor a PEP kézbesítését nyilvántartásba vették a SIPEP-ben, az útlevél státusza „érvényes”-re változik.

A PEP díjai a szükséges szolgáltatási szinttől függően eltérőek. A szolgáltatás szintjének méréséhez a SIPEP-nek tekintetbe kell vennie a PEP tényleges kézbesítési idejét.

A PEP kézbesítését egy megbízott fuvarszolgálat végzi.

---

[78] Ez egy automatizált funkció a SIPEP kérelemkezelő rendszerében a kérelem olyan személyek számára történő megadására (belső nevén „engedélyezésére”) irányulóan (a második PEP kivételével), akik betöltötték a törvényi korhatárt, érvényes személyi igazolvánnyal rendelkeznek, akikkel kapcsolatban nincs folyamatban lévő büntető eljárás, és akik nincsenek eltiltva vagy kizárva. A SEF által megadott általános PEP-ek mintegy 60%-a automatikus validálási eljárások és jóváhagyó határozatok alá tartozott, a többit a *Direção Central de Imigração e Documentação (DCID)* vizsgálta meg és hagyta jóvá.

[79] Különösen olyan kérelmezők esetében, akik nem képesek jogaik gyakorlására (kiskorúak, cselekvőképtelen vagy kizárt személyek), az igazságszolgáltatás vagy a rendőrség által kizárt személyek, vagy – második PEP esetén – akiknek kérelmét a DCID eseti alapon bírálja el.

A PEP megsemmisítése

Amennyiben egy kérelmező egy korábbi, még érvényes PEP-et nyújt be, azt az újbóli felhasználás megakadályozása érdekében a SIPEP kérelemkezelési rendszerben használhatatlanná kell tenni, így az útlevél „nem használható” nyilvántartási státuszt kap.

Finnország
Valtiontalouden tarkastusvirasto

Kibervédelmi intézkedések

Közzététel időpontja: 2017

Link a jelentéshez: Jelentés (finn nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2016–2017

A jelentés összefoglalása

Az ellenőrzés tárgya

Az ellenőrzés azt vizsgálta, hogy a lehető legeredményesebb és legköltséghatékonyabb módon alakították-e ki a központi kormányzat kibervédelmét. Az ellenőrzés középpontjában a központi kormányzat kiberbiztonságának szervezési és irányítási módja állt. Az ellenőrzés eredményeit fel lehet használni a kiberbiztonság központi kormányzaton belüli eredményességének és hatékonyságának fejlesztéséhez.
Az ellenőrzést 2016. szeptember 22. és 2017. szeptember 4. között folytatták le.
A hasznosulásvizsgálatra 2019 őszén került sor. Ennek során a nemzeti számvevőszék megvizsgálta az ellenőrzés észrevételei és ajánlásai nyomán meghozott intézkedéseket.

Az ellenőrzött szervezetek közé tartoztak a központi kormányzat kibervédelméért felelős hatóságok (a Miniszterelnöki Hivatal, a Pénzügyminisztérium, valamint a Közlekedési és Kommunikációs Minisztérium), továbbá a központi kormányzaton belüli központosított kibervédelmi feladatokért és központosított információtechnológiai szolgáltatásokért felelős hatóságok (a finn Közlekedési és Kommunikációs Hivatal Nemzeti Kiberbiztonsági Központja, a Valtori kormányzati IKT-központ, valamint a

Digitális és Népességi Adatszolgáltatási Ügynökség). Az iránymutatás eredményességének értékelését célozta továbbá az elektronikus szolgáltatásokat nyújtó központi kormányzati egységek vizsgálata (a Digitális és Népességi Adatszolgáltatási Ügynökség, a finn Traficom Közlekedési és Kommunikációs Hivatal, a Nemzeti Igazgatási Végrehajtási Hivatal és az azt felügyelő Igazságügyi Minisztérium, valamint az Igazságügyi Minisztérium IKT-szolgáltatási központja).

Az ellenőrzés során vizsgált kérdések

A kiberbiztonság felépítésének ellenőrzése során az alábbi kérdésekre keresték a választ:

- Kellően figyelembe vette-e az ellenőrzött szerv a gazdasági szempontokat a kiberbiztonság megszervezésénél?
- Támogatja-e az ellenőrzött szerv kiberbiztonsági helyzetismerete a rendszerek kiberbiztonságát?
- Kellően képes-e reagálni az ellenőrzött szerv a számítógépes visszaélésekre?

A kibervédelmi intézkedések ellenőrzési témája a finn nemzeti számvevőszék 2016–2020 közötti ellenőrzési tervében foglalt egyik témakör, „Az információs társadalom működési megbízhatóságának biztosítása” részét képezte. A központi kormányzat pénzügyei tekintetében fennálló jelentőség szempontjából az ellenőrzési témát indokolják a szolgáltatás megszakadásához és az adatvédelmi incidensekhez kapcsolódó hátrányok, valamint a gyenge kiberbiztonságnak az üzleti tevékenységekre gyakorolt negatív hatása. Az ellenőrzés az ugyanezen témakörbe tartozó, „Az elektronikus szolgáltatások működési megbízhatóságának irányítása” című ellenőrzéssel párhuzamosan zajlott. Az ellenőrzés alapvetően a szóban forgó tevékenységért felelős hatóságok dokumentumain és a velük készített interjúkon alapult.

Megállapítások és következtetések

Finnország kiberbiztonsági stratégiája meghatározza az ahhoz szükséges alapvető célkitűzéseket és politikákat, hogy meg lehessen felelni a kiberkörnyezetet érő kihívásoknak, és biztosítani lehessen annak működését. A kiberbiztonsági stratégiát egy végrehajtási program révén valósítják meg; az előrehaladást évente értékelik.

A Védelmi Minisztériumon belül működő Biztonsági Bizottság egy együttműködési testület, amely nyomon követi és koordinálja a kiberbiztonsági stratégia végrehajtását.

A kiberbiztonság hathatós megszervezése kockázatkezelési tevékenység, amelynek sikerességéhez olyan eredményes irányítási struktúrákra és rendelkezésekre van szükség, amelyek a szervezet minden szintjén beépítik a műveletekbe a kockázatkezelést. Számos más országhoz hasonlóan Finnország és központi kormányzata sem önellátó a kibervédelmi erőforrások tekintetében. Az európai uniós jogszabályok az idők során erősödtek és egyre inkább kötelező erejűvé váltak.
A finn kormányon belül a kibervédelemért viselt felelősség decentralizált, minden egyes szerv a saját kiberbiztonságáért felel. A központi kormányzaton belül a felelősségi körök kijelölése igen összetett, figyelemmel a lehetséges számítógépes visszaélések jellegére, kiterjedésére és végrehajtására.

Bonyolult volta miatt előfordulhat, hogy az anomáliára túl lassan reagálnak, a finanszírozás szűkössége pedig korlátozza a finn kiberbiztonsági stratégia végrehajtását. Az ellenőrzés megállapításai alapján a nemzeti számvevőszék az alábbi következtetésekre jutott és az alábbi ajánlásokat tette a kiberbiztonság központi kormányzaton belüli szerveződésére vonatkozóan:

Nem határozták meg a kiterjedt kiberbiztonsági visszaélések operatív kezelését

A kiterjedt kiberbiztonsági visszaélések operatív kezelésének megtervezése és a vonatkozó felelősségi körök felosztása lehetővé tenné a gyorsabb reagálást, valamint az ellenintézkedések megfelelő koordinálását és az erőforrások megfelelő elosztását. A jelenlegi működési modellben minden egyes hivatal a saját kibervédelméért felel. Ugyanakkor nem áll rendelkezésre elegendő szakértelem a kibervédelem terén, ami meggátolja a kibervédelem házon belüli vagy kiszervezés révén történő kialakítását.

A kiberbiztonsági stratégia egyes céljai nem teljesültek

A finn kiberbiztonsági stratégia végrehajtási programja révén javult a kibervédelem. Az első végrehajtási program egyes céljai ugyanakkor nem teljesültek, mivel a fellépések iránti elkötelezettség eltérő szintű volt, és nem lehetett központosított módon javítani rajta. Az új végrehajtási program csak olyan fellépéseket tartalmazott, amelyek iránt az illetékes hatóságok és más szereplők kifejezték elkötelezettségüket. Az elkötelezettség és a rendelkezésre álló erőforrások kölcsönösen függtek egymástól.

Nem volt egyértelmű, hogy a kibervédelem finanszírozási megoldásai megfeleltek a célnak

A kibervédelem fejlesztése terén fennálló különbségek részben abból adódtak, hogy eltérő mennyiségben álltak a szervezetek rendelkezésére fejlesztési erőforrások. Az állami költségvetés elkészítéséről szóló rendeletekben vagy az elkészítés folyamán nem azonosítottak olyan eljárásokat, amelyek biztosítanák, hogy a forrásokat a legfontosabb kibervédelmi célokhoz rendeljék hozzá. A hivatalok és az intézmények az adott hivatal vagy intézmény igazgatási kiadásainak meg nem határozott részeként vették fel a költségvetésbe a kiberbiztonságra szánt előirányzatokat. A finn kiberbiztonsági stratégiában leírt intézkedéseket csak annyiban hajtották végre, amennyiben azt az előirányzatok lehetővé tették.

A kibervédelmet az IKT szerveződésével kapcsolatos változásoknál is figyelembe kellene venni

Az IKT központi kormányzaton belüli szerveződésében bekövetkezett változások hatással voltak a kibervédelmi intézkedésekre. A Valtori által központosított kiberbiztonsági fejlesztés nehéznek bizonyult. Hiányosságok jellemezték a gyakorlati kibervédelmi eljárások megfelelőségének értékelését és az új intézkedések végrehajtását.

Javítani kellene a kiberbiztonsági műveletekkel kapcsolatos helyzetismeretet

A Kiberbiztonsági Központ országos szinten nyomon követte a kiberbiztonsággal kapcsolatos fejleményeket. Az ellenőrzés idején azonban nem volt kötelező jelenteni a Kiberbiztonsági Központ felé a kiberbiztonsági visszaéléseket. A helyzetet javítaná egyrészt annak előírása, hogy a kormányzati szervezeteknek jelenteniük kell a visszaéléseket, másrészt a számítógépes visszaélések felderítését szolgáló központosított eljárások lefedettségének növelése.

A fenti megállapítások alapján a nemzeti számvevőszék javasolta, hogy a Pénzügyminisztérium határozzon meg és hajtson végre egy kiterjedt operatív irányítási modellt arra az esetre, ha kiberbiztonsági események következnének be a központi kormányzat információtechnológiai szolgálatainál. A Pénzügyminisztériumnak emellett fel kell tárnia, miként kellene figyelembe venni a szolgáltatások kiberbiztonságát a szolgáltatások egész életciklusuk alatti finanszírozása tekintetében, valamint javítania kell operatív helyzetismeretét azáltal, hogy utasítja a hatóságokat a számítógépes visszaélések Kiberbiztonsági Központ felé történő jelentésére. Javasolták, hogy a

Valtori javítsa a kiberbiztonsági eljárások végrehajtását, értékelését és fejlesztését, valamint a számítógépes visszaélések felderítését.

A hasznosulásvizsgálat során megvizsgálták, miként hajtották végre az ellenőrzés során kiadott ajánlásokat. A számvevőszék megállapította, hogy a Pénzügyminisztérium – mint az ajánlások végrehajtásáért felelős illetékes hatóság – nem hozott elegendő intézkedést a megtett ajánlások nyomán. Ugyanakkor a kiberbiztonságot a Pénzügyminisztériumon kívüli hatóságok által hozott intézkedések révén is erősítették Finnországban. Folyamatban volt a kiberbiztonság stratégiai irányításának átállítása a kiberbiztonsági igazgatói modellre. 2020-ra vonatkozó költségvetési javaslatában a kormányzat növelte a kiberbiztonság erősítésében kulcsszerepet játszó központi kormányzati hatóságok számára biztosított előirányzatokat. Emellett a Valtori intézkedéseket hozott a nemzeti számvevőszék ajánlásával összhangban. Összegezve, a nemzeti számvevőszék megállapította, hogy a végrehajtásra váró ajánlások miatt további hasznosulásvizsgálatokra lesz szükség, emellett indokolt egy teljesen új ellenőrzés ezen a területen, tekintettel a kiberbiztonsági intézkedések és a digitális működési környezet folyamatban lévő változásaira és a kapcsolódó kockázatokra, valamint arra, hogy milyen jelentőséggel bír a kiberbiztonság a központi kormányzat pénzügyeire és a társadalomra nézve.

Svédország
Riksrevisionen

Elavult informatikai rendszerek – az eredményes digitalizáció akadálya

Közzététel időpontja: 2019

Link a jelentéshez: A jelentés összefoglalója (angol nyelvű változat)
Jelentés (svéd nyelvű változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Teljesítmény-ellenőrzés

Ellenőrzött időszak: 2018–2019

A jelentés összefoglalása

Az ellenőrzés tárgya

Az ügymenet szempontjából kritikus, ám elavult informatikai rendszerek jelentős hatékonysági kockázatot vetnek fel, mivel a szervezetek arányaiban több erőforrást kénytelenek fordítani pusztán a rendszer fenntartására. Ezért okkal feltételezhető, hogy az elavult informatikai rendszerek esetében nagy a rossz közpénzgazdálkodás kockázata. Ezenkívül az új informatikai rendszerek kifejlesztése bizonyos mértékben a hivatal innovációs kapacitását is lefoglalja. Ráadásul az elavult informatikai rendszerek nem csupán az érintett hivatalok számára jelentenek kockázatokat: az egy adott hivatalnál jelentkező problémák jelentős következményekkel járhatnak a tekintetben is, hogy az képes-e összehangolni műveleteit más hivatalokkal és a magánszférabeli érdekelt felekkel. Az elavult informatikai rendszerek emellett információbiztonsági szempontból is kockázatokat hordoznak.

Az ellenőrzés fő tárgyának meghatározása / Az ellenőrzés során vizsgált kérdések / Háttér

Az ellenőrzés az elavult információtechnológiai rendszerek központi kormányzati igazgatáson belüli előfordulását volt hivatott vizsgálni, értékelve, hogy megfelelő intézkedéseket hoztak-e a hatóságok és a kormány annak megelőzésére, hogy ezek a rendszerek akadályozzák az eredményes digitalizációt. Az ellenőrzés során a következő kérdéseket vizsgálták:

- Megfelelő intézkedéseket hoztak-e a hatóságok az elavult informatikai rendszerekhez kapcsolódó problémák kezelésére?
- Megfelelő intézkedéseket hozott-e a kormány az elavult informatikai rendszerekhez kapcsolódó problémák kezelésére?

Megállapítások és következtetések

- Az ellenőrzés rámutatott arra, hogy számos kormányzati hivatalnál vannak elavult információtechnológiai rendszerek. Sok hivatalnál ráadásul az ügymenet szempontjából kritikus jelentőségű informatikai rendszerek között is voltak elavultak. A svéd nemzeti számvevőszék tudomása szerint ez új információ, és korábban a központi kormányzati igazgatásban senki nem tudott a probléma mértékéről. A hivatalok mintegy 80%-a állította azt, hogy nehéznek találta fenntartani az információbiztonságot egy vagy több olyan rendszerben, amely az ügymenet szempontjából kritikus jelentőségű. A hivatalok több mint egytizede válaszolta azt, hogy ez a rendszerek mindegyikére vagy többségére igaz.
- A vizsgált hivatalok jelentős része nem alkalmazott megfelelő megközelítést az információtechnológiai támogatás fejlesztése és igazgatása tekintetében. Nem használták a meglévő operatív fejlesztési eszközöket annak meghatározásához, hogy miként járulhatna hozzá leginkább az informatikai támogatás az alapvető műveletek célkitűzéseinek megvalósításához. Az ellenőrzött hivatalok nagy része ezért nem rendelkezett arra vonatkozó általános leírással, hogy miként kapcsolódnak egymáshoz a stratégiák, az operatív folyamatok és a rendszerek. Ezáltal viszont nehézséget okozott számukra annak elemzése és megértése, hogy miként hatottak a változások a szervezet célkitűzéseire, ezért pedig nehezebb volt meghatározni a kívánatos jövőbeni helyzetet.

- A hivatalok több mint fele állította, hogy nem létezett jóváhagyott modell az informatikai rendszereik fejlesztési szakasztól a kivezetésig történő kezelését és a vonatkozó döntéshozatalt illetően (közismert nevén életciklus-menedzsment). A svéd nemzeti számvevőszék szerint ez arra utalt, hogy nem került sor strukturált és módszeres életciklus-menedzsmentre. Emellett hiányosságok voltak a kockázatelemzési tevékenység és az arra való képesség tekintetében is, hogy a megalapozott döntéshozatalhoz szükséges részletes szintre lebontsák az informatikai költségeket.

- A hatóságok közel 60 százaléka – egy vagy néhány, az ügymenet szempontjából kritikus jelentőségű rendszer kivételével – egyetlen rendszer vonatkozásában sem rendelkezett a rendszerfejlesztés életciklusára vonatkozó tervekkel. Abból adódóan, hogy számos hivatalnál hiányoztak az életciklusra vonatkozó tervek és más programozási dokumentumok, emellett hiányosságok mutatkoztak a ténylegesen elvégzett életciklus-menedzsment tekintetében, általában véve nem tekinthető úgy, hogy a hivatalok tudatos, kifejezett álláspontot alakítottak volna ki informatikai rendszereikkel kapcsolatban.

- A svéd nemzeti számvevőszék értékelése szerint az érintett minisztériumok – és ezáltal a kormány – nem rendelkeztek megfelelő ismeretekkel az elavult informatikai rendszerek előfordulására és következményeire vonatkozóan.

Az általános következtetés az volt, hogy az ellenőrzés idején a legtöbb hivatalnak nem igazán sikerült eredményesen kezelnie az elavult informatikai rendszerekkel összefüggő problémákat. A svéd számvevőszék véleménye szerint a probléma olyan súlyos és olyan kiterjedt volt, hogy akadályozta az államigazgatás további eredményes digitalizálását. Az ellenőrzés ezenkívül rámutatott arra, hogy a kormány nem tudott az elavult informatikai rendszerekkel kapcsolatos problémák fennállásáról és következményeiről. Továbbá a kormány semmiféle intézkedést nem hozott az elavult informatikai rendszerek problémájának közvetlenebb kezelése érdekében. A svéd nemzeti számvevőszék értékelése szerint ezért nem tekinthető úgy, hogy a kormányzat elegendő intézkedést hozott volna a problémák mérséklésére vagy megszüntetésére.

A területet érintő további jelentések

A jelentés címe:	A vállalkozásindítás megkönnyítése – kormányzati erőfeszítések a digitális eljárás előmozdítására (RiR 2019:14)
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (svéd nyelvű változat)
A közzététel időpontja:	2019

A jelentés címe:	A közigazgatás digitalizációja – Egyszerűbb, átláthatóbb és eredményesebb igazgatás (RiR 2016:14)
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (svéd nyelvű változat)
A közzététel időpontja:	2016

A jelentés címe:	Kilenc ügynökség információbiztonsági tevékenysége (RiR 2016:8)
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (svéd nyelvű változat)
A közzététel időpontja:	2016

A jelentés címe:	Kiberbűnözés – a rendőrség és az ügyészek hatékonysága növelhető (RiR 2015:21)
Link a jelentéshez:	A jelentés összefoglalója (angol nyelvű változat) Jelentés (svéd nyelvű változat)
A közzététel időpontja:	2015

Európai Unió
Európai Számvevőszék

Tájékoztató: Az eredményes uniós kiberbiztonsági politika előtt álló kihívások

Közzététel időpontja: 2018

Link a jelentéshez: Jelentés (23 nyelvi változat)

Az ellenőrzés típusa és időszaka

Az ellenőrzés típusa: Szakpolitikai áttekintés

Ellenőrzött időszak: 2018. április–szeptember

A jelentés összefoglalása

Az áttekintés tárgya

Ez a tájékoztató, amely nem ellenőrzési jelentés, áttekintést kíván nyújtani az Unió komplex kiberbiztonsági politikai hátteréről, és kísérletet tesz rá, hogy feltárja az eredményes szakpolitikai megvalósítás előtt álló fő kihívásokat. Tárgyalja többek között a hálózat- és információbiztonság, a kiberbűnözés, a kibervédelem és a félretájékoztatás témáját.

A számvevőszéki elemzés nyilvánosan elérhető hivatalos dokumentumok, állásfoglalások és harmadik felek által készített tanulmányok dokumentumalapú ellenőrzésén alapult. A helyszíni munkára 2018. április és szeptember között került sor, de az áttekintés a 2018 decemberéig bekövetkezett fejleményeket is figyelembe vette. Munkája kiegészítéseképpen a Számvevőszék felmérést végzett a tagállamok nemzeti számvevőszékei körében, valamint interjúkat készített az uniós intézmények fő érdekeltjeivel és a magánszektor képviselőivel.

A kiberbiztonságnak nincsen szabványos fogalommeghatározása. Gyakorlatilag mindazokat az adatok bizalmas kezelésének, sértetlenségének és rendelkezésre állásának biztosítására irányuló biztosítékokat és intézkedéseket értjük alatta, amelyek az információs rendszereknek és azok felhasználóinak az adatokhoz való jogosulatlan

hozzáféréssel, támadásokkal és károkozással szembeni védelmére szolgálnak. A kiberbiztonság csakúgy magában foglalja a kiberbiztonsági események megelőzését és felderítését, mint az azokra való reagálást és a következményeik elhárítását. Ilyen incidensek szándékosan vagy véletlenül is bekövetkezhetnek: az információk véletlen nyilvánosságra hozatala ugyanúgy a fogalom körébe tartozik, mint a vállalkozások és kritikus infrastruktúrák elleni támadások, a személyes adatok eltulajdonítása, vagy akár a demokratikus folyamatokba való beavatkozás.

Az Unió szakpolitikájának sarokköve a 2013. évi kiberbiztonsági stratégia, amelynek célja, hogy az Unió digitális környezete világszinten a legbiztonságosabbá váljon, megóvva ugyanakkor az alapvető értékeket és szabadságokat. A stratégia öt fő célkitűzést követ: i. a kibertámadásokkal szembeni reziliencia fokozása, ii. a kiberbűnözés visszaszorítása, iii. kibervédelmi politikák és kapacitások kialakítása, iv. az ipari és technológiai kiberbiztonsági erőforrások fejlesztése, valamint v. az alapvető uniós értékekkel összehangolt nemzetközi kibertér-politika kialakítása.

Megállapítások

A megbízható adatok hiánya miatt nehéz volt megállapítani, hogy mekkora hatással jár a kibertámadásokra való felkészültség elégtelensége. A kiberbűnözés gazdasági hatása 2013 és 2017 között ötszörösére emelkedett, és a kormányzatokat csakúgy sújtotta, mint a kis- és nagyvállalatokat. Ezt a tendenciát tükrözi, hogy a kiberbiztosítási díjak a 2018. évi 3 milliárd euróról 2020-ra várhatóan 8,9 milliárd euróra emelkednek. Bár 2016-ban az uniós vállalkozások 80%-a tapasztalt legalább egy kiberbiztonsági incidenst, a kockázatok felismerése még mindig riasztóan alacsony szintű. Az uniós vállalkozások 69%-a egyáltalán nem tud vagy csak alapvető ismeretekkel rendelkezik a kiberfenyegetésekkel szembeni kitettségéről, és 60%-uk soha nem becsülte fel a lehetséges pénzügyi veszteségeket. Egy globális felmérés szerint a szervezetek egyharmada inkább megfizetné a hekkerek által kért váltságdíjat, mintsem beruházzon az információbiztonságba.

A Számvevőszék megállapításai a következők voltak:

- Az Unió összetett és többrétegű kiberbiztonsági ökoszisztémájában számos érdekelt fél vesz részt. Komoly kihívást jelent a rendszer különböző elemeinek integrálása.

- Az Unió törekvése az, hogy a világ legbiztonságosabb online környezetévé váljon. Ennek eléréséhez jelentős munkára van szükség minden érintett részéről; többek között nélkülözhetetlen a stabil, biztos kézzel irányított pénzügyi háttér. Nehéz számadatokat szerezni, de a kiberbiztonsággal kapcsolatos uniós közkiadások becslések szerint évente 1–2 milliárd eurót tesznek ki. Összehasonlításképpen az Egyesült Államok szövetségi kormányzata 2019-ben mintegy 21 milliárd USA-dolláros kiadást vett költségvetésbe.

- Az információbiztonsági irányítás lényege az adatok bizalmas kezelésének, integritásának és rendelkezésre állásának biztosítására szolgáló struktúrák és intézkedések bevezetése. Nem pusztán technikai kérdésről van szó: előfeltételei az eredményes irányítás, a megbízható folyamatok és a szervezeti célkitűzésekkel összehangolt stratégiák.

- A kiberbiztonsági irányítási modellek tagállamonként eltérőek, és a kiberbiztonsággal kapcsolatos felelősség gyakran több szervezet között oszlik meg. Ezek a különbségek nemzeti szinten is akadályozhatják a nagyszabású, határokon átnyúló eseményekre való reagáláshoz és a fenyegetésekkel kapcsolatos értesülések cseréjéhez szükséges együttműködést, az Unió szintjén pedig még inkább.

- A kibertámadásokra való eredményes reagálás megtervezése alapvető fontosságú azok mielőbbi megállításához. Különösen fontos, hogy a kritikus ágazatok, a tagállamok és az uniós intézmények gyorsan és összehangoltan tudjanak reagálni. Ehhez elengedhetetlen a korai felderítés.

Ajánlások

A számvevőszéki áttekintésből kiderül, hogy az érdemi elszámoltathatóság és értékelés biztosítása érdekében el kell mozdulni az értékelési gyakorlatokon alapuló teljesítménykultúra felé. Továbbra is vannak rések a jogi keretben, és a tagállamok nem ültetik át következetesen a meglévő jogszabályokat. Mindez megnehezítheti a jogszabályok hatásának maximális érvényesítését.

Szintén kihívást jelent a beruházási szintek és a stratégiai célok összehangolása, ahhoz ugyanis növelni kell a kiberbiztonságba történő beruházások szintjét és hatását. Ez még nehezebb akkor, ha az Unió és tagállamai nem rendelkeznek világos áttekintéssel az uniós kiberbiztonsági kiadásokról. A megállapítások szerint a kibervédelemhez kapcsolódó tevékenységet folytató uniós ügynökségek nem rendelkeznek a szükséges erőforrásokkal, többek között nehézségekkel küzdenek a tehetséges munkaerő bevonzása és megtartása terén.

Betűszavak és rövidítések

APT: fejlett tartós fenyegetés

CEF: Európai Hálózatfinanszírozási Eszköz

CERT-EU: hálózatbiztonsági vészhelyzeteket elhárító csoport

COBIT: az informatikára és a kapcsolódó technológiára vonatkozó ellenőrzési célkitűzések

COVID-19: 2019. évi koronavírus-betegség

cPPP: szerződéses köz-magán társulás

CSIRT: számítógép-biztonsági eseményekre reagáló csoport

DDoS: elosztott szolgáltatásmegtagadással járó támadás

DEP: Digitális Európa program

EC3: az Europol Kiberbűnözés Elleni Európai Központja

ECA: Európai Számvevőszék

EDA: Európai Védelmi Ügynökség

EKSZ: Európai Külügyi Szolgálat

ENISA: Európai Uniós Kiberbiztonsági Ügynökség

ERKT: Európai Rendszerkockázati Testület

Esb-alapok: európai strukturális és beruházási alapok

EU: Európai Unió

Europol: A Bűnüldözési Együttműködés Európai Uniós Ügynöksége

GDP: bruttó hazai termék

GDPR: általános adatvédelmi rendelet

HR: humánerőforrás

IKT: információs és kommunikációs technológia

IoT: a dolgok internete

ISACA: Információrendszer-ellenőrök Egyesülete

ISF-P: a Belső Biztonsági Alap rendőrségi együttműködést támogató eszköze

IT: információtechnológia

KBVP: közös biztonság- és védelempolitika

MERS: közel-keleti légzőszervi szindróma

NAO: nemzeti számvevőszék

NATO: Észak-atlanti Szerződés Szervezete

NCSS: nemzeti kiberbiztonsági stratégia

NIS-irányelv: a hálózati és információs rendszerek biztonságáról szóló irányelv

PESCO: állandó strukturált együttműködési keret

RDP: távoli asztali protokoll

SAI: legfőbb ellenőrző intézmény

SARS: súlyos akut légzőszervi szindróma

TPK: többéves pénzügyi keret

UK: Egyesült Királyság

URL: webcím (egységes erőforrás-helymeghatározó)

USA: Amerikai Egyesült Államok

Glosszárium

5G: A széles sávú mobilhálózatok technológiai szabványának ötödik generációja, amelyet a mobiltelefon-vállalatok 2019-ben kezdtek világszerte bevezetni, és amely a tervek szerint a legtöbb jelenlegi mobiltelefon hálózati összekapcsoltságát biztosító 4G hálózatok helyébe lép. A megnövekedett sebesség részben a korábbi mobilhálózatokhoz képest magasabb frekvenciájú rádióhullámok használatával érhető el.

Adathalászat (phishing): Látszólag megbízható forrásból származó e-mailek küldése annak érdekében, hogy a címzettet csalárd módon rábírják arra, hogy rosszindulatú linkekre kattintson vagy megossza személyes adatait.

Adatkezelés: Műveletek elvégzése adatok vonatkozásában, különösen számítógép segítségével, információk lekérdezése, átalakítása vagy minősítése céljából.

Adatvédelmi incidens: Biztonságos vagy magánjellegű/bizalmas információk nem megbízható környezetbe történő szándékos vagy nem szándékos kiadása.

Alapvető szolgáltatásokat nyújtó szereplő: Olyan közjogi vagy magánjogi szervezet, amely kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából alapvető szolgáltatást nyújt.

Biometrikus adatok (biometria): Emberi jellemzőkkel kapcsolatos fizikai (például ujjnyomat vagy szemek) vagy viselkedési változók. A hitelesítést a számítástechnikában az azonosítás és a hozzáférés-ellenőrzés egyik formájaként alkalmazzák.

Bitcoin: 2009-ben létrehozott digitális, illetve virtuális valuta, amely peer-to-peer (felhasználó és felhasználó közti) technológiát használ az azonnali fizetések végrehajtásához.

Dezinformáció: Olyan igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy a nyilvánosság szándékos megtévesztése céljából hoznak létre, tesznek közzé és terjesztenek, és amely kárt okozhat a közérdeknek.

Digitális platform: Legalább két különböző csoport – jellemzően egyfelől beszállítók, másfelől fogyasztók/felhasználók – közötti interakciókra szolgáló környezet. Lehet hardver vagy operációs rendszer, vagy akár egy internetes böngésző és kapcsolódó alkalmazásprogramozási interfészek, vagy egyéb alapul szolgáló szoftver, amennyiben a program kódját azzal hajtják végre.

Digitális szolgáltató: A digitális szolgáltatások három típusa – online piactér, internetes keresőmotor, felhőszolgáltatások – közül egyet vagy többet kínáló szolgáltató.

Digitális tartalom: Minden olyan adat – például szöveg, hang, kép vagy videó –, amelyet digitális formában tárolnak.

Digitális vagyon: Bármi, ami digitális formátumban létezik, magánszemély vagy vállalat tulajdonát képezi, és felhasználási jog kapcsolódik hozzá (például képek, fényképek, videók, szöveges fájlok stb.).

Digitalizáció: Információk olyan digitális formátumba történő átalakításának folyamata, amelyben az információ bitekből épül fel. Az eredmény egy tárgy, kép, hang, dokumentum vagy jel leképezése olyan számsorozat létrehozásával, amely pontok vagy minták egyedi halmazát írja le.

Dolgok internete (IoT): Az interneten keresztül történő kommunikációt és adatcserét lehetővé tevő elektronikával, szoftverrel és szenzorokkal ellátott mindennapi tárgyakból álló hálózat.

Elosztott szolgáltatásmegtagadással járó támadás (DDoS): Olyan kibertámadás, amely bizonyos online szolgáltatásokat vagy erőforrásokat elérhetetlenné tesz a jogszerű felhasználók számára azáltal, hogy kezelhetetlen mennyiségű kéréssel árasztja el azokat.

Etikus hekker: Olyan személy (számítógép-biztonsági szakember), aki nem rosszindulatú vagy bűnelkövetési szándékkal, hanem a biztonság tesztelése vagy értékelése céljából hatol be egy számítógépes hálózatba.

Fejlett tartós fenyegetés: Olyan támadás, amelynek során egy jogosulatlan felhasználó hozzáfér egy rendszerhez vagy egy hálózathoz, és hosszabb ideig ott is marad anélkül, hogy felderítenék. Különösen veszélyes a vállalkozások esetében, mivel a hekkerek folyamatosan hozzáférnek érzékeny vállalati adatokhoz, ugyanakkor rendszerint nem okoznak kárt a vállalati hálózatokban vagy a helyi gépekben. A cél az adatlopás.

Felhőalapú számítástechnika: Informatikai erőforrások – például tárhely, számítási teljesítmény vagy adatmegosztási kapacitás — keresletalapú rendelkezésre bocsátása az interneten, távoli szervereken történő tárhelyszolgáltatás révén.

Féreg: A számítógépes féreg önálló kártékony számítógépes program, amely sokszorosítja magát annak érdekében, hogy átterjedjen másik számítógépekre.
A terjedéshez gyakran számítógépes hálózatot használ, a célszámítógéphez annak biztonsági hiányosságait kihasználva szerez hozzáférést.

Hálózatbiztonság: A kiberbiztonság egyazon hálózaton lévő eszközökön keresztül továbbított adatok védelmével foglalkozó része, amely azt hivatott biztosítani, hogy az információkat ne szerezhessék meg, illetve módosíthassák.

Hekker: Olyan személy, aki számítógépes, hálózatépítési vagy egyéb készségeinek felhasználásával fér hozzá jogosulatlanul adatokhoz, számítógépes rendszerhez vagy hálózathoz.

Hibrid fenyegetés: Ellenséges szándék kifejezése hagyományos és nem hagyományos hadviselési technikák (katonai, politikai, gazdasági és technológiai módszerek) célirányos keverékének alkalmazásával.

Hozzáférési adatok: A felhasználók szolgáltatásokba való be- és kijelentkezéseire vonatkozó információk, például időpont, dátum és IP-cím.

Információbiztonság: A fizikai és digitális adatok jogosulatlan hozzáféréstől, felhasználástól, közzétételtől, zavarástól, módosítástól, rögzítéstől és megsemmisítéstől való védelmét szolgáló folyamatok és eszközök összessége.

Integritás: Az információk jogosulatlan módosítás és megsemmisítés elleni védelme és valódiságának garantálása.

Kémprogram (spyware): Kártékony szoftver, amelynek célja információk gyűjtése egy személyről vagy szervezetről, és ezen információk megküldése egy másik szervezet részére oly módon, hogy az – például magánéletének megsértése vagy eszköze biztonságának veszélyeztetése révén – kárt okoz a felhasználónak.

Kiberbiztonság (kibervédelem): Az informatikai rendszerek és adatok jogosulatlan hozzáféréssel, támadásokkal és károkozással szembeni védelme céljából, azok rendelkezésre állásának, bizalmas kezelésének és integritásának biztosítása érdekében elfogadott biztosítékok és intézkedések összessége.

Kiberbiztonsági esemény: Olyan esemény, amely közvetlenül vagy közvetve károsítja vagy veszélyezteti egy informatikai rendszer, illetve az abban feldolgozott, tárolt vagy továbbított adatok ellenálló képességét és biztonságát.

Kiberbűnözés: Olyan bűncselekmények, amelyek elsődleges eszköze vagy elsődleges célja számítógépekhez és informatikai rendszerekhez kapcsolódik. Ezek lehetnek hagyományos bűncselekmények (pl. csalás, hamisítás és személyazonosság-lopás), tartalommal kapcsolatos bűncselekmények (pl. gyermekpornográfia online terjesztése vagy fajgyűlöletre uszítás), vagy kifejezetten a számítógépekkel és információs

rendszerekkel kapcsolatos bűncselekmények (pl. információs rendszerek elleni támadások, szolgáltatásmegtagadással járó támadások, rosszindulatú szoftverek vagy zsarolóvírusok).

Kiberdiplomácia: Diplomáciai erőforrások felhasználása és diplomáciai funkciók betöltése a kibertérrel kapcsolatos nemzeti érdekek biztosítása érdekében. Egészében vagy részben diplomaták végzik, akik bilaterális formában (például az USA–Kína párbeszéd keretében) vagy multilaterális fórumokon (például az ENSZ-ben) találkoznak. A diplomácia hagyományos körén kívül a diplomaták különféle nem állami szereplőkkel is kapcsolatot alakítanak ki, ideértve az internetes vállalatok (például a Facebook vagy a Google) vezetőit, technológiai vállalkozókat, illetve civil társadalmi szervezeteket. A diplomácia magában foglalhatja a más országokban a technológia révén elhallgattatott vélemények felerősítését.

Kiberfenyegetés: Olyan rosszindulatú cselekmény, amelynek célja az adatokban való károkozás, adatok ellopása vagy általában véve a digitális élet megzavarása.

Kiberkémkedés: A kiberkémkedés olyan cselekmény vagy gyakorlat, amelynek keretében az információk birtokosának engedélye vagy tudta nélkül titkokat és információkat szereznek meg magánszemélyektől, versenytársaktól, riválisoktól, csoportoktól, kormányoktól és ellenségektől személyes, gazdasági, politikai vagy katonai előny céljából, az internet, hálózatok vagy egyedi számítógépek felhasználásával.

Kiber-ökoszisztéma: Egymással kapcsolatban álló eszközök, adatok, hálózatok, emberek, folyamatok és szervezetek, valamint az ezeket a kölcsönhatásokat befolyásoló és támogató folyamatok és technológiák összetett közössége.

Kibertámadás: Adatok vagy számítógépes rendszerek bizalmas jellegének, integritásának és rendelkezésre állásának a kibertéren keresztüli gyengítésére vagy megsemmisítésére irányuló kísérlet.

Kibertámadásokkal szembeni reziliencia: A kibertámadások és a váratlan események megelőzésére és elhárítására, az azokra való felkészülésre, illetve hatásaik felszámolására való képesség.

Kibertér: Az immateriális globális környezet, amelyben számítógépes hálózatokon és technológiai eszközökön keresztül online kommunikáció folyik emberek, szoftverek és szolgáltatások között.

Kibervédelem: A kiberbiztonság egy alkategóriája, amelynek célja a kibertér katonai és egyéb megfelelő eszközökkel történő védelme katonai-stratégiai célok elérése érdekében.

Közműlétesítmények: Bármely olyan oszlop, torony, felső- vagy föld alatti vezeték, egyéb alátámasztó vagy tartószerkezet, illetve árok, tartozékaival együtt, amely felhasználható elektromos, telefonos, távirati, kábeles vagy jelző (vagy más hasonló) szolgáltatás nyújtásához vagy elosztásához.

Kriptovaluta: Olyan digitális vagyontárgy, amelyet titkosítási technikák alkalmazásával, a központi bankoktól függetlenül bocsátanak ki és cserélnek, és amelyet egy-egy virtuális közösség tagjai egymás közötti fizetési módként elfogadnak.

Kritikus információs rendszer: Olyan meglévő vagy tervezett információs rendszer, amelyet a szervezet hatékony és eredményes működtetéséhez alapvetőnek tekintenek.

Kritikus infrastruktúra: Olyan fizikai erőforrások, szolgáltatások és létesítmények, amelyek megzavarása vagy megsemmisítése súlyos következményekkel járna a gazdaság és a társadalom működésére nézve.

Mesterséges intelligencia: Az emberi intelligencia szimulálása olyan gépekben, amelyeket arra programoznak, hogy úgy gondolkozzanak, mint az emberek, és utánozzák azok cselekedeteit; bármely olyan gép, amely az emberi elméhez kapcsolódó vonásokat mutat, ideértve a tanulást és a problémamegoldást.

Nagy teljesítményű számítástechnika: Nagy sebességű adatfeldolgozásra és bonyolult számítások nagy sebességgel történő elvégzésére való képesség.

Patchelés: Egy szoftver kapcsán végrehajtott módosítássorozat, amelynek célja annak frissítése, megjavítása vagy fejlesztése, így többek között a biztonsági sebezhetőségek orvoslása.

Pszichológiai manipuláció (social engineering): Az információbiztonság területén a kifejezés arra utal, amikor embereket megtévesztés révén rávesznek bizonyos cselekvések végrehajtására vagy bizalmas információk felfedésére.

Reklámprogram (adware): Rosszindulatú szoftver, amely az áldozatok online magatartását követő kódot tartalmazó reklámtranszparenseket vagy felugró ajánlatokat jelenít meg.

Rendelkezésre állás: Az információk időbeni és megbízható hozzáférhetőségének és használhatóságának biztosítása.

Rosszindulatú szoftver (malware): Kártékony szoftver, azaz a számítógépekben, szerverekben vagy hálózatokban való károkozásra irányuló számítógépes program.

Szabotázs: Szándékos pusztításra, károkozásra vagy obstruálásra irányuló cselekedet, különösen politikai vagy katonai előny szerzése céljából.

Személyes adatok: Egy azonosítható személlyel kapcsolatos információk.

Szövegvektorizálás: Szavak, mondatok és teljes dokumentumok numerikus vektorokká való átalakítása a gépi tanulási algoritmusok általi felhasználás lehetővé tétele érdekében.

Távoli asztali protokoll (RDP): Asztali számítógép távolról történő használatára szolgáló (a Microsoft által kiadott) műszaki szabvány. Az asztali számítógépek távoli felhasználói hozzáférhetnek asztali számítógépükhöz, fájlokat nyithatnak meg és szerkeszthetnek, valamint alkalmazásokat használhatnak úgy, mintha ténylegesen az asztali számítógépüknél ülnének.

Titkosítás: Olvasható információk nem olvasható kóddá alakítása azok védelme érdekében. Az információk megtekintéséhez a felhasználónak titkos kulccsal vagy jelszóval kell rendelkeznie.

Titoktartás: Az információk, adatok és eszközök jogosulatlan hozzáféréstől és nyilvánosságra hozataltól való védelme.

Trójai program: Olyan kártékony kód vagy szoftver, amely jogszerűnek tűnik, de átveheti az irányítást a számítógép felett. A trójai program célja az adatokban vagy a hálózatban történő károkozás, azok megzavarása, ellopása, illetve általában véve valamely egyéb káros cselekedet előidézése azokkal kapcsolatban.

Választási infrastruktúra: A kampányok informatikai rendszerei és adatbázisai, a jelöltekre vonatkozó érzékeny információk, a választók nyilvántartásba vételére szolgáló és irányítási rendszerek.

Webalapú támadás: A felhasználók megbíznak abban, hogy az általuk a weboldalon megadott érzékeny személyes adatokat bizalmasan és biztonságosan kezelik.
A behatolás (támadás) azt jelentheti, hogy hitelkártyájukkal, társadalombiztosításukkal vagy egészségi állapotukkal kapcsolatos információik nyilvánosságra kerülhetnek, ami potenciálisan súlyos következményekkel járhat.

Zsarolóvírus (ransomware): Rosszindulatú szoftver, amely megtagadja a sértettől a számítógépes rendszerhez való hozzáférést, vagy olvashatatlanná teszi (általában titkosítja) a fájlokat. A támadó ezután rendszerint megzsarolja a sértettet azáltal, hogy váltságdíjhoz köti a hozzáférés visszaállítását.

Kapcsolatba szeretne lépni az EU-val?

Személyesen
Az Európai Unió területén több Europe Direct információs központ is működik. Keresse meg az Önhöz legközelebb eső központot: https://europa.eu/european-union/contact_hu

Telefonon vagy e-mailben
A Europe Direct központok feladata, hogy megválaszolják a polgárok Európai Unióval kapcsolatos kérdéseit. Vegye igénybe a szolgáltatást
— az ingyenesen hívható telefonszámon: 00 800 6 7 8 9 10 11 (bizonyos szolgáltatók számíthatnak fel díjat a hívásért),
— a rendes díjszabású telefonszámon: (+32 2) 29-99-696, vagy
— e-mailen: https://europa.eu/european-union/contact_hu

Információkat keres az EU-ról?

Online
Az EUROPA portál tájékoztatással szolgál az Európai Unióról az EU összes hivatalos nyelvén:
https://europa.eu/european-union/index_hu

Uniós kiadványok
A következő címen uniós kiadványok tölthetők le/rendelhetők meg díjmentesen/fizetés ellenében:
https://publications.europa.eu/hu/publications. Ha bizonyos ingyenes kiadványokból több példányra van szüksége, rendeljen a Europe Direct központtól vagy hazájának helyi információs központjától
(lásd: https://europa.eu/european-union/contact_hu).

Uniós jogszabályok és kapcsolódó dokumentumok
Az EUR-Lex portálról bármelyik hivatalos nyelven letölthetők az EU jogi tartalmai és az 1952-től megjelenő jogszabályai:
https://eur-lex.europa.eu

Az EU által gondozott nyílt hozzáférésű adatok
A nyílt hozzáférésű adatok európai uniós portálja (http://data.europa.eu/euodp/hu) uniós adatkészletekhez biztosít hozzáférést. Az adatok kereskedelmi és nem kereskedelmi célból egyaránt díjmentesen letölthetők és felhasználhatók.

Kapcsolattartó Bizottság

Az EU Legfőbb Ellenőrző intézményeinek Kapcsolattartó Bizottsága