Vikman László

Szempontok a kibertér egyes aktuális fenyegetéseinek jogi értékeléséhez

Military and Intelligence CyberSecurity Research Paper
2022/4.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

A kibervédelem elsődleges értelmezésében műszaki tevékenység, szofisztikált IT-eszközök és magasan képzett mérnökök területe. Nem jelentéktelen a témában azonban a klasszikusan támogató szerepben működő jogász felelőssége sem, legyen szó akár a szervezet dinamikájáról – szerződéseiről, vagy statikájáról – belső szabályozókról. Az elmúlt időszak jellemző fenyegetéseinek bemutatásán keresztül szeretnénk gondolatokat ébreszteni a területen egyre jelentősebb jogi aspektusokról.

Kulcsszavak: kiberbiztonság, fenyegetések, kiberstratégia

Primarily cyber defence is a technical activity, a realm of sophisticated IT-devices and highly trained engineers. However the responsibility of the classicly supporting lawyer is also growing, as in the dynamics of the organisation – contracts, or in the static – inner regulations. Through the presentation of the threats of the past period we try to raise some thoughts regarding the legal aspects of the matter.

Keywords: cyber security, threats, cyber strategy

BEVEZETÉS

A cégek, szervezetek kiberstratégiáinak állandó, „kötelező" tartalmi eleme a fenyegetések értékelése, egyértelmű, hogy ezekkel – komolyan vett védelmi tevékenység esetén – érdemes jogi szempontból is foglalkozni. *A jelentős kockázatok figyelembevétele, a kockázatkezelési-mátrixokba való felvétele, esetleges ellenlépések, mitigációs intézkedések előzetes tervezése elengedhetetlen a védelmi architektúrát alapjaiban meghatározó szervezet kialakításának, a hatékony védelemhez szükséges képességeknek, valamint az ehhez szükséges humán- és technológiai fejlesztéseknek a meghatározásában.* Komplex megközelítésben azonban a kibervédelem nem csupán a korszerű technológia és a kompetens mérnök-csapat összessége. *Ha mindennek hátteréből hiányzik a hatékony szervezeti felépítés* a fenyegetésekhez igazítottan gyors döntési mechanizmusokkal, a megfelelő szabályozási háttérrel és annak magabiztos értelmezési gyakorlatával, továbbá *az operatív működés megfelelő jogi támogatásával*[1] *az a hatékony védelem kialakítására tett erőfeszítéseket gátolhatja, akár meg is bénithatja.*[2]

[1] Például az adott szervezet üzemmenetéhez, felelősségi- és kockázati szintjéhez igazított beszállítói szerződések, melyek a megkívánt mértékben szabályozzák az egyes termékfelelősségi, személyes adatok védelméhez kapcsolódó, szerzői jogi, és rendelkezésre állási kérdéseket is.

[2] Ennek rendszerszintű állami és jogi kérdéseiről lásd: GARRETT DERIAN-TOTH, RYAN WALSH, ALEXANDRA SERGUEEVA, EDWARD KIM, ALIVIA COON, HILDA HADAN, JARED STANCOMBE: *Opportunities for Public and Private Attribution of Cyber Operations.* Tallinn Paper No. 12., Tallinn, NATO CCD COE, 2021.; FARKAS ÁDÁM: *A kibertér műveleti képességek kialakításának és*

Azzal a megközelítéssel is érdemes tehát az egyes fenyegetés-elemzéseket, támadásról szóló híradásokat vizsgálni, hogy ***a technikai elhárító/helyreállító lépések az eseménykezelés után hogyan kerültek beillesztésre az adott szervezet döntési láncába, az ezzel megbízott szervezeti egységek hogyan illeszkednek a szervezet vezetési-irányítási struktúrájába,*** mi garantálja a megfelelő humán-adminisztratív-anyagi támogatásukat, és hogy az egyes támadás-típusok, krízisek milyen jogi következményekkel és tapasztalat feldolgozással járnak, esetleg milyen előzetes óvintézkedések tehetők jogi szempontból a felmerült problémák hatékonyabb kezelése érdekében.

A NATO Kooperatív Kibervédelmi Kiválósági Központja (a továbbiakban: CCDCOE) a katonai szövetség egyik tudományos értelemben is legaktívabb szakosított tudáscentruma. Elemzéseinek, publikált tanulmányainak és magasan értékelt konferenciáinak szakmai üzenetei és megállapításai - az infokommunikációs technológiák össztársadalmi jelentőségének köszönhetően is - széles körben tarthatnak számot a figyelemre és megfontolásra, a hagyományos értelemben vett védelmi-biztonsági szférán túl is. Bár a 2022-es évnek az orosz-ukrán háború a biztonságpolitikai szempontból legjelentősebb és valószínűleg hosszú évtizedekre hatásokkal és súlyos következményekkel járó eseménye - amelynek szintén fontos eleme a kibertérben mindkét fél által végrehajtott tevékenységek - de ettől a kijózanítóan zord eseménytől is elvonatkoztatva érdemes áttekinteni az elmúlt év fő kiberfenyegetési trendjeit. Ezt követően néhány erre az évre prognosztizáltan erősödő tendenciát is említünk, mivel ezek mérlegelése a saját szervezet szempontjából segíthet kibervédelmi törekvéseinknek a fenyegetési környezethez adekvát kalibrálásában, illetve tágabban a hazai kooperatív kiberbiztonsági kutatások ösztönzésében.[3]

---

fejlesztésének egyes szabályozási és államszervezési alapvonalai. In: Jog Állam Politika 2019/2. szám, 63-79. o.; KELEMEN ROLAND: *Cyberfare State – Egy hibrid állammodell 21. századi születése*. In: Military and Intelligence CyberSecurity Research Paper 2022/1. szám.

[3] Ehhez lásd: KOVÁCS LÁSZLÓ: *A kiberbiztonság és a kiberműveletek megjelenése magyarország új nemzeti biztonsági stratégiájában*. in: Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata 148 : 5 pp. 3-18. , 16 p. (2020); KOVÁCS LÁSZLÓ: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus Kiadó, 2018.; KASSAI KÁROLY: *Kibertér - Aktuális változások*, Szakmai Szemle, XVII. évfolyam 1. szám 2019. március, 116. o.; BIHARI LÁSZLÓ, MAGYAR SÁNDOR: Mennyország helyett a pokolba, avagy az informatikai támogatás kihívásai. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata 18 : 4 pp. 158-169. , 12 p. (2020); ANNAMÁRIA BELÁZ, CSABA KRASZNAY, ZSOLT SZABÓ: *Cybersecurity strategy and leadership management issues*. September 2020, IMCSM Proceedings - An international serial publication for theory and practice of Management Science (pp.242-252), University of Belgrade, https://www.researchgate.net/publication/348432259_Cybersecurity_strategy_and_leadership_management_issues; KELEMEN ROLAND, SZÉPVÖLGYI ENIKŐ: *A modern technológia és ami mögötte van - Konferencia a modern technológia biztonsági kockázatairól és állam- és jogtudományi kapcsolódásairól*. Katonai Jogi És Hadijogi Szemle 4 pp. 191-197. , 7 p. (2021); KELEMEN ROLAND: *A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban*. SmartLaw Research Group Working Paper 2 pp. 1-17. , 17 p. (2021); FARKAS ÁDÁM: KIBERTÉR MŰVELET: HÍRSZERZŐ, RENDÉSZETI ÉS KATONAI MŰVELETEK ELEGYE?: GONDOLATOK AZ ANGOL NATIONAL CYBER FORCE KAPCSÁN, Military and Intelligence CyberSecurity Research Paper 2021 : 1

CCDCOE ELEMZÉS 2021-RŐL

A CCDCOE 2022. januárjában kiadott „Recent Cyber Events" 14. száma[4] a szerzők által 2021-ben leginkább dominánsnak tekinthető három kibertéri fenyegetésről szól. Ezek a zsarolóprogramok, az IT-ellátási láncok kompromittálásával végrehajtott támadások és a kémszoftverek, avagy megfigyelésre alkalmas szoftverek voltak.

A rosszindulatú programok egy külön kategóriája, a zsarolószoftverek nagy figyelmet kaptak a tavalyi évben. Ezek a rosszindulatú kódok nem csupán titkosítják, és olvashatatlanná teszik az áldozat rendszereiben tárolt adatokat, amelyeket csak „váltságdíj" ellenében oldanak fel a támadók, hanem a fenyegetés gyakran kettős, mivel a megszerzett adatok nyilvánosságra hozatalával történő nyomásgyakorlás hatására egy a hírnevére és működési prudenciájára érzékeny szervezet kétszeresen is szinte kilátástalan helyzetbe kerül (pl. egy ügyfélbizalomra építő pénzügyi szolgáltató; szenzitív adatokat kezelő szolgáltató cég; üzleti/szervezeti titkokra is rálátást nyerő auditor; stb.).

Másodlagos hatásai egy nem csupán adatokat tároló, de azokat folyamatosan a működésében használó entitás esetében időnként még komolyabbak lehetnek, mint akár az első körben akár a támadók is megbecsülték. Gondolhatunk itt az egészségügyi szolgáltatókat ért támadásokra[5], amelyek emberéleteket és ellátásbiztonságot veszélyeztetnek, vagy az elemzésben külön is kiemelt májusi Colonial Pipeline-támadás esetében, amely az USA keleti partján bénította meg a belföldi üzemanyagvezeték-rendszert vezérlő informatikai rendszereket, ezzel ellátási zavarokat és üzemanyagár-emelést is előidézve.

Ezek a támadások nem csak azt mutatták meg, hogy mennyire erősen összekapcsolódott a társadalom és az információs rendszerek, hanem azt is, hogy mennyire sebezhetővé és függővé váltunk a kritikusnak tekinthető infrastruktúráink működésétől. A zsarolóprogramok jellemzően ilyen szolgáltatásokat céloznak meg, és ezek egymással igen gyakran a kiterjedt hálózatosság miatt még annyira erős kapcsolatban is állnak, hogy valamelyik kiesése képes lehet dominó-hatás kiváltására is. Egyre nyilvánvalóbb, hogy a rezílienciához nem elegendő a robosztus és redundáns digitális rendszerek kiépítése, de *bizonyos létfontosságú funkciók vonatkozásában az „analóg" technológiák, a sziget-szerűen is működő helyi megoldások (pl. tartalék-generátorok) kialakítása is szükséges lehet.* A kritikus infrastruktúrákat – vagy magyar terminológiával, létfontosságú rendszerelemeket – érintő veszélyek jelentőségét jól mutatja, hogy a

pp. 1-8. , 8 p. (2021); FARKAS ÁDÁM: *Biztonság – Geopolitika – Digitalizáció, avagy Amael Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei*. SmartLaw Research Group Working Paper 1 pp. 1-13. , 13 p. (2021)

[4] SUNGBAEK CHO ET. AL.: Recent Cyber Events: Considerations for Military and National Security Decision Makers, Tallinn. CCDCOE, Recent Cyber Events No 14 / January 2022 https://ccdcoe.org/library/publications/recent-cyber-events-considerations-for-military-and-national-security-decision-makers-2/

[5] https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

kérdést már az USA-ban összkormányzati felelősségként és erőfeszítésként kezelik[6] és a nemzetközi összefogás is elengedhetetlen összetevője a hihető és kézzelfogható elrettentést is jelentő bűnüldöző tevékenységnek.

A második kiemelt témaként választott ***informatikai rendszerek ellátási láncok biztonságával kapcsolatos aggályokat a még 2020 végén kezdődő, de igazán 2021-ben eszkalálódó Solarwinds-incidens tette mindenki számára nyilvánvalóvá.*** A rosszindulatú kódrészletek eltávolítása az első, CISA[7] által kiadott útmutató publikálása után még hat hónappal sem fejeződött be teljesen minden érintett rendszerből. A szabványügyi kérdésekkel foglalkozó NIST által kiadott útmutató[8] megállapítása szerint: „A szervezetek ma már nem biztosíthatják magukat egyszerűen a saját infrastruktúrájuk határvédelmével, mivel a határaikat ma már lehetetlen egzaktul meghatározni; a fenyegetések szándékosan a kibervédelmi szempontból fejlett szervezetek beszállítóit célozzák, kihasználva a leggyengébb láncszemet." A Kaseya, BigNox és Gigaset incidensek szintén aláhúzták ennek a veszélynek a fontosságát.

Másik támadási irány, az „újrahasznosított" és akár nyílt forrású átvett programrészletek, csomagok és könyvtárak megfertőzése, melyeken keresztül a támadó célú kódot maga a későbbi áldozat emeli be saját környezetébe, de előfordult a szoftver-fejlesztő környezetek, eszközök kompromittálása is (Codecov).

Az ellátási-beszállítói lánc biztosítása érdekében a beszállítóknak maguknak kell felelősséget vállalniuk először a saját tevékenységeik vonatkozásában – megfelelő teszteléssel, a nyílt internettől szegregált fejlesztéssel, biztonságos konfiguráció menedzsmenttel, tanúsítvány-kezeléssel és az automatikus frissítéseket is terjesztő szoftver-platformok megerősítésével. Ha a fejlesztési folyamat egy része kiszervezésre kerül, mindenképpen védeni kell a forráskódot, és további ellenőrzéseket kell végrehajtani az esetleges sérülékenységek és rosszindulatú kódok feltárására. A beszerzések esetén a részletes specifikáció vizsgálatának egészen komponens-szintig le kell mennie, és érdemes megfontolni a beszerzett termékkel szemben valamilyen megbízható harmadik fél, egy tanúsító szervezet általi certifikációját is (akár a Common Criteria, vagy az ISO 27001 szabvány mentén)[9].

A záró téma a 2021-ben globális széles médiafigyelemmel övezett, ***a „polcról levehető" megfigyelő-szoftverek. Mivel ezek esetében legalább annyira beszélhetünk a magánszféra védelméről, mint a kiberbiztonságról, nem csoda, hogy ennek a termékcsoportnak a nemzetközi export-***

[6] Akár katonai erőforrások bevonásával is, lásd: https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

[7] Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/

[8] https://csrc.nist.gov/publications/detail/nistir/8276/final

[9] További szempontokért lásd: Executive Order on Improving the Nation's Cybersecurity, May 12, 2021, Sec. 4. Enhancing Software Supply Chain Security, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

kontrollja egyre komolyabb figyelmet kap. Az izraeli NSO Group által fejlesztett Pegasus-ról úgy tudják, hogy 2016 és 2018 közt 36 ügyfél használta. 2021 júniusában egy tényfeltáró újságírói csoport hozzájutott egy több mint 50.000 telefonszámot tartalmazó „célszemély"-listához, amelyen többek közt a francia elnök, magas rangú katolikus egyházi vezetők, és több országban emberi jogi aktivisták is előfordultak. Bár kezdetben azt állították, hogy USA és izraeli telefonszámok tiltva vannak a szoftverben, később kiderült, hogy amerikai kormányzati tisztviselők és diplomaták is érintettek voltak.

Ezt követően Izrael szigorításokat vezetett be az egyes kettős felhasználású technológiák exportjára – de érdemes szem előtt tartani, hogy korántsem ők az egyetlen exportőrei az ilyen eszközöknek. Az NSO szegmensében van pl. az orosz Positive Technologies, a német FinFisher vagy az olasz HackingTeam is. Az unió új kettős felhasználású termékekre vonatkozó szabályozása 2021. szeptember 9-én lépett hatályba[10], és bár foglalkozik a kiber-megfigyelési technológiákkal, egyelőre úgy tűnik, közvetlenül nem alkalmazható egy teljes export-tilalom kivetésére. ***Ezen termékekre vonatkozón egy egységes közösségi álláspont kialakulását, esetleg általános export-tilalom bevezetését, akár csak egységes megítélését a kapcsolódó nemzetközi jogi[11], emberi jogi kérdések értelmezése és a nemzeti megfigyelési szabályozások sokszínűsége[12] sem könnyíti meg.***

A Pegasus-incidens jól illusztrálja a nemzetközi határokon átívelő állami megfigyelő-tevékenységeket: az államok egyrészt megvédenék polgáraikat a külföldi támadásoktól, másrészt igyekeznének a saját technológiájuk exportjára és biztonsági érdekeik külföldi érvényesítésére. Így az ilyen eszközök egyszerre jelentenek lehetőséget és kihívást az illetékes hatóságok és a döntéshozók szempontjából.

EGYÉB FONTOS TRENDEK

A fenti elemzésen kívül természetesen a kiberfenyegetésekről számos más szervezet is ad és adott ki retrospektív áttekintéseket, és a közeljövő trendjeit megjósolni igyekvő felhívásokat. Annak érdekében, hogy fenyegetések – jogi aspektusokból is

[10] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2021/821 RENDELETE (2021. május 20.) a kettős felhasználású termékek kivitelére, az azokkal végzett brókertevékenységre, az azokkal kapcsolatos technikai segítségnyújtásra, valamint azok tranzitjára és transzferjére vonatkozó uniós ellenőrzési rendszer kialakításáról
„(2) … A kibertér-megfigyelési termékek tekintetében a tagállamok hatáskörrel rendelkező hatóságainak figyelembe kell venniük különösen annak kockázatát, hogy azokat belső elnyomással vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben használhatják fel."

[11] A kapcsolódó Wassenaar Egyezmény elsősorban a katonai célú felhasználásra koncentrál, a hírszerzési-megfigyelési célok nem tartoznak szigorúan véve ebbe a kontextusba.

[12] A magyar nemzeti szabályozásért lásd: 2005. évi CIX. törvény, a haditechnikai termékek gyártásának és a haditechnikai szolgáltatások nyújtásának engedélyezéséről; 13/2011. (II. 22.) Korm. rendelet a kettős felhasználású termékek külkereskedelmi forgalmának engedélyezéséről; 156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól

kihívást jelentő – sokféleségét jobban illusztrálhassuk, szemlézés szintjén érdemes néhány ilyen anyagot áttekinteni. *Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) 2021 októberben publikált Threat Landscape 2021**13** című dokumentuma nyolc fő fenyegetéscsoportot azonosított*, amelyek a 2020-2021-es időszakban meghatározták a kiberteret:

- zsarolószoftverek (ransomware);
- rosszindulatú szoftverek (malware), amelyek valamilyen negatív hatást fejtenek ki egy rendszer bizalmasságára, integritására vagy rendelkezésre állására;
- rejtett kriptobányászat (cryptojacking), amelyben az célrendszer számítási kapacitásait rejtetten kriptovaluta bányászatára használják fel;
- e-mail-el kapcsolatos visszaélések, amelyek elsősorban az e-mail olvasóját célozzák, veszik rá valamire;
- adatok elleni fenyegetések, amelyek során bizalmas és/vagy szenzitív adatok kiszivárgása, megszerzése történik;
- fenyegetések a rendszerek rendelkezésre állása vagy integritása ellen, azaz jellemzően DoS- vagy web-alapú támadások;
- dezinformáció és félrevezetés, amely a vizsgált időszakban leginkább talán a COVID-járványhoz volt kapcsolható, de a jelenben az orosz-ukrán háborúnak is kritikus jelentőségű kísérőjévé vált;
- nem rossz-szándékú veszélyforrások, mint a helytelen rendszer-konfigurációk, fizikai meghibásodások, emberi hibák.

Az ENISA dokumentumának trendelemzéséből[14] érdemes kiemelni néhány eddig még nem érintett szempontot is:

- *minden támadástípusnak megjelenik a bérbevehető, szolgáltatásként is igénybe vehető formája,* üzleti modellje, ami az attribúció feladatát még inkább nehezíti: zsarolószoftverek, DoS-támadások, phishing-kampányok vagy dezinformáció esetében;
- *a kiberbűnözők egyre inkább haszonszerzésre törekednek*, és jellemzően kriptovaluta-alapú kifizetéseket követelnek;
- *a kibertámadások egyre inkább kritikus infrastruktúrákat támadnak;*
- *az üzleti szféra és egyéb szervezetek elektronikus levelezése kiemelt célpont;*
- *a dezinformációhoz egyre fejlettebb mesterséges intelligenciát is bevetnek a támadók.*

A brit központtal, de globális ügyfélkörrel (több, mint 500 ezer szervezet) működő *Sophos 2022-re kiadott fenyegetési jelentését**15** is érdemes kiemelni. Ez az anyag*

[13] ENISA Threat Landscape 2021, 8.o. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (letöltve: 2022.04.04.)
[14] U.o. 9. o.
[15] Sophos 2022 Threat Report – Interrelated threats target an interdependent world, https://assets.sophos.com/X24WTUEQ/at/b739xqx5jg5w9w7p2bpzxg/sophos-2022-threat-report.pdf (letöltve: 2022.04.04.)

5 fontos témakört tárgyal mélyebben, elsőként a zsarolószoftverek várható jövőjét elemzi, jelezve a szolgáltatási-modell terjedését és a zsarolási spektrum szélesedését is. Ezt követik a rosszindulatú szoftverek (malware és disztribúciós rendszereik) valamint a mesterséges intelligencia, mint technológia növekvő jelentősége és hozzáférhetővé válása a fenyegetések aktorai számára. Az előrejelzést a mobilplatformokon növekedő malware-fenyegetés és a kritikus infrastruktúrák elleni támadások jellemzőinek elemzésével zárják.

A szintén angliai székhelyű *BAE Systems,* amely amellett, hogy Európa legnagyobb hadiipari beszállítója, például a SWIFT-rendszer üzemeltetésében is közreműködik, szintén kiadott egy *2022-re vonatkozó előrejelzést*[16]*. Ebben ők hét várható trendet vázolnak fel:*

- *a COVID várható lecsengésével a pénzügyi szféra ismét kiemelt célponttá válik;*
- a zsarolószoftverek üzemeltetői a Bitcoin-on túllépve, *más kriptovalutákban kívánnak majd tranzakciókat végrehajtani,* amelyek nyomonkövetése nehezebb (pl. Monero);
- az egyes szervezeteket célzó támadások *egyre inkább a személyes használatú alkalmazotti eszközökön keresztül, akár social engineering módszerek alkalmazásával valósulnak majd meg,* ami szükségessé teszi majd a szervezeti biztonsági előírások frissítését;
- a támadók *az IoT-eszközökre jellemző kezdeti, vagy lassan javított sérülékenységeket kihasználva* fogják megszerezni a kezdeti hozzáférést a rendszerekbe;
- várható, hogy meghatározott személyek hangjának utánzásával, *„deepfake"-eszközökkel és social engineering módszerekkel együtt igyekeznek majd a támadók hozzáféréseket megszerezni telefonhívásokon keresztül;*
- *a rendszereken behatolási teszteket végrehajtó és a rendszert védő szakemberek között szervezeti falak lebontása várható,* mivel a folyamatban lévő támadások korai felismerését a „Red Team" szemlélet jócskán segítheti;
- *egyre kisebbnek tűnő hibák okozhatnak egyre komolyabb üzemzavarokat,* legyen szó kritikus infrastruktúra kieséséről (pl. Colonial Pipeline zsarolószoftverrel bénítása) vagy közösségi csevegő szolgáltatásról (pl. Whatsapp konfigurációs hibája).

ZÁRÓ GONDOLATOK

A kibertérből érkező fenyegetések kvantitatív és kvalitatív mértékek szerint egyre növekednek, jól mutatja ezt a 2022 március végén kiadott, az Európai Számvevőszék által jegyzett különjelentés[17] is:

„Megállapítottuk, hogy az uniós szervek felkészültségi szintje összességében

[16] 2022 Cyber Predicitions, https://www.baesystems.com/en/cybersecurity/feature/2022-cyber-predictions (letöltve: 2022.04.04.)

[17] https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=60922 (letöltve: 2022.04.04.)

nem áll arányban a fenyegetésekkel, és kiberbiztonsági fejlettségük igen eltérő. Javasoljuk, hogy a Bizottság javítsa az uniós szervek felkészültségét: ennek érdekében tegyen javaslatot kötelező kiberbiztonsági szabályok bevezetésére, valamint növelje a hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT-EU) forrásait."

Azt, hogy egy adott szervezet – sőt tágabban akár az állam – a kiberbiztonsági stratégiájában milyen fenyegetés-térképpel számol nem csupán a kibertér realitásai határozzák meg, nyilván az adott szervezet profilja, kitettsége, erőforrásai is. Nem egyszer bebizonyosodott már, hogy önmagában egy ragyogóan kidolgozott, minden támadási vektorra kiterjedő szemlélettel és részletes kockázatkezelési mátrixxal felépített stratégia önmagában csak néhány darab papír marad, ha a menedzsment nem áll demonstratívan a kitűzött biztonsági célok mögé a szükséges anyagi- és humán-erőforrásokkal, amennyiben indokolt, akár külső szolgáltatók bevonásával. *Azonban képzésre és fejlesztésre nem csak az elsődlegesen kézenfekvő vonalakon van szükség, hanem az IT-terület támogatói oldalán is. A HR, a beszerzés mellett a jog is egy olyan kritikus támogató terület, amelynek művelőit szintén speciálisan fel kell készíteni a szaktevékenységek releváns elméleti és gyakorlati aspektusaiból.*

A jogi támogató tevékenységnek pedig önmagában is fejlődnie kell, folyamatosan figyelemmel kísérve a kiberfenyegetéseket, és értékelve ezek jogi vonatkozásait a szervezet szempontjából, felkészítve a szervezeti döntéshozót az esetleges jogi következményekre. A szervezeti kibervédelem jogi compliance-vizsgálata, jogi kockázatelemzése és ehhez a szervezetre szabott szempontrendszer és módszertan mind segíthetnek a szervezet fenyegetettségi státuszának objektívebb megítélésében, a javítandó pontok felderítésében és folyamatos, ciklikus végrehajtásukkal a védelem szintje remélhetőleg magasabb színvonalon tartható.

Az ellátási láncok veszélyeztetettsége miatt már szóba került beszállítói szerződések és beszállítók (akik lehetnek pl. külsős fejlesztők, adatkezelők, vagy távközlési szolgáltatók is) jogi szempontú vizsgálata (due diligence, cégjogi, stb.) ugyanígy felmerülhet a foglalkoztatási jellegű jogviszonyokban is. *A hatályos nemzetközi, nemzeti jogi szabályozás, a szervezet belső IT biztonsági rezsimje pedig legalább a fontosabb kérdésekben a szervezetet érő hatások és annak működése vonatkozásában értékelő jogi sérülékenység-vizsgálatok végzését indokolhatja.* Mindezeket az értékeléseket olyan mutatók, paraméterek mentén kell megvalósítani, amelyek lehetővé teszik az eredmények objektív mérését, a tapasztalatok feldolgozását, kiértékelését, és ezeknek végül hatással kell lenniük, vissza kell csatolódniuk akár a stratégiák, intézkedési tervek tartalmára, adott esetben azok felmerült igények szerinti kiigazításával.

FELHASZNÁLT FORRÁSOK

[1] ANNAMÁRIA BELÁZ, CSABA KRASZNAY, ZSOLT SZABÓ: Cybersecurity strategy and leadership management issues. September 2020, IMCSM

Proceedings - An international serial publication for theory and practice of Management Science (pp.242-252), University of Belgrade, https://www.researchgate.net/publication/348432259_Cybersecurity_strategy_and_leadership_management_issues

[2] BIHARI LÁSZLÓ, MAGYAR SÁNDOR: Mennyország helyett a pokolba, avagy az informatikai támogatás kihívásai. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata 18 : 4 pp. 158-169. , 12 p. (2020)

[3] GARRETT DERIAN-TOTH, RYAN WALSH, ALEXANDRA SERGUEEVA, EDWARD KIM, ALIVIA COON, HILDA HADAN, JARED STANCOMBE: Opportunities for Public and Private Attribution of Cyber Operations. Tallinn Paper No. 12., Tallinn, NATO CCD COE, 2021.

[4] FARKAS ÁDÁM: A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai. In: Jog Állam Politika 2019/2. szám, 63-79. o.;

[5] FARKAS ÁDÁM: Biztonság – Geopolitika – Digitalizáció, avagy Amael Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. SmartLaw Research Group Working Paper 1 pp. 1-13. , 13 p. (2021)

[6] FARKAS ÁDÁM: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye?: Gondolatok az angol national cyber force kapcsán, Military and Intelligence CyberSecurity Research Paper 2021 : 1 pp. 1-8. , 8 p. (2021)

[7] KASSAI KÁROLY: Kibertér - Aktuális változások, Szakmai Szemle, XVII. évfolyam 1. szám 2019. március, 116. o.

[8] KELEMEN ROLAND: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. SmartLaw Research Group Working Paper 2 pp. 1-17. , 17 p. (2021)

[9] KELEMEN ROLAND, SZÉPVÖLGYI ENIKŐ: A modern technológia és ami mögötte van - Konferencia a modern technológia biztonsági kockázatairól és állam- és jogtudományi kapcsolódásairól. Katonai Jogi És Hadijogi Szemle 4 pp. 191-197. , 7 p. (2021)

[10] KELEMEN ROLAND: Cyberfare State – Egy hibrid állammodell 21. századi születése. In: Military and Intelligence CyberSecurity Research Paper 2022/1. szám.

[11] KOVÁCS LÁSZLÓ: Kiberbiztonság és -stratégia. Budapest, Dialóg Campus Kiadó, 2018.

[12] KOVÁCS LÁSZLÓ: A kiberbiztonság és a kiberműveletek megjelenése magyarország új nemzeti biztonsági stratégiájában. in: Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata 148 : 5 pp. 3-18. , 16 p. (2020)

[13] SUNGBAEK CHO ET. AL.: Recent Cyber Events: Considerations for Military and National Security Decision Makers, Tallinn., CCDCOE, Recent Cyber Events No 14 / January 2022

https://ccdcoe.org/library/publications/recent-cyber-events-considerations-for-military-and-national-security-decision-makers-2/

[14] Sophos 2022 Threat Report – Interrelated threats target an interdependent world, https://assets.sophos.com/X24WTUEQ/at/b739xqx5jg5w9w7p2bpzxg/sophos-2022-threat-report.pdf (letöltve: 2022.04.04.)

[15] Executive Order on Improving the Nation's Cybersecurity, May 12, 2021, Sec. 4. Enhancing Software Supply Chain Security, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[16] 2022 Cyber Predicitions, https://www.baesystems.com/en/cybersecurity/feature/2022-cyber-predictions (letöltve: 2022.04.04.)

[17] Európai Számvevőszék különjelentése, https://www.eca.europa.eu/hu/Pages/DocItem.aspx?did=60922 (letöltve: 2022.04.04.)


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/4.

Szerző(k) / Author(s):
Dr. Vikman László

Kézirat lezárásának ideje / Manuscript closing time:
2022.06.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.