Digitális környezetünk fenyegetettsége a mindennapokban

Szerkesztette:
BENCSIK BALÁZS
SABJANICS ISTVÁN

Dialóg Campus

Digitális környezetünk fenyegetettsége a mindennapokban

DIGITÁLIS KÖRNYEZETÜNK FENYEGETETTSÉGE A MINDENNAPOKBAN

Szerkesztette:
Bencsik Balázs – Sabjanics István

Dialóg Campus Kiadó ❖ Budapest
2018

A Belügyi Tudományos Tanács kiadványa.

Szerzők

Aradi Szilárd
Bencsik Balázs
Gáspár Péter
Gombás László
Gyaraki Réka
Hrucsár Mária
Kaszás Zoltán
Kollár Csaba
Kökényesi-Bartos Attila
Kőnig Balázs
Krepsz Balázs
Solymos Ákos
Tikos Anita

Tartalom

Szerkesztői előszó

A Belügyi Tudományos Tanács, az érintett önálló belügyi szervek szakmai együttműködésével – az elmúlt évek hagyományaihoz híven – tematikusan immár hetedik alkalommal szervezett a biztonságpolitika különböző kihívásait vizsgáló nemzetközi tudományos-szakmai konferenciát, ezúttal a Doktoranduszok Országos Szövetsége társszervezésével.

A kétnapos rendezvényre 2017. november 8–9-én, Budapesten, a Duna Palotában, plenáris ülés, két nyílt és egy zárt szekcióülés keretében került sor. A konferencia egyúttal az Európai Hálózatbiztonsági Ügynökség által szervezett nemzetközi tudatosító kampány, az Európai Kiberbiztonsági Hónap magyarországi kampányának záróeseménye, valamint a „Magyar Tudomány Ünnepe 2017" rendezvénysorozat belügyi fejezetének nyitóeseménye is volt.

A konferenciát Dr. Pintér Sándor, Magyarország belügyminisztere, a konferencia fővédnöke nevében Papp Károly rendőr altábornagy, országos rendőrfőkapitány és Dr. Kovács Zoltán, a Miniszterelnökség területi közigazgatásért felelős államtitkára köszöntötte. A plenáris ülés levezető elnöke Dr. Bencsik Balázs, a Nemzeti Kibervédelmi Intézet igazgatója volt. A tudományos tanácskozást Prof. Dr. Gáspár Péter, az MTA levelező tagja az önvezető autók biztonsági kérdéseiről szóló előadásával nyitotta meg. A nyitóelőadást követően az e-közigazgatás kibervédelmi kérdései kerültek górcső alá Hajzer Károly, a Belügyminisztérium informatikai helyettes államtitkára, valamint az okosváros-fejlesztések lehetőségei Füleky Zsolt, a Miniszterelnökség építészeti és építésügyi helyettes államtitkára előadásában. A tudományos tanácskozás mintegy hatvan előadása az IT-biztonsági kutatások, fejlesztések adta lehetőségeket, valamint az IT-fenyegetések, sérülékenységek kockázatait boncolgatta.

Minden olyan fórummal, amelyen a kiberbiztonsággal foglalkozó szakemberek irányítása mellett nyílik lehetőség a kibertérből érkező veszélyek kezelését elősegítő megoldások megvitatására, felkészültebbé válhatunk, és ezáltal saját szervezetünket, intézményünket is felkészültebbé tehetjük a jövőbeni információbiztonsági kihívásokra. A konferencia résztvevői számára az előadások új ismereteket közvetítettek, rendszerszemlélettel közelítették meg és összegezték a korábban meglévő tudást. Az elért és a konferencián ismertetett szakmai-tudományos eredményeket e konferenciakötetben foglaltuk össze.

A szerkesztők

Gáspár Péter[1] *– Aradi Szilárd*[2]

Önvezető járművek funkcionális és kommunikációs biztonsági kérdései

Bevezetés

Napjainkban a járműipar szinte minden részterületén folyamatos változáson megy keresztül. A hajtásláncoknál jelenleg még lassan, de folyamatosan gyorsuló ütemben terjednek az olyan alternatív megoldások, mint a hibrid és elektromos hajtások. Ezt a folyamatot tovább gyorsította a 2015-ben kirobbant „dízelbotrány", valamint a német szövetségi bíróság 2018. februári ítélete, amely lehetővé teszi az Euro 6-os környezetvédelmi besorolásnál rosszabb dízelüzemű gépjárművek városokból történő kitiltását.

A másik jelentős tempóban fejlődő terület a vezetéstámogató rendszereké;[3] a fejlesztők célja az, hogy végül teljesen automatizált járművek közlekedjenek az utakon. Ennek elérése érdekében két technológiai terület bevonására van szükség. Az egyik a modern vezeték nélküli infokommunikációs megoldások, a másik pedig a mesterséges intelligencia területe, azon belül is a gépi tanulás. A hagyományos autógyártók és beszállítóik ezzel a tudással korábban nem rendelkeztek, így mozgástérhez jutottak a nagy nemzetközi információtechnológiai (a továbbiakban: IT) cégek. Ezek komoly hatással voltak az elmúlt évek fejlesztéseire, amelyek között találunk pozitív és negatív példákat is. Az egyik legjelentősebb fejlesztés a Google önvezető autója, a cég Waymo néven jelenleg egy publikus pilot projektet futtat egy teljesen önvezető flottával Arizona állam bizonyos városaiban. *(1. ábra)*

---

[1] Dr. Gáspár Péter egyetemi tanár, az MTA doktora. MTA Számítástechnikai és Automatizálási Kutatóintézet, BME Közlekedés- és Járműirányítási Tanszék

[2] Dr. Aradi Szilárd egyetemi adjunktus. BME Közlekedés- és Járműirányítási Tanszék

[3] Gáspár Péter – Szabó Zoltán – Bokor József – Németh Balázs (2017): *Robust Control Design for Active Driver Assistance Systems: A Linear-Parameter-Varying Approach.* Springer International Publishing. Sename, Olivier – Gáspár Péter – Bokor József (2013): *Robust Control and Linear Parameter Varying Approaches.* Berlin–Heidelberg, Springer-Verlag.

1. ábra

Waymo önvezető autó tesztelés közben

Forrás: Waymo.com. Elérhető: https://waymo.com/ (A letöltés dátuma: 2018. 09. 21.)

A fejlesztők rendkívül komolyan veszik a biztonságot,[4] és kellő figyelmet fordítanak mind a virtuális, mind pedig a valós tesztekre. Sajnos negatív tapasztalatokat is találunk az elmúlt évekből. Az egyik a Tesla Autopilot nevű rendszerével kapcsolatos, amely halálos kimenetelű balesethez vezetett.[5] Mivel a rendszer 2-es szintű vezetéstámogató rendszer (lásd következő fejezetet), ezért a balesetért jogilag a járművezető a felelős. A másik szomorú példa frissebb: az Uber tesztelés alatt álló önvezető járműve – emberi felügyelet mellett – elgázolt egy kerékpárost, aki nem élte túl az ütközést. A téma felkapottsága miatt a fejlesztők minél gyorsabban próbálnak eredményeket felmutatni, és az új szereplők nem mindig követik azokat a biztonsági és tesztelési eljárásokat, amelyek a hagyományos gyártóknál már beváltak. Mindezek komoly etikai kérdéseket vetnek fel, s ezek veszélyeztethetik az önvezető járművek társadalmi elfogadottságát.

A következő fejezetekben először bevezetjük az önvezető járművekkel kapcsolatos alapvető fogalmakat, majd a járműirányítás és a funkcionális biztonság jelenlegi helyzetét tárgyaljuk. Ezt követően bemutatjuk a magasan automatizált járművek fejlesztésének aktuális trendjeit és a felmerülő problémákat. Rámutatunk arra is, hogy a mesterséges intelligencia rendkívül tág tudományterületének mely részeit próbálják jelenleg alkalmazni a járműirányítás területén. Végül kitérünk a jogi, etikai és infrastrukturális kérdésekre, majd egy rövid kitekintést adunk arról, hogy mi várható a következő években.

[4] Gáspár–Szabó–Bokor–Németh 2017

[5] Sename-Gáspár–Bokor 2013

Az önvezető jármű fogalma és szintjei

Önvezető jármű alatt általában olyan járművet értünk, amely szenzoraival érzékeli a környezetét, értékeli a valós szituációt, majd emberi beavatkozás nélkül döntéseket hoz, amelyek alapján aktiválja a beavatkozó komponenseit, így módosítva a jármű állapotát.

Az autonóm járművek működési kérdései közül három fő megoldandó feladatot érdemes kiemelni. Az első a környezetérzékelés, amelynek során egy adott térrészt akár több szenzorral is figyelve (szenzorfúzió), az objektumokat folyamatosan követve,[6] a rendszerünk minél pontosabb és megbízhatóbb modellt állít elő a környezetről. A második a szituációértékelés, amikor a rendszer a környezeti modell alapján kiértékeli az adott közlekedési szituációt annak érdekében, hogy megfelelő döntést hozhasson. A harmadik feladat a nagy biztonságú és megbízhatóságú járműirányítás elvégzése.

A következő fontos tisztázandó fogalom a járművek önvezetési szintje. Annak érdekében, hogy egyértelmű legyen, az egyes gyártók termékei milyen mértékben és milyen körülmények között képesek az önvezetésre, a Society of Automotive Engineers (a továbbiakban: SAE) bevezetett egy hatszintű követelményrendszert, amelyet közzétett a J3016 sorszámú ajánlásában.[7] Ezeket a szinteket adjuk meg az alábbiakban, összefoglalva a leglényegesebb tulajdonságokat:

0. szint: nincs automatizálás.
1. szint: vezetéstámogatás. Egyidejűleg csak hossz- vagy keresztirányú szabályozást valósít meg. A járművezető végzi a többi tevékenységet, és felügyeli a rendszer működését.
2. szint: részleges automatizálás. Egyszerre valósít meg hossz- és keresztirányú szabályozást. A járművezető folyamatosan felügyeli a rendszer működését, és azonnal beavatkozik, ha szükséges.
3. szint: feltételes automatizálás. Teljes körű irányítás egyes vezetési módokban. A járművezető mással is foglalkozhat, és a rendszernek időt (több másodpercet) kell hagynia a járművezető részére, hogy a szükséges beavatkozást elvégezze.
4. szint: magas szintű automatizálás. Teljes körű irányítás egyes vezetési módokban, amelyekben a járművezető felügyeletére nincs szükség.
5. szint: teljes automatizálás. Teljes körű irányítás minden vezetési módban, akár járművezető nélkül is.

Habár a jelenleg megvalósított rendszerek legfeljebb 2. szintűek, a gyártók a 4. és 5. szintek megvalósítását ígérik 5–10 éven belül. Fontos azonban látni, hogy a jelenlegi közlekedési környezet emberi érzékelésre van kialakítva. Azokat az emberi képességeket és tapasztalatokat, amelyeket a járművezetéshez használunk, rendkívül nehéz szoftverekkel szimulálni. Nagyon sok nem egyértelmű, vagy akár ellentmondásos közlekedési szituáció alakulhat ki az utakon. Ezeket a járművezetők gyakran intuitív módon, valamint egymással interakcióba lépve oldják meg. A speciális helyzeteket nagyon nehéz automatizált módon kezelni, sokkal egyértelműbb szabályokra és jobban ellenőrzött infrastruktúrára van szükség.

---

[6] *Waymo Safety Report: On The Road to Fully Self-Driving* (2017). Waymo. Elérhető: https://waymo.com/safetyreport/ (A letöltés dátuma: 2018. 09. 21.)

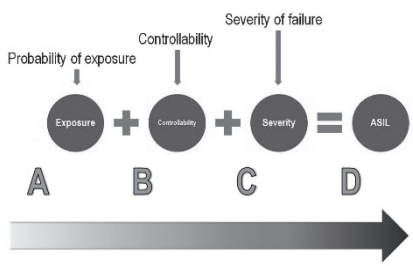
[7] *Waymo Safety Report: On The Road to Fully Self-Driving* 2017

Járműirányítás és funkcionális biztonság

A járművek esetén alapvetően kétféle biztonságot különböztetünk meg: vagyonbiztonságot *(security)* és balesetbiztonságot *(safety).* Az új, vezeték nélküli kommunikációs rendszerek miatt az elsőként említett is komoly kihívásokkal küzd, azonban mi elsősorban a járműirányításhoz kapcsolódó funkcionális biztonságra fókuszálunk a következőkben. A fejlesztőknek úgy kell megtervezniük a jármű működésébe beavatkozó irányítórendszereket, hogy minimalizálják a veszélyeztető meghibásodások valószínűségét. Erre többféle veszélyelemző és kockázatértékelő módszer létezik, amelyek segítségével a teljes fejlesztési folyamat alatt (beleértve a tesztelést és validációt is) szisztematikusan elemezhetők a rendszer biztonsági paraméterei. Ezek közül többet szabványba is foglaltak, így a járműgyártóknak egységes szabályok alapján kell biztosítaniuk azt, hogy minél alacsonyabb legyen az irányítórendszereik alkalmazásának kockázata.

A szabványok közül a lefontosabb az ISO 26262: „Road vehicles – Functional safety",[8] egy autóiparspecifikus nemzetközi szabvány, amely a biztonságkritikus rendszerek funkcionális biztonságára és a baleseti kockázatra fókuszál. Kimondottan a sorozatgyártású gépjárművek elektromos és elektronikus rendszereinek funkcionális biztonságát lehet kezelni e szabvány alapján. Legfontosabb elemei az ún. „ASIL szintek" *(2. ábra),* amely az „Automotive Safety Integrity Level" rövidítése. Ennek segítségével az egyes rendszerek és elemeik biztonsági kockázata absztrakt osztályokba sorolható, a következők szerint:

- a bekövetkezési valószínűség,
- a hiba súlyossága,
- a kezelhetőség (irányíthatóság).



2. ábra
ASIL szintek

Forrás: National Instruments. Elérhető: http://www.ni.com/white-paper/13647/en/ (A letöltés dátuma: 2018. 09. 21.)

Egy másik fontos ajánláscsoport az EURO NCAP biztonsági kiértékelési eljárásait tartalmazza.[9] Ez nagyon sok témakört ölel fel az aktív és passzív biztonsági rendszerek területén. Az önvezető járművek szempontjából ez az ajánláscsoport azért lehet fontos, mert

[8] *Special crash investigations: On-site automated driver assistance system crash investigation of the 2015 Tesla model S 70D (Report No. DOT HS 812 481)* (2018). Crash Research & Analysis Inc., Washington, D. C., National Highway Traffic Safety Administration.

[9] Törő Olivér – Bécsi Tamás – Aradi Szilárd – Gáspár Péter (2017): Cooperative object detection in road traffic. In *IFAC World Congress: IFAC-PapersOnLine.* Toulouse.

a vezetéstámogató rendszereket Európában ma ez alapján tesztelik és értékelik a gyártók: teszteljárásokat tartalmaz a különböző sebességszabályozó, menetstabilizáló, sávkövetést támogató és automatikus vészfékező rendszerekhez.

Trendek és problémák a járműautomatizálásban

Ha megvizsgáljuk az aktuális trendeket a járműiparban, azt láthatjuk, hogy az elektromobilitás és az önvezető járművek témája elsőbbséggel rendelkezik. Míg az első esetben egy részben már megoldott és aránylag jól lehatárolható problémával, az energiatárolással találkozhatunk, addig az önvezető járművek esetén rendkívül komplex műszaki kérdések mellett szabályozási és etikai kérdéseket is tartalmazó problémahalmazzal. Ennek ellenére a gyártók mindkét esetben hasonló időtávra adnak meg nagyívű terveket, amelyek jellemzően azt hangoztatják, hogy 2018–2019-ben megjelennek szériában az első 3-as szintű önvezető funkciók, majd 2020 és 2025 között a 4-es és 5-ös szintűek is. Jelenleg azonban azt látni, hogy a 2017-ben az Audi által beígért 3-as szintű alacsony sebességű funkció (autópálya torlódásasszisztens) még továbbra sem kapható szériában, és a többi gyártónak is csak 2-es szintű rendszerei vannak. Ennek megfelelően a 4-es, de különösen az 5-ös szintre vonatkozó jóslatokat és ígéreteket érdemes komoly fenntartásokkal fogadni. A Google önvezető autós fejlesztését azonban kiemelkedő projektként említhetjük,[10] amelynek keretében szériakialakítású önvezető Chrysler Pacifica Hybrid egyterűeket használhatnak a teljesen laikus önkéntesek. Ezek a járművek csak az adott városokban, de teljesen autonóm módon, emberi beavatkozás nélkül közlekednek. Ez azt vetíti előre, hogy néhány éven belül, korlátozott területen ugyan, de bárki által igénybe vehetők lesznek az önvezető járműveik.

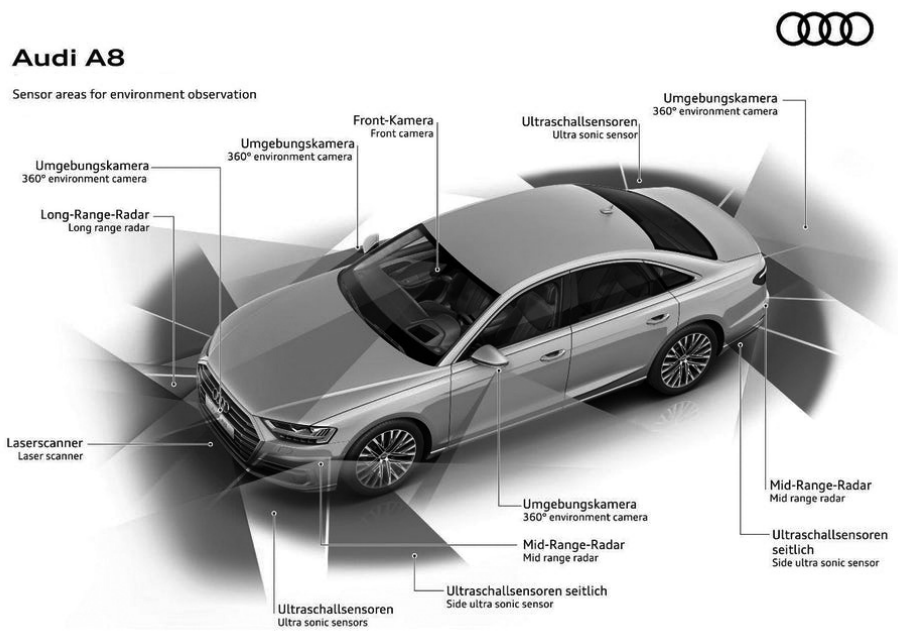
3. ábra

Példa az önvezető járművek környezetérzékelésére

Forrás: Waymo.com. Elérhető: https://waymo.com/ (A letöltés dátuma: 2018. 09. 21.)

[10] *Surface Vehicle Recommended Practice J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (2016). SAE International. Elérhető: https://www.sae.org/standards/content/j3016_201609/ (A letöltés dátuma: 2018. 09. 21.)

Ha a fejlesztési irányokat vesszük számba, akkor bizonyos kérdésekre már egyértelműbb válaszokat kaphatunk. A szenzorok területén jellemzően az tapasztalható, hogy minden gyártó a teljes térben (360 fokban) kívánja lefedni járműveit *(3. ábra),* redundáns módon, több hatótávolságra és látószögre bontva.



4. ábra

Az Audi A8 (2018) szenzorlefedettsége

Forrás: Audi.com. Elérhető: https://www.audi.com/en.html (A letöltés dátuma: 2018. 09. 21.)

Ami a technológiákat illeti, szinte minden gyártó használni kívánja a kamera, a radar, az ultrahang és a LiDAR (lézer alapú) szenzorokat is. Néhány fejlesztő próbálkozik tisztán kamera alapú megoldásokkal, de a megfelelő megbízhatóságot nem fogják tudni elérni. Az első három technológia már most is elterjedt a járművekben, ennek megfelelően tömeggyártásban a költségeik is alacsonyan tarthatók. A LiDAR szenzorok ára ugyan folyamatosan csökken, de még mindig túl drágák a sorozatgyártású járművekhez. A pontos szenzorszettek gyártónként különböznek ugyan, de az alapelvekben széles körű az egyetértés.

A másik fontos trend, ahol szintén többé-kevésbé konszenzusra jutottak a fejlesztők, az a mesterséges intelligencia alkalmazása. Abban szinte mindenki egyetért, hogy a jelenlegi szabályalapú algoritmusokkal nem lehet megoldani valamennyi komplex érzékelési, szituációértékelési és irányítási feladatot. Az egyik fő kutatási irány a gépi tanulási módszerek alkalmazása a járműirányítási feladatok megoldására. Ennek részleteit a következő fejezetben fejtjük ki.

Általánosságban elmondható, hogy az önvezető járművek alkalmazása csökkentheti a balesetek számát és növelheti a közúti közlekedés hatékonyságát. Azonban a változás bizonyosan egy elhúzódó folyamat lesz, ami azt eredményezi, hogy az automatizált járművek kezdetben drágák lesznek. Ezért érdemes felhasználói szempontból is megvizsgálni, hogy mely területeket hódíthatja meg először a technológia. Az egyik ilyen alkalmazás lehet a rövid, rögzített útvonalon mozgó minibusz szolgáltatás *(5. ábra).* Ehhez hasonló pilot projektek több helyen is megvalósultak az elmúlt években; elsősorban egyetemi campusokon, repülőtereken, esetleg kórházi, szanatóriumi környezetben lehet létjogosultságuk.

5. ábra

Az EasyMile EZ10 típusú vezető nélküli minibusz

Forrás: EasyMile.com Elérhető: http://www.easymile.com/ (A letöltés dátuma: 2018. 09. 21.)

A másik fő szolgáltatási terület lehet a taxi- és autómegosztó szolgáltatás, azonban itt is fontos szempont a járművezető kiváltásának költsége. Az önvezető funkciók közül az egyik rentábilis alkalmazás a nyerges vontatók oszlopban haladását megvalósító ún. „platooning" szolgáltatás, amely a baleseti kockázat csökkentése mellett az energiafogyasztásra is jótékony hatással lehet.[11] Várhatóan a magántulajdonban lévő személygépjárművek szintjén is megjelennek majd a különböző szintű önvezető funkciók.

Ugyanakkor az új technológiák bevezetése problémákat is felvet. Ha sikerül is kifejleszteni a megfelelő algoritmusokat, a tesztelés és validáció még óriási feladat lesz a fejlesztők és a jóváhagyó hatóságok számára. A tesztelések során a funkcionálisról szcenárió alapúra kell áttérni, és tekintettel a több tízmillió kilométernyi tesztelési igényre, erősen támaszkodni kell a szimuláció alapú megoldásokra.

[11] *ISO 26262:2011: Road vehicles — Functional safety* (2011). International Organization for Standardization. Elérhető: https://www.iso.org/standard/43464.html (A letöltés dátuma: 2018. 09. 21.)

Egy további új megoldandó probléma az önvezető autók által intenzíven használt vezeték nélküli technológiák (Connected Car) biztonsága. Ezek a rendszerek jelenleg a járművek szórakoztató és kényelmi berendezéseiben találhatók meg, segítségükkel a személyes „okoseszközök" csatlakoztathatók a járműhöz, és akár a kulcs szerepét is kiválthatják. Fontos alkalmazási terület a járművek közötti (Vehicle-to-Vehicle, V2V) és a járműinfrastruktúra (Vehicle-to-Infrastructure, V2I) hálózatok. Ezek segítségével a járművek kicserélhetik egymás menetdinamikai változóit (pozíció, sebességvektor, gyorsulásvektor, szögsebességek stb.), valamint távolról elérhetik az infrastruktúra jelzéseit és állapotát. E megoldás segítségével növelni lehet a szenzoradatok megbízhatóságát, illetve a hatóságok kezébe akár új eszközök adhatók a közlekedésirányítás vagy a szabályok betartatása területén. Ugyanakkor jelenleg tényként kell elfogadnunk, hogy a vezeték nélküli kommunikáció fizikailag „nyitott", így a vagyon és a személyes adatok védelme mellett fel kell készülni az olyan támadásokra is, amelyek közlekedési anomáliákat vagy akár balesetet is okozhatnak.

A mesterséges intelligencia alkalmazási lehetőségei

Ahogy a fentiekben már említettük, abban szinte egyhangú a vélemény, hogy elkerülhetetlen a mesterséges intelligencia alkalmazása az autonóm járművek irányítása területén. A következőkben áttekintjük, hogy mely területek adhatnak hatékony megoldásokat a legfontosabb járműirányítási problémákra.

A mesterséges intelligencia első alapvető fogalma az ágens. Ezen egy olyan algoritmust értünk, amely érzékeli környezetét, és autonóm módon cselekszik. A racionális ágens pedig a legjobb (várható) kimenetel érdekében cselekszik.[12]

A mesterséges intelligencia rendkívül széles tudományterület, ezen belül napjaink egyik legdinamikusabban fejlődő területe a gépi tanulás. Ennek két fő oka van: az első a számítógépek számítási teljesítményének évtizedek óta tartó exponenciális növekedése, a második pedig a hatalmas mennyiségű adat, ami az internet jóvoltából rendelkezésre áll. Definíció szerint egy számítógépes programról akkor mondjuk, hogy tanul egy *E* tapasztalatból a *T* feladat tekintetében, ha a teljesítménynek *T*-re vonatkozó *P* mérőszáma növekszik az *E* tapasztalattal.[13]

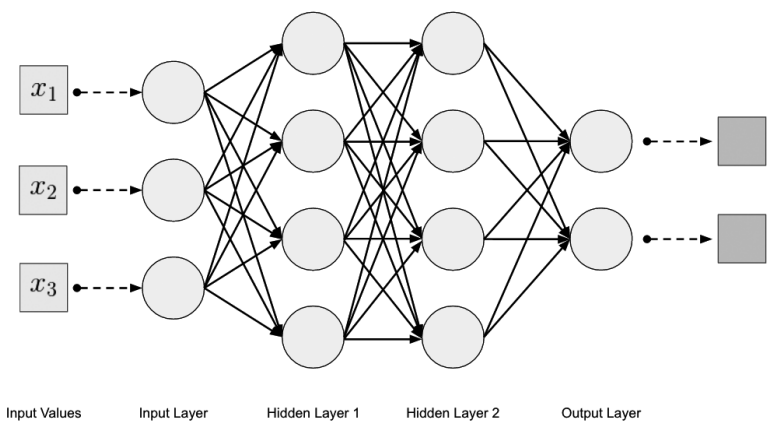
A gépi tanuláson belül három fontos csoportot különböztetünk meg, az alábbiak szerint.

- Felügyelt tanulás: címkézett adatok segítségével (azaz ismert bemenetekre ismerjük a rendszer válaszát) határozzuk meg a változók közötti függvénykapcsolatot.
- Felügyelet nélküli tanulás: következtető függvény előállítása, amely rejtett struktúrákat ír le címkézés nélküli adatokból.
- Megerősítéses tanulás: az ágens megtanulja, hogyan kell viselkednie egy adott környezetben, annak érdekében, hogy a jutalmát maximalizálja.

[12] *PROTOCOLS* (2018). Euro NCAP. Elérhető: https://www.euroncap.com/en/for-engineers/protocols/ (A letöltés dátuma: 2018. 09. 21.)

[13] *Be an early rider* (2018). Waymo. Elérhető: https://waymo.com/apply/ (A letöltés dátuma: 2018. 09. 21.)

A gépi tanuláson belül két fontos területet övez intenzív érdeklődés a járműipar részéről. Az első a mélytanulás vagy a mély mesterséges neurális hálózatok alkalmazása. A mesterséges neuron megalkotása már 1943-ban megtörtént, majd az 1960-as években Rosenblatt úttörő munkássága újabb lökést adott a téma kutatásának.[14] Azonban ezt követően az 1980-as évek végéig nem történt előrelépés, az új elméleti eredmények mellett később az egyre gyorsabb számítógépek is sokat segítettek a fejlesztésekben. Ekkor alakult ki a mélytanulás kifejezés is, amely a 2010-es évektől kezdve már a köztudatba is beszivárgott. A mélytanulás során olyan előrecsatolt neurális hálózatokat alkalmaznak, amelyek a be- és kimeneti rétegek között több rejtett réteget is tartalmaznak. Habár egy előrecsatolt neurális hálózat egy rejtett réteggel (véges számú neuronnal) is képes közelíteni folytonos függvényeket az n-dimenziós tér (R^n) egy kompakt részhalmazán, azonban több rejtett réteggel *(6. ábra)* ugyanaz a feladat kevesebb neuronnal is megvalósítható.[15]



6. ábra

Példa a többrétegű mesterséges neurális hálózatokra

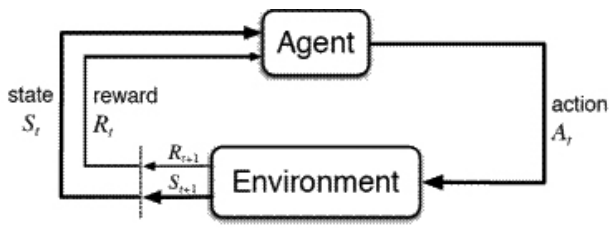
Forrás: Mitchell T. (1997): Machine Learning. McGraw Hill

Az ilyen többrétegű hálózatok kiválóan alkalmasak például klasszifikációs feladatokra, amikor a címkézett nyers szenzoradatokból betanítható egy objektumfelismerő hálózat. Ilyenkor nincs szükség klasszikus képfeldolgozási lépésekre, ezek maguktól alakulnak ki a hálózat rétegein belül. A járművekben elsősorban képfeldolgozásra használják ezeket a módszereket, amelyek a hálózat bemenete után általában konvolúciós rétegeket helyeznek el, emellett objektumklasszifikációra alkalmazzák radarjelek feldolgozásánál. Továbbá vannak olyan törekvések is, hogy a nyers szenzorbemenetekből közvetlenül próbálják előállítani a beavatkozó jeleket, ami az ún. „end-to-end-learning" feladatokhoz vezet, például a hálózat sávkövetésre való betanítását a kameraképből és a kormányszögből oldják meg.

[14] Rödönyi Gábor – Gáspár Péter – Bokor József – Palkovics László (2014): Experimental verification of robustness in a semi-autonomous heavy vehicle platoon. *Control Engineering Practice,* 28. évf. 1. sz. 13–25.

[15] Russel, Stuart – Norvig, Peter (2005): *Mesterséges Intelligencia – modern megközelítésben.* Budapest, Panem Kft.

A másik fontos terület a gépi tanuláson belül az úgynevezett megerősítéses tanulás, amely a klasszikus valószínűségi megközelítéséket próbálja ötvözni a mély neurális hálózatokkal. A megerősítéses tanulás alapelve, hogy az ágens megadott akciókat hajthat végre (cselekszik) a környezetében, amelynek hatására a környezet állapota megváltozik, és egy új állapotvektort ad vissza az ágensnek *(7. ábra).*



7. ábra

Az ágens–környezet interakció egy Markov döntési folyamatban

Forrás: ROSENBLATT F. (1957): The Perceptron – a perceiving and recognizing automaton. Report 85-460-1, Cornell Aeronautical Laboratory

A másik nagyon fontos tulajdonsága a megerősítéses tanulásnak, hogy minden egyes lépésben egy skalár értéket, az úgynevezett jutalmat is visszaadja az ágens részére. Az ágens célja, hogy a kumulált jutalom jelet hosszú távon maximalizálja. Emiatt a megerősítéses tanulásnál az állapotváltozók meghatározásán túl a jutalom definiálása is elsődleges fontosságú, hiszen ez határozza meg az optimalizációs célt. A környezetmodellezés jellemzően Markov-folyamattal történik, míg az ágens viselkedését egy ún. „policy" függvény írja le, amely az állapotok és akciók közötti összerendelést adja meg, így a cél az optimális „policy" meghatározása. Léteznek olyan módszerek is, amelyek nem közvetlenül próbálják meghatározni a „policy"-t, hanem az egyes állapotokhoz értékeket rendelnek hozzá („value" függvény) attól függően, hogy mekkora várható jutalmat lehet elérni az adott állapotból. Itt használják fel a kutatók a mélytanulás eredményeit, és mély neurális hálózatokkal közelítik a „policy" és „value" függvényeket.

A legtöbb megerősítéses algoritmus nem ismeri a környezet modelljét *(model-free),* csak a választható akciókat, az állapotvektort és a jutalmat. Ennek megfelelően az algoritmus véletlenszerű akciókkal kezdi működését, és iteratív módon keresi az optimális megoldást. A keresés során fontos megtalálni a felfedezés *(exploration)* és kihasználás *(exploitation)* egyensúlyát, azaz, hogy mennyit használjon fel még a meglévő tudásból, és mennyit próbálkozzon még véletlenszerűen. Itt a mérleg a tanulás hossza és a lokális optimumokban való beragadás között billeg. Ezek a módszerek alkalmasak lehetnek trajektória-tervezésre,[16] döntéshozásra, energia- és egyéb optimumok megtalálására. Előnyük a felügyelt tanulással szemben, hogy nem kell megadni az optimális tanítómintákat, azok maguktól alakulnak ki. Így például egy trajektória-tervezésnél nem az ember által végrehajtott trajektóriát tanul meg az ágens, hanem egy majdnem optimálisat. Érdekes példákat mutatnak erre a téma egyik vezető kutatóhelyének, a Deepmindnak az eredményei. A cég kutatói számítógépes és táblajátékokkal demonstrálják eredményeiket. A legutóbbi AlphaGo Zero algoritmusuk

[16] GIBSON, Adam – PATTERSON, Josh (2017): *Deep Learning.* O'Reilly Media.

sakkban és góban is az emberi játékosok, valamint a jelenlegi legjobb sakkgépek fölé emelkedett.[17] Úgy érte el ezt, hogy előzetes ismeretek nélkül, pusztán magával játszva tanulta meg az optimális stratégiákat.

Jogi, etikai és infrastrukturális kérdések

Röviden kitekintést adunk a járműirányítás területén kívül eső, de azokkal összefüggő megoldandó problémákra is. A jogi és az etikai háttér szorosan összefügg. Sok országban (többek között Magyarországon) bizonyos feltételekkel engedik az önvezető járművek tesztelését. Pár éven belül – várhatóan szériában is – az utakra kerülhetnek részleges önvezető funkciókkal rendelkező járművek, ezért szükséges a jogi szabályozást minél hamarabb kialakítani. Az egyik legfontosabb kérdés, hogy egy teljesen önvezető járműnek mi legyen az elsődleges biztonsági célja. Azaz, hogy egy elkerülhetetlen balesetnél a teljes kockázatot (a többi résztvevőre vonatkozó kockázatot is ideértve), vagy csak a járműben ülők kockázatát csökkentse. Társadalmi elvárás lehetne, hogy a teljes kockázatot mérlegelje, de az értékesítést ez jelentősen megnehezítené. A másik kérdés, hogy a jelenlegi közlekedési szabályokat figyelembe véve, mely szabályokat és milyen módon szeghetné meg az önvezető jármű. Például a záróvonalátlépést nem lehet teljesen szigorúan tiltani, hiszen egy szabálytalan kikerülő akár életet is menthet. Egy kisebb sebességtúllépés a forgalomtól függően akár csökkentheti is a baleseti kockázatot. Ezek szabályozása alapvető fontosságú, hiszen a gyártóknak óriási felelősségük lesz, ezért tisztában kell lenniük a lehetőségeikkel. Végül a közvélemény előtt is ismertek a morális döntési kérdések. Például az, hogy egy elkerülhetetlen baleset esetén kinek az élete ér többet. Szerencsére az önvezető járművek a várható szituációkat előre kiértékelik, és nagyon kis valószínűséggel állnak elő olyan szimmetrikus helyzetek, amelyekben mindkét választási lehetőség ugyanolyan kockázatokat rejt, így ez a kérdés talán az adott helyzet kockázatelemzésével is megoldható.

Végül mindenképpen szót kell ejteni az infrastruktúra helyzetéről. Ennek minősége és karbantartási szintje kulcsfontosságú az autonóm járművek megfelelő működéséhez. A jelenlegi jelzések és azok ellenőrzései az emberi látást, nem pedig a gépi látást veszik figyelembe. Ennek megfelelően sok olyan hiba és következetlenség előfordulhat, amely az embernek nem, azonban a gépnek problémát okoz. Az útburkolati jelek és közlekedési táblák szigorúbb szabványosítása is fontos lenne. Szintén érdemes megemlíteni az ideiglenes elterelések és jelzéseiket: gyakran találkozhatunk nem egyértelmű szituációkkal *(8. ábra),* amelyeket a korábban már leírt módon, intuíció és kooperáció alapján képesek megoldani az emberi járművezetők.

[17] Mitchell, Tom M. (1997): *Machine Learning.* McGraw-Hill.

8. ábra

Példa a nehezen értelmezhető jelzésekre

Forrás: Richmond District Blog. Elérhető: https://richmondsfblog.com/ (A letöltés dátuma: 2018. 09. 21.)

Jövőkép

Az egyik legérdekesebb kérdés a jövőre vonatkozóan, hogy mikor fogjuk elérni az 5-ös önvezetési szintet, ami elvileg azt jelenti, hogy a jármű minden közlekedési helyzetet meg tudni oldani. A jelenlegi – rendkívül sokféle – infrastruktúrát és szabályokat figyelembe véve várhatóan még sokáig lesznek legalább országos szintű korlátozások. Az európai szintű, teljes körű önvezetés kifejlesztése akár még évtizedekbe is telhet. Azonban 1–2 éven belül már elérhetővé válnak az önvezető 3-as szintű autópálya- és torlódásasszisztensek, továbbfejlesztett automata parkolási rendszerek. Valószínűleg hamarosan elterjednek a most kissé mostohán kezelt V2V és V2I rendszerek, azonban ezek csak akkor igazán hatékonyak, ha széles körben elterjednek, így esetleges kötelezővé tételük fontos lehet.

Végezetül leszögezhetjük, hogy az egyre jobban automatizált járművek mindenképpen nagyon biztonságot és energiahatékonyabb közlekedést eredményeznek a közutakon. Addig azonban még nagyon sok feladat vár megoldásra mind a járműirányítás, mind a kapcsolódó tudományágakon belül, továbbá a döntéshozóknak is fel kell készülniük az új kihívásokra.

Felhasznált irodalom

Be an early rider (2018). Waymo. Elérhető: https://waymo.com/apply/ (A letöltés dátuma: 2018. 09. 21.)

Gáspár Péter – Szabó Zoltán – Bokor József – Németh Balázs (2017): *Robust Control Design for Active Driver Assistance Systems: A Linear-Parameter-Varying Approach*. Springer International Publishing.

Gibson, Adam – Patterson, Josh (2017): *Deep Learning.* O'Reilly Media.

ISO 26262:2011: Road vehicles — Functional safety (2011). International Organization for Standardization. Elérhető: https://www.iso.org/standard/43464.html (A letöltés dátuma: 2018. 09. 21.)

Mitchell, Tom M. (1997): *Machine Learning.* McGraw-Hill.

PROTOCOLS (2018). Euro NCAP. Elérhető: https://www.euroncap.com/en/for-engineers/protocols/ (A letöltés dátuma: 2018. 09. 21.)

Rosenblatt, Frank (1957): The Perceptron – a perceiving and recognizing automaton. *Report 85-460-1,* Cornell Aeronautical Laboratory.

Rödönyi Gábor – Gáspár Péter – Bokor József – Palkovics László (2014): Experimental verification of robustness in a semi-autonomous heavy vehicle platoon. *Control Engineering Practice,* 28. évf. 1. sz. 13–25.

Russel, Stuart – Norvig, Peter (2005): *Mesterséges Intelligencia – modern megközelítésben.* Budapest, Panem Kft.

Sename, Olivier – Gáspár Péter – Bokor József (2013): *Robust Control and Linear Parameter Varying Approaches.* Berlin–Heidelberg, Springer-Verlag.

Special crash investigations: On-site automated driver assistance system crash investigation of the 2015 Tesla model S 70D (Report No. DOT HS 812 481) (2018). Crash Research & Analysis Inc., Washington, D. C., National Highway Traffic Safety Administration. Elérhető: https://crashstats.nhtsa.dot.gov/Api/Public/Publication/812481 (A letöltés dátuma: 2018. 09. 21.)

Surface Vehicle Recommended Practice J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (2016). SAE International. Elérhető: https://www.sae.org/standards/content/j3016_201609/ (A letöltés dátuma: 2018. 09. 21.)

Törő Olivér – Bécsi Tamás – Aradi Szilárd – Gáspár Péter (2017): Cooperative object detection in road traffic. In *IFAC World Congress: IFAC-PapersOnLine.* Toulouse.

Waymo Safety Report: On The Road to Fully Self-Driving (2017). Waymo. Elérhető: https://waymo.com/safetyreport/ (A letöltés dátuma: 2018. 09. 21.)

Ajánlott irodalom

Csáji Balázs Csanád (2001): *Approximation with Artificial Neural Networks.* MSc Thesis. Eindhoven.

Hegedűs Ferenc – Bécsi Tamás – Aradi Szilárd – Gáspár Péter (2017): Model Based Trajectory Planning for Highly Automated Road Vehicles. In *IFAC World Congress: IFAC-PapersOnLine.* Toulouse.

Silver, David – Schrittwieser, Julian – Simonyan, Karen – Antonoglou, Ioannis – Huang, Aja – Guez, Arthur – Hubert, Thomas – Baker, Lucas – Lai, Matthew – Bolton, Adrian – Chen, Yutian – Lillicrap, Timothy – Hui, Fan – Sifre, Laurent – Driessche, George van den – Graepel, Thore – Hassabis, Demis (2017): Mastering the game of Go without human knowledge. *Nature,* 550. 354–359.

Sutton, Richard S. – Barto, Andrew G. (2017): *Reinforcement Learning: An Intorduction.* The MIT Press.

Kaszás Zoltán[1]

CTRL, avagy kontroll a biztonságunk felett – a T-Systems kiberbiztonsági központja

Bevezetés

A negyedik ipari forradalmat éljük,[2] amely a korábbiakhoz hasonlóan alapvetően változtatja meg, forgatja fel jelenlegi viszonyainkat. Egy-egy nemzet boldogulása azon múlik, hogy miként, milyen gyorsan tud alkalmazkodni az ebből adódó kihívásokhoz.

1. ábra

Az ipari forradalmaknak a digitalizáció felé vezető lépcsőfokai

Forrás: 361Consult.com. Elérhető: https://361consult.com/digitalisierung-verstehen/was-ist-digitalisierung/die-4-industrielle-revolution-die-stufen-bis-hin-zur-digitalisierung/ (A letöltés dátuma: 2018. 09. 21.)

A kihívások a kibervédelem területén nem a jövőre, hanem a *„most"*-ra vonatkoznak. Amikor egész iparágak működése alapvetően az intelligens információs rendszerek zavartalan, hibamentes működésén múlik, és az információs rendszerekben mutatkozó legkisebb zavar is azonnali pénzügyi veszteségként jelentkezik, döntő szerepe van a biztonságnak.

A BMW-gyárban példának okáért rendkívül magas az integráltság foka, mindent az intelligens informatikai rendszer vezérel. A verzióváltásokat úgy kell végrehajtani tervezett módon, hogy a legkisebb, másodperces leállás sem megengedett. Amennyiben zavar támad, egy tízperces leállás kötbére egy hónapi jövedelemtől fosztja meg az üzemeltető informatikai céget, ilyen szigorúak a feltételek. Ez az üzemszerű működésből adódó veszély, amely

---

[1] Kaszás Zoltán vezérigazgató. T-Systems Magyarország Zrt.

[2] *„A nyugati civilizáció eddig három ipari forradalmat élt meg, a gőzgépek, szerelőszalagok és az automatizáció után most egy teljesen új, negyedik ipari forradalom zajlik. A legújabb ipari forradalom arról szól, hogy a fizikai gépek és tárgyak egy információs hálózatba kapcsolódnak, a reálgazdaság egyetlen hatalmas, intelligens információs rendszerbe integrálódik. Az ipar 4.0 pedig egy olyan koncepció, amely az újkeletű forradalom kihívásaira ad válaszokat, mégpedig elsősorban az ipari folyamatok teljes digitalizációjával. De nem csupán a technológia térhódításáról van szó, hanem az üzleti folyamatok paradigmaváltásáról is. Magyarországnak és Európának pont az ipar 4.0-ra van szüksége."* Turzó Ádám Pál (2016): *A ma ismert világot totálisan elsöpri a negyedik ipari forradalom.* Portfolio.hu. Elérhető: https://www.portfolio.hu/vallalatok/it/a-ma-ismert-vilagot-totalisan-elsopri-a-negyedik-ipari-forradalom.237125.html (A letöltés dátuma: 2018. 09. 21.)

tervezhető és elkerülhető, elkerülendő. A kibertámadás azonban olyan bizonytalansági faktort visz be a rendszerbe, amelyre szintén fel kell készülni. Egy adatokat eltulajdonító kártékony kód akár több száz napig is meghúzódhat és rombolhat észrevétlenül az informatikai rendszerben, ennek fényében nem meglepő, hogy a rendszerbetörések 54%-ára csak hónapokkal később derül fény.

Az információs rendszerek funkciói, az igazgatási modell és az azt megvalósító intelligens informatikai rendszer működése a megrendelő és a szállító együttműködésében valósul meg, ezzel szemben az informatikai biztonság területén egy új, az előző kettő szándékaival ellentétes szereplő is megjelenik, a rosszindulatú, szándékosan kárt okozó, hírszerző tényező, amely mögött egyre gyakrabban nem egyes személyek, csoportok, hanem államok állnak. A fentiek miatt ki kell építeni az államvédelmi képességet, ugyanakkor a nagy szolgáltatók önvédelme is igen fontos.

Az állam kibervédelmi szervezetei és kapcsolódásuk a vállalkozói civil szféra megoldásaihoz

Az állam kibervédelmi szervezetei

2013. április 15-én az Országgyűlés elfogadta 2013. évi L. törvényt az állami és önkormányzati szervezetek elektronikus információbiztonságáról (Ibtv.) és rendeleteit, amelyek kijelölték az információbiztonsággal foglalkozó szervezeteket, valamint azok együttműködésének szabályait. (Ibtv. 50§)

A Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) szervezetén belül három szakmai területet alakítottak ki:

- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterületet (GovCERT-Hungary, Kormányzati Eseménykezelő Központ);
- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterületet, a Nemzeti Elektronikus Információbiztonsági Hatóságot (NEIH);
- a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási és sérülékenységvizsgálati szakterületet.

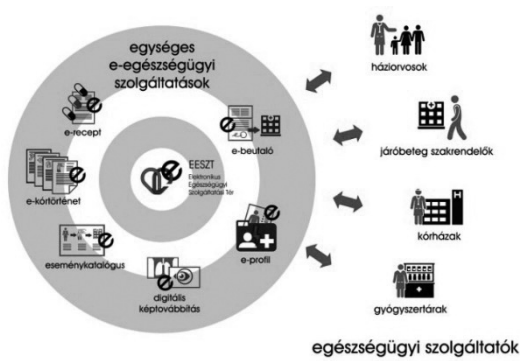
A GovCERT a kormányzati szervek kibervédelmét látja el, a Magyar Honvédség pedig létrehozta a MilCERT-et, mivel napjainkban hagyományos katonai, modern és hibrid hadviselési kihívások egyaránt előfordulnak. A virtuális, illetve kibertérben naponta több százezer támadás érhet egy országot. Ennek nyomán a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program a magyar hadiipar újjáépítését és a korszerű technológiai fejlesztéseket is célul tűzte ki.[3]

[3] *Kibervédelmi parancsnokságot létesítenek a honvédségen belül* (2018). eGov Hírlevél. Elérhető: https://hirlevel.egov.hu/2018/03/10/kibervedelmi-parancsnoksagot-letesitenek-a-honvedsegen-belul/ (A letöltés dátuma: 2018. 09. 21.)

A vállalkozói civil szféra

A vállalatok, így a T-Systems Magyarország Zrt. (a továbbiakban: TSM) is szoros kapcsolatban áll elsősorban az NKI szervezetével, különös tekintettel azokra a nagy rendszerekre, melyek az állampolgárokat jelentős, többmilliós számban érintik. Az Elektronikus Egészségügyi Szolgáltatási Tér (a továbbiakban: EESZT) egy olyan alkalmazás, amely egy modern és egységes informatikai környezetben olyan felhőalapú technológiát használó kommunikációs teret hoz létre, amely a jelenleg elérhető legmagasabb fokú adat- és kibervédelemmel ellátva kapcsolja össze az egészségügyi ellátókat egymással – beleértve a kórházi, a járóbeteg- és a háziorvosi ellátást, valamint a gyógyszertárakat is.[4] A rendszer lényege, hogy az egészségügy valamennyi szereplője bárhol beléphet az egységes platformra, és ott hozzáférhet egy adott beteg más intézményekben keletkezett adataihoz. Ezzel – ha nem is egy csapásra, de – megszűnik a korábbi leletek és zárójelentések kikérése és cipelése egyik helyről a másikra: aki orvoshoz megy, arról az adatai megadása után az orvos azonnal tudni fogja, hogy milyen gyógyszereket szed, milyen érzékenysége, allergiája van, vagy milyen betegségei, műtétei voltak korábban. Tekintettel az adatok rendkívül szenzitív voltára, a Nemzeti Kibervédelmi Intézettel rendkívül szoros kapcsolatot alakított ki a TSM, amelynek során a vállalat sérülékenységi vizsgálatokat végzett, és az egész fejlesztést kiemelt módon támogatta.

A projekt sikeresen zárult, bevezetése korszakalkotó jelentőségű volt az egészségügy számára. A projektet sikerült úgy implementálni, hogy a kibervédelem végig a fókuszban legyen, jelenleg az alkalmazást a TSM működteti és folyamatosan fejleszti, rendszerleállás a kibervédelem hiányosságai miatt vagy más okból sem fordult elő. A kormány képviseletében több fórumon, minisztériumi szinten is elismerően nyilatkoztak az itt végzett munkáról, amely mintaként szolgálhat a hasonló monumentális projektek sikeres lebonyolítására.



2. ábra

Az EESZT és az egészségügyi szolgáltatók

Forrás: Megszűnik a rendelőkben a sorban állás? (2017) Portfolio.hu. Elérhető: https://www.portfolio.hu/gazdasag/egeszseggazdasag/megszunik-a-rendelokben-a-sorban-allas.266613.html (A letöltés dátuma: 2018. 09. 21.)

[4] Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) (é. n.). Elérhető: https://e-egeszsegugy.gov.hu/eeszt (A letöltés dátuma: 2018. 09. 21.)

Kihívások a nemzetközi térben

Az informatikai rendszerek biztonsága csak nemzetközi szinten értelmezhető. A hálózatok, rendszerek integráltsága a Föld valamennyi pontjára kiterjed, nincs jelentősége annak, hogy az adott rendszer, objektum hol, melyik országban található, a kibertámadások nem ismernek államhatárokat.

Az informatikai tér szereplői folyamatosan vizsgálják a rendszereik sérülékenységét, és próbálják megakadályozni annak bekövetkezését, hogy a felfedezett sérülékenység kárt okozzon. Még a kár bekövetkezése előtt lépnek közbe, annak érdekében, hogy a kárt minimalizálják.

A hibrid hadviselés kiemelt eszköze a kiberhadviselés

A modern kor háborúja permanens, és békeidőben kezdődik. A cél a potenciális ellenség folyamatos gyengítése valamennyi létező területen. A hibrid hadviselés lényege, hogy a támadó egy adott ország teljes infrastruktúráját, politikai berendezkedését, társadalmát támadja. Ez azzal jár, hogy tipikusan nem katonai célpontot támad, hanem a közigazgatás, a gazdaság ellehetetlenítését célozza, így keltve például társadalmi elégedetlenséget, vagy csak egyszerűen zavart, kárt okoz.

A háború eddig általánosnak vélt szabályai megváltoztak az utóbbi években. Előtérbe kerültek a nem-katonai eszközök a stratégiai és politikai célok elérésében. A hibrid hadviselés egyesíti a hagyományos, az irreguláris és a *kiberhadviselést.* Az új hadviselési forma összemossa a határokat a háború és béke formális megkülönböztetése között.

3. ábra

A hibrid hadviselés

Forrás: Ministry of Defence, Singapore. Elérhető: https://www.mindef.gov.sg/oms/content/dam/imindef_media_library/photos/cyberpioneer/news/2015/mar/05mar15_news/05mar15_news.jpg (A letöltés dátuma: 2018. 09. 21.)

A Geraszimov-doktrína

Valerij Geraszimov orosz vezérkari főnök, a módszer atyja szerint a színes forradalmak és az arab tavasz teljesen átírták a hadviselés formai és tartalmi kritériumait. Az orosz hibrid hadviselés abból indul ki, hogy nem a gyengébb, hanem az erősebb fél használja az aszimmetrikus hadviselés formáit ellenfelével szemben. Híven mutatja ezt az új orosz geopolitikai stratégiát a függő helyzetű *de facto* államok létrehozása Oroszország tőszomszédságában, példa rá a Moldovából kiszakított Dnyeszter Menti Köztársaság, a Grúziától önállósodott Abházia és Dél-Oszétia, az Azerbajdzsán területéből kiszakadó Hegyi-Karabah, vagy az Ukrajnában különleges státuszhoz jutó Donyecki és Luhanszki „Népköztársaság".[5]

A Kreml szerint Washington kezdte

Geraszimov tábornok előadásában részletezte, hogy a hibrid hadviselés gyökerei Washingtonhoz kötődnek, amely világszerte alkalmazza azt rezsimek leváltására, mivel a hibrid hadviselés a nemzetközi jog szerint nem számít agressziónak.

A nyugati államokat azzal vádolta meg, hogy számos nem katonai eszközt vetnek be államok ellen, ezáltal mobilizálják a helyi lakosságot tüntetésekre, a közösségi média igénybe vételével. A vezérkari főnök szerint világos a háború és a béke közötti választóvonal elmosódása, de Moszkva mindenképp fellép a nyílt és titkos agresszió ellen.[6]

A Nyugat szerint Putyin destabilizál

Erről a Nyugatnak eltérő a véleménye, hiszen a német elhárítás egy jelentése éppen az orosz katonai hírszerzéshez köthető Fancy Bear csoportot vádolja hibrid hadviselés rendszeres végrehajtásával. A jelentés példaként hozza fel a 2015. december 23-i támadást az ukrán villamosenergia hálózat ellen, amelynek eredményeként 230 ezer ember maradt áram nélkül.

Emellett a szerb médiában erőteljesen jelen levő orosz sajtó sikeresen terjesztette el, hogy az amerikaiak és az EU nyugati nagyhatalmai szervezkednek Koszovóban. Ki akarják iktatni Milorad Dodik boszniai szerb vezetőt, és Albániának már odaígérték Macedónia felét. Az orosz beavatkozás olyan erősre duzzadt a térségben, hogy Theresa May brit miniszterelnök bejelentést tett: 2018-tól újraindítják a BBC szerb nyelvű adását, emellett nyugat-balkáni csúcsot tartanak, kiemelt figyelmet fordítanak a térséggel való biztonsági együttműködésre a kibertámadások ellen.[7]

Iráni, szaúdi kormányzati rendszerek elleni támadás

2012-ben történt két hatékony támadás az iráni és szaúdi kormányzati rendszerek ellen, amelyek során a merevlemezeken lévő adatokat teljes mértékben törölték.

A malware néven ismert támadás azért lett ennyire sikeres, mert a támadók azt egy ukrán adóbevallási program frissítésének álcázták. Ezzel a taktikával minden valamilyen formában Ukrajnában adózó céget elértek. Ez természetesen jelentős károkat okozott

[5] Káncz Csaba (2017): Eljött a hibrid háborúk kora. Privátbankár.hu. Elérhető: https://privatbankar.hu/makro/eljott-a-hibrid-haboruk-kora-305458 (A letöltés dátuma: 2018. 09. 21.)

[6] Káncz 2017

[7] Káncz 2017

az ukrán gazdaság számára: az adatvesztésen túl visszaesett a gazdasági kibocsátás is. A károk mértéke még nem pontosan beazonosítható.

Szakértők szerint e támadások nem tipikus bűnözésnek tekinthetők, a cél egyértelműen a szándékos károkozás volt. Az elkövető kiléte jelenleg sem tisztázott, mivel nincsenek konkrét bizonyítékok, csak sejteni lehet, hogy a támadás kinek állhatott érdekében.[8]

Orosz beavatkozás az Egyesült Államok elnökválasztásába

Mint ismeretes, 13 orosz állampolgár és 3 jogi személy ellen vádat emeltek a 2016-os amerikai elnökválasztási folyamatba való feltételezett orosz beavatkozás miatt, az ügyben összehívtak egy nagy esküdtszéket. A bizottság véleménye szerint a vádlottak megsértették az amerikai törvényeket, beavatkoztak az Egyesült Államok politikai folyamataiba és választásába. Csalás, banki csalás, összeesküvés és személyazonossági adatok eltulajdonítása szerepelt a vádpontok között. Az esküdtszék dokumentumai alapján a vádlottak a 2016-os elnökválasztás megzavarására már 2014-től készültek.

A vádlottak létező amerikai állampolgárok lopott személyazonossági adataiból hoztak létre hamis személyazonossági adatokat, társadalombiztosítási kártyákat és bankszámlákat. A hamis dokumentumok segítségével internetes weboldalakat és e-mail-fiókokat készítettek, amelyeken keresztül elsősorban bevándorlásról, vallási kérdésekről és a Black Lives Matter nevű afroamerikai mozgalomról közöltek álhíreket és bejegyzéseket. Valódi identitásuk elrejtése érdekében amerikai számítógépes hálózatokat alkalmaztak.

A vádlottak politikai aktivistaként is megjelentek, reklámidőt és reklámokat vettek, emellett politikai gyűlések szervezésében is részt vállaltak. Egy amerikai székhelyű csoport (meg nem nevezett) tanácsára az ingadozó választói kedvről ismert államokat vették célba. A választást követően Donald Trumpot támogató gyűléseket rendeztek az országban.

Rod Rosenstein, az Egyesült Államok főügyész-helyettese kiemelte, hogy az oroszok nem voltak képesek befolyásolni választás eredményét.

A vádemelésre Donald Trump a Twitteren reagált, hangsúlyozta, hogy ez a megállapítás felmenti őt a gyanú alól, hogy a kampánystábja együttműködött volna az oroszokkal. „Oroszország 2014-ben kezdte meg az Egyesült Államok elleni kampányát, jóval azelőtt, hogy bejelentettem indulásomat az elnökségért" – írta üzenetében Trump. Hozzátette: „a választási eredményeket nem érintette. A Trump-kampány semmi rosszat nem tett – nem volt összejátszás!" A Facebook globális politikáért felelős alelnöke is közleményt adott ki, miszerint a cég megduplázza s ezzel 20 ezerre emeli az álhíreket is figyelő biztonsági munkatársak számát, emellett aktív együttműködést folytat az FBI érintett részlegével, annak érdekében, hogy az oroszok és mások se legyenek képesek az amerikai választási folyamatokat befolyásolni. Továbbá kiemelte, hogy a vállalat vezetése és munkatársai nagyobb erőfeszítést fognak tenni a jövőbeli támadások kivédése érdekében. A fenti példák bizonyítják az informatikai rendszerek támadhatóságát.[9]

---

[8] Gálffy Csaba (2017): Nem is zsarolóvírus a 2017-es Petya. Hwsw.hu. Elérhető: https://www.hwsw.hu/hirek/57459/petya-ransomware-wiper-virus-titkositas.html (A letöltés dátuma: 2018. 09. 21.)

[9] *Elképesztő, milyen komoly volt az orosz beavatkozás az amerikai választási kampányba* (2018). Hvg.hu. Elérhető: http://hvg.hu/vilag/20180217_Elkepeszto_milyen_komoly_volt_az_orosz_beavatkozas_az_amerikai_valasztasi_kampanyba (A letöltés dátuma: 2018. 09. 21.)

4. ábra

Trump reakciója a Twitteren

Forrás: Furious Trump lets rips at ‚fake news media' for not reporting Facebook exec's tweet confirming majority of Russian spend on ads happened AFTER the election (2018). Daily Mail. Elérhető: https://www.dailymail.co.uk/news/article-5404523/Trump-cites-Facebook-VP-Saturday-tweet-storm.html (A letöltés dátuma: 2018. 09. 21.)

A potenciális veszélyforrások feltárása és a védekezés megszervezése

Kulcsfontosságú rendszerekről és újabban a hardverekről is sorozatban derülnek ki, hogy biztonsági veszélyeket, lukakat, réseket rejtenek.

A Windows rendszerek rutinszerűen frissülnek, hogy az egyre-másra felfedezett biztonsági réseket betömködje a gyártó. A biztonsági frissítések nélkül a rendszerünk összeomlik, vagy szinte biztosan támadás áldozatává válik.

A már említett állami GovCERT honlapja folyamatosan informál a felfedezett biztonsági résekről. Nemrégiben arra figyelmeztetett, hogy a Cisco Talos Intelligence Group elnevezésű szervezet felfedezett egy VPNFilter nevű szoftverkárosítót, amely a világban rendkívül elterjedt. Az eddigi adatok szerint 54 országban több mint félmillió hálózati eszközt (router) megfertőzött, és ezzel veszélyes kaput nyitott. A fertőzést a szakértők véleménye szerint az orosz titkosszolgálatok hajtották végre, feltehetően a szolgálatukban álló hackercsoportok segítségével. A valódi cél az Ukrajna ellen indított kibertámadás előkészítése lehetett, azonban ez a káros szoftver elterjedt a világ számos országában. A szakértők eredményei nyomán a szoftvert terjesztő szervert az FBI leállíttatta.

Legutóbb a számítógépek lelkében, a processzorban fedeztek fel biztonsági réseket, amelyeket csak körülményesen lehetséges befoltozni. Haladéktalanul be kell zárni a felfedezett biztonsági réseket, ám ez gyakran rendkívüli erőfeszítést igényel, jó példa erre az, ami Észtországban történt.

Észtország sok szempontból az Európai Unió informatikai mintaállama, rengeteg szolgáltatást épített az elektronikus személyi igazolványra, és olyan innovációs megoldásokat használt, amelyek jelentős újításokat hordoztak, azonban emiatt nem tesztelték azokat.

A személyiigazolvány-chipek titkosítását könnyen vissza lehetett fejteni, mert a kiválasztásuknál nem voltak elég körültekintők. Emiatt később arra kényszerültek, hogy visszavonják a hibás chippel ellátott kártyával kiadott elektronikus személyi igazolványokat, és biztonságos cserekártyákat adjanak ki.[10]

Zsarolóvírusok

A zsarolóvírusok 2016 évben kerültek a figyelem középpontjába. Károkozásuk abban nyilvánul meg, hogy a számítógépen tárolt adatokat, szövegállományokat, családi és egyéb fényképeket titkosítják, ezáltal a számítógép tulajdonosa elől elzárják. A titkosítást csak a feloldókulcs birtokában lehetséges feloldani, ezt a zsaroló hacker csak komoly pénzösszeg fejében adja át.

Gyakran előfordul, hogy a követelt összeg – általában bitcoin vagy más kriptovaluta – átadását követően sem jut hozzá a megzsarolt a titkosítás feloldását lehetővé tevő kulcshoz, az állományok továbbra is hozzáférhetetlenek maradnak.[11]

A Petya zsarolóvírus

A zsarolóvírusok közül az egyik legnagyobb sajtónyilvánosságot a Petya elnevezésű zsarolóvírus kapta. Ennek oka, hogy az addig tabuként kezelt – közvetlen életet veszélyeztető – egészségügyi rendszereket támadta meg, s ezzel méltán vívta ki a közvélemény egységes haragját. Angliai nagyvárosok és megyék kórházaiban támadta meg az egészségügyi rendszereket, és tette azokat használhatatlanná az állományok titkosítása révén. A kórházakban akadozott a számítógépes rendszerek működése, sőt a telefonrendszereké is. A hozzáférhetetlen adatokat a mentésekből igyekeztek pótolni. Az érintett kórházakban csak közvetlen életveszély esetén fogadtak betegeket, sürgősségi eseteket, a többi gyógyító tevékenységet leállítottak.[12]

A T-Systems válasza a kihívásokra – A TSM hackertámadások elleni védekezése

A fenti érvek és veszélyek alapján a hazai informatikai biztonság kérdése a jövő szempontjából kulcsfontosságú. A pénzügyi források korlátozott volta, valamint az egyre égetőbben jelentkező szakemberhiány miatt kialakult helyzetet tovább súlyosbítja, hogy az érintett vállalatok vezetése nem mindig van tisztában a kibervédelem fontosságával. A belső erőforrások korlátozott voltára, a megfelelő kompetencia megteremtésének nehézségeire nyújt

[10] *760 ezer elektronikus személyit tiltottak le Észtországban váratlanul* (2017). eGov Hírlevél. Elérhető: https://hirlevel.egov.hu/2017/11/06/760-ezer-elektronikus-szemelyit-tiltottak-le-esztorszagban-varatlanul/ (A letöltés dátuma: 2018. 09. 21.)

[11] Gálffy 2017

[12] Bolcsó Dániel (2017): Zsarolóvírus söpört végig a világon. Index.hu. Elérhető: https://index.hu/tech/2017/05/12/kibertamadas_erhetett_angliai_korhazakat (A letöltés dátuma: 2018. 09. 21.)

megoldást a T-Systems Security Operations Center (a továbbiakban: SOC). Ez a szolgáltatás a legkorszerűbb technológiával, a legképzettebb szakértőkkel áll rendelkezésre a kibervédelem területén.

Lehetőség van a reakcióidő radikális csökkentésére, és ezáltal az okozott kár jelentős csökkentésére. Az eddigi tapasztalatok alapján a károsító vírus települése, aktivizálódása, majd a károkozás észlelése is hosszabb időt vesz igénybe, nem beszélve az elhárítási időről és az elhárítás kompetenciaigényéről. Ezek a reakcióidők radikálisan lerövidülnek a fenti szolgáltatás igénybevételével.

Gyakori jelenség, hogy a beruházásokra, a rendszerek kifejlesztésére megszerezhetők a források, azonban a rendszer üzemeltetésére, a biztonság megteremtésére, a folyamatos, magas színvonalú kibervédelemre azonban rendszerint nincs forrás. Ráadásul a kibervédelem nem egy statikus helyzetre adandó statikus választ jelent, hanem a dinamikusan változó kihívásokra azonnali válaszokat igényel, ami naprakész információval, képzettséggel rendelkező szakembergárdát és eszközállományt feltételez.

CTRL

A fenti problémák megoldására hozta létre a T-Systems a CTRL Security Operations Centert, amely nagyobb befektetés nélkül teszi lehetővé a magyarországi vállalatok számára, hogy biztonságban tudják adataikat, rendszereiket.

Az utóbbi időben gyakorivá – szinte rendszeressé – vált kibertámadások miatt minden nagyvállalat volt már célpontja rosszindulatú, a saját- és az ügyféladatok megszerzésére irányuló támadásnak.

Egy-egy kártékony kód akár fél éven túl is rejtőzködhet és rombolhat észrevétlenül az informatikai rendszerben. A rendszerbetörések több mint a felére csak hónapokkal később derül fény.

A negyedik generációs T-Systems CTRL Security Operation Center már nem csupán a támadások utólagos elemzését teszik hatékonyabbá, hanem azok detektálását és elhárítását is. Ehhez szükséges mértékben külső szolgáltatásokat, erő- és adatforrásokat vonnak be, mesterséges intelligenciát és nagy adatokon használt elemzési módszereket alkalmaznak a szakemberek. A vizsgált naplóállományok az ügyfél rendszerében maradnak, azokhoz a CTRL szakemberei csak távoli hozzáférést kapnak, ezzel biztosítva a legmagasabb biztonsági fokozat elérését.

Természetesen a CTRL központ saját biztonsági zónával rendelkezik: eszközei, alkalmazásai, hálózatai szeparáltak és függetlenek a T-Systems Magyarország informatikai infrastruktúrájától, így a CTRL a legmagasabb biztonsággal, auditálható módon működik.[13]

[13] *Jön a kontroll: biztonsági szuperközpontot hozott létre a T-Systems* (2018). Hvg.hu Elérhető: http://hvg.hu/tudomany/20180425_t_systems_ctrl_security_operations_center_tsm_telekom_kiberbiztonsag_kozpont (A letöltés dátuma: 2018. 09. 21.)

A T-Systems információbiztonsági tevékenysége

Az informatikai biztonság egyfajta mérleg: egyik serpenyőjében az üzleti és törvényi elvárások, az adatvagyon értéke és a jó hírnév áll; a másikban a biztonsági rendszerek költsége és a szabályzatok megalkotásának és betartatásának nehézségei. Hazánk legsokoldalúbb informatikai biztonsági vállalataként küldetésünk, hogy az egyensúly kialakításában és folyamatos fenntartásában segítsük ügyfeleinket üzleti folyamataik megértésével, a biztonsági kockázatok felmérésével és csökkentésével.

Szolgáltatásaink több mint két évtizedes rendszerintegrátori és biztonsági tapasztalatokra, a *best practice* ajánlásokra és a nemzetközileg elfogadott metodológiákra épülnek; termékeink pedig világszínvonalú hardver-, illetve szoftvergyártók fejlesztései.

Biztonsági koncepcióink szerint csak átfogó, a tanácsadási és a megvalósítási feladatokat egyaránt magába foglaló gondolkodással lehet megfelelni az IT-biztonság egyre összetettebb kihívásainak.

Adatszivárgás elleni védelmi megoldás

A vállalat legfőbb értékét képviselő adatok szándékos vagy véletlen kiszivárgása jelentős kockázati tényező minden szervezet üzletmenete és biztonságos működése szempontjából. Fontos adatok kiszivárgása az üzleti pozíció, illetve az ügyfelek bizalmának elvesztését, vagy a jó hírnév sérülését is eredményezheti.

Az adatok kiszivárgása elleni védekezés összetett feladat: ismerni kell többek között a szervezet adatvagyonát, az adatok kiszivárgásának lehetséges csatornáit, valamint a bekövetkező kár mértékét is.

IT-biztonsági szolgáltatásaink

Cégünk 1994 óta foglalkozik IT-biztonsági megoldásokkal. Az akkoriban megjelenő új fenyegetések ellen (vírusok, internetes behatolási kísérletek) először csak magunkat próbáltuk védeni. Felismerve, hogy ezek a veszélyek ügyfeleinket is érintik, hamarosan telepítettük Magyarország első tűzfalait.

Biztonsági üzletágunkat 1999-ben hoztuk létre, hogy Unix, Windows és tanácsadói tapasztalatainkra építve az informatikai biztonság különböző területeit szakszerűbben kezelhessük.

Mára az informatikai rendszerek és a hálózati infrastruktúra életciklusánakminden biztonsági elemére kínálunk megoldást: a kockázatok elemzésétől a biztonsági politikák és szabályzatok kialakításán, az ezeket támogató eszközök szállításán és integrálásán át a biztonsági távfelügyeletig.

Megalapítása óta (2005) minden évben részt veszünk az IT-biztonság legnagyobb hazai független seregszemléjének, az Informatikai Biztonság Napjának megszervezésében, ahol a multinacionális gyártók, szállítók mellett számos hazai konkurensünk is elfogadja a kiállítói, előadói részvételre vonatkozó felkérést.

Minősítéseink, vizsgáink, partnereink

A magyar piacon egyedülálló módon, több mint 50 tanácsadói és műszaki képzettségű szakemberünk foglalkozik az IT-biztonsági feladatok ellátásával.

Szakembereink, vizsgáink

- A Cisco CCIE, CCSP komplex vizsgákkal igazolt minősítései, a McAfee, EMC-RSA, Check Point, Balabit és sok más neves biztonsági gyártó vizsgái mellett számos független képesítést is szereztünk a biztonsági területeken:
  - Certified Information System Security Professional (CISSP)
  - Certified Information System Auditor (CISA)
  - Certified Information System Manager (CISM)
  - CompTIA+
  - Certified Ethical Hacker (CEH)
  - EC-Council Certified Security Analyst (ECSA)
  - Certified in Risk and Information Systems Control (CRISC)

Partnereink az IT-biztonságban

- Cisco-Ironport – Gold Partner
- McAfee – Elite Partner
- EMC-RSA – Affiliate Elite Partner
- BalaBit – Support Partner
- Check Point – Silver Partner
- Microsoft – Certified Gold Partner, Security Solutions minősítéssel
- Attachmate-NetIQ – Associate Reseller
- Thales-nCipher – Value Added Reseller

A felsorolt gyártók mellett rendszeres projektkapcsolatban vagyunk olyan gyártókkal, mint a SafeNet, az IBM, az Entrust vagy a Websense.

IT-biztonsági szolgáltatásaink

- Kockázatok és sérülékenységek felmérése
- Határbiztonsági, határvédelmi megoldások
- Hozzáférések, jogosultságok kezelése
- Információvédelem, adatvédelem
- Incidensek kezelése, felügyelet
- Megfelelőség biztosítása *(Compliance)*

Kockázatok és sérülékenységek felmérése

Minden vállalat számára kulcsfontosságú, hogy tisztán láthassa üzleti, műszaki, informatikai kockázatait. A biztonságtudatos rendszerfejlesztés alapja a sérülékenységek folyamatos vizsgálata, a kockázatok naprakész számbavétele, és az azzal arányos védelmi lépések meghatározása.

A vizsgálatok szükségessége gyakorlatilag minden rendszer esetében igazolható, hiszen egy újonnan bevezetett informatikai elem, vagy egy már régóta működő, ugyanakkor biztonsági szempontból elhanyagolt rendszer hasonló veszélyeket rejthet magában.

Kockázatelemzési és -kezelési megoldásaink
Elemzésünkben feltárjuk és súlyozzuk a szervezetben rejlő IT-biztonsági kockázatokat (adott esetben az informatikai rendszer műszaki sérülékenységeit), és megoldást javaslunk a kezelésükre. Az elemzést biztonsági tanácsadók és szakértők végzik.

Információbiztonsági helyzetfelmérés
A szolgáltatás keretében magas szintű felmérést végzünk az információbiztonság általános szintjének feltárásáért. A felmérés azonosítja azokat a területeket, ahol jelentős eltérés van a jelenleg alkalmazott biztonsági megoldások, bevezetett folyamatok és az általánosan követett piaci gyakorlat (MSZ ISO/IEC 17799:2006)[14] között. A T-Systems akciótervet dolgoz ki az azonosított hiányosságok mérséklésére.

A feltárt hiányosságok rangsorolása révén a szervezet képes lesz korlátos anyagi és emberi erőforrásait a legkomolyabb biztonsági problémák kezelésére fordítani.

Műszaki sérülékenységek felméréses elemzése
A rendszerben több olyan kockázat rejlik, amely a magas szintű helyzetfelmérésnél mélyebb vizsgálattal, az informatikai rendszer és az alkalmazások felépítésének, működésének, beállításainak elemzésével tárható fel.

Etikus hack, behatolásvizsgálat és social engineering végrehajtása
Lényeges, hogy egy rendszer biztonsági szintjét, a szabályzatok betartását éles körülmények között is rendszeresen teszteljük. Ilyenkor a T-Systems szakértői valódi hackermódszerek bevetésével, előre kidolgozott módszertan mentén szisztematikusan végigvizsgálják az adott rendszert. Az informatikai rendszereket átvilágító megoldásokhoz kapcsolódhat a munkatársak viselkedését, biztonságtudatosságát próbára tevő úgynevezett *social engineering* vizsgálat is. A projekt végén javaslatot teszünk a hiányosságok kiküszöbölésére és a problémák megoldására.[15]

---

[14] MSZ ISO/IEC 17799:2006 szabvány: Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (2006). Magyar Szabványügyi Testület. Elérhető: http://mszt.hu/web/guest/ingyenes-szabvanylista;jsessionid=D1C233976E01F28F67F6AD6A48F41B09?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_msztwebshop_WAR_MsztWAportlet_ref=152658&_msztwebshop_WAR_MsztWAportlet_javax.portlet.action=search (A letöltés dátuma: 2018. 09. 21.)

[15] *Kockázatok és sérülékenységek felmérése* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/kockazatok-es-serulekenyseg-felmerese (A letöltés dátuma: 2018. 09. 21.)

Határbiztonsági, határvédelmi megoldások

Az internet felől érkező támadások egyre gyakoribbak és összetettebbek, ezért minden vállalat számára alapvető fontosságú a megfelelő határvédelmi rendszer kiépítése.

Ma, amikor szinte minden egérkattintáskor – történjen az böngészőablakban vagy levelezőprogramban – potenciális vírusfertőzéssel vagy más kártékony kód lefuttatásával nézünk szembe, a kockázatokkal arányos védelem nem merülhet ki egy tűzfalrendszer egyszeri letelepítésében.

A T-Systems neves gyártók megoldásaira alapozva többszintű határvédelmet kínál, a hálózati eszközökbe épített biztonsági funkciók aktivizálásától az összetett tűzfalrendszereken, behatolás-érzékelőkön keresztül a tartalomszűrő megoldásokig. Ügyfeleink igénye alapján akár 7 × 24 órás rendelkezésre állást kínálunk, hiszen a biztonsági szint folyamatos fenntartása olyan speciális kompetenciát igényel, amelyre sok vállalat nem tud saját erőforrást biztosítani.

Határvédelmi és határbiztonsági szolgáltatásaink

Tűzfalrendszerek
A tűzfalak az informatikai rendszer határvédelmi politikáját kikényszerítő eszközök, amelyek a hálózatok közötti forgalom szabályozását, ellenőrzését végzik. Cégünk mind csomagszűrő, mind alkalmazás szintű proxy tűzfalakat ajánl megoldásaiban – akár a két technológiát kombinálva.

Behatolás-érzékelő és -megelőző rendszerek, IDS/IPS
A tűzfalak által nem észlelhető, illetve a belső hálózaton történő támadások érzékelésére és elhárítására alkalmas eszközök. Feladatuk a hálózaton kommunikálni próbáló trójai programok, a jogosulatlan belépési kísérletek és egyéb, az alkalmazások vagy az operációs rendszer sérülékenységének kihasználására irányuló tevékenységek észlelése és megakadályozása.

Távoli biztonságos elérés, VPN
Megoldásaink lehetővé teszik a nyilvános hálózatokon keresztül zajló biztonságos kommunikációt, amely például a távmunka esetén elengedhetetlen. Megoldásainkban törekedünk az integrációra más határvédelmi megoldásokkal, hogy egyszerű legyen a központosított adminisztrálás és felügyelet.

Hálózatok szegmentációja
A belső hálózat biztonságának egyik alappillére, hogy a vállalati struktúrában különálló szervezetek a hálózatban is legyenek elkülönítve. Ennek eredményeképpen jól kezelhető és védhető zónák jönnek létre, amelyekben egyedi biztonsági szabályrendszert lehet kialakítani hálózati szinten. Az egyes szervezetek így csak a számukra valóban szükséges szolgáltatásokhoz, erőforrásokhoz férnek hozzá.

Kommunikációs kapcsolatok titkosítása
A szolgáltatásnak köszönhetően az adatforgalom már a belső hálózaton titkosított, így kizárható a belső hálózatról indított jogosulatlan lehallgatási kísérlet. A kommunikációs kapcsolatok titkosítása kiemelten fontos a napi szinten kritikus adatokat kezelő ügyfeleinknél, ahol alapvető szükséglet, hogy az információ a teljes kommunikáció ideje alatt csak az arra jogosult személyek számára legyen elérhető.

Hálózatihozzáférés-védelem (NAC)
Olyan technológiák kombinációja, amely lehetővé teszi a belső hálózatra csatlakozás szabályozását. A NAC megoldás folyamatosan elemzi és értékeli a végpontok megfelelőségi állapotát, és szükség esetén javítási lehetőségeket is biztosít. Alkalmazásával elkerülhető, hogy azonosítatlan vagy nem a biztonsági szabályzatokban előírt védelmi állapotú (például nem megfelelő operációs rendszer verzióval, elavult vírusirtóval rendelkező) számítógép csatlakozzon a hálózathoz.[16]

Hozzáférések, jogosultságok kezelése

Napjainkban már egy általános informatikai rendszerrel rendelkező cégnél is több alkalmazáshoz kap hozzáférést egy új felhasználó. Az idő múlásával a kolléga egyre több új feladatot, hatáskört és jogokat kap, a jogosultságok, felhasználónevek és jelszavak pedig csak halmozódnak.

A kilépett kollégák nem megfelelő kezelése ennél is kritikusabb: számos aktív bejelentkezési azonosító, postafiók, akár távoli bejelentkezési lehetőség marad véletlenül a szervezettől már távozott embernél a központosított felhasználómenedzsment hiánya miatt.

A probléma az első komolyabb auditig (rosszabb esetben visszaélésig, illegális adathozzáférésig) nem is derül ki. Megfelelő központi nyilvántartás nélkül utólag nem deríthető ki sem az adott időpontban meglévő hozzáférés jogossága, sem a jogok odaítélésének felelőse.

Szolgáltatásaink

Jogosultságok kezelése
Az alkalmazások általában komplex jogosultsági rendszerrel rendelkeznek. Jgosultságkezelési projekt alatt a hozzáférések és jogosultságok felderítését, osztályozását, rendszerezését és a kialakított rend menedzselésére alkalmas megoldás implementációját értjük. A megoldás jellemzően lehet előkészítő jellegű tanácsadói feladat, amelynek során a felderítés, rendszerezés szakaszát végezzük el, illetve megvalósítás is, amely során a jogosultságok menedzselését végző megoldást implementáljuk.

---

[16] *Határbiztonsági, határvédelmi megoldások* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/hatarbiztonsagi-hatarvedelmi-megoldasok (A letöltés dátuma: 2018. 09. 21.)

Erős azonosítás (smart card / token)
Az informatikai rendszerhez és annak alkalmazásaihoz hozzáférő felhasználók azonosítása a felhasználónév/jelszó párosnál erősebb, biztonságosabb megoldással is kezelhető. Az erős azonosítás kétfaktorú azonosítók bevezetését jelenti, vagyis a felhasználók egy olyan tárgyat kapnak, amelynek birtoklásával, valamint az eszközhöz tartozó PIN-kód ismeretével két azonosítási faktorral rendelkeznek.

Egyszerűsített bejelentkezés (Single Sign On, SSO)
A felhasználók egyetlen, kiemelkedő biztonsági szintű – egy vagy több faktorú – azonosító egyszeri beírásával, egyszerre lépnek be az összes informatikai rendszerbe és alkalmazásba. A megoldás csökkenti az üzemeltetési költségeket, javítja a nyomon követhetőséget és szabályozottságot.

Szerepkörösítés
A szolgáltatás tartalmazza a felhasználók csoportokba rendezését, illetve azok jogainak és jogosultságaiknak pontos meghatározását az informatikai rendszerekben és alkalmazásokban. A megoldás különálló egységként is alkalmas a biztonsági szint növelésére, de alapvető szerepet játszik a komplexebb jogosultságkezelési projektek során is.[17]

Információ-védelem, adatvédelem

Az adatok kiszivárgás elleni védelmének biztosítása összetett feladat, többszintű, egymást kiegészítő, integrált kontrollok szükségesek hozzá.

Szolgáltatásaink

Adat- és információszivárgás elleni védelem
Egy szervezet biztonságos és folytonos működése szempontjából a belső munkatársak lényegesen nagyobb fenyegetést jelentenek, mint a szervezeten kívülről érkező támadások. Versenytársainktól eltérően az adatvédelmet nem tekintjük megoldottnak csupán egy DLP (Data Loss Prevention) eszköz bevezetésével. A T-Systems által kialakított módszertan strukturált megközelítésen alapszik, amelynek végrehajtásával hatékonyan csökkenthető az üzletmenet szempontjából kritikus információ kiszivárgásának veszélye. A módszertan egy olyan ciklikus fejlesztési folyamat kialakításának menetét írja le, amelynek segítségével egy kockázatokkal arányos, átfogó védelmi rendszer alakítható ki és tartható karban.

DLP eszközök
Az adatok, információk a szervezet legfontosabb vagyonát képezik. A DLP olyan technológiák összessége, amelyek elsődleges feladata, hogy megakadályozzák a vezetés által stratégiai szempontból kritikusnak vagy fontosnak nyilvánított adatok kiszivárgását. A rendszer

[17] *Hozzáférések, jogosultságok kezelése* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/hozzaferesek-jogosultsagok-kezelese (A letöltés dátuma: 2018. 09. 21.)

figyeli a lehetséges szivárgási csatornákat, beleértve a pendrive-okat, laptopokat, nyomtatókat, mobiltelefonokat.

A DLP az egyik leghasznosabb és legfontosabb biztonsági megoldás. Külön szolgáltatásként is kitűnő megoldás, de kiegészítő szolgáltatásként javasolt az adat- és információszivárgás elleni szabályozó környezet kialakítása is.

Titkosítási megoldások (fájlok, meghajtók, pendrive-ok)

Az informatikai rendszerben képződő különálló állományok vagy akár a kliens gépek teljes tartalma titkosítható. A megoldás bevezetésével megakadályozható, hogy az eltulajdonított/elvesztett notebookok vagy pendrive-ok érzékeny tartalma jogosulatlan kezekbe kerüljön.

Tartalomszűrő megoldás

A szervezetek befelé vagy kifelé áramló adatforgalmában sok a káros vagy kiszűrendő tartalom. A webes és e-mail tartalomszűrők több lehetőséget kínálnak káros tartalmak bejutásának megakadályozására, de az adatok kiszivárgásának megakadályozására is felhasználhatók.

Kártékony alkalmazások elleni védelem (vírusok, malware-ek)

Az informatikai rendszerek kliensalkalmazásai állandó biztonsági kockázatnak vannak kitéve, hiszen a klasszikus fenyegetések – vírusok, kártékony kódok – mind őket támadják. A támadások ellen azok a kliensoldali alkalmazások nyújtanak hatékony védelmet, amelyek egyesítik a vírusok elleni védelem, a kártékony programok elleni küzdelem és a személyi védelmi megoldások elemeit.

Elektronikus aláírás, időpecsét, biztonságos kulcstárolás, PKI

Az informatikai rendszerekben és alkalmazásokban keletkezett állományok (például dokumentumok, e-mailek) elláthatók elektronikus aláírással és időpecséttel, amely azonosítja a dokumentum készítőjét és hitelesen rögzíti a keletkezés idejét. A biztonság tovább fokozható biztonságos kulcstároló (HSM) eszközök alkalmazásával. A PKI (Public Key Infrastructure) az ehhez szükséges hátteret teremti meg. A megoldás gyakori kiegészítője az erős azonosítás és egyszerűsített bejelentkezés.

Elektronikus aláírási infrastruktúra

Annak érdekében, hogy teljesen kihasználjuk az elektronikus aláírás lehetőségeit, a munkakörnyezet részévé kell tenni az ehhez szükséges infrastruktúrát. Ebbe beleértendő mind a kiszolgáló, mind a kliens oldal. Az ilyen rendszerek (PKI) funkciói közé soroljuk sok más mellett a hitelesítési szolgáltató (CA) felállítását, a megfelelő címtár kialakítását, vagy a meglévő használatát, és a felhasználók által használt eszközöket is (például intelligens kártya).

Tanúsítványok és intelligens kártyák életciklusának menedzsmentje

A modern elektronikus aláírással és titkosítással foglalkozó rendszerek alapja, hogy a kulcsok és egyéb elemek intelligens kártyákon legyenek tárolva. Miután a munkatársak már napi szinten használják kártyáikat a munkafolyamatokban, szükséges, hogy a kártyák lejáratát, elvesztését és más, a használatukkal összefüggő eseményeket informatikai mód-

szerekkel kövessük, támogassuk megfelelő folyamatok kitalálásával, dokumentálásával és szoftverrel.[18]

Incidensek kezelése, felügyelet

A legbiztonságosabbnak tartott informatikai rendszer vagy szabályzat bevezetése és helyes használata mellett is elkerülhetetlen a biztonsági incidensek előfordulása. Fontos kérdés tehát, hogy milyen módszereket és eszközöket alkalmazunk, milyen lépéseket teszünk a folyamatban lévő támadás érzékelésére, a további káresemény megakadályozására, vagy éppen egy-egy esemény utólagos kivizsgálására. Ezeket a célokat szolgálják a központosított naplógyűjtő és eseménykezelő rendszerek**.**

Az informatikai eszközök által generált logok (naplóadatok) nagy mennyisége miatt a naplósorok közötti összefüggések, korrelációk elemzése biztonsági naplóelemző rendszer bevezetése nélkül szinte lehetetlen. A T-Systems által kínált eszközök sikerrel birkóznak meg a feladattal. Monitoring és távfelügyeleti szolgáltatásaink olyan cégeknek is hatékony segítséget nyújtanak, amelyek nem tudják belső erőforrás biztosításával ellátni az eszközök által gyanúsnak ítélt incidensek humán intelligenciát igénylő felülvizsgálatát.

Incidenskezelési, felügyeleti megoldásaink

Naplóadatok elemzése
Az informatikai rendszerekben sok IT-biztonsági eszköz vagy a biztonságban szerepet játszó alkalmazás készít naplóállományokat. Ezek az állományok kulcsfontosságúak a rendszer biztonsági állapota és a rendszerben zajló tevékenységek követésében. A legtöbb szervezet ezeket az eseményeket nem folyamatosan figyeli, elemzéseket nem végez, sőt a bizonyítékokat sem tárolja hitelesen. A naplógyűjtő és -elemző megoldásaink erre a kihívásra kínálnak hatékony választ.

Távfelügyelet, távmenedzsment
Az IT-biztonsági megoldásokat nemcsak telepíteni kell, hanem üzemeltetni, felügyelni is. Ezekre a feladatokra a legtöbb szervezetben nincs erőforrás, ezért a biztonsági eszközök hatékonysága erősen csökken. Erre jelent megoldást a biztonsági felügyelet vagy üzemeltetés, amely a T-Systems szakembercsapatának és technológiai megoldásainak felhasználásával a biztonsági rendszer helyi vagy távoli felügyeletét látja el, és képes az incidensek észlelésére, kezelésére. Szükség esetén a teljes rendszer üzemeltetését vállaljuk. A szolgáltatás mindazon informatikai biztonsági tevékenységeket magában foglalja, amelyeknek a hatékony és megbízható végrehajtása speciális, magas szintű, naprakész informatikai biztonsági szaktudást és többéves szakmai tapasztalatot igényel.[19]

---

[18] *Információ-védelem, adatvédelem* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/informacio-vedelem-adatvedelem (A letöltés dátuma: 2018. 09. 21.)

[19] *Incidensek kezelése, felügyelet* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/incidensek-kezelese-felugyelete (A letöltés dátuma: 2018. 09. 21.)

Megfelelőség biztosítása (Compliance)

Az üzleti célok elérése érdekében az informatikai kockázatok a kockázatmenedzsment segítségével azonosíthatók, illetve menedzselhetők. A T-Systems kockázat- és megfelelőségmenedzsment portfóliójának célja e releváns kockázatok feltérképezése, kezelése, illetve a szervezet információbiztonsági állapotáért hosszabb távon felelős információbiztonsági irányítási rendszer kialakítása és fenntartása.

Az üzleti rendszerek védelme az informatikai biztonsági politika hatékony és következetes érvényesítését követeli meg. A fenntartható megfelelőség kulcsa a vállalkozás védelmét szolgáló irányelvek maradéktalan betartása és figyelemmel kisérése. A kockázat- és megfelelőség-menedzsment megoldásaink lehetővé teszik a biztonsági menedzsereknek, hogy *auditálják, kikényszerítsék* és *dokumentálják* a belső biztonsági politika és a külső szabályozások teljesítését.

Szolgáltatásaink a megfelelőség biztosítása terén

Felkészítés auditokra, ellenőrzésekre
A szolgáltatás keretében megvizsgáljuk, hogy a szervezet milyen mértékben felel meg különböző törvényi (PSZÁF, ÁSZ), anyavállalati előírásoknak, nemzetközi szabványoknak (ISO 17799, ISO 27001, PCI), ajánlásoknak (COBIT). A feltárt hiányosságok kezelésére intézkedési tervet dolgozunk ki.

Információbiztonsági audit
A magas szintű védelem kialakítása érdekében elengedhetetlen, hogy a biztonsági intézkedések bevezetésén túl a követelményeknek, illetve törvényi előírásoknak való megfelelést független szervezet (külső audit) vagy szervezeti egység (belső audit) rendszeresen ellenőrizze. A szolgáltatás keretében külső auditor módszereivel végezzük el a szervezet átvizsgálását, vagy a belső auditor számára nyújtunk szakértői támogatást. A vizsgálat során feltárjuk, milyen szinten felel meg a szervezet az audit követelményeinek, és bizonyítékokat gyűjtünk a megfelelés igazolására.

Informatikai Biztonsági Dokumentációs Rendszer elkészítése, felülvizsgálata, bevezetése (biztonsági politika és alsóbb szabályzatok), a dokumentáció és a valós helyzet összehasonlítása
Az információbiztonság hatékony irányításához szükséges, hogy az információbiztonsági irányelvek, követelmények és felelősségek egy keretrendszerben legyenek rögzítve. Az információbiztonsági szabályozási folyamat eredményeképpen létrejövő Információbiztonsági Dokumentációs Rendszer (IBDR) egymásra épülő, tartalmában, irányában és részletességében bővülő dokumentumok összességét jelenti.

Az IBDR fontosabb dokumentumai: információbiztonsági politika, szabályzat, alsóbb szintű szabályzatok/eljárásrendek, felhasználói biztonsági kézikönyv, Informatikai Katasztrófaelhárítási Terv, Üzletmenet-folytonossági Terv.

A szolgáltatás keretében elkészítjük vagy felülvizsgáljuk a IBDR-t úgy, hogy az minden törvényi és szabályozási követelménynek megfeleljen. A dokumentációs rendszert

egészben kezeljük, de igény szerint lehetőség van az egyes dokumentumok külön-külön elkészítésére is.

Informatikai katasztrófaelhárítási terv készítése (IKeT)
Az Informatikai Katasztrófa-elhárítási Terv (IKeT) célja, hogy csökkentse a szervezet informatikai infrastruktúráját érintő váratlan hatások következményeit, amelyek a szervezet folyamatos működését és/vagy az informatikai rendszerek funkcionalitását veszélyeztetik. Az IKeT továbbá biztosítja az IT környezet visszaállítását katasztrófa esetén.

Üzletmenet-folytonossági terv készítése, felülvizsgálata (BCP)
Az Üzletmenet-folytonossági Terv (BCP) az Informatikai Katasztrófaelhárítási Tervvel (IKeT) közösen készül fel olyan eseményekre, amelyek súlyos hatással vannak az üzleti folyamatokra. A BCP – az IKeT-tel szemben – nem informatikai vonatkozású, hanem alternatív üzleti folyamatokat javasol minden olyan esetre, amikor egyes üzleti folyamatok komolyabb incidens vagy katasztrófa hatására működésképtelenné válnak.

Szabályzatok betartatása
A biztonsági rendszer szabályzatainak elkészülése után gondoskodni kell azok folyamatos betartatásáról. Megoldásunk erre a problémára ad választ, ezzel segíti az auditokon való megfelelést, és a vezetőség számára megnyugtató módon tartatja be a műszaki eszközökhöz kapcsolódó előírásokat.

A feltárt műszaki sérülékenységek folyamatos menedzsmentjének kialakítása
Az informatikai rendszerek biztonsági sérülékenységeit nemcsak feltárni, hanem életciklusszerűen kezelni is kell. Erre szolgálnak azok az eszközök, amelyek a sérülékenységeket menedzselik. Alkalmazásuk nagyban hozzájárul a rendszerek sérülékenységeiből adódó kockázatok csökkentéséhez, és egyben folyamatos visszajelzést adnak a rendszerek biztonsági állapotáról.

Biztonság-tudatossági és IT-biztonsági oktatások, tanfolyamok szervezése
Egy helyesen működő rendszer esetében kiemelkedően fontos a megfelelően felkészített és tudatosan cselekvő felhasználó. A tudatosság hangsúlyozása kiemelkedően fontos, a „biztonságosan” gondolkodó munkaerő egy cég talán legjelentősebb érdeme. Latba vethetjük a legszigorúbb szabályozásokat és bonyolult biztonsági megoldásaink tömkelegét halmozhatjuk fel, de mindez semmit sem ér, ha egy alkalmazott felragasztja a monitorképernyő szélére a széfet nyitó zárkombinációt. A különböző célcsoportokon végzett szintfelmérés, majd az eredmények függvényében célzott biztonsági tréningek alkalmazása, ezek rendszeres elvégzése minden cég számára javasolt.

Kihelyezett IT-biztonsági szakértő biztosítása
A szolgáltatás keretein belül rendszeres időközönként magasan kvalifikált biztonsági szakembert biztosítunk. A szakember feladatai összetettek: segítséget nyújthat a belső biztonsági rendszerek biztonsági szempontú áttekintésében, az aktuális biztonsági kérdések

megválaszolásban, az IT-stratégia kialakításában, szabályzatok megírásában, vagy akár belső biztonsági projektek minőségbiztosításában.[20]

Végszó

A kibervédelem életünk elengedhetetlen része.

Az informatikai rendszerek nélkül életünket már el sem tudjuk képzelni. Zsebünkben hordjuk azokat az eszközöket, amelyek korábban elképzelhetetlen teljesítményre képesek, korábban elképzelhetetlen kényelmet biztosítanak számunkra. Ugyanakkor ezek korábban elképzelhetetlen mértékben tesznek bennünket kiszolgáltatottá – megfelelő és folyamatos védelmük nélkül szinte életképtelenné válunk, és ez megengedhetetlen. Ez a kettősség szövi át életünket, és mindent meg kell tennünk azért, hogy a világunk egyre biztonságosabbá váljon ebben az értelemben is.

Felhasznált irodalom

760 ezer elektronikus személyit tiltottak le Észtországban váratlanul (2017). eGov Hírlevél. Elérhető: https://hirlevel.egov.hu/2017/11/06/760-ezer-elektronikus-szemelyit-tiltottak-le-esztorszagban-varatlanul/ (A letöltés dátuma: 2018. 09. 21.)

Be an early rider (2018). Waymo. Elérhető: https://waymo.com/apply/ (A letöltés dátuma: 2018. 09. 21.)

Bolcsó Dániel (2017): Zsarolóvírus söpört végig a világon. Index.hu. Elérhető: https://index.hu/tech/2017/05/12/kibertamadas_erhetett_angliai_korhazakat (A letöltés dátuma: 2018. 09. 21.)

Csáji Balázs Csanád (2001): *Approximation with Artificial Neural Networks.* MSc Thesis. Eindhoven.

Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) (é.n.). Elérhető: https://e-egeszsegugy.gov.hu/eeszt (A letöltés dátuma: 2018. 09. 21.)

Elképesztő, milyen komoly volt az orosz beavatkozás az amerikai választási kampányba (2018). Hvg.hu. Elérhető: http://hvg.hu/vilag/20180217_Elkepeszto_milyen_komoly_volt_az_orosz_beavatkozas_az_amerikai_valasztasi_kampanyba (A letöltés dátuma: 2018. 09. 21.)

Gálffy Csaba (2017): Nem is zsarolóvírus a 2017-es Petya. Hwsw.hu. Elérhető: https://www.hwsw.hu/hirek/57459/petya-ransomware-wiper-virus-titkositas.html (A letöltés dátuma: 2018. 09. 21.)

Gáspár Péter – Szabó Zoltán – Bokor József – Németh Balázs (2017): *Robust Control Design for Active Driver Assistance Systems: A Linear-Parameter-Varying Approach.* Springer International Publishing.

Határbiztonsági, határvédelmi megoldások (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/hatarbiztonsagi-hatarvedelmi-megoldasok (A letöltés dátuma: 2018. 09. 21.)

Hegedűs Ferenc – Bécsi Tamás – Aradi Szilárd – Gáspár Péter (2017): Model Based Trajectory Planning for Highly Automated Road Vehicles. In *IFAC World Congress: IFAC-PapersOnLine.* Toulouse.

[20] *Megfelelőség biztosítása (Compliance)* (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/megfeleloseg-biztositasa (A letöltés dátuma: 2018. 09. 21.)

Hozzáférések, jogosultságok kezelése (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/hozzaferesek-jogosultsagok-kezelese (A letöltés dátuma: 2018. 09. 21.)

Incidensek kezelése, felügyelet (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/incidensek-kezelese-felugyelete (A letöltés dátuma: 2018. 09. 21.)

Információ-védelem, adatvédelem (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/informacio-vedelem-adatvedelem (A letöltés dátuma: 2018. 09. 21.)

ISO 26262:2011: Road vehicles — Functional safety (2011). International Organization for Standardization. Elérhető: https://www.iso.org/standard/43464.html (A letöltés dátuma: 2018. 09. 21.)

Jön a kontroll: biztonsági szuperközpontot hozott létre a T-Systems (2018). Hvg.hu Elérhető: http://hvg.hu/tudomany/20180425_t_systems_ctrl_security_operations_center_tsm_telekom_kiberbiztonsag_kozpont (A letöltés dátuma: 2018. 09. 21.)

Káncz Csaba (2017): Eljött a hibrid háborúk kora. Privátbankár.hu Elérhető: https://privatbankar.hu/makro/eljott-a-hibrid-haboruk-kora-305458 (A letöltés dátuma: 2018. 09. 21.)

Kibervédelmi parancsnokságot létesítenek a honvédségen belül (2018). eGov Hírlevél. Elérhető: https://hirlevel.egov.hu/2018/03/10/kibervedelmi-parancsnoksagot-letesitenek-a-honvedsegen-belul/ (A letöltés dátuma: 2018. 09. 21.)

Kockázatok és sérülékenységek felmérése (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/kockazatok-es-serulekenyseg-felmerese (A letöltés dátuma: 2018. 09. 21.)

Megfelelőség biztosítása (Compliance) (é. n.). T-Systems. Elérhető: https://www.t-systems.hu/megoldasok/infrastruktura/it-biztonsagi-infrastruktura/megfeleloseg-biztositasa (A letöltés dátuma: 2018. 09. 21.)

Megszűnik a rendelőkben a sorban állás? (2017) Portfolio.hu. Elérhető: https://www.portfolio.hu/gazdasag/egeszseggazdasag/megszunik-a-rendelokben-a-sorban-allas.266613.html (A letöltés dátuma: 2018. 09. 21.)

Mitchell, Tom M. (1997): *Machine Learning.* McGraw-Hill.

PROTOCOLS (2018). Euro NCAP. Elérhető: https://www.euroncap.com/en/for-engineers/protocols/ (A letöltés dátuma: 2018. 09. 21.)

Rosenblatt, Frank (1957): The Perceptron – a perceiving and recognizing automaton. *Report 85-460-1,* Cornell Aeronautical Laboratory.

Rödönyi Gábor – Gáspár Péter – Bokor József – Palkovics László (2014): Experimental verification of robustness in a semi-autonomous heavy vehicle platoon. *Control Engineering Practice,* 28. évf. 1. sz. 13–25.

Russel, Stuart – Norvig, Peter (2005): *Mesterséges Intelligencia – modern megközelítésben.* Budapest, Panem Kft.

Sename, Olivier – Gáspár Péter – Bokor József (2013): *Robust Control and Linear Parameter Varying Approaches.* Berlin–Heidelberg, Springer Verlag.

Silver, David – Schrittwieser, Julian – Simonyan, Karen – Antonoglou, Ioannis – Huang, Aja – Guez, Arthur – Hubert, Thomas – Baker, Lucas – Lai, Matthew – Bolton, Adrian – Chen, Yutian – Lillicrap, Timothy – Hui, Fan – Sifre, Laurent – Driessche, George van den – Graepel, Thore – Hassabis, Demis (2017): Mastering the game of Go without human knowledge. *Nature,* 550, 354–359.

Special crash investigations: On-site automated driver assistance system crash investigation of the 2015 Tesla model S 70D (Report No. DOT HS 812 481) (2018). Crash Research & Analysis Inc., Washington, D. C., National Highway Traffic Safety Administration. Elérhető: https://crashstats.nhtsa.dot.gov/Api/Public/Publication/812481 (A letöltés dátuma: 2018. 09. 21.)

Surface Vehicle Recommended Practice J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (2016). SAE International. Elérhető: www.sae.org/standards/content/j3016_201609/ (A letöltés dátuma: 2018. 09. 21.)

Törő Olivér – Bécsi Tamás – Aradi Szilárd – Gáspár Péter (2017): Cooperative object detection in road traffic. In *IFAC World Congress: IFAC-PapersOnLine.* Toulouse.

Turzó Ádám Pál (2016): *A ma ismert világot totálisan elsöpri a negyedik ipari forradalom.* Portfolio.hu. Elérhető: www.portfolio.hu/vallalatok/it/a-ma-ismert-vilagot-totalisan-elsopri-a-negyedik-ipari-forradalom.237125.html (A letöltés dátuma: 2018. 09. 21.)

Waymo Safety Report: On The Road to Fully Self-Driving (2017). Waymo. Elérhető: https://waymo.com/safetyreport/ (A letöltés dátuma: 2018. 09. 21.)

Hivatkozott jogszabályok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)

Ajánlott irodalom

Dömös Zsuzsanna (2017): Pár év és a drognál is nagyobb üzlet lehet a zsarolóvírus. 24.hu. Elérhető: https://24.hu/tech/2017/12/30/par-ev-es-a-drognal-is-nagyobb-uzlet-lehet-a-zsarolovirus (A letöltés dátuma: 2018. 09. 21.)

GOvCERT Jelentés (2018). GovCERT. Budapest.

Incidenskezelés szolgáltatásként (2017). HWSW. Elérhető: www.hwsw.hu/hirek/57169/t-systems-soc-bizonsag.html (A letöltés dátuma: 2018. 09. 21.)

Bencsik Balázs[1] *– Tikos Anita*[2]

A kiberbiztonsági kihívások globális és hazai trendjei

Bevezetés

A 21. században a társadalom technológiafüggősége, a digitális eszközök és technológia térnyerése olyan jelentős mértékű, hogy mára szinte behálózta az életünk mindennapi tevékenységeit, munkafolyamatait és hivatali ügyintézését. A kibertér térnyerésének és a digitális technológia elterjedésének köszönhetően az irodából, otthonról vagy akár útközben is elintézhetjük magán- illetve munkahelyi feladatainkat. Ez jelentősen megkönnyíti az életünket, de számos veszélyt és fenyegetést is hordoz magában, abban az esetben, ha nem megfelelő körültekintéssel, nem tudatosan használjuk a technológia adta lehetőségeinket.

Ezen trendnek megfelelően napjainkban egyre elterjedtebbé válik az úgynevezett Internet of Things (a továbbiakban: IoT), azaz a dolgok internete is. Az IoT-eszközök olyan eszközök, amelyek képesek kétirányú kommunikációt folytatni más eszközzel, adatokat, információkat továbbítanak azok számára, vagy a felhőalapú technológia segítségével eltárolják, illetve továbbítani tudják az információt a világ bármely részére. Az IoT-technológián alapuló eszközöket okos vagy smart eszközöknek is nevezzük. Ennek megfelelően IoT-eszköz lehet telefon, számítógép, tablet és televízió, de ami ennél különlegesebb, hogy már olyan eszközök is fel vannak vértezve ilyen technológiával, mint például az autó, a villanykörte, a hűtőszekrény vagy akár egyes orvosi eszközök is.

Láthatjuk, hogy szinte az életünk minden apró szegmensét behálózzák az okos megoldások, az IoT-technológia, így nagyon fontos, hogy minden eszköz esetében törekedjünk a megfelelő és biztonságos használatra, a biztonsági beállítások körültekintő elvégzésére, az adataink védelme érdekében.

Egyértelmű, hogy mára a kibertér minden túlzás nélkül az életünk legapróbb szegmenseiben is jelen van. E tendenciának és a fékezhetetlen technikai fejlődésnek köszönhetően ugrásszerűen növekszik a lehetősége a sérülékenységeknek és a támadható eszközöknek, rendszereknek.

Egyre gyakoribbá válnak mind az állami, mind a civil szektort érintő kibertámadások. Világszerte évi 400 milliárd dollárra, azaz több mint 115 ezer milliárd forintra[3] becsülhetők a kiberbűnözők által okozott károk a globális kibertérben.

---

[1] Dr. Bencsik Balázs igazgató. Nemzeti Kibervédelmi Intézet

[2] Tikos Anita nemzetközi referens. Nemzeti Kibervédelmi Intézet

[3] Bucsky Péter (2018): Téged is megloptak? Interjú Keleti Arthur IT-biztonsági szakértővel. Elérhető: http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/ (A letöltés dátuma: 2018. 09. 21.)

Kibertérnek nevezzük a „globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét" a 2013. évi Ibtv. alapján.[4] Általános jellemzője, hogy globális, folyamatosan bővülő virtuális hálózat, amely decentralizáltságából fakadóan egymagában egyetlen állam által sem szabályozható. Ennek köszönhetően jelentős biztonsági kockázatokat jelent minden egyes felhasználó számára.

Az Európai Hálózatbiztonsági Ügynökség (a továbbiakban: ENISA) 2012 óta minden év októberében nemzetközi kampányt szervez a kiberbiztonsági hónap témájában (European Cyber Security Month, a továbbiakban: ECSM). Az ECSM célja, hogy az európai uniós állampolgárok kiberbiztonsági tudatosságát növelje, valamint a kibertérben megjelenő fenyegetéseket széles körben megismertesse. A kiberbiztonsági hónap keretében képzéseket, tudatosító előadásokat tartanak az európai uniós tagországok intézményei, ezek koordinálását az ENISA ügynökség végzi.

A 2017. év kampányának kiemelt témái az alábbiakat ölelték fel:[5]

- IT-biztonság a munkahelyen: zsarolóvírusok, adathalászat, malware, biztonsági mentések;
- információbiztonsági és adatvédelmi kihívások: az EU-s szabályozások (NIS irányelv, GDPR) végrehajtásának gyakorlati kihívásai;
- IT-biztonság otthon: IoT, otthoni hálózatok, online csalás, gyermekvédelem;
- kiberbiztonsági képességek: oktatás, tréning, e-képességek, kiberkihívás.

A kampányhoz Magyarország immár második alkalommal csatlakozott 2017-ben. A kampánnyal összefüggő feladatokat, valamint az érintett nemzeti és EU-s felekkel való kapcsolattartást és egyeztetést a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) látta el. A 2017. évi kampány során az NKI célja az volt, hogy az információbiztonsággal foglalkozó kormányzati és nem kormányzati cégeket, egyetemeket, iskolákat, szervezeteket bevonja a kampányba, és az együttműködés keretében minél szélesebb réteget érjenek el.

A kampány egyedülálló lehetőséget nyújt a köz- és magánszféra szereplőinek együttműködését ösztönző kezdeményezések elindítására.

A megszervezett események között szerepeltek konferenciák, kerekasztal-beszélgetések, kifejezetten egy-egy szakmai témára koncentrálva, tudatosító szakmai napok, workshopok, webinarok, valamint különböző előadások egyetemisták számára.

A jelentősebb események közé a következők tartoztak:

- A kiberhónap magyarországi nyitóeseményét, a Nemzeti Kiberbiztonsági Konferenciát (CYBERSEC2017.HU) 2016. október 3–4-én rendezték meg.
- 2016. október 9-én a Nemzeti Közszolgálati Egyetemen került sor „A NIS és GDPR hatása az európai kiberbiztonságra" című kerekasztal-beszélgetésre Magyarország és Észtország szakértőinek bevonásával.
- A „Nők az informatikában" (WITSEC) szakmai napja 2016. október 11-én zajlott.

---

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

[5] *European Cyber Security Month 2017 Deployment Report* (2018). ENISA. Elérhető: https://www.enisa.europa.eu/publications/european-cyber-security-month-2017 (A letöltés dátuma: 2018. 09. 21.)

- A „Félelem és Védelem” című workshopra ugyanezen év október 10-én került sor Szegeden, a Neumann János Számítógép-tudományi Társaság szervezésében, az NKI együttműködésével. A workshop a helyi civil szakmai közösségnek, középiskolásoknak és egyetemistáknak szólt.
- A kiberhónap magyarországi zárórendezvénye, a „Digitális környezetünk fenyegetettsége a mindennapokban” című konferencia a Belügyi Tudományos Tanács szervezésében zajlott le.

A kiberhónap sikerességét mutatja a megrendezett eseményeken túl a kampányhoz csatlakozó partnerek száma, amely évről évre növekvő mértéket mutat. A 2017-es kampány során már 20 partner csatlakozott az NKI által koordinált magyarországi kampányhoz.

Dataprotection.eu Kft.

1. ábra

Kiberhónap partnerek Magyarországon 2017-ben

Forrás: Kiberhonap.hu. Elérhető: https://kiberhonap.hu/partnereink (A letöltés dátuma: 2018. 09. 21.)

Miért van szükség ilyen átfogó kiberbiztonsági programokra?

A kibertámadásoknak komoly nemzetbiztonsági, gazdasági, illetve a társadalom mindennapi életére is veszélyt jelentő következményei lehetnek. Ezt a feltevést támasztja alá a Világgazdasági Fórum éves globális kockázati rangsora is, amelyben a hagyományos veszélyek – például háborús konfliktusok, terrorizmus, természeti katasztrófák stb. – mellett minden évben egyre előrébb sorolódnak a kibertér fenyegetései.

Olyannyira kritikus probléma ez, hogy a világ országai közül Kanada, Svédország, Norvégia, Finnország, Dánia, Hollandia, Japán, az Egyesült Arab Emírségek, Malajzia és Szingapúr is első helyen említi meg a kibertámadásokat, mint a társadalomra és gazdaságra leginkább kockázattal bíró „jelenséget".

A jelenség komplexitását jól jelzi, hogy a kibertámadások két legkiemelkedőbb alkategóriájának tekintjük 2015 óta a kiberkémkedést és az adatlopást, e területeken főleg a gazdasági következmények jelentősek.

Globális fenyegetések

A kibertérben megjelenő kockázatok exponenciális növekedési tendenciáját figyelhetjük meg az elmúlt évek során. A McAfee & Centre for Strategic and International Studies *Nettó veszteség: a kiberbűnözés globális költségének becslése (Net losses: Estimating the Global Cost of Cybercrime)* című tanulmánya szerint a kiberbűnözés gazdasági hatása a 2013–2017 közötti időszakban ötszörösére nőtt, 2019-ig pedig ez az érték akár meg is négyszereződhet.[6]

Az Europolnak a súlyos és szervezett bűnözésre vonatkozó fenyegetésértékelése szerint a kiberbűnözés és a „hagyományos" bűnözés közötti határvonal elmosódása figyelhető meg, hiszen a bűnözők számára az internet megfelelő felület a tevékenységük kiterjesztésére, illetve további eszközöket nyújt a bűncselekmények elkövetéséhez. Az internet nyújtotta anonimitás és személytelenség biztonságot és bátorítást nyújt a bűnözők számára, illetve nagyon megnehezíti, szinte lehetetlenné teszi a bűnözők nyomon követését és az igazságszolgáltatás kezére adását.[7]

Az NKI rendelkezésére álló adatok és információk szerint 2016 óta több mint négyezer zsarolóvírus-támadás történik naponta világszerte, amely 300%-os növekedést jelent a 2015-ös adatokhoz képest.

A legutóbbi, 2017. májusi zsarolóvírus kampány mutatja igazán a támadás egyes ágazatokra és országokra gyakorolt valós hatását, hiszen több mint 150 országban, több mint 190 ezer rendszert érintett, beleértve az olyan alapvető szolgáltatásokat is, mint a kórházak által nyújtott egészségügyi szolgáltatások. A korábban jellemző számítógépes kártevők célja főként az adatlopás, vagy a kritikus rendszerek megbénítása, valamint a zombihálózatok bővítése volt, napjainkban viszont az olyan károkozók elterjedése figyelhető meg, amelyek fájlokat tiltanak le, alkalmazásokat zárnak le, és a feloldásukért pénzt követelnek a felhasználótól. Az egyik ilyen kiemelkedő támadássorozat volt a WannaCry zsarolóvírus-hullám, amely mondhatjuk, hogy az elmúlt évek eddigi legnagyobb és legtöbb felhasználót és szervezetet elérő támadássorozatának bizonyult.

A vírus gyors terjedésének legfőbb oka egy minden Windows verzióban (az XP-től egészen a Windows 10-ig) megtalálható sebezhetőség volt. Ez a sebezhetőség viszont önmagában még nem lett volna elég a kártevő térnyeréséhez, ehhez jelentősen hozzájárultak a felhasználók is. Mi volt a felhasználók szerepe a támadás során? A Microsoft már 2017.

---

[6] *Net losses: Estimating the Global Cost of Cybercrime* (2014). McAfee & Centre for Strategic and International Studies. Elérhető: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf (A letöltés dátuma: 2018. 09. 21.)

[7] *Serious and Organised Crime Threat Assessment (SOCTA)* (2017). Europol. Elérhető: https://www.europol.europa.eu/socta/2017/ (A letöltés dátuma: 2018. 09. 21.)

március közepén kiadta a sérülékenység javítására szolgáló frissítést, amelyet számos felhasználó nem engedélyezett a gépére telepíteni, elhalasztotta vagy figyelmen kívül hagyta annak letöltését. Ennek köszönhetően több héttel a vírus térnyerése után még mindig akadt számtalan olyan Windows alapú számítógép, amelyikre nem került fel a sérülékenységet kijavító és a kártevő elkerüléséhez szükséges frissítés.

A kártevő hihetetlen sebességgel söpört végig az egész világon, szinte felmérhetetlen károkat okozva cégeknek, szervezeteknek és magánembereknek egyaránt.

2016 folyamán egy trójai típusú káros kód elterjedésének lehettünk tanúi, amely szintén Windows alapú operációs rendszereket támadott. Az áldozatok bitcoinban fizetendő váltságdíj ellenében kapták meg a támadótól a hozzáférő kódot a saját rendszerükhöz. Hasonló támadást észleltek 2017-ben is a WannaCry hullámot követően, de ez még a WannaCrynál is gyorsabban terjedt. Kéretlen leveleken keresztül jutott el az áldozatokhoz, titkosította a felhasználó merevlemezének adatait, majd a titkosított jelszót, feloldókulcsot válságdíj ellenében kínálta a felhasználónak, károsultnak. A Petya elnevezésű kártevő főként Ukrajnát támadta, onnan is indult ki a MeDoc nevű ukrán cég egyik platformjának feltörésével, a cég nevében számtalan fertőzött e-mailt küldtek, valamint a MeDoc gépéről megszerezték a felhasználóik belépési adatait. A MeDoc-nál így megszerzett adatokat is titkosította, és a helyreállításért, a feloldó kulcsért kriptovalutát kért a támadó vírus. Aztán a szakértők gyorsan rájöttek, hogy itt már nem a pénzügyi haszonszerzés volt a cél, hanem inkább a káoszkeltés és a gazdasági károkozás, főleg Ukrajnában. A Petya aktívan terjedt világszerte, így további jelentős károkat okozott még Oroszországban, Lengyelországban, Olaszországban és Németországban is.

Megfertőződött többek kötött a csernobili atomerőmű állapotát monitorozó rendszer, a kijevi reptér biztonsági rendszere és a kormányzati infrastruktúra, valamint az orosz Rosznyeft egyik rendszere is. De érintett volt az Oreo kekszet gyártó Mondelēz cég, a Mars, a Nivea, valamint – érdekességként – az OTP Bank ukrán leányvállalata is. Ekkor már egyértelmű volt, hogy ez már nem kifejezetten a Petya nevű kártevő, hanem inkább már egy pusztításra törekvő, törlő fertőzés (wiper), amely esetében nem lehet visszaállítani az adatokat, mivel a vírus „eldobja" a feloldókulcsot. Ennek a fertőzésnek a hivatalos neve PetrWrap lett.

A felhasználók és a vállalatok

Ma már mindenki által ismert az a megközelítés, hogy a kibertér lehet a modern világ új hadszíntere. Nemcsak a bűnözők, hanem egyes nagyhatalmak is a hagyományos eszközök helyett egyre gyakrabban a diszkrétebb kibereszközökkel szereznek érvényt akaratuknak és céljaiknak, például a belső demokratikus folyamatokba történő beavatkozás útján. A dezinformációs kampányok, álhírek és kritikus infrastruktúrák elleni kiberműveletek egyre inkább terjednek, és az eddigi gyakorlatunktól eltérő válaszreakciót igényelnek. Az új technológiák tovább terjedése (például IoT) és kiugrásszerű fejlődése tovább fogja gazdagítani a kibertérben rossz szándékúan, támadásra vagy befolyásolásra felhasználható eszközöket és szolgáltatásokat.

Ez is bizonyítja, hogy a digitális átalakulással és fejlődéssel egyre jelentősebb és változatosabb fenyegetésekkel kell szembenézünk, ezért kiemelkedő fontosságú a megfelelő

kiberbiztonsági környezet, és az erre vonatkozó szabályok kialakítása. Elengedhetetlen a társadalmunk és gazdaságunk számára kulcsfontosságú hálózatok és szolgáltatások esetében a megfelelő kiberbiztonsági intézkedések megvalósítása. Az ezen szolgáltatásokat érő támadások vagy incidensek felmérhetetlen károkat okozhatnak, valamint visszavethetik a fogyasztók bizalmát az új technológiák iránt.

A kitettségeket nemcsak a vállalati hálózatok és szabályok, hanem a felhasználók szintjén is szükséges kezelni, hiszen mint minden rendszerben, itt is az ember a leggyengébb láncszem. Az Eurostat 2016. évi *Digitális gazdaság és társadalom az EU-ban (Digital economy & society in the EU)* című felmérése szerint az EU polgárainak a 71%-a valamilyen személyes adatot megosztott már online.[8]

A felmérés eredményei alapján a leggyakrabban megosztott adattípusok a kapcsolattartási adatok (az internethasználók 61%-a) voltak, amelyet a személyes adatok, például név, születési idő vagy a személyi igazolvány száma (52%) és a fizetési adatok, például hitel/betéti kártya vagy bankszámlaszám (40%) követtek.

A felmérés kimutatja továbbá, hogy az EU-s állampolgárok közel több mint egyötöde (22%) szolgáltatott már ki más személyes adatokat, például fényképeket, tartózkodási helyét vagy az egészségére, a foglalkoztatására vagy a jövedelmére vonatkozó információkat különböző online felületeken, platformokon.

2. ábra

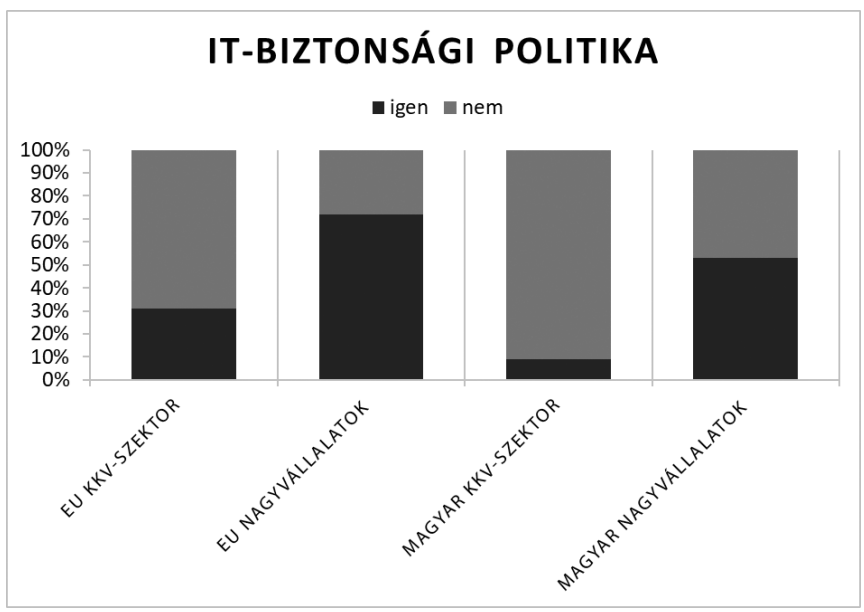
Személyes adatok megosztása online

Forrás: A szerző szerkesztése az Eurostat 2016-os adatai alapján. *Digital economy & society in the EU* (2016). Eurostat. A vonatkozó adatok a *http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-3a.html* aloldalon találhatók

[8] *Digital economy & society in the EU* (2016). Eurostat. Elérhető: http://ec.europa.eu/eurostat/cache/infographs/ict/ (A letöltés dátuma: 2018. 09. 21.)

Az Eurostat említett felmérésének eredményei szerint a fiatalabb generációk könnyebben elérhetővé teszik a személyes adataikat, ugyanis a 16–24 éves internethasználók több mint háromnegyede (78%) osztott meg valamilyen személyes információt online, szemben a 65–74 év közötti felhasználók 57%-ával.

A felhasználókon túl a vállalatoknak, szervezeteknek is modern, napjaink kihívásainak megfelelő információbiztonsági technológiával és szabályrendszerrel kell rendelkezniük, az adataik, rendszerek és dolgozóik biztonsága érdekében. Az Eurostat felmérése ezért megvizsgálta a vállalatok digitális szokásait is. A felmérés alapján napjainkban gyakorlatilag az összes EU-ban működő vállalkozás (98%) használ számítógépeket, és közülük csak 31%-uk rendelkezik formálisan meghatározott informatikai biztonságpolitikával, belső szabályozásokkal. A magyarországi adatok szerint a kkv-szektor vállalatainak mindössze 9%-a és a nagyvállalatoknak valamivel több mint 50%-a rendelkezett biztonsági politikával.



3. ábra

Informatikai biztonságpolitika a vállalatok körében

Forrás: A szerző szerkesztése az Eurostat 2016-os adatai alapján. *Digital economy & society in the EU* (2016). Eurostat. A vonatkozó adatok a *http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-1.html* aloldalon találhatók

Az Eurostat felmérésének eredményeiből kitűnik, hogy a biztonságos és tudatos digitális jelenlét terén még jelentős fejlődésre van szükség mind az állampolgárok, mind pedig a vállalatok szintjén. Ezen cél elérésének számos módja lehet, a folyamatos oktatástól, tudatosítástól egészen a szigorú jogszabályok és ellenőrzési mechanizmusok kialakításáig.

Az EU válasza a növekvő kihívásokra

Az IKT piaci jellemzői

Jelenleg az Európai Unióban az IKT, azaz infokommunikációs szektor döntő mértékben harmadik országokban fejlesztett és gyártott hardvereszközökön, illetve szoftvereken alapul, ami egyes területeken monopolisztikus vagy oligopolisztikus ellátási láncok kialakulásához vezetett. Ezen IKT-rendszerek ma már csak biztonságtudatos módon fejleszthetők és üzemeltethetők a kibertérben folyamatosan jelen lévő fenyegetettség miatt. A gyártói biztonságtudatosság, a számítógép-biztonsági és incidenskezelő csoportok (CSIRT-ek) hálózata, illetve a kibervédelmi jogszabályok lehetővé teszik a kibertámadásokból adódó kockázatok bizonyos mértékű kezelését. A legnagyobb probléma az, hogy a kibertérben nem érvényesül az arányosság elve: a kétszer nagyobb tűzfal nem jelent kétszer nagyobb védelmet, sőt egy apró hiba egy teljes IKT-ökoszisztémát tehet ki potenciális támadásoknak a hiba javításáig, ami hónapokig is elhúzódhat.

Az IKT-szektorban a termékek és szolgáltatások kiemelkedően magas innovációs tartalmának, illetve a globális internet miatti mobilitásnak köszönhetően a gyártói koncentráció kiemelkedő. Néhány nagyvállalat – sok esetben állami támogatás és összefonódás mellett – oligopolisztikus piacot alakított ki világszerte, ezért gyakorlatilag megkerülhetetlenné váltak az IKT-rendszerek biztonságának garantálása szempontjából. Ezen gyártók és szolgáltatók döntően nem uniós tagállamokban működnek.

Az Európai Bizottság 2017 szeptemberében egy átfogó, ambiciózus kiberbiztonsági csomagot bocsátott ki, mely a megnövekedett kiberfenyegetésekre, valamint az egységes digitális piac elérésének akadályaira kíván megfelelő válaszokat, mechanizmusokat és jogi biztosítékokat létrehozni.

A kiberbiztonsági csomag magában foglalja az Európai Bizottság közleményét a felülvizsgált EU-s kiberbiztonsági stratégiáról, egy jogszabályjavaslatot, az ún. Kiberbiztonsági Jogszabályt (Cybersecurity Act) – amely az ENISA (European Union Agency for Network and Information Security, Európai Uniós Hálózat- és Információbiztonsági Ügynökség) mandátumának felülvizsgálatára vonatkozik, egy Európai Kiberbiztonsági Ügynökség létrehozásával –, továbbá a kiberbiztonsági tanúsítás kérdéskörére irányuló rendelkezéseket. A csomag részét képezi az ún. blueprintre vonatkozó bizottsági ajánlás is, mely ismerteti, hogy a kiberbiztonságot miként illesztik be a meglévő uniós szintű válságkezelési mechanizmusokba, és meghatározza a tagállamok egymás közötti együttműködésének, valamint a tagállamok és az illetékes uniós intézmények, szervezeti egységek, ügynökségek és testületek együttműködésének céljait és módszereit a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való reagálás terén.[9]

Fontos kiemelni, hogy kibertérből érkező fenyegetések a szuverén állam számos különböző működési területét érintik, ezért nem lehet meghatározni olyan univerzális védekezési stratégiát, amely egyaránt hatékony az IKT-gyártók hibáiból adódó sérülékenységek, a bűnözői csoportok támadásai, illetve potens állami szereplők által kifejtett offenzív

[9] Az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") szóló rendelettervezet. Elérhető: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en (A letöltés dátuma: 2018. 09. 21.)

tevékenységek ellen. A fenyegetések potenciális hatásainak a felmérése is problematikus terület, mivel nehéz rangsorolni a veszteség súlyossága szempontjából egy milliárdos gazdasági kémkedési ügyet, egy emberéleteket követelő ipari kiberszabotázs akciót, illetve a demokratikus választási rendszer befolyásolására tett kísérletet a kibertérben. Sajátos veszélyforrást jelent a szuverén állam polgáraival szemben tömegesen elkövetett illegális adatgyűjtés, ami a személyes adatok megsértéséhez, sőt akár az állampolgárok döntéseinek tömeges manipulációjához és a demokratikus értékek sérüléséhez is vezethet.

A kiberbiztonsági támadások, fenyegetések nem maradnak országhatárokon belül, ezért törekedni kell arra, hogy olyan szabályozásokat fogalmazzunk meg, amelyek nemzetközi szintűek és a világ minden részén egységesen alkalmazhatók. Ennek megfelelően a határokon túli, nemzetközi együttműködés kérdéskörét is prioritásként kezeli a kiberbiztonsági csomag, így célkitűzésként fogalmazza meg az EU–NATO együttműködés elmélyítését, a nemzetközi regionális és bilaterális kapcsolatokban a kiberbiztonság, válságkezelés és megelőzés terén történő együttműködést, valamint a harmadik országokkal történő együttműködés során a kapacitásépítés támogatását és a jó tapasztalatok megosztását.

A csomag számos javaslatot fogalmaz meg a kiberbűnüldözés terén történő együttműködés, a kibertámadás-elhárítás kidolgozására, az állami és magánszektor együttműködésének elősegítésére, a kutatás-fejlesztés terén megvalósítandó együttműködésre, valamint a kiberkészségbázis létrehozására.

A továbbiakban az itt felvázolt kibercsomag egyes témáit és elemeit ismertjük.

Biztonsági tanúsítási keretrendszer

Az informatika igen gyorsan változó iparág, egyes területein elengedhetetlenül fontos az új technológiákhoz való hozzáférés (például tudományos munkák, programozás stb.). Tagadhatatlan, hogy a kiberbiztonsági csomag egyes javaslataival az EU területén működő szervezetek némi hátrányba és késedelembe kerülhetnek, például a tanúsítás szükségessége miatt az engedélyeztetési folyamat idején. Ugyanakkor nagyon fontosnak tartjuk a gyors változások megfelelő és állandó követését, figyelését, az azokra való felkészülést hálózatbiztonsági szempontokból, hiszen az egyes biztonsági események, működésben bekövetkező sérülések, meghibásodások, továbbá a támadások jelentős hányada éppen a legújabb fejlesztések és változások során következik be vagy várható, jelentős mértékben a nem kellő védelmi felkészültség miatt.

A kialakítandó tanúsítási keretrendszer célja, hogy az egységes tanúsítás bevezetésével javuljon a termékek és szolgáltatások biztonsága, tájékoztassa és meggyőzze az állampolgárokat az érintett IKT-termékek és szolgáltatások biztonsági tulajdonságairól, ezzel pedig növekedjen a beléjük vetett bizalom. Hosszú távon a termékekbe és szolgáltatásokba vetett bizalom növekedése az uniós szintű piac fellendüléséhez vezethet. A javaslat egyik ambíciója, hogy a biztonsági aspektus már a kezdeti szakaszban, a termékek és szolgáltatások tervezése és fejlesztése során is figyelembe veendő szempont legyen, így megvalósulhasson az úgynevezett „security by design” elv.

Ezért a kiberbiztonsági csomag javaslatot fogalmaz meg a tanúsítás kérdéskörének EU-s szinten történő szabályozására is. Ennek megfelelően az EU egy jogszabályjavaslat

keretében létrehozza az európai kiberbiztonsági tanúsítási keretrendszert az IKT-termékekre és szolgáltatásokra vonatkozóan.

Az európai kiberbiztonsági tanúsítási keretrendszer általános célja annak igazolása, hogy a keretrendszer szabályainak megfelelően tanúsított IKT-termékek és szolgáltatások megfelelnek a meghatározott kiberbiztonsági követelményeknek. Ebbe beletartozna például a (tárolt, továbbított vagy más módon feldolgozott) adatok védelmének képessége a véletlen vagy illetéktelen tárolással, feldolgozással, hozzáféréssel, nyilvánosságra hozatallal, megsemmisítéssel, véletlen elvesztéssel vagy módosítással szemben.

A keretrendszernek a jelenleg létező európai kiberbiztonsági tanúsítási rendszerekkel összehangolt létrehozása lehetővé teszi majd egyfelől, hogy az ilyen rendszerek részeként kiállított tanúsítványok minden tagállamban érvényesek legyenek, illetve minden tagállam elismerje őket, továbbá megfelelő megoldást biztosítana a piac jelenlegi széttagoltságának problémáira.

Az unió kiberbiztonsági tanúsítási keretszabályozása a meglévő szabványokra hagyatkozna azon technológiai követelményeket és értékelő eljárásokat illetően, amelyeknek jelenleg meg kell felelniük az adott termékeknek az egyes tagállamokban, nem pedig egy teljesen új EU-s technológiai szabványokat dolgozna ki.

A jogszabály nem vezet be közvetlenül működőképes tanúsítási rendszereket, ehelyett egy úgynevezett keretrendszert alakít ki az IKT-termékekre és szolgáltatásokra vonatkozó egyedi tanúsítási rendszerek (európai kiberbiztonsági tanúsítási rendszerek) létrehozása számára. Ezen európai kiberbiztonsági tanúsítási rendszereket az Európai Bizottság felkérésére, az európai kiberbiztonsági tanúsítási csoport segítségével az ENISA feladata lenne kidolgozni. Az így elkészülő tanúsítási rendszereket a Bizottság fogadja el hivatalosan, végrehajtási jogi aktusok révén.

Az ilyen rendszereknek olyan konkrét elemeket kell tartalmazniuk, mint az érintett termékek és szolgáltatások kategóriáinak azonosítása, a kiberbiztonsági követelmények részletes leírása (szabványok vagy műszaki előírások), a konkrét értékelési kritériumok és módszerek, valamint a biztonság elérendő szintje (alapvető, jelentős vagy magas).

A javaslatban foglaltak szerint a szabályozás ellenőrzési, felügyeleti és végrehajtási feladatai a tagállamokra hárulnak. Ennek érdekében a tagállamoknak létre kell hozniuk egy nemzeti tanúsítás-felügyeleti hatóságot. A hatóság feladata felügyelni, hogy a tagállam területén letelepedett megfelelőségértékelő szervezetek és az általuk kiállított tanúsítványok megfelelnek-e a rendelet előírásainak és a vonatkozó európai kiberbiztonsági tanúsítási rendszereknek. A nemzeti tanúsítás-felügyeleti hatóságok illetékesek a tagállam területén letelepedett megfelelőségértékelő szervezetek által kiállított tanúsítványokkal kapcsolatos, természetes és jogi személyek által benyújtott panaszok kezelésére is.

Végül pedig a javaslat létrehozza az európai kiberbiztonsági tanúsítási csoportot, amely az egyes tagállamok nemzeti tanúsítás-felügyeleti hatóságaiból áll. A csoport fő feladata, hogy tanácsot adjon a Bizottságnak a kiberbiztonsági tanúsítási politikát érintő kérdésekben, és együttműködjön az ENISA-val az európai kiberbiztonsági tanúsítási rendszerek tervezetének kidolgozásában. Az ENISA feladatai közé fog tartozni a jogszabálytervezet szerint, hogy a európai kiberbiztonsági tanúsítási csoport titkársági feladatait ellássa, illetve, hogy a nyilvánosság számára elérhető, naprakész nyilvántartást vezessen az európai kiberbiztonsági tanúsítási keretrendszer részeként jóváhagyott rendszerekről. Az ENISA a szabványtestületekkel is kapcsolatot tartana fenn, hogy biztosítsa a jóváhagyott

rendszerekben használt szabványok megfelelőségét, és hogy azonosítsa a kiberbiztonsági szabványokat igénylő területeket.

Kiberdiplomácia

A 2017 júliusában elfogadott, a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések EU-s kerete (úgyevezett „kiberdiplomáciai eszköztár")[10] létrehoz egy a közös kül- és biztonságpolitika keretébe tartozó intézkedésgyűjteményt, amely intézkedések az EU politikai, biztonsági és gazdasági érdekeit sértő kibertevékenységekre adott reakciók erősítését hivatottak megvalósítani. Ez az eszköztár a bilaterális diplomáciai vagy politikai egyeztetéstől egészen a szigorú, akár gazdasági korlátozó intézkedésekig számos különböző erősségű és hatású reagálási lehetőséget fogalmaz meg. A keretrendszer fontos lépést jelent az uniós és tagállami szintű jelző- és reagálási kapacitások fejlesztésében. Az eszköztár hosszú távon hozzájárul a konfliktusok megelőzéséhez, a kiberbiztonságot fenyegető veszélyek mérsékléséhez, illetve a nemzetközi kapcsolatok stabilitásának növekedéséhez egyaránt. Remélhetőleg az eszköztárban meghatározott eszközök használata visszatartó hatást gyakorol a potenciális agresszorok magatartására, így hosszú távon csökkenteni fogja a támadások és kiberincidenesek számát. Az eszköztár felhasználása kapcsán fontos kritérium, hogy a rossz szándékú kibertevékenységekkel szemben megfelelően arányos reagálást biztosítson. A támadás állami vagy nem állami szereplőknek tulajdonítása a továbbiakban is a minden forrást igénybe vevő hírszerzésre alapozott, szuverén politikai döntés marad.

Az EU–NATO együttműködés fontossága

A kiberbiztonság kérdéskörét és a kibertérben való stabilitás biztosítását prioritásként kezeli az EU és a NATO egyaránt. Ennek megfelelően 2016. július 8-án közös EU–NATO nyilatkozatot fogadtak el a kiberbiztonság, hibrid fenyegetések és védelem terén történő együttműködési célok megfogalmazása érdekében. A stratégia célja az Unió és a NATO közötti együttműködés kibővítése, a párhuzamos és összehangolt EU–NATO gyakorlatok szervezésével, illetve a kiberbiztonsági követelmények és szabványok kölcsönös átjárhatóságának kiszélesítésével.

A hibrid fenyegetések vonatkozásában a stratégia célja a már korábban létrejött együttműködések és közös erőfeszítések, különösen a hibrid fenyegetésekkel foglalkozó uniós információs- és elemzőcsoport és a NATO hibrid fenyegetéseket elemző csoportja közötti együttműködés elmélyítése, élénkítése az ellenállóképesség és a kiberválságokra való reagálás erősítése érdekében.

[10] *A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről* (2017). Elérhető: http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf (A letöltés dátuma: 2018. 09. 21.)

A Kiberbiztonsági Vészhelyzet-elhárítási Mechanizmus és a Kiberbiztonsági Vészhelyzet-elhárítási Alap

Mivel egyes kiberbiztonsági incidensek jelentős hatással lehetnek a gazdaság működésére és az emberek mindennapi életére is, ezért lényeges megfontolni egy vészhelyzeti válságmechanizmus kidolgozását, illetve a létező biztonságpolitikai válságmechanizmusok kiberbiztonságra történő kiterjesztését.

A kibercsomag részét képezi azon tervezet is, mely felvázolja a kiberbiztonsági szempontok beillesztését az integrált uniós politika válságreagálási rendszerébe, illetve az EU általános riasztási rendszereibe.

A kiberbiztonsági aspektusnak a válságmechanizmusokba való hatékony beillesztésén túl fontos lenne egy Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozása is, a más uniós biztonságpolitikai területeken meglevő, hasonló válságmechanizmusokhoz kapcsolódó alapok példája nyomán. Az Alap lehetővé tenné, hogy egy jelentősebb és átfogóbb incidens esetén, vagy azt követően a tagállamok támogatást, segítséget kérjenek a gyors reagálás megvalósításához, esetleg a vészhelyzeti válaszlépések megvalósításának finanszírozására.

Természetesen az Alap felhasználására csak azon tagállamoknak nyílna lehetőségük, amelyek az uniós előírásoknak és szabályoknak megfelelő kiberbiztonsági rendszert alakítottak ki (még az incidens bekövetkezése előtt), megfelelően végrehajtották a NIS irányelv rendelkezéseit, illetve fejlett nemzeti kockázatkezelési és felügyeleti keretrendszerrel rendelkeznek.

A kiberbiztonsági kompetenciahálózat és az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont

Az EU stratégia napirendjére tűzte a kutatás és kompetenciafejlesztés fellendítésének és uniós szinten történő koordinálásának kérdéskörét is. Alapvető célja, hogy az Európai Unió szintjén fejlesszék a közösség digitális gazdaságának, társadalmának és demokráciájának biztonsága érdekében a kulcsfontosságú kritikus infrastruktúrákat és digitális szolgáltatásokat.

Ez a köz- és magánszféra együttműködésével, az akadémiai és a kutatás-fejlesztési területek bevonásával valósulhat meg a leghatékonyabban. A PPP együttműködés fontosságát már a korábbi stratégiai dokumentumok is kiemelt célként fogalmazták meg. A Bizottság előrejelzése szerint a közszféra és magánszféra közötti kiberbiztonsági partnerség 2020-ig várhatóan 1,8 milliárd euró befektetést generál.[11] A világ más területein az együttműködésbe befektetett összeg ezt jelentősen meghaladja. Az Egyesült Államokban például az előzetes tervek szerint 2017-ben 19 milliárd dollárt biztosítottak a kiberkutatás-fejlesztésre a Fehér Ház által kiadott 2016. évi „kiberbiztonsági intézkedési terv" alapján.[12]

---

[11] *Közös közlemény az Európai Parlamentnek és a Tanácsnak. Ellenállóképesség, elrettentés, védelem: az unió erőteljes kiberbiztonságának kiépítése* (2017). JOIN(2017) 450 final. Elérhető:http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN (A letöltés dátuma: 2018. 09. 21.)

[12] *FACT SHEET: Cybersecurity National Action Plan* (2016). The White House Office of the Press Secretary. Elérhető: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (A letöltés dátuma: 2018. 09. 21.)

Az EU a kiberbiztonsági képességének megerősítése céljából az európai uniós tagállamok kiberbiztonsági kompetenciaközpontjainak hálózatba szervezését tervezi, valamint a hálózat központjaként létre szándékozik hozni egy úgynevezett Európai Kiberbiztonsági Kutatási és Kompetenciaközpontot. Ez a hálózat és annak központja serkentené a kiberbiztonság területén a technológia fejlesztését és bevetését, segítené a K+F támogatások hatékony elosztását, uniós és nemzeti szinten kiegészítené a terület kapacitásépítési erőfeszítéseit, valamint lehetőséget nyújtana nagyobb K+F projektek megvalósítására több tagállam kutatóközpontjainak közös kezdeményezéseként.

Első lépésként az Európai Bizottság a nemzeti központok hálózatba szervezését szeretné megkezdeni. A pilot projektként funkcionáló első szakaszban a Horizon2020 keretből 50 millió eurót biztosítana a hálózat kialakítására.

A tervezet szerint a jövőben a kutatási területek a következő generációs digitális technológiák fejlesztésére is fókuszálnának, lefedve így a mesterséges intelligenciát, a kvantum számítástechnikát, a blokkláncot és a biztonságos digitális személyazonosságot.

Kiberkészségbázis kiépítése

A 2017. évi Global Information Security Workforce tanulmány előrejelzése szerint a kiberbiztonsági szakemberhiány a privát szektorban 2022-re 350 ezer fő lesz, de globális szinten akár az egymillió főt is elérheti.[13] Ezen probléma megoldása érdekében fejleszteni kell a kiberbiztonsági oktatást. Szükség van még több kiberbiztonsági szakember képzésére, ami az IKT-szakemberek kiegészítő kiberbiztonsági képzése, illetve új kiberbiztonsági szakképzések útján történhet.

A szakemberek képzésén túl fontos, hogy a többi szakterület (például: mérnöki tevékenység, közoktatás, menedzsment vagy jog) oktatási tervébe is be kell építeni az alapvető kiberbiztonsági tananyagot, amelynek célja, hogy a jövő szakembereinek gondolkodásába itt is beépüljön a biztonsági aspektus figyelembevételének fontossága, illetve, hogy a munkájuk és mindennapi életük során tudatosan és biztonságosan mozogjanak a kibertérben.

A kiberbiztonság fontosságának megértését, tudatosítását, a kiberbűnözés veszélyeinek ismertetését az alapvető digitális készségek és tudás elsajátítását már az általános és középiskolai tanulmányok során meg kell kezdeni. Ez a folyamat hozzásegítheti a tanulókat ahhoz, hogy a későbbiekben tudatosan, biztonságosan és megfontoltan használhassák a digitális szolgáltatásokat és eszközöket a kibertérben.

Az EU célkitűzései között szerepel, hogy kialakítson egy uniós szintű egységes portált, ahol az összes tudatosításra alkalmas eszközt összegyűjti egy úgynevezett egyablakos rendszerben, tanácsot adva a felhasználóknak az egyes támadások, fertőzések megelőzéséhez, elkerüléséhez és észleléséhez. A portálon javaslatokat, információkat és segítséget találhatna a felhasználó arra vonatkozóan, hogy mi a teendő, ha valamilyen informatikai támadás áldozata, IT-biztonsági incidens elszenvedője lesz, továbbá a portálon elérhetővé tenné az ilyen eseményeknél szükséges bejelentési mechanizmusok elérhetőségeit, linkjeit.

---

[13] *2017 Global Information Security Workforce Study* (2017). Center for Cyber Safety and Education. Elérhető: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf (A letöltés dátuma: 2018. 09. 21.)

Az állampolgárok oktatása, tudatosítása, képességeinek folyamatos fejlesztése kiemelkedő fontosságú, hiszen a kiberbiztonsági csomagban lévő adatok alapján az incidensek 95%-át valamilyen szándékos vagy nem szándékos emberi tévesztés, hiba vagy figyelmetlenség idézi elő. Ezért fontos felismernünk és minden szervezet, illetve természetes személy számára tudatosítanunk, hogy a kiberbiztonság mindannyiunk felelőssége. Ennek megfelelően a személyes, vállalati és közigazgatási szinten egyaránt egy olyan figyelmes és tudatos magatartásnak (kiberhigiéniai szokásrendszernek) kell kialakulnia, amelynek keretében minden résztvevő megérti az aktuális fenyegetéseket, és megfelelő eszközökkel, képességekkel rendelkezik a támadások felismerésére, az azokkal szembeni hatékony védekezésre.

Az EU-nak és a tagállamoknak prioritásként kell kezelniük a kiberbiztonsági tudatosítást, a tudatosság fejlesztését. Kifejezetten javasolt a megvalósításuk az iskolák, az egyetemek, az üzleti közösség és a kutatási szervek számára kidolgozott, célzott tudatosító kampányok révén. Az kibercsomag célja az ENISA által 2012 óta minden év októberében tartott kiberbiztonsági hónap kampány (ECSM) folyamatos bővítése és frissítése annak érdekében, hogy a kampány mindig az aktuális trendekre és fenyegetésekre tudja felhívni az állampolgárok figyelmét, illetve azért, hogy minél szélesebb közönséget tudjon hatékonyan megszólítani. A tudatosítás témakör esetében fontos felhívni a figyelmet az online félretájékoztató kampányok és a közösségi médiában megjelenő álhírek káros hatásaira. A tagállamoknak a meglévő tapasztalataikat egymással megosztva, közösen kell szembenézniük ezekkel a kihívásokkal, többek között a közelgő 2019. évi európai parlamenti választásokra való felkészülés során.

Összegzés

A digitális technológia megállíthatatlan fejlődése és a kibertér életünk minden területére való kiterjedése mára megállíthatatlan folyamat. Ahogy a fenti példákból láttuk, ez a fejlődés számos lehetőséget és egyben veszélyt is hordoz magában.

A fejlődést nem lelassítani vagy megállítani kell, hanem megpróbálni alkalmazkodni hozzá, kihasználni a benne rejlő lehetőségeket és előnyöket. Nagyon fontos, hogy ebben az új, fejlett digitális technológiával teli világban megtanuljunk biztonságosan és magabiztosan mozogni.

Ahhoz, hogy ezt meg tudjuk valósítani, az államoknak, vállalatoknak, fejlesztőknek, gyártóknak, szolgáltatóknak, állampolgároknak/felhasználóknak, sőt még a nemzetközi szervezeteknek, közösségeknek is fel kell ismerniük a maguk a szerepét és felelősségét.

Az Európai Bizottság által megfogalmazott kibercsomag koncepció számos kulcsfontosságú, egymásra épülő és egymást kiegészítő intézkedést azonosított. Sajnos nem elég a szigorú jogszabályok megalkotása, ellenőrzése és szankcionálása ezen területen, hiszen a kiberbiztonság megteremtése és annak fenntartása az információbiztonságban érintett valamennyi szereplő közös felelőssége, és megvalósításuk elképzelhetetlen a felek együttműködése nélkül.

Ezt az üzenetet fogalmazta meg a 2017. évi kiberhónap kampány nyitó konferenciájának a mottója is: „A kiberbiztonság közös felelősségünk”.

Felhasznált irodalom

2017 Global Information Security Workforce Study (2017). Center for Cyber Safety and Education. Elérhető: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf (A letöltés dátuma: 2018. 09. 21.)

Bucsky Péter (2018): Téged is megloptak? Interjú Keleti Arthur IT-biztonsági szakértővel. Elérhető: http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/ (A letöltés dátuma: 2018. 09. 21.)

Digital economy & society in the EU (2016). Eurostat. Elérhető: http://ec.europa.eu/eurostat/cache/infographs/ict/ (A letöltés dátuma: 2018. 09. 21.)

European Cyber Security Month 2017 Deployment Report (2018). ENISA. Elérhető: https://www.enisa.europa.eu/publications/european-cyber-security-month-2017 (A letöltés dátuma: 2018. 09. 21.)

FACT SHEET: Cybersecurity National Action Plan (2016). The White House Office of the Press Secretary. Elérhető: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (A letöltés dátuma: 2018. 09. 21.)

Kiberhonap.hu – Partnereink (é. n.). Elérhető: https://kiberhonap.hu/partnereink (A letöltés dátuma: 2018. 09. 21.)

Net losses: Estimating the Global Cost of Cybercrime (2014). McAfee & Centre for Strategic and International Studies. Elérhető: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf (A letöltés dátuma: 2018. 09. 21.)

Serious and Organised Crime Threat Assessment (SOCTA) (2017). Europol. Elérhető: https://www.europol.europa.eu/socta/2017/ (A letöltés dátuma: 2018. 09. 21.)

Hivatkozott jogszabályok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv) (2013). Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (A letöltés dátuma: 2018. 09. 21.)

A Tanács következtetései a kiberdiplomáciáról (2015). Az Európai Unió Tanácsa. Elérhető: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf (A letöltés dátuma: 2018. 09. 21.)

A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017). Elérhető: http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf (A letöltés dátuma: 2018. 09. 21.)

Az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály") szóló rendelettervezet (2017). Elérhető: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en (A letöltés dátuma: 2018. 09. 21.)

Az Európai Bizottság 2017/1584 Ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (2017). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32017H1584 (A letöltés dátuma: 2018. 09. 21.)

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről (2016). Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU (A letöltés dátuma: 2018. 09. 21.)

Közös közlemény az Európai Parlamentnek és a Tanácsnak. Ellenállóképesség, elrettentés, védelem: az unió erőteljes kiberbiztonságának kiépítése (2017). JOIN(2017) 450 final. Elérhető:http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN (A letöltés dátuma: 2018. 09. 21.)

Ajánlott irodalom

Európai Kiberbiztonsági Hónap Magyarországon. Elérhető: https://kiberhonap.hu/ (A letöltés dátuma: 2018. 09. 21.)

Harangi László (2017): Újabb durva zsarolóvírus pusztít Európában és Amerikában. PCWorld. Elérhető: https://pcworld.hu/pcwlite/ujabb-durva-zsarolovirus-pusztit-europaban-es-amerikaban-230639.html (A letöltés dátuma: 2018. 09. 21.)

Világhódító útjára indult Petya, a zsarolóvírus (2017). Magyar Nemzet. Elérhető: https://mno.hu/belfold/vilaghodito-utjara-indult-petya-a-zsarolovirus-2405259 (A letöltés dátuma: 2018. 09. 21.)

World Economic Forum: Global Risks 2018: Fractures, Fears and Failures (2018). Elérhető: http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#hide/fn-1 (A letöltés dátuma: 2018. 09. 21.)

Kőnig Balázs[1]

Kiberbiztonsági kutatások és oktatás a közszolgálatban[2]

Bevezetés

A kibertérben történő események vitathatatlanul hatással vannak a fizikai világra, ezt az elmúlt pár év még azok számára is megtanította, akik magukat a lehető legjobban megpróbálják kizárni a digitális létből. Elég csak arra gondolni, hogy 2017 januárjában beiktatták az Egyesült Államok első olyan elnökét, akinek megválasztásában fontos szerepet játszott a közösségi hálózatokon keresztüli befolyásolás egy külső szereplő által, vagy éppen arra, hogy a magyar médiát egy informatikai támadás és annak utózöngéi uralták majdnem egy hónapon keresztül 2017 augusztusában. Megemlíthető még az a két globális kártékonykód-kampány (WannaCry, NotPetya), amelyek 2017 májusában és júniusában több országban és iparágban is komoly károkat okoztak, bemutatva a kiberfegyverek lehetséges hatásait.

Az idő előrehaladtával nemhogy csökkennének, de inkább nőnek, sőt egyre aktuálisabbak a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló Korm. határozat szavai, miszerint: „[…] Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja, és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani."[3]

A kibervédelmi kutatás és oktatás keretei a Nemzeti Közszolgálati Egyetemen

2011-ben Magyarország kormánya határozott arról, hogy a közszolgálat különböző szereplőit és utánpótlásának oktatását egyetlen intézményben egyesíti, és 2012. január 1-jével létrehozta a Nemzeti Közszolgálati Egyetemet (a továbbiakban: NKE).[4] Az akkor három karból álló egyetemen azóta ötkarúra bővült:

- Államtudományi és Közigazgatási Kar (a továbbiakban: ÁKK);
- Hadtudományi és Honvédtisztképző Kar (HHK);
- Rendészettudományi Kar (RTK);

---

[1] Dr. Kőnig Balázs titkár. Nemzeti Közszolgálati Egyetem, Kiberbiztonsági Akadémia

[2] A fejezet Krasznay Csaba adjunktus, az NKE Kiberbiztonsági Akadémia programigazgatója és Kovács László egyetemi tanár, intézetvezető, a Kiberbiztonsági Kiemelt Kutatóműhely vezetőjének anyagai alapján készült

[3] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról (NKS)

[4] 2011. évi CXXXII. törvény a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról (NKEtv.)

- Nemzetközi és Európai Tanulmányok Kar (NETK);
- Víztudományi Kar, Baja (VTK).

Ezeken a karokon felül az egyetem három karközi intézettel is rendelkezik:
- Államkutatási és Fejlesztési Intézet (ÁKFI);
- Katasztrófavédelmi Intézet (KVI);
- Nemzetbiztonsági Intézet (NBI).

Valamilyen módon ezek mindegyike foglalkozik a kiberbiztonság egyes részkérdéseivel, a szervezeti önállóság miatt azonban az oktatás-kutatás területén egyetemi szintű koordinációra volt szükség. A karok többségénél egy-két oktató foglalkozott a kiberbiztonsággal, jellemzően választható tárgyak keretében, így nem volt sem órarendi lehetőségük, sem pedig széleskörű szakismeretük arra, hogy a szükséges alapismereteket átadják az érdeklődő hallgatóknak. A karok eltérő órarendje és az egyes campusok távolsága miatt a meglevő szinergiák kihasználására sem nyílt lehetőség.

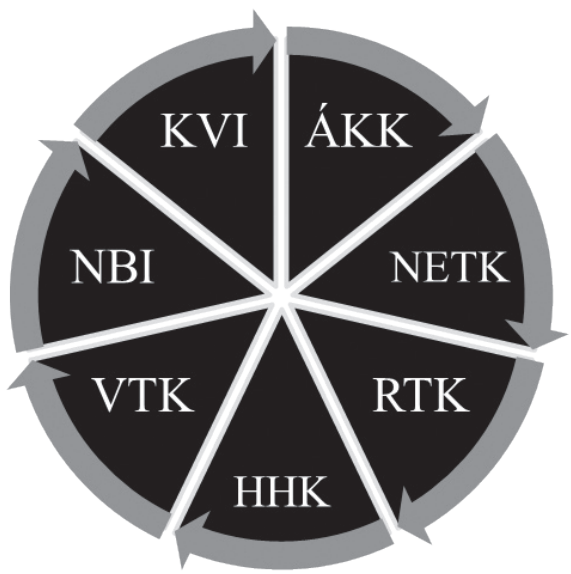
Az egyetem vezetése időben észlelte ezt a kihívást, és megállapította, hogy a kiberbiztonság olyan horizontális szakterület, amely megköveteli a szakmai koordinációt az oktatással és kutatással foglalkozó szereplők között. Ezen koordináló tevékenység megvalósítása érdekében jött létre 2017. március 1-jével a Kiberbiztonsági Akadémia (a továbbiakban: KBA), amely egy az NKE Rektora által alapított egyetemi központi programkeret. Feladata, hogy a programigazgató vezetésével, egy Szakmai Irányító Testület (a továbbiakban: SZIT) támogatásával integrálja és szervezze az NKE képzési egységei (karok, intézetek) és a kutatóműhelyek kiberbiztonsági munkáinak szinergiáit, képzési és kutatási programok szervezésével növelje azok eredményességét és hatékonyságát.

A SZIT irányításával és a programigazgató vezetésével tehát a Kiberbiztonsági Akadémia elsődleges feladata olyan nemzetközi és hazai célcsoportokra irányuló képzési programok, szakmai rendezvények és publikációk szervezése, amelyek
- az NKE-n folyó képzési és kutatási erőforrások szinergiáira épülnek,
- rugalmasan és gyorsan reagálnak a kormányzati fejlesztési igényekre,
- az NKE IT-erőforrásait hatékonyan integrálják egy közös cél érdekében,
- az eltérő hivatásrendeknél is „átfogó szemléletet” érvényesítenek,
- a legkorszerűbb IT-technológiával összhangban készülő fejlesztéseket generálnak.

Az NKE részéről a SZIT tagságába tartozik az öt kar és az érintett karközi intézetek kiberbiztonsági kérdésekkel megbízott vezető oktatói, valamint azok a külső szervezetek, amelyek meghatározó szerepet játszanak a magyar kibervédelem rendszerében. A SZIT tagjai a következő szervezetek:
- Nemzeti Adatvédelmi és Információszabadság Hatóság, melynek elnöke egyben a SZIT elnöke is,
- Belügyminisztérium (a továbbiakban: BM),
- BM Országos Katasztrófavédelmi Főigazgatóság,
- Alkotmányvédelmi Hivatal,
- Nemzetbiztonsági Szakszolgálat,
- Katonai Nemzetbiztonsági Szolgálat,
- Igazságügyi Minisztérium,

- Honvédelmi Minisztérium,
- BM Országos Rendőr-főkapitányság (a továbbiakban: ORFK), Nemzeti Nyomozó Iroda, Kiberbűnözés Elleni Főosztály,
- Magyarország kiberkoordinátora,
- Külgazdasági és Külügyminisztérium,
- Miniszterelnökség.

A kiberbiztonsággal kapcsolatos kutatási hátteret a Ludovika Kiemelt Kutatóműhely a Közigazgatás- és Közszolgáltatás-fejlesztési Operatív Program (a továbbiakban: KÖFOP) pályázat keretében benyújtott Kiberbiztonsági Kiemelt Kutatóműhelye (Kiberbiztonsági KKM) nyújtja.



1. ábra

A kibervédelmi kutatás és oktatás szervezetei az NKE-n

Forrás: A szerző és Krasznay Csaba közös szerkesztése

Jogszabályi háttér

A fenti szervezetrendszer feladatainak jogi alapjait, a kiberbiztonság jogi fogalmát és fontosságát a fent már említett NKS, illetve az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény (a továbbiakban: Ibtv.) teremti meg,[5] és határolja el az elsősorban műszaki tartalmú információbiztonságtól.

[5] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

Ezek szerint: az „*elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”,[6] míg a „*kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez”.[7]

Magyarország Nemzeti Kiberbiztonsági Stratégiája szerint pedig a stratégia „célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is”,[8] azaz közel sem a mérnöki feladatokra koncentrál.

Az államoknak, így Magyarországnak is biztosítania kell kiberterének védelmét, ami az egyes közszolgálati hivatásnemekben megkívánja olyan szakértők jelenlétét, akik a szükséges és elégséges mértékben értik az információbiztonság műszaki megközelítését, de saját szakterületükön is magas szintű hozzáértésről tesznek tanúbizonyságot.

Kiberképességek a közszolgálatban

Petró Csilla és Stréhli-Klotz Georgina 2014-es cikkükben részletesen kifejtik, hogy „az állami feladatok biztonságos és hatékony ellátása érdekében hangsúlyt kell fektetni a feladatellátást végző személyi állomány minőségére, munkavégzési képességére, közérzetére” mindhárom hivatásrend (civil közigazgatás, rendvédelmi, honvédelmi) esetében.[9] Ez különösen igaz azokra, akik a kiberbiztonsági területen dolgoznak, hiszen egyrészt főleg a fiatalabb, 20–30 éves korosztály választja magának ezt a területet, amelynek a szigorú szabályok szerint működő közszolgálat esetleg túl kötött lehet, másrészt a piaci szféra elszívó hatása minden más specializációnál komolyabban jelentkezik, hiszen globális szinten egymillió betöltetlen, kiberbiztonsághoz kapcsolódó állás van, jóval magasabb bérezéssel, mint amit az állami hivatalok biztosítani tudnak.[10] A magyar közszolgálatból Rajnai Zoltán mk. ezredes, Magyarország kiberkoordinátorának közlése szerint kétezer szakember hiányzik. Fontos tehát meghatározni, milyen képességfejlesztés szükséges hazánk kibervédelmének megerősítéséhez rövid- és középtávon.

---

[6] Ibtv. 1. § (1) bekezdés 15. pont

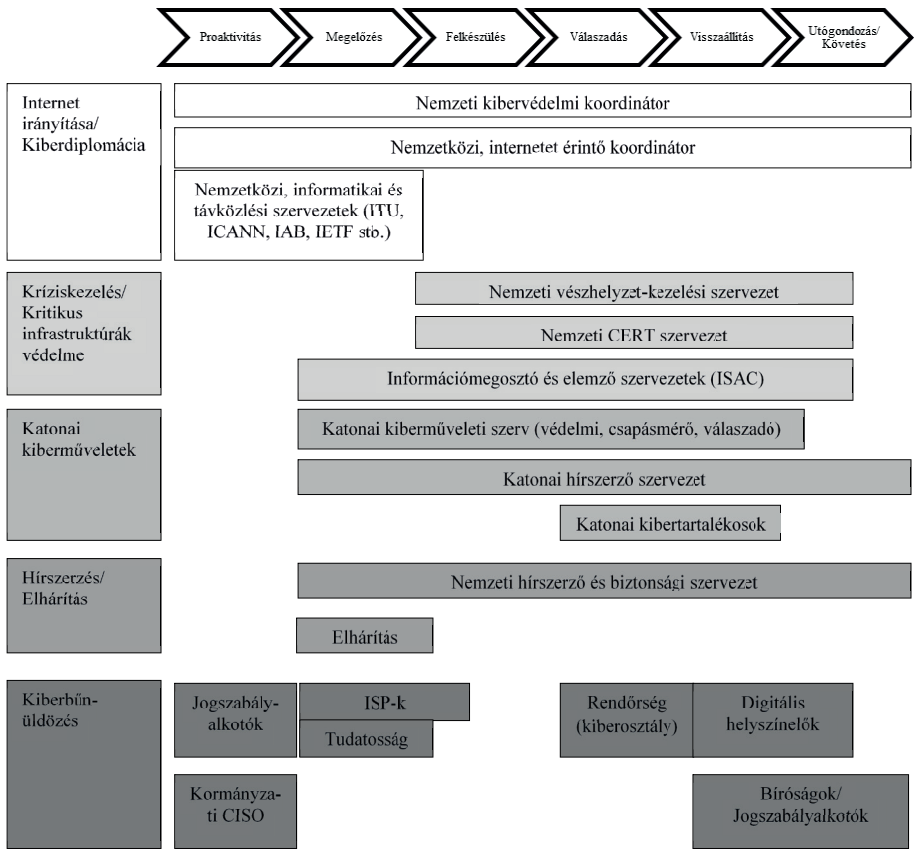
[7] Ibtv. 1. § (1) bekezdés 27. pont

[8] 1. melléklet az 1139/2013. (III. 21.) Korm. határozathoz 1. pont

[9] Petró Csilla – Stréhli-Klotz Georgina (2014): Formálódó új közszolgálati életpálya, különös tekintettel a munkaköralapú rendszer bevezetése irányába tett hazai kísérletekre. *Polgári Szemle,* 10. évf. 3–6. sz. 369–389.

[10] Morgan, Steve (2016): Hackerpocalypse: A Cybercrime Revelation. Cybersecurity Ventures. Elérhető: https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/ (A letöltés dátuma: 2018. 09. 21.)

Hazánk kibervédelmi rendszere egyrészt erősen centralizált, hiszen a feladatok nagy része a Belügyminisztérium alá tartozó szervezeteknél jelenik meg, rajtuk kívül pedig a Honvédelmi Minisztérium, a Külgazdasági és Külügyminisztérium, valamint a Miniszterelnökség rendelkezik kisebb-nagyobb feladatrendszerrel, másrészt viszont meglehetősen fragmentált, hiszen az egyes minisztériumokon belül, illetve alájuk rendelve számos szervezet munkáját kell összehangolni. Az alábbi ábra a NATO Kiberbiztonsági Kiválósági Központjának Nemzeti Kiberbiztonsági Keretrendszerét mutatja be, amely felsorolja, hogy milyen feladatok adódhatnak állami részről.[11]



2. ábra

A kibervédelem életciklus modellje

Forrás: National Cyber Security Framework Manual. LUIIJF, Eric – HEALEY, Jason 2012

[11] LUIIJF, Eric – HEALEY, Jason (2012): Organisational Structures & Considerations. In KLIMBURG, Alexander ed.: *National Cyber Security Framework Manual.* Tallinn, NATO CCD COE Publications. 108–145.

Magyarországon jelenleg a következő szervezetek töltenek be kulcsfontosságú szerepet a fenti keretrendszerben:

- Nemzeti kibervédelmi koordinátor: a 484/2013. (XII. 17.) Korm. rendelet hozta létre ezt a pozíciót, kiberkoordinátor néven;[12]
- Nemzetközi, internetet érintő koordinátor: a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról szóló 19/2016. (VIII. 31.) KKM utasítás szerint a minisztérium Erőforrás-diplomácia és Új Típusú Biztonsági Kihívások Főosztályán működő Kibertér Koordinátor feladata ennek a szerepkörnek a betöltése;
- Nemzetközi, informatikai és távközlési szervezetek: a fontosabb nemzetközi szervezetek kiberbiztonságért felelős vezető pozícióit több esetben is Magyarország delegáltjai töltik be;
- Nemzeti vészhelyzet-kezelési szervezet: alapvetően a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján a létfontosságú rendszerek kibervédelméért a Belügyminisztériumon belül működő Országos Katasztrófavédelmi Főigazgatóság tartozik felelősséggel;
- Nemzeti CERT szervezet: az Ibtv. hozta létre a kormányzati eseménykezelő központot, amely funkciót jelenleg a Nemzetbiztonsági Szakszolgálaton belül a Nemzeti Kibervédelmi Intézet látja el (GovCERT-Hungary);
- Információmegosztó és elemző szervezetek (ISAC): kimondottan ilyen szervezet a tanulmány írásának idejében nem működik Magyarországon;
- Katonai kiberműveleti szerv (védelmi, csapásmérő, válaszadó): a Honvédelmi Minisztérium, a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat lát el részfeladatokat ezen a területen, de a katonai kiberműveletek fő letéteményese ez utóbbi szervezet;
- Katonai hírszerző szervezet: a kibertérben történő katonai hírszerzés a Katonai Nemzetbiztonsági Szolgálat feladata;
- Katonai kibertartalékosok: a tartalékosok bevonása a katonai célú kibervédelembe jelenleg nem megoldott;
- Nemzeti hírszerző és biztonsági szervezet: bár a magyar jogrend egyetlen polgári nemzetbiztonsági szervezetnél sem nevesíti a kibertér védelmét, mégis valamennyi magyar titkosszolgálatnak közvetve van feladata, ugyanakkor a nemzetközi gyakorlat alapján ez elsősorban belbiztonsági feladatkört takar, amely a belügyminiszterhez tartozó titkosszolgálatok érintettségét jelenti;
- Elhárítás: megerősítve az előző pontot, kimondottan a kibertérből érkező fenyegetések titkosszolgálati elhárítása sincsen nevesítve. Az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról szóló 282/2016. (IX. 21.) Korm. rendelet[13] azonban a polgári nemzetbiztonsági

[12] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

[13] 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról

mesterképzési szak követelményeinél mind a technikai felderítő, mind a terrorelhárítási specializációnál megemlíti a kibertámadások elhárításának fontosságát, így közvetve arra a következtetésre lehet jutni, hogy az érintett titkosszolgálatok, illetve a Terrorelhárítási Központ épít ilyen képességeket;
- Jogszabályalkotók: a kiberbiztonsággal kapcsolatos jogszabályalkotást bármelyik érintett minisztérium kezdeményezheti, de jellemzően a Belügyminisztérium kezdeményezi a szakterület jogszabályalkotását;
- ISP-k: az internetszolgáltatók a Hun-Cert csoporton keresztül vesznek részt a magyar kibervédelemben;
- Tudatosság: annak ellenére, hogy a Nemzeti Kiberbiztonsági Stratégia egyértelműen kiemeli a tudatosságépítés fontosságát, nincsen egyértelmű felelőse a kérdésnek;
- Kormányzati CISO: az Ibtv. rendelkezései alapján nem egy kiemelt kormányzati információbiztonsági vezető van, hanem minden, a törvény hatálya alá tartozó szervezetnél van egy dedikált felelős;
- Rendőrség: a Nemzeti Nyomozó Irodán belül működő Kiberbűnözés Elleni Főosztály az utóbbi években kiemelt csúcsszervként foglalkozik az informatikai bűncselekményekkel;
- Digitális helyszínelők: bár statútuma szerint a Nemzetbiztonsági Szakszolgálat is rendelkezik ilyen képességekkel, a kiberbűnözés esetében elsődlegesen a Kiberbűnözés Elleni Főosztály Forenzikus Osztálya hajtja végre a digitális nyomrögzítéssel kapcsolatos feladatokat;
- Az igazságszolgáltatás szervezetei: a magyar gyakorlatban a kiberbűnözéshez kapcsolódóan elsősorban az ügyészségi szervezetek részéről érezhető aktivitás, a bíróságok elsősorban igazságügyi szakértők bevonására építenek.[14]

Kihívások a kiberbiztonság oktatásában

Krasznay Csaba, az NKE-KBA programigazgatója 2017 során több mélyinterjút folytatott az előző fejezetben felsorolt szervezetek illetékes vezetőivel annak érdekében, hogy megismerje az egyes intézmények kiberbiztonsági szakemberekkel szembeni elvárásait, ezek alapján ki tudjon alakítani bizonyos profilokat, majd meg tudja állapítani, hogy mi az a közös tudásmag, amely a közszolgálati kibervédelemben feltétlenül szükséges. Emellett fontos szempontként szerepelt az is, hogy kiderüljön, hol lehet kapcsolat az egyes hivatásrendek között, hiszen a közszolgálati életpályamodell egyik elengedhetetlen eleme az átjárhatóság. Az interjúk alapján az alábbi kiberképességekre van szükség a közszolgálatban:
- A kiberbiztonság általános megértésének képessége;
- Incidensmenedzselési képesség;
- Stratégiai, vezetői képességek.

[14] Som Zoltán – Papp Gergely Zoltán (2016): Tudásfejlesztés a kiberbűnüldözésben – Lehetőségek és kihívások. *Hadmérnök,* 11. évf. 2. sz. 170–182.

Képességfejlesztés az egyes felsőoktatási szinteken

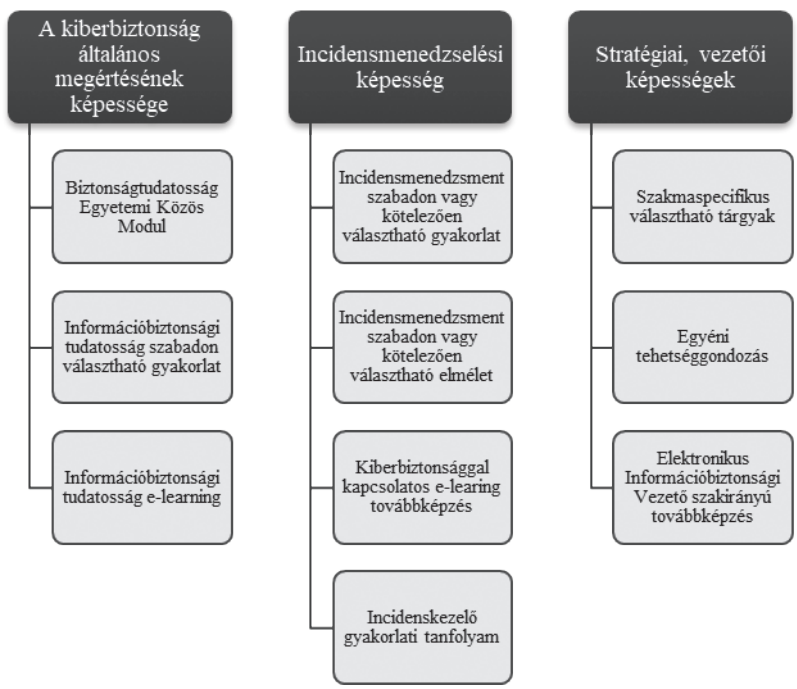
Magyarországon a közszolgálati oktatások erősen centralizáltak, a legtöbb feladatot a Nemzeti Közszolgálati Egyetem látja el. Az egyetem intézményfejlesztési tervében és küldetésében a közszolgálati utánpótlásképzés biztosítása mellett kiemelt hangsúlyt kap a közszolgálati életpályamodellt támogató továbbképzési rendszer működtetése. A kiberbiztonsági képességfejlesztésnek tehát kiváló helyszíne lehet az egyetem. A kibervédelmi szervezetek vezetőivel készült interjúk alapján a fent említett képességek a felsőoktatási keretrendszerben az alábbiak szerint fejleszthetők.

- A kiberbiztonság általános megértésének képessége:
  - Alapszinten: elengedhetetlenül fontos minden NKE-s alapképzési szakon foglalkozni a kiberbiztonság kérdésével, lehetőleg már az első évtől kezdve, már csak azért is, mert az infokommunikációs eszközök használata minden hivatásrend esetében végig fogja kísérni a végzettek pályafutását.
  - Alap- és mesterszinten: tekintettel arra, hogy a hallgatók a saját digitális létük védelmében is érdekeltek, érdemes olyan választható tárgyakat indítani, amelyek egy félév során, gyakorlati óra keretében, részletesen is be tudják mutatni, milyen kihívásokkal találkozhatnak a számítógépek és mobileszközök használata során. Az NKE-ÁKK-n jelenleg is elérhető egy „Információbiztonsági tudatosság" nevű tantárgy, amelynek hallgatói az éves visszajelzések alapján igénylik az egyes támadások kivédéséhez szükséges alapvető műszaki ismereteket is, így a tárgyat érdemes számítógépes támogatással tanítani.
  - Továbbképzési szinten: az NKE-ÁKK Vezető- és Továbbképzési Központja évente több mint 70 ezer közszolgálati tisztviselő továbbképzéséről gondoskodik, sok esetben e-learning formában. Ezen e-learning tananyagok közül egyre több foglalkozik a kiberbiztonsággal és speciálisan a biztonságtudatosság növelésével.
- Incidensmenedzselési képesség:
  - Alapszinten: a gyakorlati megközelítésű, biztonságtudatossággal foglalkozó gyakorlati tárgyra építve lehetőség nyílik arra, hogy a kiberbiztonsági incidensek hátterét és összefüggéseit mélyebben is megismerjék a hallgatók, választható vagy műszaki területhez közelebb álló specializációk esetén (egyes katonai és rendészettudományi képzések esetében) kötelezően választható tárgy keretében. Ez a tantárgy már igényel bizonyos fokú hálózati és informatikai ismereteket, így érdemes az elméleti és gyakorlati ismereteket is vegyíteni.
  - Továbbképzési szinten: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet előírja az egyetem számára azt, hogy minden évben új e-learning képzéseket készítsen a rendeletben megfogalmazott három célcsoport (elektronikus információs rendszer biztonságáért felelős személy, elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, elektronikus információs rendszerek védelméért felelős vezető) részére. Ezek az oktatások a teljes közszolgálat számára hozzáférhetők, és megfelelő alapot nyújtanak azoknak, akik már

aktív tisztviselőként szeretnének kiberbiztonságra specializálódni. Az incidenskezelési képesség kiépítéséhez azonban laboratóriumi gyakorlatra is szükség van.

- Stratégiai, vezetői képességek:
  - Alap-, mester- és doktori szinten: a vezetői információk alapján a magyar közszolgálat évente körülbelül 30–50 fő, nem műszaki orientációjú specialistát, szakértőt, vezetőt tud bevonni a kiberbiztonsággal foglalkozó szakterületekre. Semmiképpen nem tömegképzésről beszélünk tehát, sokkal inkább egyéni tehetséggondozásról, amelyben ugyanannyira fontos a saját specializáció mély ismerete, mint az együttműködési képesség a társterületekkel.
  - Továbbképzési szinten: a már gyakorló közszolgálati szakemberek közül is egyre többen szeretnének a hivatásrenden belül új specializációt választani és a kiberbiztonságra váltani. Számukra a hivatásrend ismert, így a kibertér specialitásait kell velük megismertetni. Erre ad lehetőséget az egyetemen az Ibtv. alapján elindított Elektronikus Információbiztonsági Vezető szakirányú továbbképzés, amely két félévből áll, és mind elméleti, mind gyakorlati tantárgyakat tartalmaz.

A javasolt képzési struktúrát az alábbi ábra mutatja be:



3. ábra

Javasolt kiberbiztonsági képzési struktúra

Forrás: Krasznay Csaba NKE-KBA programigazgató szerkesztése

Külön érdemes kiemelni az NKE-n a tanulmány írásának idején kidolgozás alatt álló Kiberbiztonsági MA képzést, amely kifejezetten és specializáltan a fenti igények kielégítését célozza, a tervek szerint három lehetséges specializációval.

Összefoglalás

A virtuális térből érkező fenyegetések kezelése nem kizárólag műszaki probléma többé. A kihívások nagy része közvetve vagy közvetlenül fenyegeti az ország biztonságát, illetve kezd kialakulni egy olyan negatív társadalmi biztonságpercepció, melyre az államnak reagálnia kell. Felkészült közszolgálati szakembergárda nélkül mindez nem lehetséges. Magyarországon a Nemzeti Közszolgálati Egyetem feladata és felelőssége a közszolgálati hivatásrendek oktatása, így ebben az intézményben is gondoskodni kell a megfelelő kiberbiztonsági oktatás-kutatási háttér megteremtéséről. A nemzetközi példák jó kiindulási alapot adnak az oktatás irányainak meghatározására, de nincsen olyan univerzális recept, amelyet egy az egyben adaptálni lehetne. Egyrészt azért, mert világszerte még mindig az információbiztonság, azaz a műszaki szemlélet oktatása a jellemző, másrészt azért, mert kevés olyan felsőoktatási intézmény létezik, amely az NKE-hez hasonló módon a teljes közszolgálatot lefedi.

Felhasznált irodalom

Luiijf, Eric – Healey, Jason (2012): Organisational Structures & Considerations. In Klimburg, Alexander ed.: *National Cyber Security Framework Manual.* Tallinn, NATO CCD COE Publications. 108–145.

Morgan, Steve (2016): Hackerpocalypse: A Cybercrime Revelation. Cybersecurity Ventures. Elérhető: https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/ (A letöltés dátuma: 2018. 09. 21.)

Petró Csilla – Stréhli-Klotz Georgina (2014): Formálódó új közszolgálati életpálya, különös tekintettel a munkaköralapú rendszer bevezetése irányába tett hazai kísérletekre. *Polgári Szemle,* 10. évf. 3–6. sz. 369–389.

Som Zoltán – Papp Gergely Zoltán (2016): Tudásfejlesztés a kiberbűnüldözésben – Lehetőségek és kihívások. *Hadmérnök,* 11. évf. 2. sz. 170–182.

Hivatkozott jogszabályok

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról (NKS)

2011. évi CXXXII. törvény a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról (NKEtv.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról

484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

Ajánlott irodalom

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

Kovács László – Krasznay Csaba (2018): Cyber security as a horizontal issue in Hungarian public service. KÖFOP publikáció, megjelenés alatt.

Krasznay Csaba (2018): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. KÖFOP publikáció, megjelenés alatt.

Hrucsár Mária[1]

Biztonságtudatosság
A Belügyi Tudományos Tanács Digitális Biztonságtudatosság Munkacsoportjának tevékenysége

Bevezetés

A technikai innováció mindent elsöprő fejlődésének hatására a 21. század embere a globális kibertérben találja magát. Élete nagymértékben függ az őt körülvevő komplex, ugyanakkor sérülékeny elektronikus információs rendszerektől, s noha a digitalizáció eredményeként újabb és újabb szolgáltatások könnyíthetik, színesíthetik mindennapjait, a kibertámadások reális veszélyének árnyékában az információbiztonság értéke felbecsülhetetlen. A kibertér fogalmát William Gibson használta először az *Izzó króm* című novellásкötetében, megfogalmazásában „a kibertér olyan háromdimenziós konszenzuális hely, amelyben az információ látható, hallható, sőt tapintható".[2] A kibertér a számítógépes hálózatok és az általuk összekötött számítógépek és egyéb berendezések által alkotott virtuális teret jelenti, amelynek angol elnevezése a „cyberspace". A kibertér az a környezet, amelyben a digitális információ (adat) technikai eszközökön (számítógépes hálózatokon) keresztül áramlik, elektronikus adatok tárolódnak, online adatforgalom és kommunikáció zajlik.

A fenyegetettségek, sérülékenységek megjelennek a közigazgatásban, a gazdaság és a társadalom működéséhez szükséges infrastruktúrák különböző területein, mint például az energiaellátás, ivóvízellátás, kommunikációs rendszerek, informatikai hálózatok területein. Az állampolgárok szintjén ezek a veszélyek akkor jelennek meg, ha az említett komplex rendszerekben működési zavarok lépnek fel, vagy az őket érintő személyes adatok sérülnek.

A hálózati és információs rendszerek széles körű elterjedése a közigazgatásban egyúttal komoly technológiai függőséget is eredményezett. Ezen rendszerek integritásának a sérülése jelentős, egyes esetekben beláthatatlan nemzetgazdasági és nemzetbiztonsági károkat okozhat (például a WannaCry zsarolóvírus a brit egészségügyben, vagy a NotPetya/MeDoc Ukrajnában).

A probléma sajátossága, hogy kizárólag a klasszikus védelmi metodikákat követve (például objektum- vagy tűzvédelem) már nem lehet hatékonyan fellépni a támadások ellen, mivel az informatikai rendszerekben nem érvényesül az arányosság elve (nagyobb érték – nagyobb lakat). Akár egy minimális hiba – 1 bitnyi információ – is alkalmas lehet

---

[1] Hrucsár Mária IT-menedzsment vezető. Országos Rendőr-főkapitányság, Gazdasági Főigazgatóság

[2] Gibson, William et al. (1986): *Izzó króm.* Budapest, Valhalla Páholy

arra, hogy a több szintű védelmi mechanizmust megkerülve a támadás hatékony legyen, és a védett adatvagyon kompromittálódjon, vagy a rendszer elérhetetlenné váljon.

Az információs infrastruktúrák elleni támadási módszerek egyre összetettebbek, ezek megismerése, a veszélyek azonosítása és a kockázatok reális felmérése különösen fontossá, a számítógépes hálózatok világa pedig virtuális harctérré válik.

A hadviselés színtere az ókortól napjainkig folyamatos változáson ment keresztül a technológiai fejlődéssel párhuzamosan, a nyílt csataterekről egyre inkább a virtuális világ felé, a technológiai, informatikai szférába helyeződött át, a 21. század elejére kiegészült a fentiekben már emlegetett kibertérrel. Ebben a személytelen virtuális térben óriási a tét, a kulcsfontosságú személyes, pénzügyi, banki, kormányzati, katonai, kritikus infrastruktúrákat érintő rendszerekhez való hozzáférés és minél több adat, információ megszerzése forog kockán. Napjainkra a kiberbűnözés 500 milliárd dolláros bevételt termelő, a drogkereskedelemből nyerhető hasznot is megelőző üzletté vált. A támadók egyrészt a haszonszerzésre törekszenek, másrészt nem riadnak vissza a kormányzati rendszerek támadásától sem. Az utóbbiak azonban már szervezett, összehangolt, komoly erőforrást igénylő támadásokat jelentenek, amelyek mögött akár állami szereplők is állhatnak.

Amióta kiemelten foglalkozom információbiztonsági kérdésekkel, keresem azokat a feladatokat, tevékenységeket, amelyek által hazánk kiberbiztonsági képességét emelni lehet. Így 2017. év nyarán csatlakoztam a Digitális Biztonságtudatosság Munkacsoport munkájához Krasznay Csaba, a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Akadémia programigazgatójának felkérésére. A 2017. november 8–9-én megrendezett „Digitális környezetünk fenyegetettsége a mindennapokban" című nemzetközi tudományos-szakmai konferencián a Digitális Biztonságtudatosság Munkacsoport munkájáról, eredményeiről számoltam be a résztvevőknek.

A Digitális Biztonságtudatosság Munkacsoport létrehozása

Magyarország Nemzeti Kiberbiztonsági Stratégiája[3] célul tűzte ki a felhasználók biztonságtudatosságának fejlesztését, a Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014–2020[4] is kijelenti, hogy „jelenleg a közigazgatási folyamatok biztonsági szempontból leggyengébb láncszeme az ügyintéző", és kiemelten kezeli a kompetenciák fejlesztését és a biometrikus technológiák alkalmazásának elterjesztését az információkhoz való illetéktelen hozzáférés megakadályozása érdekében, de a legfőbb célja a személyazonossággal való visszaélések megakadályozása. A Nemzeti Infokommunikációs Stratégia[5] átfogó célkitűzései között szintén megtalálható a digitális kompetenciák fontossága, a digitális írástudás, a stratégia felhívja a figyelmet, hogy ügyelni kell arra, a számítógép-használat,

[3] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (A letöltés dátuma: 2019. 09. 21.)

[4] Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014–2020. Elérhető: http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (A letöltés dátuma: 2018. 09. 21.)

[5] Nemzeti Infokommunikációs Stratégia 2014–2020. Elérhető: http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (A letöltés dátuma: 2018. 09. 21.)

a szoftverek, informatikai és igazgatási rendszerek, ismeretek hiánya ne okozzon semmilyen hátrányt se az állampolgároknak, se az közigazgatás tisztviselőinek.

A munkacsoport céljai

Figyelembe véve a fenti stratégiai irányokat, az *ad hoc* Digitális Biztonságtudatosság Munkacsoport célul tűzte ki, hogy a teljes közigazgatási szektorra vonatkozó ajánlásokat, tananyagokat, e-learning kurzusokat dolgoz ki, s fontosnak tartja a közigazgatásban dolgozó teljes állomány képzését, továbbképzését. Szükséges, hogy a közigazgatás informatikai rendszereit használók – *a közigazgatásban dolgozó teljes állomány* – megismerjék a tényleges veszélyeket, az információbiztonsági kockázatokat, és elsajátítsák az ezekkel szembeni védekezés módjait, ezáltal növekedjen a szervezetek e-biztonsága.

A legfőbb cél a biztonságtudatos magatartás kialakítása, szinten tartása, később fokozása.

Az informatikai eszközök és szolgáltatások igénybevételéhez számos jogszabályi és belső szabályozási előírás fogalmazódott meg az elmúlt évek során, amelyek sokszor csupán a munkát nehezítő, olykor akadályozó tényezőknek tűnnek a felhasználók szemében. Az informatikai-, valamint az információbiztonság megvalósításához szükség van egy *olyan szervezeti szemléletváltásra, amely révén az érintettek elsajátítják a biztonságtudatos viselkedési normákat,* valamint megismerik a biztonságtudatos felhasználói *magatartásra* vonatkozó intézkedések megkerülésének hatásait és lehetséges következményeit.

A munkacsoport megalakulása, a részt vevő szervezetek

Az ismertetett előzmények alapján a Belügyi Tudományos Tanács (a továbbiakban: BTT) kezdeményezésére 2017. május 9-én alakult meg a Digitális Biztonságtudatosság Munkacsoport, Magyarország kiberkoordinátora irányításával. Ezen belül is két albizottság jött létre, egy szakmai és egy didaktikai. A szakmai albizottság az oktatási tananyag szakmai tartalmát állította elő, lektorálását a Nemzeti Közszolgálati Egyetem munkatársaival közösen végeztük. A didaktikai munkacsoport feladata, hogy megtalálja a tananyag átadásának, oktatásának leghatékonyabb formáját. 2018 során ezt a munkát végezzük.

A *1. ábrán* láthatjuk, hogy a közigazgatás és civil szervezetek széles köre dolgozik együtt a munkacsoportban, a Belügyminisztérium érintett egységei mellett az egyetemek, kutatóintézetek és az információbiztonsággal összefüggő hatóságok, kulcsszereplők, ami garancia arra, hogy a készülő tananyagokba nagy fokú tudás, tapasztalat integrálódjon az információbiztonságról.

1. ábra

A Digitális Biztonságtudatosság Munkacsoport tevékenységében részt vevő szervezetek

Forrás: A szerző szerkesztése

A digitális kompetenciák fejlesztését támogató, a közigazgatás szereplőinek szánt online tanagyag a tervek szerint 2018-ban készül el.

A munkacsoport tevékenysége

Eddigi tevékenysége során a munkacsoport azonosította a kiberbiztonságra ható veszélyeket, meghatározta azok relevanciáját a közszférában dolgozók oktatása szempontjából. Ennek során arra jutott, hogy mivel egy szervezet támadása esetén a támadó mindig a legolcsóbb és leghatékonyabb eszközt fogja használni, sokszor elég a leggyengébb láncszemet megtalálni, és onnan kiindulva, már a védelmi vonalakon belül el lehet jutni a tényleges célszemélyhez vagy rendszerhez.

A kibertámadások legegyszerűbb útja a „humán tűzfal" megtörése.

Mi vagyunk a leggyengébb láncszem vagy az első és legintelligensebb védelmi vonal? A humán faktor jelentősége a támadások elleni hatékony védekezésben kiemelten fontos, de a „leggyengébb láncszem" típusú felhasználótól nem várható el, hogy a hálózati és információs rendszereket és a szofisztikált támadási formákat megértése, a bonyolult biztonsági szabályzatokat és eljárások elsajátítsa. Fontos cél ezért, hogy ne a felhasználótól és a betarthatatlan szabályzatoktól várjuk az információs rendszerek védelmét, hanem adjunk a felhasználók kezébe egyszerű és hatékony eszközöket (például jelszómenedzser, idegen pendrive-ok tiltása, spam- és internetszűrő stb.), és tegyünk meg mindent a biztonságtudatosságuk növelése érdekében.

Ennek figyelembevételével dolgozza ki a munkacsoport a rövid, egyszerű, a napi gyakorlatban jól alkalmazható tananyagot. A felhasználói szintű oktatási anyag elkészítése mellett szükség van egy a szakmai szempontokat hangsúlyozó, rendszergazda, rendszermérnök szintű, illetve egy kifejezetten menedzsment megközelítésű, vezetőknek szóló oktatási anyag elkészítésére is, amely anyagok figyelembe veszik az aktuális információbiztonsági technológiai trendeket.

Felhasználóként tudatában kell lennünk annak és vállalnunk kell annak a felelősségét, hogy mi vagyunk az első és legintelligensebb védelmi vonal, így munkahelyünk biztonsága, esetleg jövője múlhat rajtunk.

A kiberbiztonsági kihívások és trendek áttekintésével meghatároztuk az oktatás során átadandó üzenetek körét, és ezek tartalmát is kidolgoztuk. Témánként érthetően leírtuk az adott problémát, a probléma megoldásait, tippeket fogalmaztunk meg, kapcsolódó anyagokat és linkeket gyűjtöttünk össze, és gyakorta ismételt kérdéseket (GYIK) is megjelenítettük.

Az üzenetekkel kapcsolatban is megfogalmaztunk az elvárásokat: egyszerűek, praktikusak, gyakorlatiasak és észszerűen betarthatóak legyenek. Az előírások betartása és betartatása tekintetében megjelenik a vezetői felelősség, a vezetői példamutatás, fontos azonban hangsúlyozni, hogy a vezetői ellenőrzések során ne csak szankcionáljuk, hanem pozitív motivációt is alkalmazzunk.

A biztonságtudatosság fejlesztése során kiválasztott üzenetek

Az alábbiakban a tananyagok alapját képező 14 üzenetből egy-egy meghatározó elemre hívom fel a figyelmet, terjedelmi okok miatt csupán egy-egy gondolatot kiemelve.

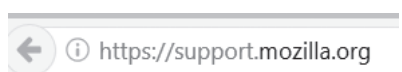
Címsor ellenőrzés, avagy nézd meg, hová lépsz be!

A webes felületekre való bejelentkezésekkel kapcsolatos figyelemfelhívó üzenet az iFrame-támadás problémák, átirányítások miatt került bele a kidolgozandó tananyagok közé.

Mára a mindennapi munka részévé vált az interneten való böngészés a munkahelyen, a közintézményekben, a szórakozóhelyeken vagy éppen otthonunkban.

A tananyag célja, hogy felhívja a felhasználók figyelmét, hogy a webcímek esetében mit és hogyan, illetve hányszor kell ellenőrizni. Erre vonatkozóan mindenkinek akadnak saját tapasztalatai, amelyekre támaszkodhat.

Nézzük például az alábbi három címsort: észrevehetők-e az eltérések a látszólag azonosnak tűnő címeknél?



1. valós cím.

2. módosított cím

3. módosított cím

Az első egy helyes cím, a 2. példában könnyen felfedezhetjük az eltérést, mivel egy betű („s”) hiányzik a címből, ami a kapcsolat titkosítására utal. A 3. példával már kicsit nehezebb dolgunk van, mivel a használt „Calibri” betűtípusnál a kis „L” betű = „l” és a nagy „i” betű = „I” között alig észrevehető a különbség, talán egy milliméter az eltérés.

A csalók gyakran ismert vagy hivatalos weboldalak hamis verzióit használják, hogy becsapják az oda látogató felhasználókat adathalászat céljából. Az adathalászok előszeretettel tulajdonítanak el felhasználói azonosítót, jelszavakat, bankszámla-, bankkártya adatokat, PIN-kódokat, számítástechnikai eszközünkön tárolt információkat és még sorolhatnánk. A felhasználók figyelmét arra hívjuk fel, hogy a böngészés során ellenőrizzék a címsort, és vegyék észre a kattintás előtt a különféle „furcsaságokat", amilyen például a bemutatott betűelírás volt.

Olyan furcsaságokat keressenek a címsorban vagy egy hivatkozásban, mint például

- egy rosszul tagolt cégnév, rövidítés,
- egy duplikált betű,
- betű elírása (például: „a" helyett „o"),
- egy extra karakter (például: „." vagy „_") a tartománynév végén, esetleg elején.

A tananyagban számos tanácsot, tippet is adunk a felhasználóknak, hogy mit tehetnek az adathalászat elkerülése érdekében. A felhasználó a legtöbb böngészőben, amennyiben a weboldalon lévő hivatkozás fölé helyezi egerét (érintőképernyő esetén rajta tartja az ujját), akkor láthatóvá tudja tenni a valós URL-t (Uniform Resource Locator – egységes erőforrás-azonosító), vagy ismertebb nevén webcímet, amelyet érdemes leellenőrizni a kattintás előtt.

Tipp gyanús oldal esetén
Egy adott honlap távolról is leellenőrizhető biztonsági szempontból a következő weboldalról, amennyiben kétségek merülnek fel megbízhatóságával kapcsolatban:

https://sitecheck.sucuri.net

A Sucuri SiteCheck szkenner ellenőrzi a megadott URL-t (például: magyarorszag.hu) az ismert rosszindulatú programok, a honlaphibák és a lejárt szoftverek szempontjából, továbbá megvizsgálja, hogy a honlap szerepel-e a feketelistán.

E-mail: levélben érkező támadások felismerése és kivédése

A felhasználó figyelmét ezzel az üzenettel arra hívjuk fel, hogy mielőtt megnyit egy e-mailt, mindig nézze meg a feladót, és ellenőrizze! A legtöbb támadás levélben érkezik, és valamilyen linket tartalmaz, amelyet elrejthetnek egy képbe, videóba, QR-kódba, valamilyen dokumentumba vagy tömörített fájlba.

2. ábra
A levélben érkező csatolmányok veszélyei

Forrás: A szerző szerkesztése

Levélben is átjöhet a vírusellenőrző program által fel nem ismert vírus. Az ugyanis időbe telik, amíg egy-egy újonnan megírt és csatolmányként szétküldött programról kiderül, hogy valójában vírus, és bekerül a vírusellenőrző programok adatbázisaiba.

Egy adathalász vagy csaló e-mail szinte teljesen ugyanúgy néz ki, mint az eredeti, de mindig vannak árulkodó jelek, amelyekre figyelni kell. Számítógépes vírusok jöhetnek hamisított feladótól érkező e-mailekben is. A látszólag egy barátunktól, ismerősünktől érkező levél nem biztos, hogy valóban az illetőtől származik. Gyanakodjunk, ha ritkán kapunk valakitől levelet, vagy tőle nem megszokott tárgyban ír, ha nem megfelelő magyarságú a levél, vagy ha bármilyen linket tartalmaz. A bankunk sem kéri soha e-mailben azonosító adatainkat, hiszen ismeri azokat. A Facebook is hemzseg a kártékony linkektől. Soha ne kattintsunk olyan linkre, amely úgy kezdődik, hogy „nem fogod kitalálni, mi történt…", „hihetetlen, hogy…", és még sorolhatnám a gyakorlati tanácsokat, amelyek a készülő tananyagba is belekerülnek.

Tipp: Mielőtt megnyitunk egy e-mailt, mindig nézzük meg a feladót!
Ne nyissunk meg olyan e-mail mellékletet, amely ismeretlen és nem beazonosítható feladótól származik, mert könnyen lehet, hogy vírust vagy egyéb kártékony kódot tartalmaz!

A nyilvános wifi használatának veszélyei

A mobil- és okoseszközök nagyarányú elterjedésével szükséges, hogy a mobilitásunkat folyamatos internetelérés is biztosítsa. Ennek egyik formája a mobilinternet, amely csökkenő árának és a roamingdíjak szabályozásának is köszönhetően egyre elterjedtebb. Ezzel együtt is még mindig elég gyakran találkozhatunk nyilvános wifi-hálózatokkal, sőt egyre több fejlesztésnek része a közösségi hozzáférési pontok kiépítése, ezáltal is ösztönözve az e-szolgáltatások elterjedését.

Ezen hálózatoknak a legfontosabb és egyben leghátrányosabb tulajdonsága, hogy a rajta továbbított adatok teljesen nyíltan haladnak keresztül, egy esetleges támadó akár szöveges formában is képes olvasni az átvitt adatokat, mint például a jelszavakat.

A nyilvános wifipontok használata rengeteg adatot szolgáltathat a hálózatokat rendszeresen monitorozó kiberbűnözők számára, és ha a felhasználó nem elég körültekintő, könnyen áldozattá válhat. A publikus wifin zajló adatforgalom lehallgatásához a bűnözők részéről különösebb szakértelem sem kell, elég egy csalihotspot üzemeltetése, vagy akár csak egy egyszerű böngésző-kiegészítő használata.

Szintén itt kell kitérni a wifi használatának megosztására, hiszen egyre többen használják úgy a mobilinternetüket, hogy ezzel több eszközt is kiszolgálnak úgy, hogy az egyik eszköz wifihotspotként működik. Vigyázni kell, hogy ilyenkor milyen beállításokat használunk, mert nemcsak abba a hibába eshetünk, hogy bárki rácsatlakozik a mi eszközünkre, ezáltal használva a mobilinternetünk sávszélességét, de rossz beállítással ugyanúgy sebezhetővé tesszük a saját készülékünket, és kiszolgáltatjuk azt a kiberbűnözőknek.

A fentiek elolvasása után kézenfekvő lenne, hogy sose használjunk ingyenes hálózatot. Nyilvánvalóan lehetnek olyan helyzetek, amikor ez elkerülhetetlen, ezért az ismert veszélyek figyelembevételével, körültekintő használattal csökkenthető az ingyenes wifi használatának kockázata.

Ellenőrizzük a nyilvános wifihálózatot: Győződjünk meg arról, hogy a wifiálózat valóban ahhoz az üzlethez, közlekedési eszközhöz, közösség térhez stb. tartozik-e, ahol tartózkodunk. Általában az ilyen elérhetőséget jól látható helyen feltüntetik, a hálózat nevével együtt, így meggyőződhetünk arról, hogy valóban arra a hálózatra csatlakozunk. Elkerülendő, hogy egy nagyon hasonló nevű (esetleg egy karakterben eltérő) álwifihotspotra kapcsolódjunk, amelyet kiberbűnöző működtet.

Kapcsoljuk ki az eszközünk adatmegosztási funkcióját: Gyakran használjuk ezt a funkciót, amikor eszközünkkel másokkal közös munkakörnyezetben kívánunk dolgozni. A baj akkor következik be, amikor ezt a funkciót bekapcsolva hagyjuk, megfeledkezünk a „nyitott kapuról", és csatlakozunk a nyilvános hálózatra, mert így a „nyitott kapun" keresztül bárki, akár akaratlanul is hozzáfér az eszközünkön tárolt adatokhoz.

Lehetőleg használjunk biztonságos böngészést: A hagyományos *http* protokoll helyett használjunk *https* protokollt. Ilyenkor a címsorban egy kis lakat mutatja, hogy a böngészőben az adatok biztonságosan kerülnek továbbításra. A mobileszközökön telepíthető kiegészítő a böngészőkhöz, ami alapértelmezetten választja a *https* protokollt. Ha egy oldal nem biztonságos, akkor nem ajánlott megnyitni, de nyilvános wifielérés esetén kifejezetten tilos.

Használjunk virtuális magánhálózatot (a továbbiakban: VPN): Amennyiben munkavégzéshez szükséges mobileszközünket nyilvános hálózaton keresztül akarjuk használni, akár rendszeresen, mert sokat utazunk, akkor a munkahely és a mobileszköz között a kommunikáció biztonságossá tehető VPN-kliens alkalmazásával. Ebben az esetben a VPN-kliens egy biztonságos, kódolt csatornát épít ki a mobileszköz és a munkahely között, így az ezen folyó adatforgalom kívülről gyakorlatilag feltörhetetlen.

Használjunk vírusirtót és tartsuk naprakészen: Sose kapcsolódjunk úgy nyilvános hálózatra, hogy nincs semmilyen védelmi rendszer az eszközünkön, mert így esélyünk sincs biztonságban tudni az adatainkat.

Tipp: Hivatalos ügyeinket ne nyílt wifihálózatról intézzük!
Használjunk kétlépcsős hitelesítést, mert ha valaki el is lopja egy nyilvános hálózaton keresztül a jelszavunk, sokat akkor sem ér vele!

Ha végeztünk a böngészéssel egy nyilvános hálózaton, akkor lépjünk ki az előzőleg használt szolgáltatásokból! Ha ezt megtettük, akkor a hálózatot is felejtessük el a készülékünkkel!

Az alkalmazások telepítésének veszélyei

Az otthoni és munkahelyi személyi számítógépek és mobileszközök használatakor felmerülő feladatok megoldása során új alkalmazások telepítése válhat szükségessé. Ennél az üzenetnél a felhasználók figyelmét arra hívjuk fel, hogy csak megbízható forrásból telepítsenek programokat. Ennek során használják a hivatalos forrásokat, például a Google Play Store, Apple App Store, Microsoft Store, illetve a termékgyártók hivatalos oldalait.

Az illegális forrásból származó alkalmazások telepítésének veszélyeire is felhívjuk a felhasználók figyelmét, bemutatjuk számukra a főbb kártékony viselkedési mintázatokat, amelyek előfordulhatnak, ha nem megbízható forrásból telepítenek egy-egy alkalmazást. Ilyenek lehetnek például a következők:

- A számítógép vagy mobileszköz fölötti távoli irányítás lehetőségének megteremtése (botnet zombie, backdoor).
- A felhasználói és üzleti adatok eltulajdonítása és kártékony felhasználása (keylogger, phishing helper, data scraper).
- Kéretlen reklámok megjelenítése, adatok gyűjtése a felhasználó beleegyezése nélkül.
- Alapértelmezett alkalmazások és internetes szolgáltatások (például internetes keresőmotor) kártékony céllal történő átkonfigurálása, lecserélése.
- A felhasználó adatait kriptográfiai módszerekkel titkosító, zsaroló kártevők (ransomware) telepítése.
- A felhasználó biztonsági tudatosságát kihasználó, félrevezető álalkalmazások (scareware) telepítése, hamis vírusriasztások megjelenítése, további kétes alkalmazások vagy szolgáltatások megvásárlására történő felszólítás.

Tipp: Korlátozzuk a felesleges funkciókat!
Számos alkalmazás lehetőséget nyújt a felhasználóról vagy az általa kezelt adatokról gyűjtött statisztikai és egyéb információk körének korlátozására. Az ezzel kapcsolatos beállítások gyakran rejtve, nem egyértelmű megjelöléssel (például „részvétel a felhasználói élmény javítása programban", „testre szabott keresési javaslatok"), a felhasználó biztonságát kevéssé szolgáló alapértelmezett beállítással lelhetők fel. Javasolt ezen beállítások, hozzájárulások tudatos korlátozása, a felhasználási szándék és a biztonsági elvárások ismeretében.

Mobileszköz használata

Az okos mobileszközök elterjedése sok esetben összemossa a munkaidőt a szabadidővel. Utazás közben a telefonunkról elérjük a munkahelyi e-mailjeinket, munka közben tudunk ismerőseinkkel csetelni, képeket megosztani stb. Mindez megnöveli a támadások lehetőségét, hiszen, ha a mobiltelefonunkról egy kevésbé vagy egyáltalán nem biztonságos kapcsolatról jelentkezünk be munkahelyi levelezésünkhöz, hiába van egyébként a munkahelyünkön jól védett, biztonságos rendszer, a támadók megkerülhetik rajtunk keresztül azt, és könnyedén hozzáférhetnek védett adatokhoz, hálózatokhoz. A *social engineering*hez hasonlóan ez sem kizárólag a kiberbűnözök által alkalmazott eljárás.

2013 óta, amikor Edward Snowden nyilvánosságra hozta az amerikai Nemzetbiztonsági Ügynökség (NSA) megfigyeléssel kapcsolatos eljárásait, a laikusok számára is világossá vált, mennyire könnyen hozzáférhető „kíváncsi fülek" számára a mindennapos kommunikációnk.

Tudatosítsuk magunkban: ha telefonunk elveszett, elsősorban nem az eszközért kár, hanem azon adatok miatt érdemes aggódni, amelyek a telefonon keresztül máshol (a felhőben vagy a szervezetnél) elérhetők. Az okoseszköz egy ugrópont a személy és egy adott szervezet értékes információihoz való hozzájutáshoz, ezért az erre vonatkozó tananyagrész a mobileszközök biztonságos használatára hívja fel a felhasználók figyelmét.

Az Europol által a kiberbűnüzésről készített jelentésből kitűnik, hogy a legnépszerűbb bűnelkövetési forma a kibertérben a kártékony kódokkal való visszaélés. Az okos mobil-

eszközök esetében is igen gyakoriak az úgynevezett zsarolóvírusok, amelyek a megfertőzött telefonok/tabletek tartalmát titkosítják, a feloldásért cserébe pedig pénzt követelnek – többnyire virtuális fizetőeszközben, elsősorban bitcoinban. Az esetek nagy részében természetesen a követelés teljesítése után sem kapjuk vissza fájljainkat, így nem érdemes fizetni a zsarolóknak. A nem biztonságtudatos eszközhasználat nagymértékben növeli kitettségünket a rosszindulatú támadással szemben.

Az okoseszközök alkalmazásából származó kockázatokat egy szervezetnek szükséges kezelnie, erre a Mobile Device Management (a továbbiakban: MDM) rendszerek alkalmasak. A mobileszközök és a rajtuk tárolt információk, alkalmazások, illetve a kommunikációs folyamatok központi, távoli védelmére, flottában történő menedzselésére az MDM-rendszerek megoldást adnak, ugyanakkor a felhasználói tudatosság itt sem mellőzhető.

Tipp: Fontos és érzékeny információkat ne tároljunk titkosítatlan adattárolón!
Mindig nézzünk utána az általunk használt mobil operációs rendszer biztonsági beállításainak, tájékozódjunk, milyen módon lehet az eszközön levő adatokat titkosítani, baj esetén pedig távolról mindent törölni!

Munkahelyi- és magáneszközök használata

A tananyagban két dologra hívjuk fel a figyelmet, egyrészt a munkahelyi eszközök magáncélú használatának veszélyeire, másrészt a saját eszközök munkában való használatának információbiztonsági vonatkozásaira. Ha a cégtől nem kapunk, akkor otthonról hozunk mobileszközt, egyébként is sokszor jobb eszközünk van otthon, de vajon a levelezés és egyéb céges rendszerek hozzáférhetőségeinek beállítása hogyan valósul meg a magán mobileszközön?

Számos kockázati tényező merül fel ennél a komplex kérdéskörnél, nézzük meg például, hogy milyen veszélyei vannak a munkahelyi levelezőrendszer magáncélú használatának!

Munkahelyi e-mail-címmel történő regisztráció: az e-mail-cím felépítéséből következtetni lehet a munkáltatóra, amely esetenként üzleti titkot is sérthet. Ez az állami és közigazgatási szektorban fokozottabb kockázati tényezőt jelent, mivel a csatorna célzott külső támadásra is felhasználható. Ennek gyakori elemei a kéretlen levelek (spam), adathalászat (phishing), kémprogramok (spyware) és kártevő programok (malware), reklámprogramok (adware) és vírusok. Az esetleges támadás irányulhat a munkáltató irányába, illetőleg a munkavállaló személyére is. A támadás következményei igen súlyosak is lehetnek: a szervezet által üzemeltetett informatikai rendszer részleges vagy teljes blokkolása, terhelése, az üzletmenet folytonosságának megszakítása, amelynek hátterében pénzügyi, gazdasági, politikai, személyes vagy egyéb érdekek állhatnak. A munkáltatónak mindenekelőtt meg kell teremtenie a megfelelő belső szabályozást, például meg kell alkotnia a munkahelyi eszközök, így többek között az e-mail-fiók, céges laptop használatának, ellenőrzésének szabályairól szóló normát. A szabályozás mellett az információbiztonsági tudatosságra irányuló képzéseknek különösen fókuszálniuk kell erre a területre.

A védelem fontos elemei a BYOD (a saját eszközökre vonatkozó „Hozd a magadét!”) szabályozás, illetve a Mobil Device Management alkalmazás.

Tipp: Munkahelyi e-mail-címmel ne regisztráljunk magáncélból sehová!
Jó gyakorlat lehet, ha a munkáltató bizonyos időközönként emlékezteti a munkavállalókat arra, hogy milyen előírások vonatkoznak a munkahelyi e-mail-fiók használatára, és be nem tartásuknak milyen következményei vannak.

A közösségi médiában közzétett adatok

A közösségi médiában (Facebook, Twitter, Instagram, LinkedIn stb.) keletkező, nyilvánosan hozzáférhető hatalmas információtömeg mágnesként vonzza a rosszindulatú kíváncsiskodókat, a számítógépes és a hagyományos bűnözőket.

A közösségi oldalon folytatott aktivitásunk figyelemmel kísérése, valamint az ott magunkról, esetleg rólunk megosztott információk összegyűjtése, negatív célú felhasználása napjainkban igen jellemzővé vált. Személyiségprofil készíthető rólunk. Ez a személyiségprofil felhasználható egy bennünket érintő, rossz szándékú (bűnözői vagy egyéb deviáns [internetes zaklatás, szexuális kizsákmányolás, illetve titkosszolgálati felhasználás]) befolyásolás, manipuláció, kapcsolatfelvétel, kapcsolatépítés során.

Meg kell értenünk, hogy bármennyire biztonságtudatosan is használjuk ezeket a felületeket, az információ kikerül a saját felügyeletünk alól azáltal, hogy mi magunk adunk hozzáférést ismerőseinknek, ők az adatokat lementhetik, tovább oszthatják az információkat, ugyanakkor az alkalmazás szolgáltatója is hozzáférhet az adatainkhoz, hackerek támadhatják a közösségi média felületeket biztosító informatikai rendszereket.

Szándékaink ellenére olyanok is megismerhetik, archiválhatják az általunk közétett adatokat, akiknek ehhez mi nem adtunk engedélyt, és ezeket az információkat e személyek akár évek múlva is felhasználhatják, közzé tehetik.

A tananyagban megoldásokat, tanácsokat adunk a biztonságos használatra, beállításokra.

Tipp: Tudatosság és önmérséklet!
A ránk vonatkozó információknak a közösségi média profilunkban történő elhelyezése során tanúsítsunk önmérsékletet, ezeken a felületeken csak a szükséges mértékben osszunk meg személyes adatokat. Kerüljük az ismerőseinkre, munkahelyünkre vonatkozó bizalmas, nem közérdekű információk megosztását is.

A munkára használt nyilvános felhő alapú rendszerek veszélyei

A felhőszolgáltatásoknak számos előnye van, de az „ingyen” prémiumszolgáltatásnak megvan a maga ára is: nem is sejtjük, mi mindent tud rólunk a keresőóriás.

Azok alapján, hogy egy felhő milyen szolgáltatást nyújt, háromféle felhőt és egy „egyéb kategóriát” különböztetünk meg:

- Szoftver szolgáltatás (SaaS): a szoftvert magát nyújtja szolgáltatásként. Például: Google Docs.

- Platform szolgáltatás (PaaS): az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja, méghozzá terheléselosztással és szoftverfrissítéssel. Például: OpenShift (RedHat), Google App Engine.
- Infrastruktúra szolgáltatás (IaaS): virtuális hardvert szolgáltat (szerver, tárhely, számítási kapacitás). Például: Google Compute Engine, Amazon EC2.
- Tárhely szolgáltatás (SaaS): ez az „egyéb kategória". Ilyenek a biztonsági mentéshez adott tárhelyek, vagy a szinkronizáláshoz nyújtott támogatások. Például: Google Drive, Dropbox, Amazon S.

A kapcsolattartás, munkavégzés, értékelés, elismerés örömének átélése tipikus „felhőélmény", amely egyre jobban, növekvő mértékben igényeli a felhasználó felhőben való tartózkodását. A „bárhol, bármikor és bárkivel" kapcsolatteremtés lehetőségének igénybevétele a felhőalkalmazásokon keresztül történik, ilyenek például a Dropbox, az iCloud és a Google Drive.

A Google szerverein ott van az is, mit csináltunk tegnap este. A tananyagban 25 pontban soroljuk fel, hogy mit tud rólunk a Google, kinek és mit írunk, mi van a gépünkön, mit néztünk a YouTube-on, milyenek a vásárlási szokásaink, mi a telefonszámunk, a címünk, illetve hogyan látszik minden online tevékenységünk. A Secure Access titkosítja az adatainkat, ugyanakkor mindent rögzíthetővé tesz a Google számára.

A Google adatvédelmi irányelvei között elolvashatjuk, hogy a cég gyűjtheti a telefonhívásaink adatait, hogy kit és mikor hívtunk, és mindezt tárolja is. Azt is rögzíti, hogy mikor és milyen weboldalakat nézünk meg, és ha a Google helyérzékelő szolgáltatásait is igénybe vesszük, akkor azt is tudja és tárolja, hogy mikor és hol tartózkodunk.

Azt reméljük, hogy a felhasználó, miután végignézte az általunk összeállított listát, s ennek alapján átgondolja a saját listáját, kicsit máshogy nyitja majd meg a Gmailt a következő levélnél.

Tipp: Vegyünk igénybe az Európai Unió adatvédelmi előírásainak, normáinak, ajánlásainak megfelelő felhőszolgáltatást, amennyiben arra szükségük van!

Munkahelyi környezet, jelszó

A felhasználói munkahely elhagyásakor sok esetben nem történik meg a képernyő zárolása, a bizalmas információk elzárása az illetéktelenek elől. Ezáltal a munkaállomás felhasználhatóvá válik a bejelentkezett felhasználó megszemélyesítésére, jogainak kihasználására.

A dokumentumok, munkaanyagok tárolása nem mindig következetes. Az íróasztalon felejtett bizalmas információk (naptárbejegyzések, szerződések, névjegykártyák, apró jegyzetek) rengeteg segítséget nyújtanak az információk megszerzéséhez, de egy identitáslopás kivitelezéséhez is.

Felhívjuk a felhasználók figyelmét a jelszó feltörésének, megszerzésének veszélyeire, megoldásokat adunk a kidolgozott tananyagban többek között arra is, hogy milyen a jó jelszó. A jól megválasztott jelszó jellemzői a következők:

- minimum 8 karakter hosszú, és nem egyezik meg a felhasználónévvel;
- tartalmaz kis- és nagybetűt, számot és valamilyen különleges karaktert;

- nem azonos az alapértelmezett jelszavakkal, különös tekintettel az adminisztrátori jelszavakra;
- nem utal a jelszó használójára (például olyan személyes információkat sem tartalmaz, mint a felhasználó neve, születési dátuma, családtagja neve, háziállata neve, kedvenc autómárkája, hobbija stb.);
- nincsenek benne egymást követő karakterek (például 123456, QWERTY stb.);
- lehetőség szerint nem értelmes, szótári szavakból áll.

Tipp: Jelszavak helyett alkalmazzunk jelmondatokat, az egyes magánhangzókat cseréljük ki számokra, ezzel is megnehezítve a jelszavunk feltörését! Kerüljük a többszörös jelszóhasználatot, az egyes rendszerekbe történő bejelentkezéshez válasszunk eltérő jelszavakat!

Social Engineering technikák

A *social engineering* támadások során a humán tényező azért kedvező célpont, mert a felhasználó különféle hardver- és szoftvereszközöket használ, hozzáféréssel rendelkezik a különféle adatbázisokhoz, rendszerekhez vagy ügyféladatokhoz. A munkavállalók kapcsolatban állnak, információkat osztanak meg egymással, valamint különféle belső és bizalmas adatokkal rendelkeznek, amelyek a támadók számára értékeseknek tekinthetők. Éppen ezért kiemelkedő jelentőségű, hogy az alkalmazottak tudatában legyenek a *social engineering* támadások módszereinek, annak érdekében, hogy a támadás bekövetkezésének valószínűségét csökkenteni lehessen.

3. ábra

Miért éppen engem támadnának meg?

Forrás: A szerző szerkesztése

Az ember ideális célpontnak tekinthető továbbá a kihasználható tulajdonságai miatt. Ilyen tulajdonságok például a segítőkészség, naivitás, kíváncsiság, nyitottság, befolyásolhatóság, érdeklődés, fáradtság vagy túlterheltség. A tananyag célja, hogy az alkalmazottak tudatában legyenek a *social engineering* támadások módszereinek, és felismerjék azokat. A tananyagban részletesen bemutatjuk azokat a szempontokat, amelyekre érdemes odafigyelni. Az emberek többsége nem is sejti, hogy irodai szemetese valóságos aranybánya is lehet egy *social engineer* számára. A kukában ugyanis rengeteg olyan dolog található, amely segítséget nyújthat egy esetleges támadás előkészítéséhez, például jelszavas cetlik, céges információk, az alkalmazott olyan személyes adatai, amelyek elősegíthetik az illető személyazonosságának felvételét, identitásának ellopását, valamint olyan információ birtokába is juthatnak a támadók, amellyel megvesztegetni vagy zsarolni lehet a célszemélyt.

Tipp: Használjunk iratmegsemmisítőt!
A szemetesbe soha ne dobjunk a munkahellyel kapcsolatos vagy személyes adatokat tartalmazó iratokat!

A pendrive használatának veszélyei

Az otthonról (munkahelyen kívülről) pendrive-on hozott adatokkal a munkahelyi hálózatot fokozott veszélynek tesszük ki, mert a kártevők, kártékony kódok napjainkban leginkább megtévesztő e-mailek csatolmányaiként (például: tömörített dokumentum, kép) és Microsoft Office (Word, Excel stb.) fájlokba beépülve terjednek. Mai napig elrettentő példa, hogy 2007-ben az iráni urándúsító rendszereket egy pendrive-on bejuttatott malware, a Stuxnet teljesen működőképtelenné tette.

Munkahely. Fáradtság. Kávészünet! Friss levegő… és egy pendrive a földön! Mivel segítő szándékkal szeretnénk a tulajdonosának visszaadni, munkaszobánkba visszatérve a számítógépünkhöz csatlakoztatjuk a pendrive-ot, bízva abban, hátha van rajta egy kép, egy dokumentum, amiről beazonosíthatjuk a tulajdonost.

A támadók jóindulatunkat kihasználva érik el, hogy a fertőzött pendrive a védett munkahelyi infrastruktúrához csatlakozzon, és a rajta lévő kártékony program elinduljon.

A tananyagban az adathordozók, titkosított pendrive-ok használatát tekintjük át információbiztonsági szempontból, konkrét megoldásokkal, tippekkel.

Tipp: Soha, semmilyen körülmények között ne csatlakoztassunk talált pendrive-ot a számítógéphez!

Mi tegyünk, ha bekövetkezett a baj?

Ha az adott számítástechnikai eszköz nem a megszokott módon működik, akkor nagy valószínűséggel valamilyen támadás áldozataivá váltunk. A munkatársaktól és a vezetőktől rendszerint nem várható el, hogy az információbiztonsági támadásokat maguk hárítsák el, de az igen, hogy azokat felismerjék és jelezzék a megfelelő informatikai szakemberek felé, tudják a hiba, incidens bejelentésének módját, és a lehető legrövidebb időn belül megtegyék

a szükséges lépéseket. Az ezzel foglalkozó tananyagrész így arról szól, hogyan vegyük észre, hogy támadás áldozatai lettünk, hogyan tudjuk ezt megelőzni, és mit tegyünk, ha bekövetkezett a baj.

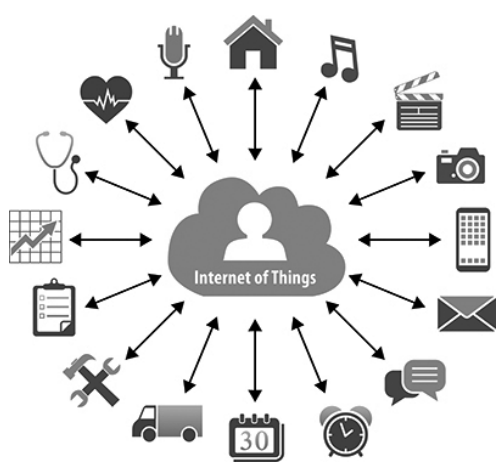
Például, ha hosszabb ideig tart, amíg a rendszer elindul, vagy a gép a szervezeti szerverhez csatlakozik, és a működése lassabb, esetleg hamarabb melegszik fel, zajosabban működik, több időt vesz igénybe a kikapcsolás/leállás, vagy eleve nem is kapcsol ki, akkor gyanakodhatunk, hogy valamilyen támadás ért bennünket. Amennyiben a rendszer nem engedi a vírusadatbázis frissítését, illetve a böngésző segítségével nem lehet elérni a vírusvédelmi alkalmazás weboldalát, vagy nem lehet onnan semmit sem letölteni, szintén érdemes felvenni a kapcsolatot a rendszergazdával.

Tipp: Mit tegyünk, ha ugyan elővigyázatosak voltunk, mégis bekövetkezett a baj? Munkatársként és vezetőként azonnal szóljunk a rendszergazdának!

Az IoT-okoseszközök használatának veszélyei

Az okos- vagy Internet of Things (a továbbiakban: IoT) eszközök olyan tárgyak, amelyek beépített mikroszámítógépet tartalmaznak (SoC – System on Chip), és valamilyen adatkommunikációs képességekkel rendelkeznek. Ide sorolják az okos környezeti szenzorokat, IP-kamerákat, az okosórát, okostelefont, okostévét, okoshűtőgépet, okoskenyérpirítót és számos más okoseszközt.

Az IoT rövidítést úgy is lefordíthatjuk a magunk használatára, hogy „valaki más számítógépe az otthonodban". Kezeljük ennek megfelelően az eszközt, ne bízzunk meg benne, illetve a gyártóban feltételek nélkül!



4. ábra

Az IoT főbb elemei

Forrás: How communication firms can monetize IoT beyond connectivity. Readwrite.com. Elérhetőség: https://readwrite.com/2017/05/06/how-communication-service-providers-can-monetize-iot-beyond-connectivity-il4/ (A letöltés dátuma: 2018. 09. 21.)

Különösen veszélyesek azok az IoT-eszközök, illetve funkciók, amelyek a felhasználó tudta és kifejezett beleegyezése nélkül rögzítenek adatokat és felvételeket a környezetükről, s ezeket a gyártó szervere felé továbbítják. Sok esetben a kép- és hangrögzítő eszközök félrevezető visszajelzéseket adnak a működési állapotukról, és akkor is üzemkészek, illetve aktívak, amikor a felhasználó ezt nem is feltételezi.

A megvásárolni kívánt IoT- vagy okoseszköz kiválasztásakor az anyagiak, a dizájn és a funkcionalitás mellett legyen szempont az eszköz biztonsági funkcióinak minősége, a terméktámogatás, beleértve a rendszeres sérülékenység-javítócsomagok kiadását a teljes életcikluson keresztül. A tananyagban ezekre a veszélyekre hívjuk fel a figyelmet, gyakorlati tanácsokat is adva.

Tipp: Ismerjük meg az általunk használt IoT-eszköz vagy okoseszköz biztonsági és adatvédelmi beállításait! Tájékozódjunk, milyen módon lehet az eszközön levő adatokat titkosítani, baj esetén pedig távolról mindent törölni!

Jogok és kötelezettségek

Az Európai Parlament és a Tanács 2016. április 27-én, négy év előkészületet követően fogadta el az új adatvédelmi csomagot, az általános adatvédelmi rendeletként ismert GDPR-t, amelyet 2018. május 25. napjától kell alkalmazni.[6] Ha az érintett szempontjából nézzük, az adatvédelem arról szól, hogy az állampolgár kontrollt tud gyakorolni a személyes adatai felett. Ezt a lehetőséget az adatkezelés létrejötte után az érintetti jogok jelentik az egyének számára. A GDPR III. fejezete tartalmazza az érintetti jogokat: a megfelelő és átlátható tájékoztatáshoz való jog, az érintett hozzáférési joga, a helyesbítéshez való jog, a törléshez való jog („az elfeledtetéshez való jog"), az adatkezelés korlátozásához való jog, az adathordozhatósághoz való jog, valamint a tiltakozáshoz való jog. Tananyagunkban ezekre a pontokra hívjuk fel az érintettek figyelmét, gyakorlati példák megadásával.

Nézzük például a törléshez való jogot! Minden érintett kérheti, hogy az a szervezet, amelyik a személyes adatait kezeli („adatkezelő"), törölje azokat. Az ilyen kérésnek az adatkezelő a jogszabály által előírt esetekben köteles egy hónapon belül eleget tenni. Ezen jog alapján bárki visszavonhatja például egy adatkezeléshez adott hozzájárulását, illetve kérheti, hogy jogellenesen kezelt személyes adatait töröljék.

Példa: a felhasználó regisztráltál egy webshopba, amely így, hozzájárulása alapján kezeli bizonyos személyes adatait (például név, e-mail-cím, lakcím, telefonszám). Amennyiben úgy dönt, hogy mégsem kíván rendelni, kérése alapján az üzemeltető cég köteles törölni a felhasználói fiókját, és így az ahhoz megadott személyes adatait.

[6] Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32016R0679 (A letöltés dátuma: 2018. 09. 21.)

Tipp: Ahhoz, hogy tudjuk, milyen módon kérhetjük személyes adataink törlését, nézzük meg az adatkezelő által rendelkezésünkre bocsátott és az adott honlapon elérhető adatkezelési tájékoztatót!

Ennek tartalmaznia kell az adatkezelő elérhetőségét, illetve a jogaink gyakorlásával kapcsolatos információkat is.

Összegzés – hol tartunk most?

A Digitális Biztonságtudatosság Munkacsoport áttekintette a kiberbiztonsági kihívásokat és trendeket a közigazgatás szempontjából, és meghatározta azt a 14 üzenetet, amelyeket a közigazgatásban dolgozók részére el akar juttatni, információbiztonsági szempontból az átadandó üzenetek szakmai tartalmát kidolgozta, ennek lektorálása folyamatban van. Ezt követően a didaktikai albizottság meghatározza az üzenetek átadásának leghatékonyabb formáját, 2018. évben elkészülnek a tananyagok, és megkezdődhet a közigazgatás felhasználóinak oktatása.

Az informatikai világ újgenerációs kártevői reális és komoly veszélyt jelentenek társadalmunk működésének alapjaira, a rendelkezésre álló informatikai erőforrások megsokszorozásával a különböző hackercsoportok az aktuális érdekeiknek megfelelően támadnak.

Legfőbb célunk ezért a digitális biztonságtudatosság szintjének növelése, egyszerű, praktikus, gyakorlatias ismeretek átadásával.

A kiberbiztonság megteremtésének kulcseleme a digitális eszközök és kommunikáció biztonságos használatához szükséges kompetenciák fejlesztését szolgáló elektronikus tananyagok és képzési rendszer kialakítása, oktatása, a biztonságtudatos elektronikus üzemeltetési, fejlesztési és felhasználói kultúra kialakítása, a közigazgatásban dolgozók digitális írástudásának fejlesztése. Tudjuk, hogy százszázalékos biztonságot nem lehet elérni, de megfelelő tudatossággal a kormányzati, a gazdasági és a civil élet szereplői, a kockázatokkal arányos védelmi profilok alkalmazásával, sokat tudnak tenni azért, hogy adataik és elektronikus információs rendszerelemeik biztonságban legyenek, s a társadalom alapműködéséhez szükséges infrastruktúrák, a gazdaság motorját biztosító elektronikus informatikai rendszerek zavartalanul működjenek.

Felhasznált irodalom

Gibson, William – Shirley, John – Sterling, Bruce – Swanwick, Michael – Shire, Lewis (1986): *Izzó króm.* Budapest, Valhalla Páholy.

Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014–2020. Elérhető: http://www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (A letöltés dátuma: 2018. 09. 21.)

Nemzeti Infokommunikációs Stratégia 2014–2020. Elérhető: http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (A letöltés dátuma: 2018. 09. 21.)

Hivatkozott jogszabályok

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (A letöltés dátuma: 2018. 09. 21.)

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32016R0679 (A letöltés dátuma: 2018. 09. 21.)

Ajánlott irodalom

1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Elérhető: http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (A letöltés dátuma: 2018. 09. 21.)

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (A letöltés dátuma: 2018. 09. 21.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (A letöltés dátuma: 2018. 09. 21.)

2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. Elérhető: http://www.kozlonyok.hu/kozlonyok/Kozlonyok/10/PDF/2008/31.pdf (A letöltés dátuma: 2018. 09. 21.)

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.350656 (A letöltés dátuma: 2018. 09. 21.)

Az Europol mobilkártevőkkel kapcsolatos tudatosító dokumentuma. Elérhető: https://www.europol.europa.eu/sites/default/files/documents/Hungary.pdf (A letöltés dátuma: 2018. 09. 21.)

Graham, Luke (2017): Cybercrime costs the global economy $450 billion: CEO. CNBC.com. Elérhető: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (A letöltés dátuma: 2018. 09. 21.)

Magyarország Nemzeti Katonai Stratégiája (2012). Honvédelmi Minisztérium. Elérhető: http://www.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf (A letöltés dátuma: 2018. 09. 21.)

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem.

Szalai Tihamér – Szűcs Péter – Miltényi Gábor – Rigó Ernő – Krasznay Csaba – Szűcs Tibor – Mezei József – Tar János – Luklíder Gabriella – Koós István – Poór Péter – Kollár Csaba – Róka Tamás – Árvay Viktor (2017): A Belügyi Tudományos Tanács Digitális Biztonságtudatosság Munkacsoport által kidolgozott információbiztonság tudatosság képzés munkaanyaga. Kézirat.

Ziolkowski, Katharina ed. (2013): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. Tallinn, NATO CCD COE Publication. Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/PeacetimeRegime.pdf (A letöltés dátuma: 2018. 09. 21.)

Solymos Ákos[1]

Az incidenskezelés humán szenzorai és fejlesztésük

Felhasználók régen és ma, próféták és az Y–Z generáció

A Maslow-szükséglethierarchiában a biztonság közvetlenül a fiziológiai szükségletek után következik. Azonban ez a biztonság mást jelent az egyes generációknak. Az egyes generációk közösségi médiához való viszonyát így jelzi egy amerikai tanulmány: a *baby boom* idején születettek (1940–1950-as évek) az úgynevezett „próféták", az X generáció (1960–1970-es évek) a „nomádok", az Y generáció (1980–1990-es évek) a „hősök", a Z generáció (2000-es évek) a „művészek" és a 2010 után születettek az Alfa-generáció. A biztonsághoz mindenki máshogy viszonyul.[2]

A számítástechnika és később az informatika első művelői és felhasználói még az újdonság erejével fedezték fel a technológia adta lehetőségeket, kevésbé volt téma és kevésbé volt fontos a biztonság az átlagfelhasználónak. Természetesen ebben az időben is az államvédelmi szervek és egyéb szolgáltatok igyekeztek mindenkitől védeni az adataikat, de ez akkor még elég költséges elfoglaltság volt. Az internet térnyerésével és az információmegosztás sebességének növekedésével járt együtt az információ értékének a növekedése is. Manapság pedig a Z generáció az, amelyik munkavállalóként megjelenik és hozza magával a saját informatikai szokásait. Hogy ebben hol és hogyan szerepel a biztonság, az más kérdés.

Az Y és Z generáció

Ahogy átalakult az informatikai technológia, ahogy az informatikai eszközök egyre nagyobb tudásúak és egyre kisebbek lettek, úgy formálták át minden család életét. Manapság sok szülő büszke arra, hogy milyen ügyesen nyomkodja a hároméves a YouTube-ot, miközben a gyerek nem tud felvenni egy kabátot, vagy nem tudja megkötni a cipőjét. Átalakultak a prioritások.

Az informatikában is igaz ez. Manapság kialakult az a generáció, az Y, Z (és hamarosan az Alfa) generáció, amelynek tagjai jelentős részben függőségben szenvednek mind az informatikai eszközüktől – ez legfőképp az okostelefont jelenti –, mind magától

---

[1] Solymos Ákos szakértő a Konzultáció és Tanácsadási Szolgáltatások vezetője. Quadron Kibervédelmi Kft.

[2] *Mik a generációk közötti eltérések a közösségi média világában?* Hrenko Digital Agency. Elérhető: https://www.hrenko.hu/blog/mik-generaciok-kozotti-elteresek-kozossegi-media-vilagaban/ (A letöltés dátuma: 2018. 09. 21.)

az információktól és a kommunikációs csatornáktól. Egy kutatás szerint, ha e fiataloktól elveszik a telefonjukat, elveszítik a biztonságérzetüket, pánikba, majd depresszióba esnek. A Maslow-szükséglethierarchiához hasonlóan fel lehet építeni ezen generációk informatikai eszközökhöz és szolgáltatásokhoz kapcsolódó szükséglethierarchiáját is. Ebben legalul helyezkedik el maga az eszköz és a hozzá kapcsolódó erőforrások (energia, térerő), majd jön a kommunikációs hálózati-, internetelérés wifin vagy 4-5G szolgáltatáson. Ezután következnek azok a programok, amelyek a kommunikáció fenntartásában segítenek, amelyek összekapcsolják őket a társaikkal, majd a közösségi oldalak, ahol az egyéb, szélesebb körű információkat begyűjtik és megosztják. Mindezek után következik csak az, hogy mindezt biztonságos módon tegyék.

Látszódik, hogy bár az információ felértékelődött, a mennyisége is annyira megnőtt, hogy sokszor az információk birtokosai is alulértékelik ezeket. Ez pedig egyenes út a figyelmetlenséghez, a felelőtlenséghez.

Biztonság megteremtése szervezeti szinten

Tekintve, hogy az információvédelem a mai napig nem szerepel megfelelő súllyal semmilyen iskolai tananyagban, ezért a cégek és szervezetek egyik fő feladata, hogy az új munkavállalókat, beleértve az ifjabb generációkat, megtanítsák mind a saját adataik, mind a céges adatok megvédésére. A cél, hogy kialakuljon a biztonságtudatosság. Az összes szabványban, ajánlásban és egyes hazai ágazati törvényekben is szerepel a biztonsági oktatás, mint nagyon fontos biztonsági kontroll.

Ilyenek az ISO27001,[3] PCI-DSS szabványok,[4] a COBIT,[5] a NIST[6] és a CIS[7] kontroll ajánlásai, valamint az EU-s és hazai jogszabályok is: a General Data Protection Regulation (a továbbiakban: GDPR),[8] a 2013/L. törvény,[9] a 41/2015. BM rendelet,[10] valamint a pénzügyi szervezeteknek szóló 7/2017. MNB ajánlás az informatikai rendszer védelméről.[11]

---

[3] *MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági-Irányítási Rendszerek. Követelmények.* Lásd részletesebben: Magyar Szabványügyi Testület. Elérhető: http://www.mszt.hu/web/guest/msz-iso-iec-27001 (A letöltés dátuma: 2018. 09. 21.)

[4] *Payment Card Industry Data Security Standard (PCI DSS).* PCI Security Standards Council. Elérhető: https://www.pcisecuritystandards.org/pci_security/ (A letöltés dátuma: 2018. 09. 21.)

[5] *COBIT 5.* Isaca.org. Elérhető: https://www.isaca.org/cobit/pages/default.aspx (A letöltés dátuma: 2018. 09. 21.)

[6] *NIST Controls.* National Institute of Standards and Technology – U. S. Department of Commerce, National Vulnerability Database. Elérhető: https://nvd.nist.gov/800-53 (A letöltés dátuma: 2018. 09. 21.)

[7] *TOP 20 Security Controls.* CIS – Center for Internet Security. Elérhető: https://learn.cisecurity.org/20-controls-download (A letöltés dátuma: 2018. 09. 21.)

[8] Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32016R0679 (A letöltés dátuma: 2019. 09. 21.)

[9] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (A letöltés dátuma: 2018. 09. 21.)

[10] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.350656 (A letöltés dátuma: 2018. 09. 21.)

[11] A Magyar Nemzeti Bank 7/2017. (VII. 5.) számú ajánlása az informatikai rendszer védelméről. Magyar Nemzeti Bank. Elérhető: https://www.mnb.hu/letoltes/7-2017-informatikai-rendsz-ved.pdf (A letöltés dátuma: 2018. 09. 21.)

Ha az egyénnél – legyen az bármilyen korú vagy végzettségű – megteremtjük a biztonságtudatos és kockázatérzékeny gondolkodást, akkor sokkal könnyebb a céges biztonsági szabályokat megértetni és elfogadtatni vele. Ez fontos lépés, mivel a biztonság sok esetben gátolja a funkcionalitást. Épp ezért, ha a felhasználók értik is a biztonsági kontrollokat, nem csak elfogadják, akkor sokkal könnyebben megtalálható az a bizonyos arany középút.

A felhasználó mint az incidenskezelés legfontosabb szenzora

Az oktatás nem egyenlő a tudatosítással. Egyre gyakrabban halljuk az „érzékenyítés" kifejezést is, ami hasonló jelentéstartalommal bír, talán annyi plusszal, hogy benne van: a felhasználókat érzékennyé kell tenni a kockázatokra. Tarthatunk akármennyi biztonsági oktatást, ha a felhasználók nyűgnek gondolják és megpróbálják kijátszani a szabályokat, kontrollokat. Csak az a felhasználó tudja hatékonyan értelmezni és alkalmazni a kontrollokat, aki tudatosan teszi ezt, és érzékeny a kockázatokra, biztonsági problémákra. A PPT – People, Process, Technology hármasból, mint kontrollcsoportból, a People, az ember az egyik legfontosabb érzékelő, ha biztonsági incidensek felismeréséről beszélünk. Főleg, ha figyelembe vesszük, hogy a cégek jelentős többsége nem rendelkezik a biztonsági folyamatok és technológiák széles skálájával. Akkor marad az ember, mint érzékelő. Ezért őt kell felkészítenünk arra, hogy mit kellene észrevennie. Ezen a felkészítésen rengeteg potenciális incidens megelőzése és felismerése múlik. A cél világos, de dupla az eredmény. Ugyanis, ha a felhasználó fel van készítve a fenyegetettségek és kockázatok felismerésére, akkor ezt minden olyan helyen, ahol informatikai rendszert használ, alkalmazni fogja. Azaz otthon is meg fogja tudni védeni a saját adatait, ez pedig rendkívül fontos a felhasználó munkahelyen kívüli élete szempontjából.

Kötelező képzések a fejlettebb szervezeteknél

Ahogy korábban említettem, az oktatás és képzés nem egyenlő feltétlenül a tudatosítással. A nagy szervezetek már eljutottak oda – saját jól felfogott érdekük vagy jogszabályi előírások betartása miatt –, hogy biztonsági oktatásokat tartsanak. Vannak olyan biztonsági képzések, amelyeket törvények és jogszabályok írnak elő, például a tűzvédelem, a munkavédelem területén, vagy pénzintézeteknél a pénzmosás megelőzése, illetve a GDPR kapcsán kötelezően oktatandó személyes adatok védelme.

Ezen kívül azonban, ha egy szervezet rendelkezik biztonsági kontrollokkal, vagy azokat egy létező szabvány vagy ajánlás mentén építette fel, akkor ott is megjelennek szabályok, amelyeket a felhasználóknak és egyéb érintett csoportoknak ismerniük kell. Ilyen szabályozó elemek lehetnek az Informatikai Biztonsági Politika (a továbbiakban: IBP), az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ), az internet és levelezőrendszer használatának speciális szabályai (például tiltott műveletek), az adatvédelem szabályai, az adatszivárgás megelőzésre vonatkozó szabályok és kontrollok, illetve a fizikai rendre vonatkozó „tiszta asztal szabályozás" („Clean Desk").

Biztonságtudatosság – Elektronikus Munkavédelmi Oktatás

A biztonságtudatosság nem új keletű dolog. Régen is rájöttek már arra, hogy dolgozzon a dolgozó bármivel, ha azt nem jól használja, akkor vagy a gép, a berendezés megy tönkre, és leáll a termelés, a munkafolyamat, vagy megsérül a dolgozó, ekkor szintén többletköltségek jelentkeznek, mivel őt pótolni kell, ráadásul ugyanúgy megszakadhat a folyamat, ami akár konkrét pénzügyi veszteséget is okozhat.

„A biztonságtudatosság építésének célja olyan ismeretek, gondolkodásmód és viselkedésminták átadása a munkatársak és az ügyfelek részére, amelyek alkalmazásával csökkenteni tudják a maguk és a szervezet kockázati szintjét, a kockázatokból fakadó költségeket és veszteségeket, időben érzékelni tudják a potenciális incidenseket."[12]

Az említett esetek a mai korra is igazak, annyi kiegészítéssel, hogy már nemcsak a fizikai gépek, termelő berendezések kiesése okozhat leállást, hanem az ezeket irányító informatikai rendszerek kiesése is. Mégis furcsa, hogy nincs (akár törvény által előírt) elektronikus munkavédelmi oktatás az olyan munkakörökben dolgozóknak, akik adatokkal, számítógépekkel vagy egyéb informatikai rendszerekkel dolgoznak. Ha ők nem értik, nem ismerik és nem tartják be a szabályokat, az szintén az üzletmenet folytonosságának megszakadását eredményezheti, bevételkieséssel, többletráfordításokkal, sőt személyes adatokat érintő incidensek esetén még nagyon komoly büntetési tételekkel is. (A GDPR megsértésekor legfeljebb 2 vagy 4%-a a cég globális éves forgalmának, vagy legfeljebb 10 vagy 20 millió euró.)

A biztonságtudatosság építésnek egyéb további pozitív hatásai is vannak:

- Biztonságosabb infrastruktúra (például hibák és gyengeségek jelzése);
- Hatékonyabb incidenskezelés, gyorsabb reagálási idők;
- „Egészséges paranoia" kialakulása;
- Magabiztosabb munkavállalók, hatékonyabb munkavégzés;
- Kockázatalapú gondolkodás;
- Elégedettebb ügyfelek, kevesebb üzletmenet-folytonossági incidens;
- Biztonsági területek elfogadottságának növekedése – jobb együttműködés.

IT-biztonság közérthetően

A Neumann János Számítógép-tudományi Társaság hosszú évek óta törekszik rá, hogy a magyar lakosság és minden számítógépet használó birtokában legyen a megfelelő informatikai tudásnak. A társaság egyik fontos tevékenysége a European Computer Driving Licence – Európai Számítógép-használói Jogosítvány (a továbbiakban: ECDL) rendszer működtetése és koordinálása.

Az ECDL (Európán kívül ICDL, vagyis International Computer Driving Licence) az informatikai írástudás nemzetközileg egységes bizonyítványa. A program nemzetközi irányítását az ECDL Alapítvány végzi, amelyet a CEPIS (Council of European Professional

[12] Solymos Ákos (2017): Szervezeten belüli incidenskezelési gyakorlatok szervezése. In *Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*. „Incidensmenedzsment", VII. fejezet. Budapest, Nemzeti Közszolgálati Egyetem

Informatics Societies) hozott létre 1996-ban, a finn számítógép-használói jogosítvány továbbfejlesztése, az informatikai írástudás nemzetközi szabványának terjesztése céljából.

2013-tól érhető ez az IT-biztonság modul is, mint szabadon választható vizsgamodul. 2017-ben a Neumann Társaság kiadott egy ingyenesen letölthető elektronikus könyvet, amely tartalmazza mindazon ismereteket, amelyeket manapság egy felhasználónak információvédelem kapcsán tudnia kell. Ez az elektronikus könyv, túl azon, hogy bárki számára hasznos, gyakorlati ismereteket ad át, egyben az előbb említett ECDL IT-biztonság modul tankönyve is. A könyv megírásában társszerzőként vettem részt, Erdős Máté Péterrel közösen.

A könyv fő tartalmi elemei:

- Biztonsági alapfogalmak;
- Információrendszerek (hardver, szoftver, hálózat);
- Fenyegetések, támadások;
- Fenyegetettségi és támadási trendek az elmúlt évekből;
- Védelem kialakítása;
- Felhasználók felelőssége biztonsági események során;
- Bizalmasság, sértetlenség, rendelkezésre állás;
- Adatvédelmi megfontolások (GDPR);
- Komplex védelmi megoldások;
- Kibertér és Nemzeti Kibervédelmi Intézet;
- Rosszindulatú szoftverek, egyéb támadások;
- E-mail-fenyegetések és zsarolóvírusok;
- Adathalászat felismerése;
- Mobileszközök védelme;
- Jelszavak kezelése, jelszószéf, egyéb hitelesítés (sms);
- Titkosítási eljárások (háttértárak, irodai programok, levelezés);
- Wifi-routerek biztonságos beállításai;
- Azonnali üzenetküldés;
- Tűzfalak;
- Biztonságos böngészés az interneten (private üzemmódok);
- Közösségi oldalak biztonsága;
- Biztonságos törlés;
- Digitális aláírás;
- Mentési megoldások;
- Biztonságos áramellátás – szünetmentes tápok;
- Végpontvédelem otthonra;
- Biztonságos internet bankolás;
- Biztonságos bankkártya használat – internetes fizetés;
- Internetes zaklatás megelőzése, felismerése, kezelése.

A könyv nemcsak szövegeket, hanem 47 különböző ábrát, fotót, képernyőképet is tartalmaz, amelyek segítenek az olvasottak értelmezésében, megértésében és alkalmazásában.[13]

[13] Erdős Péter Máté – Solymos Ákos (2018): *IT biztonság közérthetően.* Verzió: 3.0. Neumann János Számítógéptudományi Társaság. Elérhető: http://njszt.hu/de/it-biztonsag-kozerthetoen (A letöltés dátuma: 2018. 09. 21.)

Felhasznált irodalom

A Magyar Nemzeti Bank 7/2017. (VII. 5.) számú ajánlása az informatikai rendszer védelméről. Magyar Nemzeti Bank. Elérhető: https://www.mnb.hu/letoltes/7-2017-informatikai-rendsz-ved.pdf (A letöltés dátuma: 2018. 09. 21.)

COBIT 5. Isaca.org. Elérhető: https://www.isaca.org/cobit/pages/default.aspx (A letöltés dátuma: 2018. 09. 21.)

Erdős Péter Máté – Solymos Ákos (2018): *IT biztonság közérthetően.* Verzió: 3.0. Neumann János Számítógép-tudományi Társaság. Elérhető: http://njszt.hu/de/it-biztonsag-kozerthetoen (A letöltés dátuma: 2018. 09. 21.)

Mik a generációk közötti eltérések a közösségi média világában? Hrenko Digital Agency. Elérhető: https://www.hrenko.hu/blog/mik-generaciok-kozotti-elteresek-kozossegi-media-vilagaban/ (A letöltés dátuma: 2018. 09. 21.)

MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági-Irányítási Rendszerek. Követelmények. Lásd részletesebben: Magyar Szabványügyi Testület. Elérhető: http://www.mszt.hu/web/guest/msz-iso-iec-27001 (A letöltés dátuma: 2018. 09. 21.)

NIST Controls. National Institute of Standards and Technology – U. S. Department of Commerce, National Vulnerability Database. Elérhető: https://nvd.nist.gov/800-53 (A letöltés dátuma: 2018. 09. 21.)

Payment Card Industry Data Security Standard (PCI DSS). PCI Security Standards Council. Elérhető: https://www.pcisecuritystandards.org/pci_security/ (A letöltés dátuma: 2018. 09. 21.)

Solymos Ákos (2017): Szervezeten belüli incidenskezelési gyakorlatok szervezése. In Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. „Incidensmenedzsment", VII. fejezet. Budapest, Nemzeti Közszolgálati Egyetem.

TOP 20 Security Controls. CIS – Center for Internet Security. Elérhető: https://learn.cisecurity.org/20-controls-download (A letöltés dátuma: 2018. 09. 21.)

Hivatkozott jogszabályok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (A letöltés dátuma: 2018. 09. 21.)

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.350656 (A letöltés dátuma: 2018. 09. 21.)

Az Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A32016R0679 (A letöltés dátuma: 2019. 09. 21.)

Gombás László[1]

Digitális Armageddon

A hőskortól a mesterséges intelligenciáig

Az alábbiakban áttekintem, hogy az elmúlt tíz év alatt hogyan változott a világ digitális fele, illetve, ha biztonságról beszélünk, pontosan mik is azok, amiket védeni szeretnénk, és mi az, ami fenyegeti őket.

A fejlődést mindig hajtotta és hajtja valami. I. (Hódító) Vilmos normann hercegtől, majd a szigetország meghódítása után immár angol királytól származik az alábbi idézet, ő állítólag a következő szavakkal lelkesítette népét: „Ha bátran harcolsz, győzelem, dicsőség és gazdagság vár reád, másként elpusztítanak, vagy rabként szolgálhatod ki a legkegyetlenebb ellenség szeszélyeit."

Folyamatosan gyorsuló világban élünk; az üzleti vezetők egyre több információt kérnek tőlünk és egyre gyakrabban teszik ezt. Ennek a folyamatnak az eredménye az úgynevezett *big data* jelenség.[2] Napjainkra már senki sem lepődik meg azon, ha valaki mesterséges intelligenciával támogatott informatikai megoldásokat említ.

Kezdjük a rögtön a mesterséges intelligencia definíciójával. Olyan eszközről beszélünk, illetve kellene beszélnünk, amelynek a képességei megegyeznek az emberével. Érzékeli a környezetét, ugyanúgy gondolkodik, mint mi, valamint problémamegoldásra is képes. Szükségünk is van rá, hiszen egyre több információt gyűjtünk és tárolunk különféle rendszerekben. Vállalati és egyre gyakrabban saját igény is az, hogy 24 órában elérhetőek legyünk.

Rohamosan terjedtek el a ma használt okoseszközök, amelyek többnyire éjszakára sincsenek kikapcsolva – hiszen így mindig el lehet bennünket érni e-mailen vagy telefonon. A lakásunkat és az életünket telerakjuk egyéb, nagyon kellemes és hasznos dologgal, értem ezalatt az Internet of Thingst (a továbbiakban: IoT)[3] és hozzá tartozó dolgokat: videó- és zenelejátszó, fájlmegosztó stb. Ez egyébként azért is érdekes, mert egyre több szolgáltatási

---

[1] Gombás László műszaki vezérigazgató-helyettes. Datron Távközlési Zrt.

[2] A *big data* fogalma alatt azt a komplex technológiai környezetet (szoftvert, hardvert, hálózati modelleket) értjük, amely lehetővé teszi olyan adatállományok feldolgozását, amelyek annyira nagy méretűek és annyira komplexek, hogy feldolgozásuk a meglévő adatbázis-menedzsment eszközökkel jelentős nehézségekbe ütközik. Leegyszerűsítve: a *big data,* mint fogalom a nagyon nagy mennyiségű, nagy sebességgel változó és nagyon változatos adatok feldolgozásáról szól.

[3] A dolgok internete (angolul: Internet of Things, rövidítve: IoT) olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internet alapú hálózaton egy másik eszközzel kommunikálni. A fogalom más szavakkal hálózatba kötött „intelligens" eszközöket takar.

igény van. Ezeket az eszközöket legjobban az informatikai felhő szolgálja ki, hiszen az bárhol elérhető, könnyen bővíthető, rugalmas, flexibilis, széles hálózati lefedettsége van, tehát ennél jobb teret nem is találhatnánk.

Milyen tendenciák figyelhetők meg a 2006–2016 közötti időszakban az adatkezelés és felhasználás kapcsolatában?

Érdemes megvizsgálni, hogyan változott az adatok felhasználása, elérési és tárolási módja.

2006 végén még a Myspace volt a legdivatosabb és legfontosabb közösségi portál. Méretében a 11. lett volna a rangsorban a „népessége" alapján, ha virtuálisan egy országot képzeltünk volna el.[4] Ma a Facebooknak mintegy 2,2 milliárd aktív felhasználója van – gyakorlatilag ezzel a legnagyobb virtuális ország, megelőzve Kínát, Indiát, a lakosság együttes összlétszáma alapján.

A világ 7,6 milliárd lakosának fele egyébként online elérhető, és egyharmada rendelkezik valamilyen közösségi média oldallal is, amit mobilkészüléken vagy a megszokott internetfelületeken ér el.[5]

2006-ban 1,5 exabyte méretű adatot hoztunk létre digitálisan, ami megegyezik az előző ötezer év emberi információinak a mennyiségével. Ezt az adatot egyébként egy terabiten tudtuk továbbítani másodpercenként.[6]

Napjainkban 2,5 exabyte digitálisan tárolt adatot hozunk létre. A lényeges különbség azonban az, hogy ez a mennyiség egyetlen nap alatt keletkezik. Ezt a napi adatmennyiséget, ha HD-videóként fognánk fel, 90 évig nézhetnénk a televízióban folyamatosan, napi 24 órában.[7]

A 10 évvel ezelőtt elérhető 1 terabyte/szekundum helyett most már 43 terabyte/szekundum sebességgel tudunk kommunikálni.[8]

Összefoglalva: emberi ésszel nehezen felfogható, 250 millió gigabyte mennyiségű adat keletkezik, és ezt kellene valamilyen úton-módon biztonságban tartanunk.

A gyorsuló világ egyben azt is jelenti, hogy olyan iskolák és szakmák jönnek létre, amelyek még nem léteznek. Egy IDC-tanulmány szerint, mire valaki elvégez egy tanfolyamot, gyakorlatilag már mindegy is – az alapok nyilván megmaradnak, de az ott szerzett

---

[4] *The Expanding Digital Universe. A Forecast of Worldwide Information Growth Through 2010* (2007). IDC. Elérhető: www.tobb.org.tr/BilgiHizmetleri/Documents/Raporlar/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf (A letöltés dátuma: 2018. 09. 21.)

[5] *Number of internet users worldwide from 2005 to 2017 (in millions).* Statista.com. Elérhető: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (A letöltés dátuma: 2018. 09. 21.)

[6] Khoso, Mikal (2016): How Much Data is Produced Every Day? Northeastern University.edu. Elérhető: http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/ (A letöltés dátuma: 2018. 09. 21.)

[7] *Digital Data Storage is Undergoing Mind-Boggling Growth.* EETimes.com. Elérhető: http://www.eetimes.com/author.asp?section_id=36&doc_id=1330462&image_number=3 (A letöltés dátuma: 2018. 09. 21.)

[8] Anthony, Sebastian (2014): 43Tbps over a single fiber: World's fastest network would let you download a movie in 0.2 seconds. Extremetech.com. Elérhető: https://www.extremetech.com/computing/187258-43tbps-over-a-single-fiber-worlds-fastest-network-would-let-you-download-a-movie-in-0-2-milliseconds (A letöltés dátuma: 2018. 09. 21.)

információkat fel kell frissíteni. A gyerekek olyan iskolába fognak járni, amelyek még nem léteznek, és olyan dolgokat fognak tanulni, amikről még nem is hallottunk.[9]

Utánanéztem, hogy milyen munkakörök várhatóak a jövőben, és igen érdekeseket találtam egyes futurológusok előrejelzésében. Három területet ragadtam ki: a pénzintézetet, az autógyártást és az informatikát. Érdekes lesz majd egy banki beszélgetés, ügyintézés során például kriptovaluta-bankárral találkozni, vagy lopáshelyreállító specialistával, aki a digitális valutámat fogja helyreállítani. Az autógyártás területén a „vezető nélküli vezetés" élménytervező mérnök vagy a „vezető nélküli autó operációsrendszer" fejlesztő mérnök szintén érdekes új munkakör. Az IT-területen a drónüzemeltető, illetőleg a digitális lakatos megint csak különlegesnek tűnik.[10]

Hogy jobban megértsük, mennyi adatok kezelünk, a Google statisztikáit érdemes tanulmányozni. A Google adatai alapján hatvanezerszer keresünk rá valamire, hetvenezer YouTube videót tekintünk meg, hétezer *tweet*et küldünk el, és nyolcszáz fotót osztunk meg az Instagramon; összesen közel 50 gigabyte digitális forgalmat generálva – másodpercenként.[11]

Ugyan az internet segítségével minden mindennel össze van kötve, mégsem olyan szép ez a szép új világunk. Ezt a mennyiségű adatot vírusok, különböző intelligens eszközök és hackerek támadják, óriási adatszivárgásokat okozva.

A sötét oldal is fejlődik

Annak idején az úgynevezett „albán vírus" nevű vírusparódia még humorosnak hatott, amikor a következő üzenettel jelentkezett be: „Üdvözlöm! Én egy albán vírus vagyok, de az országom technológiai lemaradottsága miatt sajnos nem tudok kárt okozni az ön gépében. Ezért kérem, hogy legyen szíves törölni egy fontos állományát, majd továbbküldeni engem más felhasználók részére. Köszönöm az együttműködését! Üdvözlettel: albán vírus."[12]

A másik kedvencem, amit még szegény édesanyám is mindig emleget: „fiam, addig piszkálod ezeket a vírusos számológépeket, amíg te is megbetegszel." Olyan újságcikk is megjelent régen, ami azt igazolja, hogy ez valós félelem volt annak idején.

Akik velem egykorúak, emlékeznek még egy alapműre: Kis János és Szegedi Imre tollából a *Vírushatározó* című könyvre,[13] ami akkor még név szerint felsorolta a vírusokat. Napjainkra a vírusok száma elérte a 430 milliót – most elég nagy könyvet kellene készíteni!

Mikor kerülhet bele valami egy vírusadatbázisba? Egy antivírus gyártó mikor mondhatja, hogy egy adott program vírus? Mi van akkor, ha van felhasználói interakció? Én, mint felhasználó, például telepítem ezt a vírust, tudok telefonszámos segítséget kérni az

---

[9] *The Expanding Digital Universe* 2007

[10] *Futurist Thomas Frey on „162 Future Jobs: Preparing for Jobs that Don't Yet Exist".* YouTube.com. Elérhető: https://www.youtube.com/watch?v=QxiiDFdZkm8 (A letöltés dátuma: 2018. 09. 21.)

[11] Liberatore, Stacy (2016): What happens in an internet second: 54,907 Google searches, 7,252 tweets, 125,406 YouTube video views and 2,501,018 emails sent. DailyMail.co.uk. Elérhető: http://www.dailymail.co.uk/sciencetech/article-3662925/What-happens-internet-second-54-907-Google-searches-7-252-tweets-125-406-YouTube-video-views-2-501-018-e-mails-sent.html (A letöltés dátuma: 2018. 09. 21.)

[12] *Albanian virus.* Imgur.com. Elérhető: https://imgur.com/gallery/4N2T6eq (A letöltés dátuma: 2018. 09. 21.)

[13] Kis János – Szegedi Imre (1992): *Vírushatározó.* Cédrus Kiadó Kft. Elérhető: http://mek.oszk.hu/07300/07366/07366.pdf (A letöltés dátuma: 2018. 09. 21.)

alkotójától, stb. Ezt a gyakorlatban is kipróbáltam a Fliporával, spanyol számon tudtam magyarul segítséget kérni a fejlesztőjétől az eltávolításhoz. Jogi határon táncolunk, ezért van az, hogy időnként jönnek olyan kellemetlen érzések, hogy az adott programot ugyan el kellene távolítani egy víruskeresőnek, de mégsem sikerül megvalósítani.

Ha elindulunk az 1990-es évektől, akkor mindig volt egy „aha" érzésünk. Elindultunk onnan, hogy szekvenciális víruskeresés, ezután megtanultuk azt, hogy a vírusok tudnak polimorfok lenni, vagyis nem biztos, hogy karaktersorozat alapján meg tudjuk őket találni.

Elterjedtek az Office típusú dokumentumok, jöttek a makróvírusok, és lám, egy dokumentum is tud kárt okozni már. A CIH-vírus kapcsán tanultuk meg, hogy tönkre lehet tenni vele egy számítógépet fizikailag is.

Eljutottunk a metamorf *multi-homed* vírusokhoz, ami azt jelenti, hogy olyan vírust készíthetnek, ami működik például Windows operációs rendszeren, de mobiltelefonon is van párja. A SCADA-rendszereket támadó vírusoktól a zsarolóvírusokig jutottunk el, és a fejlődés jelen pillanatban is tart.

Egyre intelligensebbek a vírusok és támadási formák is, erre bizonyíték az úgynevezett Watering hole attack, a FrancoPhoning, a Human error.

Hova vezet ez az egész? Óriási adatszivárgásokról szóló cikkek jelentek meg a sajtóban. Alapvetően üzleti és személyes információk szivárognak ki, és az esetek többségében hackertámadások következtében történik mindez. A Smart City, Smart Grid, Smart Home programok további tízmillió eszköznek a bekötését eredményezik, amelyek több petabyte új adatot hoznak elő, a maguk problémáival együtt.

Merre megyünk tovább, mit hoz a jövő?

Az IDC elemzése gyakorlatilag azt mondja, hogy 2020-ra át kell menni egy digitális transzformáción ahhoz, hogy egy vállalkozás nyereséges legyen. Az IDC megfogalmazott egy úgynevezett 3rd Platformot, ami a digitális termékek, szolgáltatások és a kapcsolódó ismeretek halmaza.

A szolgáltatások 67%-a Cloud (felhő) alapúvá fog alakulni, a cégek 30%-a pedig valamilyen VR (virtuális valóság) technológiát fog használni.

2020-ra várhatóan az egészségkutatók egyharmada fog olyan alkalmazást vagy szoftvert fejleszteni, ami az emberi testben fog működni, szorosan integrálódva azzal.[14]

[14] Press, Gil (2016): Top 10 Tech Predictions For 2017 From IDC. Forbes.com. Elérhető: https://www.forbes.com/sites/gilpress/2016/11/01/top-10-tech-predictions-for-2017-from-idc/#5bc0671a4aad

Felhasznált irodalom

Albanian virus. Imgur.com. Elérhető: https://imgur.com/gallery/4N2T6eq (A letöltés dátuma: 2018. 09. 21.)

Anthony, Sebastian (2014): 43Tbps over a single fiber: World's fastest network would let you download a movie in 0.2 seconds. Extremetech.com. Elérhető: https://www.extremetech.com/computing/187258-43tbps-over-a-single-fiber-worlds-fastest-network-would-let-you-download-a-movie-in-0-2-milliseconds (A letöltés dátuma: 2018. 09. 21.)

Digital Data Storage is Undergoing Mind-Boggling Growth. EETimes.com. Elérhető: http://www.eetimes.com/author.asp?section_id=36&doc_id=1330462&image_number=3 (A letöltés dátuma: 2018. 09. 21.)

Futurist Thomas Frey on „162 Future Jobs: Preparing for Jobs that Don't Yet Exist". YouTube.com. Elérhető: https://www.youtube.com/watch?v=QxiiDFdZkm8 (A letöltés dátuma: 2018. 09. 21.)

Khoso, Mikal (2016): How Much Data is Produced Every Day? Northeastern University.edu. Elérhető: http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/ (A letöltés dátuma: 2018. 09. 21.)

Kis János – Szegedi Imre (1992): *Vírushatározó.* Cédrus Kiadó Kft. Elérhető: http://mek.oszk.hu/07300/07366/07366.pdf (A letöltés dátuma: 2018. 09. 21.)

Liberatore, Stacy (2016): What happens in an internet second: 54,907 Google searches, 7,252 tweets, 125,406 YouTube video views and 2,501,018 emails sent. DailyMail.co.uk. Elérhető: http://www.dailymail.co.uk/sciencetech/article-3662925/What-happens-internet-second-54-907-Google-searches-7-252-tweets-125-406-YouTube-video-views-2-501-018-e-mails-sent.html (A letöltés dátuma: 2018. 09. 21.)

Number of internet users worldwide from 2005 to 2017 (in millions). Statista.com. Elérhető: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (A letöltés dátuma: 2018. 09. 21.)

Press, Gil (2016): Top 10 Tech Predictions For 2017 From IDC. Forbes.com. Elérhető: https://www.forbes.com/sites/gilpress/2016/11/01/top-10-tech-predictions-for-2017-from-idc/#5bc0671a4aad

The Expanding Digital Universe. A Forecast of Worldwide Information Growth Through 2010 (2007). IDC. Elérhető: www.tobb.org.tr/BilgiHizmetleri/Documents/Raporlar/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf (A letöltés dátuma: 2018. 09. 21.)

Kökényesi-Bartos Attila[1]

A Számítógépes Bűnözéssel Foglalkozó Ügyészi Hálózat

A hálózat megalakulása

2014. évben a Fővárosi Főügyészség saját szervezetén belül hálózatot hozott létre az információs rendszerekkel elkövetett bűncselekmények növekvő száma miatt. A hálózatban a kerületi ügyészségek, valamint a főügyészség érintett szervezeti egységeinek egy-egy képviselője vett részt, akik az egyes ügyekben felmerülő, informatikai jellegű problémákat saját levelezőlistán vitatták meg egymással, és havonta szervezett képzéseken bővítették rálátásukat az informatikai kérdésekre.

Az Európai Unió GENVAL elnevezésű, a tagállamok értékelésére bevezetett rendszerében a 7. körös értékelés minden tagállamot a kiberbűnözéssel szembeni felkészültség szempontjából mérte fel. Ennek során Magyarországon is értékelő látogatást tett egy szakértői csoport, amelyet egy kérdéssor kitöltése előzött meg. Ezzel összefüggésben országos szintű, több szervezetet érintő egyeztetések folytak a kérdéssor pontos megválaszolása érdekében.

Ezeken az egyeztetéseken a Belügyminisztérium meghívására az ügyészség képviselői is részt vettek. Ezzel párhuzamosan, még a szakértői csoport látogatása előtt, felmerült az igény arra, hogy a Fővárosi Főügyészség által létrehozott és hatékonyan működő hálózathoz hasonló, országos szintű hálózat jöjjön létre.

A legfőbb ügyész az erre vonatkozó előterjesztést 2015 decemberében fogadta el, s ezzel megalakult a Számítógépes Bűnözéssel Foglalkozó Ügyészi Hálózat (a továbbiakban: hálózat). A hálózatot 2016-ban a GENVAL értékelő bizottság rendkívül kedvező fejleményként jelölte meg a látogatását lezáró szóbeli értékelésében. Mindez tovább erősítette azt a meggyőződést, hogy a hálózat hatékonyan támogathatja az ügyészségi munkát.

A hálózat célja

A hálózat célja egy mondatban összefoglalható: informatikusok bevonásával, képzések tartásával és egy adatbázis létrehozásával informatikai támogatást nyújtani az ügyészeknek. A rövid megfogalmazás azonban meglehetősen széles tevékenységet ölelhet fel.

---

[1] Dr. Kökényesi-Bartos Attila Legfőbb Ügyészségre kirendelt főügyészségi csoportvezető ügyész. Legfőbb Ügyészség, Informatikai Főosztály

A hálózat felépítése

A hálózat szakmai vezetője a Legfőbb Ügyészség Nyomozás Felügyeleti és Vádelőkészítési Főosztályának képviselője, míg a hálózat informatikai vezetője a Legfőbb Ügyészség Informatikai Főosztályának képviselője.

Mindez biztosítja, hogy az ügyészségnek mind a büntetőjogi szakterületén, mind az információtechnológiával foglalkozó, informatikusokat is felügyelő funkcionális területén dolgozó, szakértelemmel rendelkező képviselői egyenlő mértékben kapnak részt a hálózat munkájából, s így rendelkezésre áll valamennyi ismeret, ami az informatikai környezetben elkövetett bűncselekményekkel kapcsolatos problémák megértéséhez és a hatékony felléphez szükséges.

A hálózat tagjait is ezen elvek alapján jelölték ki. A hálózatban részt vesz:

- 1-1 informatikus valamennyi főügyészségről,
- 1-1 ügyész a megyei főügyészségekről és a Fővárosi Főügyészségről,
- 1 ügyész a Legfőbb Ügyészség Terrorizmus, Pénzmosás és Katonai Ügyek Főosztályáról,
- 1 ügyész a Legfőbb Ügyészség Büntetőbírósági Ügyek Főosztályáról,
- 1 ügyész a Legfőbb Ügyészség Gyermek- és Fiatalkorúak Bűnügyeinek Önálló Osztályáról,
- 1 ügyész a Legfőbb Ügyészség Kiemelt, Korrupciós és Szervezett Bűnözés Elleni Ügyek Főosztályáról.

Az országos hálózat munkájának segítésére a Fővárosi Főügyészség példájához hasonlóan valamennyi megyei főügyészség létrehozta a saját helyi hálózatát, vagy másként oldotta meg azt, hogy az adott főügyészségen működő hálózati tag a szervezeti egység ügyészeinek ügyeiben felmerülő, informatikai hátterű problémákról értesüljön.

A hálózat ismertetett felépítése biztosítja azt, hogy az ügyészség összes érintett szervezeti egységében felmerülő kérdésekre rálátása legyen, s felölelje a büntetőjogi és informatikai terület képviselőit egyaránt.

A hálózat hatóköre

Napjainkban rendkívül elszaporodtak azon bűncselekmények, amelyek a fizikai valóságban is elkövethetőek, de egyben az informatikai környezetben is megvalósulhatnak. Például internetes aukciós oldalakon elkövethető csalás vagy internetes fórumokon zaklatás.

Az ezen bűncselekmények elleni hatékony büntetőjogi fellépéshez is szükségesek a technikai ismeretek, amelyek segítségével megérthető az elkövetői magatartás, megállapítható, hogy milyen új bizonyítékok honnan és hogyan szerezhetők be, miként rögzíthetők, s később hogyan értelmezhetők más bizonyítékokkal együtt.

A fentiek miatt a hálózat által biztosítandó informatikai ismeretek rendkívül széles körben lehetnek szükségesek. Ezért a hálózat tevékenységi körének, azaz hatókörének meghatározása szándékosan szélesre szabott, az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye szerint kiberbűncselekménynek

minősülő cselekményeken túl a további, informatikai környezetben jellemzően elkövetett cselekmények köre is beletartozik.

Pontos hatókörébe beletartozik valamennyi, a Büntető Törvénykönyvről szóló 2012. évi C. törvény szerinti bűncselekmény, amely informatikai környezetben is megvalósulhat, illetve megvalósul a gyakorlatban. Ezt a hatókört folyamatosan felül is vizsgálják a gyűjtött statisztikai adatok és tapasztalatok alapján.

A sorozatban elkövetett cselekmények kezelése

Három példán keresztül szeretném bemutatni a hálózat működésének előnyeit.

Az első a több sértettet érintő, sorozatban elkövetett cselekmények köre, amely cselekmények az internet, illetve informatikai eszközök segítségével sokkal könnyebben valósíthatók meg tömegesen.

A hálózat intézkedési terve az eddigi években kiemelten foglalkozott ezzel a problémával, mivel az informatikai eszközökkel a bűncselekmények nemcsak nagyobb számban követhetők el, hanem egy adott földrajzi területhez is kevésbé kötődnek. Egy elkövető ugyanazon cselekményével megkárosíthat az ország valamennyi szegletében élő sértetteket.

A sértettek jellemzően a saját lakhelyükhöz közel eső hatóságoknál tesznek feljelentést. Ezzel az ország területén szétszóródó, egymástól elkülönülő eljárások kezdődnek, ami erőforrás-pazarlást jelent. Az elkövető kilétének azonosítása érdekében a hatóságok az érintett szolgáltatókat egyesével mind megkeresik a közel azonos adatok beszerzése érdekében. Emellett a bizonyítékok szétaprózódnak a külön zajló eljárásoknál, ami csökkenti az eredményes eljárások esélyét.

Az ismertetett probléma felismerése óta a hálózat igyekszik olyan megoldásokat találni, amelyekkel felismerhetők és egyesíthetők az együtt hatékonyan kezelhető, egy elkövetőhöz tartozó ügyek. Erre jelentett egyfajta megoldást az, hogy a hálózaton belüli információcsere valamennyi szervezeti egységre kiterjed.

Jó példa erre azon eset, amikor a hálózati tagok között jogi minősítési kérdésben indult informális tapasztalatcsere a mobiltelefonok egyenlegének feltöltése kapcsán észlelt csalásokról. Ennek során megállapítást nyert a visszajelzésekből, hogy a hasonló cselekmények több esetben büntetés-végrehajtási intézetekben található telefonokhoz köthetők, amivel több rendőr-főkapitányság kiemelten foglalkozott. Ezt követően lehetőség nyílt annak vizsgálatára, hogy mely ügyek egyesítése célszerű, illetve az ügyészek közösen figyelemmel kísérhették a nyomozó hatóság erre irányuló lépéseit is.

Egy másik esetben pénzintézetek által kibocsátott készpénz-helyettesítő fizetési eszközökkel való visszaélés miatti eljárásokban derült fény arra, hogy egy bizonyos pénzintézettől érkező feljelentések száma kimagasló valamennyi főügyészségen, s az eljárások rendszerint eredménytelenek. Ennek oka az ügyek együtt kezelésével szintén könnyebben felderíthető volt.

A nemzetközi együttműködés előkészítése

A magyar elkövetőkhöz köthető és nemzetközi kapcsolatok nélkül is eredményesen felderíthető cselekményeken túl létezik több olyan bűncselekmény is, ami nemzetközi hatással jár.

2017. évben például robbanásszerűen elterjedt a WannaCryptor (WannaCry) zsarolóvírus, ami öt nap alatt hozzávetőlegesen 300 ezer sértettet érintett 150 országban, s már a kezdetekben 27 nyelven elérhető szöveggel követelte a sértettektől egy bizonyos összeg megfizetését a vírus által titkosított adatok titkosításának feloldásáért cserébe.

Az ilyen jellegű cselekményekkel szembeni fellépés nemzeti szinten közel lehetetlen feladat, és a célzott, más ország felé irányuló jogsegély megkeresésekkel sem lehet könnyen előbbre jutni, hiszen nem ismert, hogy hol indult eljárás, ki milyen ismeretekkel rendelkezik, és hol találhatóak érdemi bizonyítékok.

Ennek megoldásában segíthet az Eurojust, amelynek feladata a hasonló ügyekben a koordináció támogatása, szükség szerint közös nyomozócsoportok alakításával, koordinációs értekezletek szervezésével.

Az Eurojust ezen tevékenységet egészíti ki a European Judicial Cybercrime Network (a továbbiakban: EJCN). Ezen szervezet a magyar hálózathoz hasonló felépítésű, azonban az Európai Unió tagállamaiból kerülnek ki a tagjai, így ezen a szinten teszi lehetővé az informális egyeztetést.

Az EJCN-nek tagja a magyar ügyészség képviselője is, amivel a magyar hálózat szervesen kapcsolódik az EJCN munkájához. Ezzel akár egy helyi ügyészség felügyelete alatt folyó ügyben felmerülő informális kérdésben is felmérhető, hogy mely európai uniós tagállamnál várható érdemi segítség jogsegély megkeresés esetén, illetve hasonló ügyekben hol, milyen tapasztalattal, milyen hatékony módszerekkel rendelkeznek. Ez elősegítheti a jogsegély megkeresések sikerességét, valamint az Eurojust munkáját is.

Zsarolóvírusok esetében a hálózat informális csatornáin feltett kérdésekkel napok, esetenként órák alatt ellenőrizhető volt, hogy hány ügy indult magyar sértettek feljelentései alapján a kérdéshez kapcsolódó cselekménnyel összefüggésben, így Magyarország mennyiben érintett a WannaCryptor zsarolóvírus fertőzésében. Ez az információ az EJCN-en keresztül valamennyi EU-tagállamból beszerezhető volt, ami rálátást biztosított az Eurojustnak arra, hogy szükséges-e koordinációs értekezlet összehívása, s azon mely tagállam részvétele indokolt.

Az informatikai technológiai kérdések tisztázása

A hálózat harmadik kiemelendő előnye a bonyolult informatikai technológiai kérdések megfejtésére vonatkozik.

Erre jó példa a Darknet esete. A Darknet az internet olyan része, ami csak speciális alkalmazással érhető el, a megszokott internetes keresőalkalmazásokkal nem mutatható ki, program hiányában még a pontos darknetes címek beírásával sem.

A Darknet eléréséhez használható alkalmazás (The Onion Router, azaz TOR) az üzeneteket háromszoros titkosítással látja el, és három különböző állomáson keresztül küldi el.

Ezek az állomások a titkosítások feloldásához szükséges kulcsok közül csak egyet-egyet ismernek. Ez biztosítja, hogy sem a címzett, sem az adatot továbbító rendszerek nem ismerik egyszerre az adatot küldő számítógép elérhetőségét és a küldemény tartalmát.

Az anonimitás előnyeit a bűnözők is hamar felismerték, és a Darkneten hoztak létre olyan piactereket, amelyeken jogsértő szolgáltatásaikat, termékeiket megvásárlásra felajánlják.

Annak megértése, hogy egy ilyen környezetben hogyan lehetséges az elkövetők kilétének azonosítása, s az elkövetés felderítése, értelemszerűen mélyebb informatikai ismereteket igényel. Ezen a területen az eredményes fellépéshez rendkívül fontos a bevált, hatékony gyakorlati megoldások megosztása.

Erre szintén lehetőséget nyújt a hálózat a keretein belül megvalósított tudásbázissal. Ez az ügyészségi belső hálózaton elhelyezett oldal keresést tesz lehetővé a feltöltött dokumentumok tartalmában, amivel a nagy adatmennyiségtől függetlenül a releváns információ mindenki számára könnyen és gyorsan elérhető.

A tudásbázisba folyamatosan számos dokumentumot töltenek fel:

- hazai/nemzetközi képzések előadásait,
- úti jelentéseket kiküldetésekről,
- ügyészségi állásfoglalásokat,
- releváns híreket, hírösszefoglalókat,
- szakkifejezéseket, útmutatókat informatikai környezetben elkövetett bűncselekményekhez,
- statisztikákat, az Országos Kriminológiai Intézet kutatási eredményeit,
- bírósági határozatokat,
- képzési információkat, anyagokat (Europol, International Association of Prosecutors – Global Prosecutors E-crime Network, Central European Police College, EU Intellectual Property Office és más szervezetek oktatóanyagait, kiadványait).

A tudásbázishoz saját belső útmutatóit, gyakorlati anyagait a Nemzeti Adó- és Vámhivatal, a Budapesti Rendőr-főkapitányság és a Nemzeti Nyomozó Iroda ezen területtel foglalkozó szervezeti egysége is rendelkezésre bocsátotta. Ezen szervezetektől saját kapcsolattartót is kijelöltek a hálózattal való együttműködésre, s meghívás alapján résztvevőként vagy előadóként közreműködnek a hálózat rendezvényein.

A rendezvényekre rajtuk kívül az Országos Bírói Hivatalon keresztül bírák is meghívást kapnak annak érdekében, hogy a felmerülő informatikai kérdésekről szintén értesüljenek.

Összefoglalva elmondható, hogy a hálózat hatékonyan támogatja az ügyészi tevékenységet az informatikai környezetben elkövetett bűncselekmények vonatkozásában.

Kollár Csaba[1]

Mutatószámok a szervezetek életében, különösen az információbiztonság területén

Bevezetés

A rendszerelvű vállalati/szervezeti működésben,[2] az üzem- és gyártásszervezésben, a vállalati/szervezeti (munka)folyamatok megvalósításában és ellenőrzésében nem ismeretlen a mérés, s így a különféle mutatószámok alkalmazása sem. Maynard több mint negyven évvel ezelőtt szerkesztett, gazdasági mérnököknek szóló könyvének fókuszában is a mérés áll, több fejezetben foglalkozik többek között a mérési eljárásokkal, illetve a mérési módszerek alkalmazásával.[3] A méréstechnika fontosságát a Czichos által szerkesztett, mérnöki tudományokkal foglalkozó könyv is kiemeli, s a H fejezetben részletesen szól egyebek mellett a mérőrendszerekről és mérőláncokról, a mérőtagok átviteli tulajdonságairól, a mérési hibákról, a mérési jel feldolgozásáról, a szenzorokról, a digitális méréstechnikáról.[4]

Természetesen nevezett szerzők mellett megannyi méréssel kapcsolatos könyv született a műszaki és a gazdasági területen egyaránt, amelyeknél a matematikai és mérési módszerek és eljárások fejlődése újabb ismeretekkel gazdagította a téma iránt érdeklődő szakembereket. Logikusnak tűnhetne, hogy a biztonság, s azon belül az informatikai és információbiztonság szintén azok közé a területek közé tartozik, amelyeknél egy jól kidolgozott és kiforrott, a gyakorlatban számos esetben ellenőrzött és kipróbált mérési rendszert (vagy akár több mérési rendszert is) lehetne használni a hálózati és végponti elemek, eszközök, berendezések stb. működésének, illetve a működésükkel kapcsolatos biztonsági kritériumok, valamint a rajtuk feldolgozásra kerülő adatok és információk biztonságának monitorozására, valamint a mért adatok feldolgozására, kielemzésére, és szükség szerint a beavatkozásra. Sajnos rendszerint ez nem így van. Ez azért is meglepő, mivel a vállalati, szervezeti, üzemi folyamatok jelentős részét a vállalatirányítási információs rendszerek (ERP) működtetik,[5] az ügyfélkapcsolatok kezelésében megannyi hatékony CRM-megoldás

---

[1] Dr. Kollár Csaba PhD, doktorandusz, belügyminisztériumi gyakornok. Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] Kollár Csaba (2017): A szervezeti információbiztonsági folyamatok monitorozása és a vezetői döntések támogatása kulcs teljesítménymutatók segítségével. I. rész – Az információbiztonság rendszerelméleti megközelítése. *Szakmai Szemle,* XV. évf. 4. sz. 43–56.

[3] Maynard, Harold B. ed. (1977): *Gazdasági mérnöki kézikönyv.* Budapest, Műszaki Könyvkiadó.

[4] Czichos, Horst ed. (1993): *HÜTTE: A mérnöki tudományok kézikönyve.* Budapest, Springer Hungarica.

[5] Hetyei József szerk. (2004): *ERP rendszerek Magyarországon a 21. században.* Budapest, Computer Books.

áll rendelkezésre,[6] s olyan fogalmak jelennek meg a szakirodalomban, mint az adatbázisok, adattárházak, adatbányászat, adatvédelem, titkosítás. Az elkövetkező néhány évben a szervezetek a versenyképességük megőrzése érdekében komoly beruházásokat hajtanak végre, és a termelési-gyártási folyamataikat már az Ipar 4.0 elvárásai szerint alakítják át.[7] Az Innomine Group által idézett IVSZ definíciója szerint az Ipar 4.0 „magában foglal számos új keletű automatizálási, adatátviteli és gyártási technológiát – lefedve minden olyan innovatív technológiai fogalmat és értékláncot, ami az ipari termelést kiberfizikai rendszerek, szenzoros hálózatok, mobilkommunikáció és online/felhő szolgáltatások segítségével újítja meg".[8]

Hiba lenne azt állítani, hogy ez a fejlődés csak a profitorientált szervezeteket érinti, hiszen a közigazgatás „elektronizálódásának" jogi keretét több törvény és rendelet is megadja, mint például az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet, az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI. 13.) Korm. rendelet, az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet. Adott tehát a szervezeti/üzleti érdek (profit, hosszú távú eredményes működés, elégedett vásárlók stb.), valamint a törekvés a közigazgatás elektronikus-informatikai folyamatainak a fejlesztésére. Ami egyelőre hiányzik, az a biztonsági és kiemelten az adat-, információ- és informatikai biztonság kulcsmutatószámainak és -indexeinek a kidolgozott és egységes módszertana, noha a mutatószámokról szóló részben olyan, több éve elkészített anyagokra is hivatkozom, amelyek kiválóan megalapozzák a témát.

Jelen tanulmány – ha nem is vállalkozik a kötött és korlátozott keretben a módszertan teljes és részletes bemutatására, de – segítséget kíván adni a területen dolgozó magyar szakembereknek a teljesítménymutatóban (Key Performance Indicator, a továbbiakban: KPI) rejlő lehetőségek megismeréséhez.

---

[6] Payne, Adrian (2006): *CRM kézkönyv. Ügyfélkezelés felsőfokon.* Budapest, HVG Könyvek.

[7] Gilchrist, Alasdair (2016): *Industry 4.0. The industrial internet of things.* New York, Apress.

[8] *IPAR 4.0 – Fogalomtár, fontosabb tanulmányok, legfőbb szereplők* (2016). Budapest, Innomine Group.

A fontosabb mutatószámok áttekintése

Írásom jelen részében összefoglalom Schliemann és Mishra,[9] Khanduja,[10] Glen,[11] De Lutiis,[12] Baroudi,[13] Parmenter,[14] Aiello,[15] Wanick,[16] Huwyler,[17] Bharadwaj,[18] valamint Hubbard és Seiersen[19] írásai, előadásai alapján, hogy melyek azok a 3-4 betűs mozaikszavak, amelyek már megjelentek a gazdasági területen és néhányuk az informatika területén is.

A leggyakrabban használt mutatószámfajta a *KPI,* amelynek célja, hogy magas szintű áttekintést nyújtson a szervezet és főbb operatív egységeinek múltbéli teljesítményéről, szinte kizárólag a történelmi adatokra irányulva. Ezek a történelmi adatok rendszerint az informatikai rendszert (beleértve az adatbázisokat és az adattárházat is) monitorozó/felügyelő alkalmazások által rögzített naplóbejegyzésekben találhatóak meg nyers formában (a bejegyzésekből manuálisan kell kigyűjteni), vagy az alkalmazás feldolgozza könnyebben érthető riport formájában és/vagy infografika (adatvizualizáció) segítségével ismerteti meg a szakemberekkel a rendszerállapotokat.

A kockázatokkal foglalkozik a *KRI* (Key Risk Indicator, a továbbiakban: KRI), amely olyan kockázati mutatókat foglal magában, amelyek a vállalat különböző területein a fokozott kockázati kitettség korai figyelmeztető jelzéseire szolgálnak. A KRI-k segítik azonosítani azokat a kulcsfontosságú területeket, ahol (1) komolyabb ellenőrzésre, (2) az ellenőrzési protokoll újragondolására, vagy (3) (új) piaci lehetőségek feltárására van szükség. Megalkotásuk célja, hogy hasznos információt nyújtsanak a lehetséges rövid, közép-, illetve hosszú távú vállalati teljesítményt befolyásoló várható kockázatokról. A szervezetek életében számos kockázattal lehet számolni, úgymint:

- biztonsági kockázatok,
- csalás vagy korrupció kockázata,
- geopolitikai kockázatok,

---

[9] Schliemann, Maximo Neira – Mishra, Ravi (2012): *Establishing Key Risk Indicators for IT.* Metricstream, s.l.

[10] Khanduja, Meetu (2012): Key Result Area (KRA) and Key Performance Area (KPA). Elérhető: https://hrdictionaryblog.com/2012/12/06/key-result-areakra-and-key-performance-areakpa/ (A letöltés dátuma: 2018. 03. 27.)

[11] Glen, Bruce (2006): You Can't Manage It If You Can't Measure It. ISACA konferenciaelőadás.

[12] De Lutiis, Paolo (2014): Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection. ETSI konferenciaelőadás.

[13] Baroudi, Rachad (2011): *KPI Mega Library 2010 – 17.000 key performance indicator.* Scotts Valey, Rachad Baroudi.

[14] Parmenter, David (2010): *Key performance indicators. Developing, implementing, and using winning KPIs.* New Jersey, John Wiley & Sons.

[15] Aiello, Steven (2017): IT Security KPIs: 4 Effective Measurements for your Organization. Elérhető: https://www.thinkahead.com/blog/security-kpis-4-effective-measurements-organization-pt-1/ (A letöltés dátuma: 2018. 03. 27.)

[16] Wanick, Brit (2017): KPI v. KRI v. KCI: Key Cyber Security Indicators. Elérhető: https://www.fourv.com/blog/kpi-v.-kri-v.-kci-key-cyber-security-indicators (A letöltés dátuma: 2017. 11. 02.)

[17] Huwyler, Herman (2018): Key Indicators: KPIs, KRIs, KCIs and KLIs. Elérhető: http://mydailyexecutive.blogspot.hu/2011/06/key-indicators-kpis-kris-kcis-and-klis.html (A letöltés dátuma: 2018. 03. 27.)

[18] Bharadwaj, Maninder (2011): Measuring The Value of Information Security. Deloitte oktatási anyag. Elérhető: http://isacabangalore.org/isacabc/main/media/downloads/2011conf/23measuringvalue.pdf (A letöltés dátuma: 2018. 03. 27.)

[19] Hubbard, W. Douglas – Seiersen, Richard (2016): *How to measure anything in cybersecurity risk.* New Jersey, Wiley & Sons.

- jelentési kockázatok,
- piac dinamikájával kapcsolatos kockázatok,
- reputációs kockázatok,
- szabályozási megfelelés kockázata,
- szerződésekkel kapcsolatos kockázatok,
- üzleti megszakítási kockázatok,
- versenytársakkal kapcsolatos kockázatok.

Jenei úgy véli, hogy „a sikeres vállalati kockázatkezelés alapja, hogy a vállalat a működéséből adódó kockázatokat jól felismeri-e, és hatékonyan tudja-e kezelni".[20] Írásművében négy modellt ismertet: (1) ERM keretrendszer, (2) ISO 31000:2009 szabvány, (3) M_o_R (Management of Risk) modell és (4) GRC (Governance, Risk Management, and Compliance – irányítás, kockázatkezelés, megfelelés) modell, és megállapítja, hogy ezekben az alábbi lépések azonosak:

- kockázatazonosítás,
- kockázatértékelés és -elemzés,
- kockázatok kezelése,
- kockázatok felülvizsgálata, megfigyelése.

Véleményem szerint a KRI-k megalkotása, bevezetése és használata támogatja az említett modellek hatékonyságának és eredményességének a növelését.

Az információbiztonság területén a KRI-k szerepe abban nyilvánul meg, hogy segítségükkel számszerűen ki lehet fejezni az érzékelőkkel, illetve a mérőpontokon mért fenyegetések és sebezhetőségek súlyosságát. Az eredmények alapján ki lehet jelenteni, hogy a kritikus eszközökkel összefüggésbe hozható biztonsági események nagyobb kockázatot jelentenek, mint a nem kritikusokkal összefüggők. Bharadwaj a KRI-kkel kapcsolatban úgy fogalmaz, hogy a KRI „egy vagy több KPX összefoglalója vagy korrelációja, amely jelzést ad az információbiztonsági program egészének alapvető kockázatáról".[21] Az információbiztonság területén általában négy KRI-t különböztetünk meg: (1) információvédelem, (2) nem megfelelő használat, (3) fenyegetéskezelés, (4) hozzáférés-szabályozás (jogosultságok kezelése).

A kulcsfontosságú eredményt nyújtó területekkel foglalkozik a *KRA* (Key Result Area, a továbbiakban: KRA), amelyik egy előzetesen meghatározott időtartamra vonatkozó várható kimenetelt vagy végeredményt határoz meg. Ha a KRA-t a humánerőforrás-gazdálkodás területén használják, akkor a cél az, hogy meghatározzák a munkavállaló munkakörét, lehetővé tegyék a számára, hogy jobban tisztázza szerepét, feladatát a szervezetben, valamint, hogy összehangolja ezt a szerepet a vállalat által meghatározott szerepével, feladatával. A jól megalkotott KRA-k egyértelműsítik, hogy mit mérnek, elvárás, hogy számszerűsíthetőek legyenek, illetve az is, hogy a mérést viszonylag könnyen lehessen elvégezni. A KRA-k közé sorolják az alábbi felsorolásban szereplő, eredményt nyújtó területeket:

---

[20] Jenei Tünde (2016): Leggyakrabban használt kockázatkezelési modellek összehasonlítása. *International Journal of Engineering and Management Sciences (IJEMS)* Vol. 1. No. 1. Elérhető: https://www.researchgate.net/publication/306042047_Leggyakrabban_hasznalt_kockazatkezelesi_modellek_osszehasonlitasa (A letöltés dátuma: 2018. 09. 21.)

[21] Bharadwaj 2011

- minőségellenőrzés,
- működési költség ellenőrzése,
- nyilvántartás,
- termékmenedzsment,
- vevői elégedettség.

A legfontosabb teljesítményterületek a *KPA*-k (Key Performance Area, a továbbiakban: KPA), amelyeket az adott munkavállalónak (például: az információbiztonsági igazgatóságon dolgozó személynek) teljesítenie kell, illetve amelyekért egyénileg vagy munkacsoportban felelős. KPA-nak tekinthető többek között:

- optimális erőforrás-felhasználás,
- folyamatok fejlesztése,
- biztonsággal és megelőzéssel kapcsolatos tervek elkészítése és megvalósítása, illetve ellenőrzése,
- a vállalati üzletpolitikának való megfelelés.

A kulcs ellenőrző indikátor (*KCI* – Key Control Indicator, a továbbiakban: KCI) azt jelzi, hogy egy vállalat mennyire ellenőrzi a környezetét és annak kockázati szintjét, illetve mennyire hatékonyan működik egy adott kontroll. Az informatikai biztonság területén ilyenek például a NIST Cybersecurity Framework funkcionális területei (azonosítás, védelem, észlelés, válaszolás és visszaállítás). Az alábbiakban a Xactium tanácsadó vállalat KCI-specifikációjára vonatkozó ajánlását[22] mutatom be egy konkrét példán keresztül *(1. táblázat).*

1. táblázat

Az Xactium példája egy KCI specifikációra

KCI neve	a munkavállalói felügyelet gyakorisága				
Leírás	a munkavállalók számára biztosított ellenőrzés mérése				
Kapcsolódó ellenőrzés	munkavállalói felügyelet				
Gyakoriság	havonta				
Üzletág	emberi erőforrás-gazdálkodás				
Mérés 1.	*Név*	*Típus*	*Felső/alsó*	*Küszöb*	*Sárga küszöb*
	az előző havi felügyeletben részesülő alkalmazottak száma (%)	százalék	alsó érték (minden érték <= a küszöbértékhez piros)	70%	80%

Forrás: A szerző szerkesztése a Xactium ajánlása alapján

[22] *Understanding Key Control Indicators & how they can reduce risk* (2018). White paper, Xactium. Elérhető: https://www.xactium.com/download-the-whitepaper-understanding-key-control-indicators-and-how-they-can-reduce-risk (A letöltés dátuma: 2018. 03. 27.)

A legfontosabb teljesítménymutató index (*KPX* – Key Performance Index, a továbbiakban: KPX) egy vagy több KPI összefoglalója vagy korrelációja, amely jelzi a biztonsági program egy meghatározott területének általános teljesítményét.

A legfontosabb teljesítménybiztonsági mutatók (a továbbiakban: *KPSI*-k) az információbiztonsági folyamatok érettségi szintjét mérik (észlelés, észlelési folyamat). Rendszerint öt érettségi szintet lehet megkülönböztetni a CMM (Capability Maturity Model, a továbbiakban: CMM) alapján,[23] amelyet a *2. táblázat* ismertet.

2. táblázat

A szervezetek biztonsági szintjei a CMM érettségi modell szerint

érettségi szint	*képesség*	*eredmény*
0 – nem létező	a képesség hiányzik	nincs
1 – kezdeti/ad-hoc	a szervezet felismerte a biztonsági kultúra fontosságát, de nem tudatosan készíti fel a munkatársakat	megindult a biztonsági kultúra fejlesztése
2 – ismétlődő	a szervezet vezetése elvárja a biztonsági kultúra kialakítását, de nem törekszik tervszerűen rá	törekszenek a jogszabályi megfelelésre
3 – szabályozott	a szervezet létrehozta a biztonsági kultúra fejlesztési programot, de korlátozottak a megvalósítás eszközei	a jogszabályoknak való megfelelés valószínű
4 – menedzselt	eredményes a program megvalósítása, tudatosan részt vesznek benne a felhasználók	a szabályok szerint folyamatosan megfelelő szinten menedzselt
5 – optimalizált	a biztonsági kultúra fejlett, áthatja a szervezetet, és a kultúra fejlesztése beépült a szervezet folyamataiba	mutatószám rendszer segítségével irányított és fejlesztett

Forrás: A szerző szerkesztése Horváth 2013 alapján

A teljesítménybiztonsági mutatószámokkal kapcsolatban az alábbiakban a De Lutiis neve alatt jegyzett[24] ETSI (Európai Távközlési Szabványügyi Intézete, a továbbiakban: ETSI) GS ISI 003 V1.1.2 számú dokumentumban bemutatott KPSI-táblázatot közlöm *(3. táblázat).*

[23] Horváth Gergely Krisztián (2013): *Közérthetően (nem csak) az IT-biztonságról.* Budapest, Kormányzati Informatikai Fejlesztési Ügynökség.

[24] De Lutiis 2014

3. táblázat
KPSI-táblázat

Megnevezés	*Leírás*		
Név	A KPSI teljes neve		
KPSI-index	A KPSI indexszáma abban a mutatószám-gyűjteményben, amelyikben használják		
Ellenőrzési iránymutatások	A kritikus ellenőrzéssel kapcsolatos leírások, javaslatok, iránymutatások		
Leírás, indokoltság	A KPSI részletes leírása, használatának indoklása és területe		
Indikátor meghatározása	Melyek azok a mutatók, illetve mérési adatok, amelyek alapján az adott indikátort meg lehet határozni		
További indikátor meghatározása	További mutatók és mérési adatok, amelyek kapcsolatba hozhatók az adott KPSI-vel		
Az ideális érték	Itt a KPSI-nek azt az értékét kell megadni – amennyiben rendelkezésre áll –, amelyik az ideális állapothoz tartozik		
0. szint	*1. szint*	*2. szint*	*3. szint*
Ez a cella tartalmazza a szervezet érettségi szintjéhez tartozó rövid elvárást az emberek, eszközök és folyamatok tekintetében	1. érettségi szint leírása: alapvető elvárások és megfelelés-orientáltság	2. érettségi szint leírása: érett és integrált	3. érettségi szint leírása: fejlett és üzletorientált

Forrás: A szerző szerkesztése De Lutiis 2014 alapján

Az ismertetett mutatószámok egymáshoz való kapcsolódása

Szinte valamennyi mutatószámnál találhatunk szakmailag is értelmezhető kapcsolódási pontot a többi mutatószámmal. Tanulmányomban Bharadwaj oktatási anyaga alapján ismertetem a KPI, KPX és KRI kapcsolatát.[25] Az *1. ábrán* látható, hogy a kulcsmutatószámok megalkotásának az első lépése az, hogy a mérést elvégezzük annak érdekében, hogy rendelkezésünkre álljanak a szükséges mérőszámok. Az informatikai rendszer működésével és állapotával kapcsolatos mérőszámok – ahogy arra már utaltam – a különböző szoftverek és alkalmazások naplófájljaiban találhatók meg, illetve lehetőség van arra is, hogy a szenzorokkal ellátott Internet of Things intelligens eszközök (a továbbiakban: IoT) (különösen ipari környezetben, illetve okosvárosoknál és okosotthonoknál) segítségével mért adatok jelentsék a kulcsmutatószámok megalkotásának az alapját.

Az alábbiakban megnevezek néhány mérési adatot és mérőszámot az informatikai, adat- és információbiztonság területén.

Mérési adat:

- a hálózat maximális sávszélessége,
- a végpontok védelmét biztosító szoftver- és alkalmazáslicencek száma,
- az ellopott/elveszett eszközök száma,

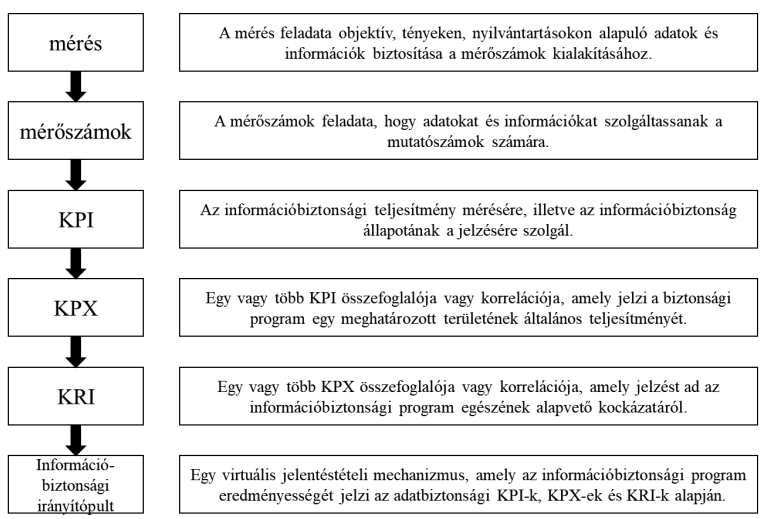
[25] Bharadwaj 2011

- azoknak a (hálózati) eszközöknek a száma, amelyek az informatikai rendszer védelmét biztosítják,
- helyhez kötött (asztali) számítógépek száma,
- laptopok száma,
- vezeték nélküli (okos)telefonok száma.

Mérőszám:

- a biztonsági figyelmeztetések száma adott időben,
- a javítócsomagok száma,
- a kritikus biztonsági figyelmeztetések száma hetente/havonta,
- a kritikus javításra/frissítésre szoruló eszközök száma adott időben,
- a szerverre telepítendő javítások telepítési ideje,
- adott időpillanatban rendelkezésre álló mobileszközök száma,
- adott pillanatban azon mobileszközök száma, amelyek biztonsági védelemmel rendelkeznek,
- az asztali számítógépekre, illetve laptopokra telepítendő javítások telepítési ideje,
- az automatikus frissítést igénylő eszközök száma.

A szakirodalom nem egységes és nem következetes a mérési adatok és a mérőszámok, illetve a KPI-k közötti szétválasztás tekintetében. A Deloitte például a mérőszámok közé sorolja a havi rendszerességgel bejelentett biztonsági események számát vagy a naprakész vírusvédelemmel ellátott informatikai eszközök számát havi bontásban.[26] Véleményem szerint ezek inkább már a KPI-k közé tartoznak, amelyekről a következő részben írok részletesebben.



1. ábra

A KPI, KPX és KRI kapcsolata

Forrás: A szerző szerkesztése

[26] BHARADWAJ 2011

A KPI-k fajtái és típusai

A szakirodalom a KPI-fajták, illetve KPI-típusok tekintetében sem egységes, Wilsey például a logikai modell alapján négyféle típust különböztet meg, úgymint: (1) bemeneti, (2) folyamat, (3) kimeneti és (4) eredmény.[27] *Bemenetnek* tekintünk minden olyan erőforrást (idő, pénz, nyersanyag stb.), aminek hatása van a kulcsfolyamatokra. Az információbiztonság területére is értelmezhető ez a kijelentés, azzal a megkötéssel, hogy a fókuszba az adatok és az információk kerülnek. A *folyamatoknál* a minőségen, a hatékonyságon és a következetességen, valamint ezen fogalmak mérésén van a hangsúly. Olyan mérési módszert kell kialakítani és használni, amelyik releváns és objektív adatokkal szolgál magáról a folyamatról (különösen a kulcsfolyamatok tekintetében). Az információbiztonságnál a folyamat alatt elsősorban az adatok bizalmasságával, sértetlenségével és rendelkezésre állásával kapcsolatos tevékenységeket, illetve ezek mérését értjük. A folyamatok hatással vannak a munkára, a szervezet vagy valamely egysége működésére, így *a kimenetnél* ezt a hatást, illetve a terméket/szolgáltatást vizsgáljuk. Az információbiztonságnál ez lehet például a végponti berendezések fertőzésmentes állapotával kapcsolatos információ. Az információbiztonságnál az *eredmény* az informatikai eszközöket (számítógépek, laptopok, okostelefonok) használók elégedettsége. Mihăiloaie a KPI tipológiája kifejezést használja, és öt típust különböztet meg (a bemutatott példák az információbiztonság területére értelmezhetők), úgymint:

1. stratégiai vagy operacionális:
   a) stratégiai: az informatikai szolgáltatásokat igénybe vevők elégedettsége (ettől függ a szolgáltatási szerződés meghosszabbítása),
   b) operacionális (működési): az informatikai eszközök meghibásodási gyakorisága, rendelkezésre állás,
2. bemenet, folyamat, kimenet, eredmény (egyezik Wilsey típusaival),
3. kvalitatív, vagy kvantitatív:
   a) kvalitatív (minőségi): az informatikai szolgáltatásokat igénybe vevők elégedettségi indexe, amit például elégedettségi kérdőívvel lehet mérni,
   d) kvantitatív (mennyiségi): óránként ellenőrzött e-mailek száma, mennyi időbe telik, hogy az üzenetek az informatikai rendszer legelső védelmi pontjától eljussanak a címzett postaládájába,
4. vezető vagy időben lemaradó (megítélése a kontextustól függ):
   a) vezető: a jövőbeli értékeket befolyásolja, például: hány ember végezte el meghatározott időpontig a biztonságtudatossággal kapcsolatos oktatást,
   b) lemaradó: múltbéli teljesítményt jelzi,
5. hatékonyság vagy hatásosság:
   a) hatékonyság: mennyi időt, energiát, költséget használtak fel a kívánt kimenet érdekében. Például: adott műszakban az információbiztonsággal foglalkozó szakemberek száma,

[27] Wilsey, David (2017): Types of KPIs: The Logic Model and Beyond. Elérhető: www.balancedscorecard.org/BSC-Basics/Blog/ArtMID/2701/ArticleID/1099/Types-of-KPIs (A letöltés dátuma: 2018. 03. 28.)

b) hatásosság: sikerült-e a kívánt kimeneteket generálni. Például: havonta hány esetben nem sikerült megakadályozni a rendszer érezhető lassulását, esetleg összeomlását a túlterheltség miatt.[28]

A fentiek alapján – némiképp eltérő logikai és tartalmi értelmezéssel – én 8 KPI-fajtát különböztetek meg, ezek a következők:

1. Folyamat KPI: az informatikai biztonsági folyamatok (például: incidenskezelés) hatékonyságát méri. Például: a rendszer leállásától az újraindulásig eltelt idő.
2. Beviteli KPI: eszközök, erőforrások fejlesztésére fordított idő/pénz. Például: a Security Operations Center (Biztonsági Központ, a továbbiakban: SOC) munkatársainak a továbbképzési ideje.
3. Kimeneti KPI: az informatikai rendszer eredményességének mutatószáma. Például: a végfelhasználóhoz elérkező kártékony e-mailek aránya.
4. Vezető KPI: azon tevékenységek mérése, amelyek jelentős hatást gyakorolnak az informatikai rendszer jövőbeli teljesítményére. Siker/kudarc előrejelzése. Például: az informatikai biztonsági rendszer tartós meghibásodása.
5. Veszteség KPI: az informatikai rendszer meghibásodásából eredő veszteség. Például: e-mail-szolgáltatás kimaradása (perc).
6. Eredmény KPI: az informatikai rendszer használatából eredő előnyök, eredmények. Például: az új levelezőrendszer bevezetéséből származó időmegtakarítás.
7. Kvalitatív KPI: minőségi, leíró jellegű KPI. Például: a munkavállalók szubjektív biztonságtudatossága (valamilyen skálán vagy százalékban).
8. Kvantitatív KPI: mennyiségi, mérhető, skálázható, statisztikai módszerekkel feldolgozható. A legtöbb KPI ebben a kategóriába tartozik. Például: 1000 e-mailből hány százalék fertőzött.

A KPI-k fajtáival némi átfedést mutatnak a KPI-típusok, amelyek közül tanulmányomban négyet nevezek meg:

1. Kvantitatív: objektíven mérhető, mennyiségi adatok. Például: bejelentett biztonsági események száma.
2. Kvalitatív: például a munkavállalók biztonságtudatosságát mérő különböző tesztek eredményei.
3. Mérföldkő: bizonyos időpont vagy tevékenység elvégzésének dátuma, például: tanúsítvány felülvizsgálati ideje.
4. Küszöbérték: elér valamilyen szintet, vagy beleesik valamilyen tartományba. Például: az informatikai incidensek gyakorisága tartósan átlag feletti szinten van.

[28] Mihăiloaie, Cristina (2015): KPIs. How many types are there? Elérhető: http://www.performancemagazine.org/kpis-how-many-types-are-there/ (A letöltés dátuma: 2018. 03.28.)

A KPI-k megalkotásának és használatának lépései

A KPI-k megalkotásánál és használatánál választhatunk többek között a három-,[29] az öt-,[30] illetve a kilenclépéses módszer[31] között. Tanulmányomban az információbiztonság fókuszában részletesebben az ötlépéses módszert ismertetem, így az alábbiakban csak felsorolás jelleggel írok a kilenclépéses módszerről.

A kilenclépéses módszer lépései:

1. Tekintsük át a stratégiai terv megvalósításában elért eredményeket!
2. Válasszuk ki a stratégiához legjobban illeszkedő KPI-ket!
3. Számszerűen határozzuk meg az adott KPI célját öt évre!
4. Az öt évet (stratégiai szint) bontsuk évenkénti célokra!
5. Nézzük meg, hogy a többi KPI (amelyeket nem a stratégiával közvetlen összefüggésben határoztunk meg) hogyan kapcsolódik az előző pontokhoz!
6. A KPI-k célját az ügyfélorientáltság szerint fogalmazzuk meg!
7. Fogalmazzuk meg a KPI céljait a belső munkatársak/folyamatok fókuszában!
8. A KPI-célokat kapcsoljuk össze!
9. Fordítsunk kellő figyelmet a KPI-k varratmentes kapcsolódására és a belső összefüggések megfogalmazására!

Az ötlépéses módszernél első lépésként a *célokat* határozzuk meg. Célunk lehet többek között:

- folyamatos információk szerzése és kiértékelése,
- vezetői döntések meghatározása,
- a rendszer biztonságosabbá tétele,
- a munkavállalók tevékenységének objektívabbá tétele,
- a különböző incidenstípusok arányának meghatározása és időbeni változásának vizsgálata,
- információbiztonsági oktatási programok kidolgozása, hogy az érintett munkavállalók biztonságtudatossági szintje emelkedjen,
- a költségek csökkentése,
- a rendelkezésre álló erőforrások optimális felhasználása.

A második lépés a *kritikus sikertényezők* meghatározása a célokból. A kritikus sikertényezők (a továbbiakban: CSF) korlátozott számú kulcsfontosságú tevékenységet jelentenek. Céljuk, hogy az egyének, az osztály vagy a szervezet a meghatározott sikerre összpontosítson. A kritikus sikertényezők olyan konkrét feltételek, amelyek mérik vagy megkönnyítik az üzleti célok elérését, meghatározott időn belül. Például: az elkövetkező egy évben 20%-kal kell csökkenteni az informatikai incidensek számát.

---

[29] Gruer, Ivan (2014): New IT Innovation Development (N.I.T.I.D) method Step 4: Evaluate Solutions (Tripadvisor Case Study). Elérhető: https://ivangruer.com/2014/12/01/new-it-innovation-development-n-it-i-d-method-step-4-evaluate-solutions-tripadvisor-case-study (A letöltés dátuma: 2018. 03. 28.)

[30] Enhorning, Peder (2013): 5 Steps to Actionable Key Performance Indicators. Elérhető: https://unilytics.com/5-steps-to-actionable-key-performance-indicators (A letöltés dátuma: 2018. 03. 28.)

[31] Jackson, Ted (2018): How To Set KPI Targets: 9 Steps To Drive Results. Elérhető: https://www.clearpointstrategy.com/how-to-set-kpi-targets (A letöltés dátuma: 2018. 03. 28.)

A harmadik lépésként meghatározzuk a *KPI-ket* a kritikus sikertényezőkből. A KPI-k olyan számított tevékenységek, események, történések stb., amelyek révén látható, hogy a CSF-ek elérése mennyire reális, és még időben megfelelő (vezetői) intézkedéseket lehet hozni. Érdemes foglalkozni az alábbi kérdésekkel:

- Hány KPI-re van szükség?
- Hogyan határozzuk meg a KPI-ket?
- Mennyire tartós egy KPI?
- Hogyan lehet mérni a KPI értékét?
- Mikor veszíti el egy KPI az értékét, illetve a fontosságát?
- A KPI-portfólió elemei milyen módon változtathatóak?
- Vannak-e lánc (egymáshoz kapcsolódó) KPI-k?

Célszerű lehet ennél a lépésnél a KPI-k jobb megértése érdekében KPI-lapokat készíteni. A Deloitte az alábbi KPI-lapot javasolja *(2. ábra):*

KPI neve	A KPI rövid neve, verziószáma, a készítés dátuma, sorszáma
KPI státusza	Kidolgozás alatt, tesztelés alatt, bevezetve, kivezetve
Leírás	A KPI leírása – mit takar/jelent az adott mutató?
Feladat	Mi a feladata, mit kér a KPI, miért fontos ez a mutató?
Érdekelt felek	Kire vonatkozik a KPI?
Típus	Mennyiségi, minőségi, mérföldkő, küszöb
Fontosság	Alacsony, közepes, magas
Egység/osztály	Milyen szervezeti egységet érint?
Módszer	Annak a módszere, hogy hogyan kell mérni a KPI-t
Mérés tárgya	SOC-hatékonyság, vállalati fenyegetettség, IBIR, érettség stb.
Eszközök	Azok az eszközök, amelyek a mérést és jelentést támogatják
Gyakoriság	Nap, hét, hónap, negyedév, év, több mint egy év
Megjegyzés	Kiegészítő információk. A szabály megalkotásához vagy a szabályozáshoz szükséges?

2. ábra

KPI-lap

Forrás: A szerző szerkesztése a Deloitte alapján

A negyedik lépés az *adatgyűjtés*. Az adatgyűjtés célja, hogy rendelkezésre álljanak a KPI-k és a többi mutatószámok kiszámításához szükséges adatok, információk.

Érdemes választ keresni az alábbi kérdésekre:

- Honnan származzanak az adatok?
- Ezek egyébként is rendelkezésre állnak, vagy le kell őket szűrni/válogatni?
- Mennyire fogadunk el egy adatforrást validnak?
- Milyen gyakran vegyünk mintát?
- Milyen módszerrel vegyünk mintát?
- Hogyan különböztethetők meg a függő és független adatok?

A záró, ötödik lépés a KPI-k *kiszámítása* a rendelkezésre álló adatok alapján. A KPI-ket abszolút vagy relatív módon (érték, százalék, forint) fejezzük ki, s rendszerint valamilyen időszakra vonatkoznak.

Az alábbiakban Gruer háromlépcsős elképzelését ismertetem egy általa publikált gyakorlati példán keresztül.[32] Nevezett szerző (1) az új igények, (2) a követelmények, valamint (3) a KPI-k alapján építi fel modelljét. A példában *(4. táblázat)* a *big data*hoz köthető ötletek, a szükséges informatikai infrastruktúra, illetve a KPI-k szerepelnek.

4. táblázat
A KPI-k megalkotása

Big Data ötletek (igények)	*IT-infrastruktúra megoldások (követelmények)*	*KPI-k*
A folyamatok megkönnyítése	Felhasználói webes felület	Következetlenség, késedelem a kérések teljesítését illetően
Integrált ellátási lánc létrehozása	Kapcsolat a beszállítókkal, kapcsolat az ügyfelekkel	A megosztható információk száma/aránya, az információk célba juttatási ideje (késés), a kapcsolatok típusai
Felhasználói élmények létrehozása	Közösségi hálózat, közösségi aktivitás támogatása, kimutatások	Kimutatások száma, fajtái, infrastruktúra szükséglete számokban és műszaki paraméterekben kifejezve (például: sávszélesség)
Fogyasztói elköteleződés támogatása	Kapcsolat külső vállalatokkal	Megosztandó információk mennyisége, az információk célba juttatási ideje (késés), kapcsolatok típusai
Statisztikák és riportok biztosítása	Adatelemzés, prediktív eszközök	Adatredundancia, adatkorreláció, az adatok reprezentativitása, adatbevitel torzításai (hiba, eltérés), prediktív hiba és eltérés, sejtésekre alapozott elemzés mennyisége

Forrás: A szerző szerkesztése Gruer 2014 alapján

Záró gondolatok

A szervezetek működésének mérése, illetve a mutatószámok szerinti (objektív) jellemzése egyre inkább az alapvető elvárások közé tartozik azoknál a szervezeteknél, amelyek hosszú távon szeretnék megőrizni piaci pozíciójukat, helyzetüket. Kulcsfontosságú teljesítménymutatókkal mérik többek között a munkavállalók teljesítményét, a műszaki-gazdasági folyamatokat. A mutatószámok meghatározása, a mérési adatok megléte és kiértékelése mellett legalább annyira fontos az, hogy meghatározott időközönként (hetente, havonta stb.) ezekből az adatokból és információkból objektív tartalmú és jól értelmezhető riportok, jelentések készüljenek. Ez igaz (pontosabban igaznak kellene lennie) az informatikai-, az adat- és az információbiztonság területén is. Ami a jövőt illeti, a riportok és az egyszerűbb

[32] Gruer 2014

összehasonlítások mellett az adatbányászat módszereivel az egyes kulcsmutatószámok biztosabban határozhatók majd meg, és az adatvizualizáció révén könnyebben mutathatók be. A matematikai-statisztikai eljárások hangsúlyosabban fognak megjelenni, így az idősoros elemzés részeként a trendvonal megrajzolása, a szezonalitás, a prognosztika, a leíró statisztikák közül a gyakoriság, az átlag, a módusz, a medián, a terjedelem, a szórás számítása. De a rendelkezésre álló adatok alapján szükség lesz becslésre, a valószínűségszámítás módszereire, a korreláció meghatározására is. Ahogy a szociometria és a hálózatkutatás segítségével a társadalmi, gazdasági, műszaki problémák közötti rejtett összefüggések feltárhatók, úgy a kulcsmutatószámok hálózatkutatás segítségével történő kapcsolódásainak megismerése (KPI-metria) megannyi új ismerettel gazdagítja majd a vállalatirányítási és információbiztonsági szakembereket.

A jövőt illetően abban is biztos vagyok, hogy a fent említett módszerek és eljárások révén az eddiginél lényegesen szofisztikáltabb és megalapozottabb következtetéseket lehet megfogalmazni, és egyre kisebb kockázattal járó döntéseket lehet hozni, különösen, ha ezekben a folyamatokban és tevékenységekben ki tudjuk majd használni a mesterséges intelligenciában, illetve a kvantumszámítógépekben rejlő lehetőségeket. Tanulmányomat az egyik leghíresebb menedzsmenttanácsadással foglalkozó szakembernek, Peter Druckernek tulajdonított idézettel szeretném zárni: „ha nem tudod megmérni, nem tudod menedzselni sem”.

Felhasznált irodalom

Aiello, Steven (2017): IT Security KPIs: 4 Effective Measurements for your Organization. Elérhető: https://www.thinkahead.com/blog/security-kpis-4-effective-measurements-organization-pt-1/ (A letöltés dátuma: 2018. 03. 27.)

Baroudi, Rachad (2011): *KPI Mega Library 2010 – 17.000 key performance indicator.* Scotts Valey, Rachad Baroudi.

Bharadwaj, Maninder (2011): Measuring The Value of Information Security. Deloitte oktatási anyag. Elérhető: http://isacabangalore.org/isacabc/main/media/downloads/2011conf/23measuringvalue.pdf (A letöltés dátuma: 2018. 03. 27.)

Czichos, Horst ed. (1993): *HÜTTE: A mérnöki tudományok kézikönyve.* Budapest, Springer Hungarica.

De Lutiis, Paolo (2014): Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection. ETSI konferenciaelőadás.

Enhorning, Peder (2013): 5 Steps to Actionable Key Performance Indicators. Elérhető: https://unilytics.com/5-steps-to-actionable-key-performance-indicators (A letöltés dátuma: 2018. 03. 28.)

Gilchrist, Alasdair (2016): *Industry 4.0. The industrial internet of things.* New York, Apress.

Glen, Bruce (2006): You Can’t Manage It If You Can’t Measure It. ISACA konferenciaelőadás.

Gruer, Ivan (2014): New IT Innovation Development (N.I.T.I.D) method Step 4: Evaluate Solutions (Tripadvisor Case Study). Elérhető: https://ivangruer.com/2014/12/01/new-it-innovation-development-n-it-i-d-method-step-4-evaluate-solutions-tripadvisor-case-study (A letöltés dátuma: 2018. 03. 28.)

Hetyei József szerk. (2004): *ERP rendszerek Magyarországon a 21. században.* Budapest, Computer Books.

Horváth Gergely Krisztián (2013): *Közérthetően (nem csak) az IT-biztonságról.* Budapest, Kormányzati Informatikai Fejlesztési Ügynökség.

Hubbard, W. Douglas – Seiersen, Richard (2016): *How to measure anything in cybersecurity risk.* New Jersey, Wiley & Sons.

Huwyler, Herman (2018): Key Indicators: KPIs, KRIs, KCIs and KLIs. Elérhető: http://mydailyexecutive.blogspot.hu/2011/06/key-indicators-kpis-kris-kcis-and-klis.html (A letöltés dátuma: 2018. 03. 27.)

IPAR 4.0 – Fogalomtár, fontosabb tanulmányok, legfőbb szereplők (2016). Budapest, Innomine Group.

Jackson, Ted (2018): How To Set KPI Targets: 9 Steps To Drive Results. Elérhető: https://www.clearpointstrategy.com/how-to-set-kpi-targets (A letöltés dátuma: 2018. 03. 28.)

Jenei Tünde (2016): Leggyakrabban használt kockázatkezelési modellek összehasonlítása. *International Journal of Engineering and Management Sciences (IJEMS).* Vol. 1. No. 1. Elérhető: https://www.researchgate.net/publication/306042047_Leggyakrabban_hasznalt_kockazatkezelesi_modellek_osszehasonlitasa (A letöltés dátuma: 2018. 09. 21.)

Khanduja, Meetu (2012): Key Result Area (KRA) and Key Performance Area (KPA). Elérhető: https://hrdictionaryblog.com/2012/12/06/key-result-areakra-and-key-performance-areakpa/ (A letöltés dátuma: 2018. 03. 27.)

Kollár Csaba (2017): A szervezeti információbiztonsági folyamatok monitorozása és a vezetői döntések támogatása kulcs teljesítménymutatók segítségével. I. rész – Az információbiztonság rendszerelméleti megközelítése. *Szakmai Szemle,* XV. évf. 4. sz. 43–56.

Maynard, Harold B. ed. (1977): *Gazdasági mérnöki kézikönyv.* Budapest, Műszaki Könyvkiadó.

Mihăiloaie, Cristina (2015): KPIs. How many types are there? Elérhető: http://www.performancemagazine.org/kpis-how-many-types-are-there/ (A letöltés dátuma: 2018. 03. 28.)

Parmenter, David (2010): *Key performance indicators. Developing, implementing, and using winning KPIs.* New Jersey, John Wiley & Sons.

Payne, Adrian (2006): *CRM kézikönyv. Ügyfélkezelés felsőfokon.* Budapest, HVG Könyvek.

Schliemann, Maximo Neira – Mishra, Ravi (2012): *Establishing Key Risk Indicators for IT.* Metricstream, s.l.

Understanding Key Control Indicators & how they can reduce risk (2018). White paper, Xactium. Elérhető: https://www.xactium.com/download-the-whitepaper-understanding-key-control-indicators-and-how-they-can-reduce-risk (A letöltés dátuma: 2018. 03. 27.)

Wanick, Brit (2017): KPI v. KRI v. KCI: Key Cyber Security Indicators. Elérhető: https://www.fourv.com/blog/kpi-v.-kri-v.-kci-key-cyber-security-indicators (A letöltés dátuma: 2017. 11. 02.)

Wilsey, David (2017): Types of KPIs: The Logic Model and Beyond. Elérhető: https://www.balancedscorecard.org/BSC-Basics/Blog/ArtMID/2701/ArticleID/1099/Types-of-KPIs (A letöltés dátuma: 2018. 03. 28.)

Krepsz Balázs[1]

A Nemzeti Adó- és Vámhivatal internetbűnözés elleni fellépése, internetes bizonyítékok felderítése

A NAV Bűnügyi Főigazgatósága

A Nemzeti Adó- és Vámhivatal (a továbbiakban: NAV) két fő szervezeti ága az Adó- és Vámhatóság, valamint a Bűnügyi Főigazgatóság. A Bűnügyi Főigazgatóság önálló bűnügyi nyomozó szerv, amely évente ötezer bűnügyi nyomozást folytat le. A főigazgatóságok főosztályai országos szinten koordinálják a bűnügyi nyomozásokat, a nemzetközi együttműködést, valamint a szervezet jogi, informatikai és személyzeti hátterét.

A bűnügyi szervezetnek hét területi (Bűnügyi Igazgatóságok) és egy kiemelt nyomozó szerve van, a Központi Nyomozó Főosztály. A NAV nyomozati hatásköre az alábbi főbb csoportokban határozható meg:

- Állami vagy uniós bevételeket károsító bűncselekmények: költségvetési csalás és kapcsolódó jogsértések. Ebbe a bűncselekményi kategóriába tartozik a csempészet, jövedéki törvénysértés, állami vagy EU-s támogatásokkal történő visszaélések és egyéb, a költségvetést károsító bűncselekmények.
- Nemzetközi tilalmak megsértése: gazdasági, haditechnikai, kettős felhasználású termékekkel kapcsolatos tilalmak megszegése.
- Hamisítás, illetve a szerzői jogok megsértése.
- Engedély nélküli külkereskedelmi tevékenység.
- Egyéb, a fentiekhez kapcsolódó bűncselekmények: pénzmosás, okirat- és bélyeghamisítás stb.

A NAV-hoz tartozó internetes bűncselekmények trendjei

Az internetes bűncselekmények amellett, hogy közvetlen kárt okoznak a legális kereskedőknek és jogtulajdonosoknak, egyben az állami bevételeket is nagymértékben csökkentik. A Business Software Alliance (a továbbiakban: BSA) jelentései alapján a szoftverek 39%-a illegális Magyarországon, ami nemcsak jelentős anyagi károkat okoz, hanem Magyarország átlagos IT-sebezhetőségét is jelentősen megnöveli, mivel az illegálisan terjesztett szoftverek

[1] Krepsz Balázs osztályvezető. Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága, Központi Nyomozó Főosztály, Információ-Technológiai Osztály

nem kapják meg a szükséges technikai támogatást, biztonsági frissítéseket, továbbá kártékony kódokat is tartalmazhatnak.

A szerzői joggal védett filmek, zenék, szoftverek illegális megosztása a világon évente közel 100 millió dollár vagyoni hátrányt okoz a jogtulajdonosoknak és közvetve az állami költségvetéseknek. Amíg az 1990-es években Magyarországon virágzó iparág volt a művészeti alkotások terjesztése, addig az internetes kalózkodás miatt napjainkra jelentősen hanyatlottak a legális terjesztési vonalak, visszaestek az értékesítések, munkahelyek szűntek meg, és az adóbevételek is jelentősen csökkentek.

A magyar webshopok éves összesített forgalma meghaladja a 150 milliárd forintot, a tényleges bevételek egy része után a forgalmi adókat nem fizetik meg. Ezen felül az interneten keresztül értékesített áruk 2–3%-a összesen több milliárd forint értékű hamisítvány, amelyek egy része nemcsak a jogtulajdonosok jogi és pénzügyi érdekeit sérti, hanem egészségügyi vagy egyéb társadalmi, biztonsági kockázatokat is hordoz.

A fenti jogsértések közvetve a legális, valamint az illegális szolgáltatásokat ingyen igénybe vevő felhasználókat is hátrányosan érintik.

A NAV internetbűnözés elleni fellépése

A NAV internetes bűnözés elleni fellépésének célja a szervezet stratégiai céljaihoz, bűnügyi hatásköréhez kapcsolódik. A szervezet alapvető célja a magyar és az uniós költségvetés érdekeinek védelme, az állami bevételek biztosítása, a szerzői és iparjogvédelmi jogok védelme, valamint a nemzetközi áruforgalom ellenőrzése.

A Nemzeti Adó- és Vámhivatal internetbűnözés elleni fellépése három fő tevékenységből áll:

1. Illegális weboldalakkal kapcsolatos eljárások, amelyek lehetnek bűnügyi, vám- vagy adóeljárások. A leggyakoribb jogsértések, amelyek a NAV hatáskörébe tartoznak:
   - Szerzői jogsértések:
     - Jogvédett művek (film, zene, szoftver, e-book) illegális megosztása. Ez főként bűnügyi felderítő tevékenységet és nyomozásokat jelent.
     - Jogvédett ábrákkal ellátott termékeket árusító weboldalak elleni fellépés. Részben bűnügyi, szabálysértési, részben vámhatósági és adóeljárások során.
   - Iparjogvédelmi jogsértések (hamisítás):
     - Védjeggyel ellátott hamis termékeket árusító weboldalak elleni fellépés. Főként vámhatósági ellenőrzések és feljelentések alapján, bűnügyi nyomozások lefolytatásával.
   - Adóelkerüléssel működő webhelyek elleni fellépés. Adóeljárások vagy bűnügyi felderítés és nyomozás.
   - Tiltott vagy engedélyhez kötött termékek forgalmazásának megakadályozása.
   - A hatáskörbe tartozó bűncselekményekhez kapcsolódó internetes pénzmosás felderítése.
2. Nemzetközi vám- vagy bűnügyi akciókban történő részvétel, amelyek célja a jogellenesen működő webhelyek elleni fellépés.
3. Bármilyen nyomozás során folytatott nyílt forrású internetes kutatás, közösségiháló-elemzés, egyéb internetes bizonyítékok felkutatása és rögzítése. A modern

bűnüldözés egyik alapköve lett az elektronikus adat, mint bizonyíték. Ezeket ma már nemcsak a házkutatások helyszínein talált elektronikus eszközökről foglalhatjuk le, hanem azok a nyílt internetről is származhatnak.

Az internetes szerzőijog-sértések elleni fellépés

Az interneten megvalósuló, a NAV hatáskörét érintő bűncselekmények egyik jellemző elkövetési módszere a zeneművek, filmek, szoftverek és e-bookok illegális megosztása az interneten. A Bűnügyi Főigazgatóság ezen a téren 2011-től az illegális fájlmegosztó webhelyek, szerverek, torrentoldalak azonosítását, az elkövetők felderítését és a nyomozások lefolytatását tűzte ki fő célul.

A legjellemzőbb elkövetési módszerek:

- Illegális megosztószerverek működtetése, ez esetben az elkövető a szerver üzemeltetője. Ezek főként File Transfer Protocol (a továbbiakban: FTP) technológián alapuló fájlmegosztó szerverek, amelyekről előfizetés után lehet közvetlenül tartalmat letölteni.
- Torrentoldalak, ez esetben az elkövetők az alábbiak lehetnek:
  - *Release* csoportok: filmek kép- és hanganyagát felveszik, szerkesztik, majd az interneten megosztják.
  - *Tracker* tulajdonosok: a torrentoldalak működtetői.
  - *Seed* szerver üzemeltetők: olyan szervereket üzemeltetnek, amelyek nagyobb sávszélességen osztják meg a műveket, gyorsítva az illegális szolgáltatásokat.
  - Nagy megosztók, akik több száz vagy több ezer művet osztanak meg egy webhelyen.
- Weblink-gyűjtemények, amelyeknél az elkövető a weboldal üzemeltetője és a nagyszámú művet megosztó linkelők. A linkgyűjtemények egyre inkább terjednek, mivel egyszerű és ingyenes a használatuk, és az elkövetők a reklámokból jelentős bevételre tehetnek szert.
- Egyéb fájlmegosztó szolgáltatások üzemeltetői, ahol az elkövető minden esetben a megosztó. Ilyenek a zenemegosztó oldalak, fórumok, blogok stb.

Az FTP vagy egyéb közvetlen megosztás technológiai megoldásaival az interneten megvalósuló szerzői bűncselekmények esetén az elkövetők spamben, e-mailen vagy internetes hirdetések útján keresik meg az internetes felhasználókat. A felhasználók különböző pénzügyi szolgáltatások – banki átutalás, emelt díjas SMS, internetes pénzügyi szolgáltatások, virtuális valuták – útján fizetnek elő az illegális szolgáltatásra. A befizetés után SMS-ben, e-mailben kapnak belépőkódokat az illegális szerverekre. A szervertermekben tárhelyet bérlő alvállalkozók sok esetben szintén együttműködnek az elkövetőkkel, és megosztoznak az illegális jövedelmen. A pénzt az elkövetők további bankszámlákra utalják tovább, és a pénzmosási rendszer végén készpénzben veszik ki az illegális jövedelmet. A bankszámlák általában olyan személyek vagy cégek nevén vannak, amelyek nem köthetők közvetlenül az elkövetőkhöz, akik a pénzforgalmat netbank szolgáltatáson keresztül bonyolítják. A készpénzt felvevő személy pedig általában nem vesz részt közvetlenül az illegális fájlmegosztásban, csak jutalék ellenében dolgozik az elkövetőknek.

A torrentoldalak üzemeltetői nem kérnek pénzügyi ellenszolgáltatást az illegális megosztásért, viszont a weboldalakon elhelyezett reklámok után jelentős összegekhez jutnak. Annak érdekében, hogy a weboldal vonzó legyen, az illegális szolgáltatást jelentősen gyorsító *seed* szervereket is üzembe helyeznek.

A linkgyűjtemények az illegálisan megosztott műveket külső tárhelyekről osztják meg, és csak a letöltési linkeket teszik közzé. A linkeket az üzemeltető, a tárhely bérlője vagy egyéb felhasználók küldik be a weboldalra. A felhasználók a weboldalra kihelyezett linkeken keresztül jutnak el a tárhelyen tárolt művekig, ahol azokat szabadon megtekinthetik. Az elkövetők a weboldalakon elhelyezett reklámok után jelentős illegális bevételhez jutnak. A linkgyűjtemények weboldalai gyakran felhőszolgáltatással, távoli szerverről működnek, ezért nehéz lenyomozni azok tulajdonosait.

A NAV bűnügyi fellépése során sosem volt cél a felhasználók kriminalizálása, hanem a forrásoknak a megszűntetése, és a nagy károkat okozó, legtöbbször anyagi haszonra törekvő szervezett kalózcsoportok tagjainak büntetőjogi felelősségre vonása.

A bűnügyi fellépés eredményei:

- 2011-től 31 kiemelt internetes ügy felderítése, amelyekben 36 gyanúsított ellen indult eljárás;
- 2011-től 15 bűnözői csoport ellen indult nyomozás, akik illegális weboldalakat működtettek;
- közel ötven szervergép került lefoglalásra;
- az elkövetési érték közel 20 milliárd forint;
- az illegálisan megosztott, azonosított jogvédett művek száma meghaladja az 50 ezret;
- az illegális szerverek száma az elmúlt öt évben a felére csökkent;
- az egyéb ügyekkel együtt 26 vádemelési javaslat történt;
- három esetben a pénzmosás bűncselekmény is megállapításra került.

Az interneten keresztül nyújtott szolgáltatásokkal, kereskedelemmel összefüggő adójogszabályok kijátszása, az adófizetés kikerülése elleni fellépés

Világszinten egyre inkább növekszik azoknak a weboldalaknak és internetes piactereknek a száma, ahol különböző legális termékeket árusítanak, de az értékesítés után esedékes forgalmi adókat nem vagy csak részben fizetik meg az adóhatóság felé. A legnagyobb weboldalakhoz köthető illegális beszállítási cégrendszerek több milliárd forint adóbevétellel is megkárosíthatják az állami költségvetést. A jogsértések felderítése érdekében a Nemzeti Adó- és Vámhivatal adó és bűnügyi szervei is folyamatosan monitorozzák a kereskedőoldalakat, és szükség esetén együttműködnek az elkövetők azonosításában és felelősségre vonásában.

Az áruk és szolgáltatások interneten keresztül történő értékesítése egyre nagyobb teret nyer, ezért az ellenőrzés és hatósági fellépés folyamatos erősítésére van szükség ezen a téren is. Ennek érdekében a bűnügyi és az adóhatóság szorosan együttműködik a jogsértések azonosításában és felderítésében.

A felderítési folyamatban és a közvetett bizonyításban is egyre fontosabbak az internetes kutatásból származó információk és bizonyítékok. A tapasztalatok alapján az ilyen ügyek sokszor nemzetközi kapcsolatokkal is rendelkező szervezett bűnözői körökhöz

kapcsolódnak, de az üzletszerűség szinte minden egyes ügyben megállapítható, és gyakran pénzmosás gyanúja is felmerül.

Hamis, jövedéki termékek internetes kereskedőoldalakon történő értékesítése

Az internetes piactereken, de néhány esetben már önálló weboldalakon is jelentős mennyiségű hamis terméket vagy jövedéki árut értékesítenek. A leggyakrabban hamisított termékek: karóra, parfüm, napszemüvegek, ékszerek, ruházati termékek, műszaki cikkek, gyógyszerek, de egyéb illegális termékek is megjelennek ezeken a webhelyeken, mint a vényköteles gyógyászati készítmények, cigaretta, alkohol és más jövedéki termékek.

Elsősorban a NAV adóhatósága vizsgálja az internetes piactereket, ahonnan próbavásárlásokat is végeznek. Ha az értékesített termékek értéke meghaladja a bűncselekményi értékhatárt, akkor az adóhatóság feljelentést tesz, és a büntetőeljárást a Bűnügyi Főigazgatóság valamelyik szerve folytatja le. A felderítésben és a nyomozásban is döntő szerepet játszik az internetes kutatás, valamint az adatbányászat. A NAV vámhatósága pedig az eljárások tapasztalatai alapján felépített kockázati profilok alapján vizsgálja a külföldről beérkező csomagokat a hamis és tiltott termékek felderítése érdekében.

A gyakori nemzetközi akciók is folyamatosan célpontba veszik a Darknetről vagy az illegális weboldalakról, piacterekről származó küldeményeket. Jellemző elkövetési magatartás, hogy a darknetes piacterekről rendelt illegális árukat olyan kis csomagokban küldik Magyarországra, amelyek a bejelentés szerint a 22 dollárt meg nem haladó, vámmentes sávba esnek. Mivel ilyen, főként postai küldeményekből naponta több ezer érkezik, nem lehetséges minden egyes csomag átvizsgálása, csak szúrópróbaszerű ellenőrzésre vagy a kockázati profilba eső csomagok átvizsgálására van erőforrás. Az ellenőrzések automatizálása és további, erre a célra szolgáló vizsgálóeszközök beszerzése is szerepel a NAV rövid távú céljai között.

A NAV speciális IT-egységeinek feladata a hatáskörébe tartozó jogsértések felderítésében és nyomozásában

A NAV adóhatósága és a Bűnügyi Főigazgatóság is rendelkezik speciális IT-egységekkel. Ezek feladatai:

- Weboldalak, internetes piacterek monitorozása. Konkrét információk alapján weboldalak, fórumok, piacterek rendszeres figyelése, ez alapján célzott ellenőrzések kezdeményezése lehetséges.
- A hatóság birtokába jogszerűen került adatok alapján a jogsértő weboldalak azonosítása, további eljárások kezdeményezése.
- Folyamatban lévő ügyekben internetes kutatás, amelynek célja az elkövetők azonosítása, kapcsolataik feltárása, internetes bizonyítékok rögzítése.
- Helyszíni intézkedés során történő adatmentések (számítógépek, mobiltelefonok, egyéb elektronikai eszközök), valamint a lefoglalt digitális eszközök szakértői vizsgálata.
- Bűnügyi szervek informatikai támogatása.

- Az internetes bűnözés elleni nemzetközi akciókban való részvétel, nemzetközi együttműködés külföldi speciális egységekkel (például Europol Copy Operation In Our Sites akció [a továbbiakban: IOS], Customs Against Internet Crime [a továbbiakban: C@IC] együttműködés, egyéb akciók). Az IOS akciók célja a nemzetközi források alapján azonosított, hamisításban vagy szerzői jogsértésben érintett weboldalak megszűntetése, lefoglalása, eljárások lefolytatása. A C@IC együttműködés célja az EU vámhatóságainál működő IT- és Cybercrime-egységek tapasztalatcseréje, képzése.
- Az IT-egységek a tapasztalatok átadásával részt vesznek az egyetemi oktatásban, a fiatalokat célzó szemléletformáló képzésekben, a hazai és nemzetközi szakértői fórumokon és rendezvényeken.

Internetes bizonyítékok felderítése: nyílt forrású internetes kutatás a NAV gyakorlatában

Az internetes nyomozások és kutatások kihívásai

Az internetes nyomozások és bizonyítékok felkutatása során gyakran szembesülünk kihívásokkal. Ezek jellemzően a következők:

- Az elkövetők azonosításának leggyakoribb módszere az IP-címek lenyomozása. Az elkövetők azonban a saját IP-címeiket proxyszerverekkel, VPN-szolgáltatásokkal vagy egyéb módszerekkel védhetik, használhatnak TOR-rendszereket is, így sok esetben nehezen vagy egyáltalán nem azonosíthatók ez alapján.
- Az elkövetők a kommunikációhoz olyan applikációkat használnak, amelyek a titkosított adatforgalom miatt a jelenleg rendelkezésre álló technológiával nem lehallgathatók.
- Az internet nem ismeri az országhatárokat. A nemzetközi jogsegélyek lassúak és sok esetben eredménytelenek.
- Az elkövetők gyakran hamis adatokkal próbálják félrevezetni a hatóságokat.
- Az elkövetők rendszeresen használnak olyan módszereket, amelyek megnehezítik a pénz útjának nyomon követését. A virtuális valuták az illegális forrásból származó vagyon eltűntetésére, a pénzmosásra alkalmasak.
- A jogellenes adattartalmú szerverek nem közvetlenül, hanem proxyszerverek útján kommunikálnak.
- Az elektronikus eszközök titkosítása sok esetben lehetetlenné teszi az elektronikus bizonyítékok beszerzését.
- Az elkövetők egyedi védelmi rendszerekkel látják el számítógépeiket, így egy rosszul végrehajtott helyszíni intézkedés során pillanatok alatt megsemmisülhetnek a releváns adatok.
- Az elektronikus bizonyítékok sok esetben a felhőben tárolódnak, és nehezen hozzáférhetők, vagy nagyon gyorsan megsemmisíthetők.

A nyomozóhatóságoknak és azokon belül különösen az IT-egységeknek a hazai és nemzetközi, hatósági és civil szervezetekkel (például egyetemekkel) történő együttműködés során is törekedniük kell a legjobb gyakorlatok, a leghatékonyabb eszközök átvételére, használatára, továbbá az informatikai tudásbázis folyamatos és professzionális fejlesztésére.

Mire jó az internetes kutatás?

Az internetes kutatás eredményei olyan adatokat, bizonyítékokat tárhatnak fel, amelyek döntő jelentőségűek lehetnek egy bűnügyi felderítés vagy nyomozás során. A kutatás célja és eredménye nem behatárolható, gyakorlatilag bármilyen, az interneten talált információ alkalmas rá, ami alátámasztja a bűncselekmény elkövetését, feltárja az elkövetők vagy cégek kapcsolatrendszerét, a személyek azonosítását, elérhetőségeit, tartózkodási helyét, vagy egyszerűen további vonalakat határoz meg a felderítés folyamatában. A nyílt forrású internetes kutatás leggyakoribb céljai az alábbiak lehetnek:

- Egy adott ügyben érintett weboldal tényleges működtetőjének, működési helyének azonosítása.
- Egy adott ügyben érintett személyek azonosítása, elérhetőségeinek felkutatása, kapcsolatrendszerének feltárása.
- Körözött személyek tartózkodási helyének megállapítása.
- Jogsértő weboldalak, illetve jogsértést elkövető felhasználók azonosítása, weboldalak működésének megfigyelése, oldalak mentése, az ügyhöz kapcsolódó weboldalak elemzése.
- A pénz útjának nyomon követése internetes fizetési rendszerek esetén.
- Cégek azonosítása, működésükről adatok gyűjtése.
- Fényképek elemzése és kutatása az interneten.
- Egy adott ügyhöz kapcsolódó weboldalak, híroldalak, adatok keresése és rögzítése.
- Geoadatok, földrajzi adatok kutatása.
- E-mail-fiókok azonosítása, mentése.
- Közösségiháló-elemzések.
- Chat, fórum és egyéb közösségi oldalak megfigyelése.
- Egyéb célzott adatkutatások, igények alapján.
- Új trendek, eszközök, megoldások keresése, önképzés.

Webszervereket üzemeltető elkövetők kilétének megállapítása

Az internetes webszervert működtetők esetén az alábbiak vezethetnek bizonyítékokhoz:

- internetes adatgyűjtés, közösségiháló-elemzés,
- weboldal regisztrálójának adatai,
- weboldalak elemzése,
- szervert működtető cégnél fellelhető adatok,
- érintett bankszámlák adatai, banki *log*ok,
- e-mail-használók azonosítása, levelezés letöltése, elemzése,
- fel- és letöltési adatok (*log* fájlok),

- a számítógépeken talált bizonyítékok, kommunikációra használt applikációk adatai,
- emelt díjas szolgáltatási szerződések,
- internetes fizetési rendszerek nyomon követése,
- bannerszolgáltatók adatai,
- mobiltelefonokon tárolt adatok.

Az internetes kutatás eszközei

Az internetes kutatás eszközeinek felsorolása gyakorlatilag lehetetlen. A legjellemzőbbek a következők:

- Internetes nyilvántartások (például: www.centralops.net). Ezek alapján meghatározhatjuk egy webcím tulajdonosi adatait, tovább azt, hogy a weboldalhoz rendelt IP-cím melyik szolgáltató tartományába tartozik, ami támpontot ad a kiszolgáló szerver fizikai helyének meghatározásához.
- Szerverek elérési útjának elemzése (*traceroute* elemzés). Ezzel a módszerrel feltárható, hogy egy weboldalra milyen szervereken keresztül juthatunk el. Ebből információt szerezhetünk arra, hogy az adott IP-cím kiszolgálója ténylegesen melyik országban, illetve melyik szerverterem hálózati eszközén keresztül kommunikál.
- Keresések kép alapján, képelemzés. A képek visszakeresésére használható böngésző bővítményekkel a keresett képhez nagyon hasonló képek kereshetők. Szerencsés esetben egy keresett képet akár több helyen is megtalálhatunk, így azonosíthatjuk a képen szereplő személyt vagy tárgyat.
- Elérhetőségek keresése (e-mail, *nickname,* nevek, címek, telefonszámok stb.). Az adatok alapot nyújthatnak a további nyomozáshoz, illetve azok alapján további *account*okat, egyéb elérhetőségeket vagy kapcsolatokat tárhatunk fel.
- Weboldalak elemeinek elemzése. A weboldal elemzésével azonosíthatunk a weboldalhoz kapcsolt közösségi oldalakat, hirdetési oldalakat vagy egyéb olyan webhelyeket, ahol jóval több adatot tudhatunk meg a működtetőkről.
- Közösségi oldalak azonosítása, chatek, fórumok elemzése. A kommentek tartalmából következtethetünk a másik fél személyére, továbbá kommunikálhatunk is vele, ha annak törvényi feltételei fennállnak.
- *Crawling* (tömeges adatok rendezett letöltése). Gyorsan, automatikusan nagy mennyiségű adatot tölthetünk le ezekkel az alkalmazásokkal egy adott weboldalról, amely alapja lehet egy elemzésnek, vagy egyéb eljárási cselekményeknek.
- Fizetési rendszerek azonosítása, pénz útjának követése. A legtöbb esetben ez segít az egyébként anonim elkövetők azonosításában és az illegális forrásból származó jövedelem felkutatásában.
- Weboldalak működésének megfigyelése, rögzítése. A weboldalak megfigyelésével és a változások nyomon követésével kaphatunk a nyomozásokat segítő információkat.
- Webstatisztikák. A weboldal statisztikai adatai segítenek az illegális oldalak látogatottsági adatainak a legális vagy hasonló webhelyekkel való összehasonlításában.
- Kapcsolódó weboldalak keresése. Az adott weboldal témájához kapcsolódó vagy azonos IP-címekről futó oldalak esetén további információhoz juthatunk az üggyel vagy az elkövetőkkel kapcsolatban.

- Archív oldalak. Az internetes archívumokba mentett weboldalak segítenek bemutatni egy weboldal változásait, korábbi felépítését.
- Weboldalak mentése. A weboldalak jövőbeni esetleges megszűnése miatt érdemes az üggyel kapcsolatos weboldalak offline változatát lementeni, mert ez a későbbiekben bizonyítékként felhasználható.
- Weboldalakról képek készítése bizonyítékként való felhasználás céljából.
- Indexelt Google keresések. Az összetett keresésekkel szűkíthetjük és konkretizálhatjuk a kereséseket, például egy személyhez köthető weboldalak, közösségi oldalak azonosítása céljából.
- Speciális keresőszolgáltatások (a nyílt forrású internetes kutatáshoz használatos OSINT-gyűjtemények). Ezeken az oldalakon több ezer szabad felhasználású keresőoldalt, illetve alkalmazást találhatunk, amelyek segítségünkre lehetnek az internetes kutatásban.
- Közösségiháló-elemzések. A bűnügyi nyomozások során leggyakrabban használt módszer, amely segít egy az ügyhöz köthető személy kapcsolatrendszerének, illetve a személyéhez köthető releváns adatoknak az azonosításában.

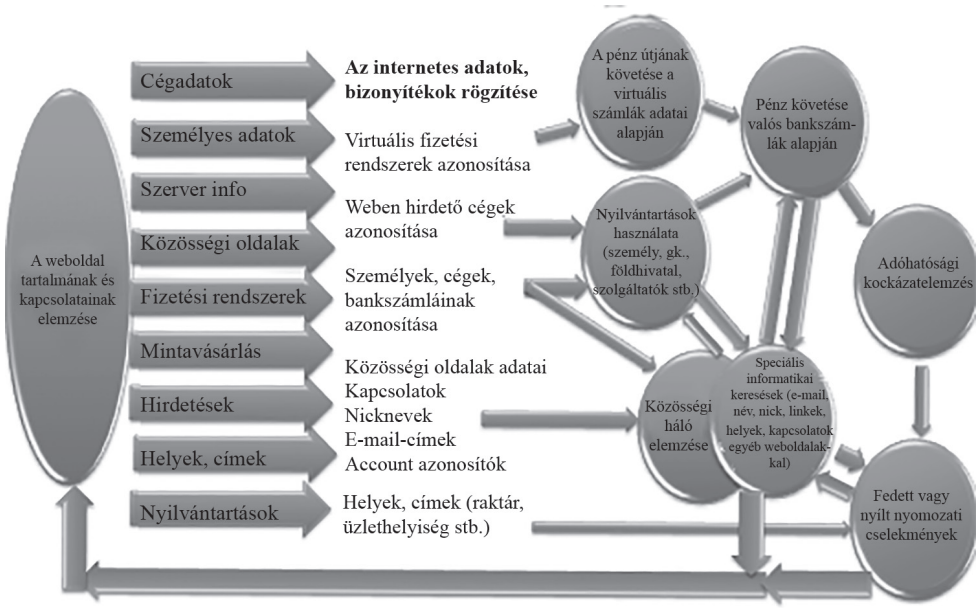
Weboldal-elemzések, a pénz útjának nyomon követése

Egy weboldalon számos olyan információt találhatunk, amely segítheti a nyomozást. A weboldal tartalmazhat cégadatokat, személyes adatokat, lekérhetünk szerverinformációkat, azonosíthatunk közösségi oldalakat, fizetési rendszereket, végezhetünk mintavásárlást, ellenőrizhetjük a hirdetéseket, találhatunk helyeket, címeket, nyilvántartási adatokat.

Az első fontos feladat az internetes adatok rögzítése. Ezek lehetnek közösségi oldalak adatai, kapcsolati adatok, *nickname*-ek, e-mail-címek, *account* azonosítók, telefonszámok vagy egyéb olyan adatok, amelyek alapján végezhetünk közösségiháló-elemzést és speciális internetkutatást. Ezeket az adatokat összevethetjük hivatalos nyilvántartások adataival, ahonnan további adatokhoz juthatunk, ezek alapján újabb adatokat gyűjthetünk egyéb weboldalakról.

Az egyik legfontosabb nyomozati eszköz mindig a pénz útjának nyomon követése, akár virtuális, akár valós bankszámlák adatai alapján. Innen szintén szerezhetünk olyan információkat, amelyek további internetes kutatást tesznek szükségessé. Esetenként felkérhetjük az adóhatóságot ellenőrzések és kockázatelemzések elvégezésére, és minden esetben hatékony eszköz a fedett nyomozás, vagy az elkövetők azonosítása érdekében végzett nyílt intézkedések foganatosítása. Ezek során szintén gyakran merülnek fel olyan információk, amelyek további internetes kutatás során ellenőrizhetők.

A teljes felderítési folyamat során érdemes újra és újra elvégezni az internetes kutatást az időközben felmerülő adatok alapján.



1. ábra

A pénz útjának nyomon követése webtartalom alapján

Forrás: A szerző szerkesztése

Darknet és virtuális valuták

Az internetes bűnözés egyik gyakran használt helyszíne a Darknet, amely bárki számára elérhető. A távoli informatikai folyamatok, a kiszolgálók tényleges IP-címei szinte lenyomozhatatlanok. A Darkweben található illegális piactereken szabadon rendelhetők illegális termékek (fegyver, kábítószer, tiltott anyagok, bankkártyaadatok, felhasználói adatbázisok, illegális tevékenységet segítő alkalmazások, gyógyszerek stb.).

Fizetésre virtuális valutákat – legtöbbször bitcoint – használnak. A megvásárolt termékeket elrejtve, csomagküldő vagy postai szolgáltatásokon keresztül küldik. Csak a Darknet monitorozásával, keresésekkel szinte lehetetlen a webshopot működtetők, eladók vagy vevők azonosítása, a tranzakciók nyomon követése. A felderítés fontos eleme ezért a nyílt interneten található adatok kutatása a darknetes információk alapján, továbbá az operatív eszközök használata. A virtuális valutákkal történő tranzakciók elemzése is támpontot adhat az elkövetők kilétének azonosítására. Egy adott bitcoin *wallet*be utalt, illetve onnan továbbított tranzakciók elemzése során olyan átváltó vagy szolgáltató azonosítható, amely esetleg valós adatokat szolgáltathat az egyébként anonim felhasználóról. Előfordulhat olyan eset, hogy az elkövetők bitcoint váltanak valós valutára, vagy valamilyen egyébként legális áruházból, szolgáltatótól rendelnek különböző termékeket, ahol a virtuális valutát fizetőeszközként elfogadják, így esetenként a szolgáltatásokat igénybe vevő valós személyeket is azonosítani lehet.

A NAV hatáskörébe tartozó bűncselekmények közül nagyon kevés valósul meg a Darkneten, ilyen nyomozás még nem indult. Viszont a virtuális valuták alkalmasak a pénzügyi bűncselekményekből származó illegális vagyon eltűntetésére, pénzmosásra, továbbá vagyonbiztosításként a virtuális pénz lefoglalása is fontos lehet a hatóságok számára, ezért ezen a téren is szabályozás kidolgozása van folyamatban. Fontos, hogy a házkutatások során a nyomozók felismerjék az elektronikus bitcoin *wallet*eket, az azokhoz tartozó privát és titkos kulcsokat, és rendelkezésükre álljon egy olyan eljárásrend, amely alapján a virtuális valuták lefoglalását végre tudják hajtani.

Gyaraki Réka[1]

Az egészségügyi intézményeket érő kibertámadások

Bevezetés

Az informatikai rendszerek alkalmazása nagyban megkönnyíti az adatok kezelését, tárolását, továbbítását és hozzáférhetővé tételét. Ezen tulajdonságok miatt ma már szinte nincs olyan terület, ahol ne használnának valamilyen informatikai eszközt, hálózatot.

Az elmúlt időszakban egyre több hír jelenik meg az állami-, valamint magánszférát érő kibertámadásokról, amelyek például a zsarolóvírusok miatt hozzáférhetetlenné váló adatok vagy akár DOS-támadások miatt elérhetetlenné váló weboldalak formájában jelentkeznek.

Az információs rendszerek lehetnek belső vagy külső hálózatok, illetve ezek együttese is. A hálózatokhoz történő hozzáférési jogosultság lehet egységes, valamint az adott munkavégzéstől, beosztástól függően szintenként vagy személyenként eltérő, sávos rendszerű. A rendszerek biztonságossága fontos, kiemelkedő munkát igénylő tevékenységet feltételez a rendszerhasználó szervezetben.

Ez nem minden esetben elég, hiszen az elektronikus információrendszert érő incidens nem a védelmet ellátó személyzet számától függhet, hanem a képzetlenség és a tudatosság hiánya az, ami még a legbiztonságosabb rendszereket is sérülékennyé teheti.

A tanulmányban a kritikus infrastruktúrákat érő támadások közül a kórházakat és egészségügyi intézményeket érő kibertámadásokról lesz szó, amelyek veszélyeztetik az intézmények működését, valamint érintik a betegeket és a betegjogokat is.

A kritikus infrastruktúra és kritikus információs infrastruktúra

A kritikus infrastruktúráról (a továbbiakban: KI) szintén rengeteg szó esik, ám a kritikus információs infrastruktúráról már kevesebb. Az, hogy mit is jelent és hol húzódik a különbség, a következőkben választható meg.

A kritikus infrastruktúra alatt az Európai Bizottság *Zöld könyv*e szerint olyan egymással összekapcsolódó, interaktív és egymástól kölcsönösen függésben lévő infrastruktúraelemek, létesítmények, szolgáltatások, rendszerek, folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van a társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság,

[1] Dr. Gyaraki Réka tanársegéd, doktoranda. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Kiberbűnözés Elleni Tanszék

nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában. Kritikus infrastruktúrának minősülnek azok a hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotórészei, amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszú távon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. Hazánkban a 2012. évi CLXVI. törvény[2] hatálybalépése óta a létfontosságú rendszerelemek kifejezést használják, ennek ellenére a tanulmányban maradok a 40/2013/EU direktíva[3] alapján a kritikus infrastruktúra kifejezésnél, mivel ezt az irányelv is így alkalmazza.

A kritikus infrastruktúrának tíz ágazata van, amelyekhez további alágazatok tartoznak:

1. energia,
2. infokommunikációs technológia,
3. közlekedés,
4. víz,
5. élelmiszer,
6. egészségügy,
7. pénzügy,
8. ipar,
9. jogrend/kormányzat,
10. közbiztonság/védelem.

A kritikus infrastruktúrák védelme tehát kiemelt jelentőségű, mivel a felsorolásból is látható, hogy a társadalom életét átfogó területekről van szó, így az infrastruktúrákat érő akár fizikai, akár a kibertéren keresztül érkező támadások az állampolgárok érdekeit (életét) veszélyeztetik, így negatív hatással vannak az adott országra, nemzetre.

Vizsgálatom tárgya az egészségügyi ágazat, amelyhez hat alágazat tartozik: az aktív fekvőbeteg-ellátás, a mentésirányítás, az egészségügyi tartalékok és vérkészletek, a magas biztonsági szintű biológiai laboratóriumok, az egészségbiztosítási informatikai rendszerek és a gyógyszer-nagykereskedelem.[4]

A kritikus információs infrastruktúra azokat az információs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúraelemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából, mint a távközlések, a számítógépek és a szoftverek, az internet, műholdak stb.[5]

Az egészségügy különböző területein, az egészségügyi intézményekben a betegek ellátásához, a betegnyilvántartásokhoz, az orvosi műszerek használatához, illetve vala-

---

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (A letöltés dátuma: 2018. 09. 21.)

[3] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=fr (A letöltés dátuma: 2018. 09. 21.)

[4] 2012. évi CLXVI. törvény, 2. melléklet

[5] Haig Zsolt – Kovács László (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány. Nemzeti Közszolgálati Egyetem. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (A letöltés dátuma: 2018. 09. 21.)

mennyi, fentebb felsorolt alágazatok kezeléséhez elektronikus információs rendszereket is használnak. Azaz a felsorolt adatbázisokat, eszközöket, rendszereket érő bármilyen informatikai támadás a visszaéléseken kívül az adatok jogellenes megszerzéséhez, valamint életet, egészséget veszélyeztető incidensekhez is vezethet.

A kiberbiztonság

Ahogy a világ számos régiója, úgy az Európai Unió és Magyarország is felismerte, hogy a bűnözés egyik legdinamikusabban fejlődő ágát az informatikai rendszereket érő támadások jelentik, amelyek veszélyeztetik a gazdaságot, a társadalmat és nem utolsósorban az állampolgári biztonságot, illetve a nemzet biztonságát. Ezzel párhuzamosan a kritikus infrastruktúra elleni incidensek – így az egészségügyi ágazat és annak alágazatai esetében is –, a működés megzavarása vagy megsemmisítése mind az állampolgárok számára, mind a kormányzat működésében súlyos következményekkel jár.

A fentieket figyelembe véve érthető, hogy a kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése.[6]

A 1139/2013. (III.12) kormányhatározattal hirdették ki Magyarország Kiberbiztonsági Stratégiáját, amely kimondta, hogy a *„kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez”*.[7] A dokumentum leszögezi: Magyarország a jelen és a jövő kihívásaihoz igazodva követelményként rögzíti, hogy a magyar kibertér nyújtson biztonságos és megbízható környezetet:

a) az egyének és közösségek számára a szabad, félelemmentes, a személyes adatok védelmét garantáló kommunikáción keresztül a társadalmi fejlődéshez és integrációhoz,
b) a gazdasági szereplők számára a hatékony, innovatív üzleti megoldások kialakításához,
c) a jövő generációi számára az értékelven alapuló tanuláshoz és az egészséges lelki fejlődést eredményező, sérülésmentes tapasztalatszerzéshez,
d) az elektronikus közigazgatás számára, hozzájárulva az állami szolgáltatások innovatív és előremutató fejlesztéséhez.[8]

---

[6] *Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér.* Elérhető: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (A letöltés dátuma: 2018. 04. 17.)

[7] A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (A letöltés dátuma: 2018. 09. 21.)

[8] 1. melléklet az 1139/2013. (III. 21.) Korm. határozathoz. Magyarország Kiberbiztonsági Stratégiája, 8.

A kibertámadások

Tisztázzuk a kibertámadás, illetve az informatikai rendszerek elleni támadások fogalmát. A kibertámadás – amelynek célja csak a károkozás – lehet kifinomult vagy primitív, attól függően, hogy a támadó milyen kapacitással rendelkezik, illetve mi a célpontja a támadásnak. Precíz támadásokat csak államok vagy nagyon erős bűnözői csoportok indíthatnak.[9] Olyan fenyegetésnek is lehet nevezni a kibertámadást, amely az infokommunikációs rendszerek ellen irányul, és amely az abban tárolt adatokat, információkat vagy a rendszereket alkalmazó személyeket, társaságokat fenyegeti, illetve amelynek célja, hogy a megtámadott rendszerek működését ellehetetlenítse, hozzáférhetetlenné tegye, vagy a rajta tárolt információkat megszerezze, módosítsa.

Az egészségügyi ellátóhálózat, valamint egyéb adatkezelő szerv egészségügyi és személyi adatkezelési szabályozásáról

Az egészségügy kritikus infrastruktúrának minősül, az egészségügyi és személyi adatok megszerzése és felhasználása bűncselekmény, ezek védelme az állam kizárólagos feladata. Az adatok, felhasználhatóságuk széles spektruma miatt, veszélyeztetettek, megszerzésük vagy hozzáférhetetlenné tételük, megváltoztatásuk a betegellátó rendszerben, akár egy sürgősségi beavatkozás során is kockázatot jelenthet, ami téves diagnózist, a beteg nem megfelelő kezelését és akár súlyos egészségkárosodást vagy halált is előidézhet. Ugyanakkor az adatok tárolását és elérését biztosító informatikai rendszeren kívül minden egyéb eszköz is veszélyeztetett lehet, amelyhez valamilyen informatikai rendszer tartozik (például életmentő berendezés, vagy éppen az intézmény áramellátása).

Egészségügyi adatnak minősülnek az 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről alapján:

- azok az információk, amelyek a beteg testi, értelmi- vagy lelkiállapotára, a kóros szenvedélyére, illetőleg a megbetegedésére, elhalálozására vonatkoznak;
- azon adatok, amelyek a beteg gyógykezelésére, ellátására vagy vizsgálata során az orvosi kezelés alatt keletkezett diagnózisokat, leleteket, a kórtörténet leírását, szenvedélybetegségre vonatkozó információt állapítanak meg;
- azon adatok, amelyek a fent említett adatokkal kapcsolatba hozhatók.[10]

[9] Orbók Ákos (2013): A kibertér, mint hadszíntér. Elérhető: http://biztonsagpolitika.hu/publikaciok-2013/orbok-akos-a-kiberter-mint-hadszinter-2013-julius-19 (A letöltés dátuma: 2018. 04. 16.)

[10] 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99700047.TV (A letöltés dátuma: 2018. 04. 16.)

Összességében elmondhatjuk, hogy az egészségügyi intézmények által kezelt információk felölelik a születéstől a halálig az érintettek teljes kórképet, beleértve a fennálló és kezelt betegségeket, egészségügyi problémákat, genetikai adatokat[11] (amelyekből akár az utódok esetleges betegségére is lehet következtetni).

Az egészségügyi adatok különleges adatoknak minősülnek, amelyek kezelését a személyes adatokénál szigorúbb feltételekhez kell kötni, ami különösen érezhető az európai általános adatvédelmi rendelet (a továbbiakban: GDPR) bevezetése után.

Az Európa Tanács Miniszteri Bizottsága 1997-ben ajánlást fogadott el az egészségügyi adatok védelmének legfontosabb alapelveiről, ami által a hazai jogi szabályozásban is teret nyert az egészségügyi és személyazonosító adatok törvényi szintű kezelése.

Orvosi titoktartás

Az orvosi titoktartási kötelezettség már ismert klasszikus szabály. Az egészségügyi ellátásban részt vevő személy a betegnek az ellátás során tudomására jutott egészségügyi és egyéb személyes adatait (személyazonosító adatok) bizalmasan köteles kezelni, és azt csak a jogszabály, hatósági határozat vagy a beteg nyilatkozata által feljogosított személyekkel jogosult közölni.

Álláspontom szerint ma már – volumenében – a problémát nem feltétlenül a verbális adatközlés (a titoktartás megszegése) valósíthatja meg, hanem az egészségügyi informatikai infrastruktúra egyes részeit (eszközeit) ért külső vagy belső támadás, behatolás, amely az egészségügyi adatokat éri, de akár az elektronikus információs rendszer segítségével működő egészségügyi berendezések, gépek működésének megakadályozását, illetve részleges vagy teljes ellehetetlenülését is okozza.

Az egészségügyben alkalmazott informatikai eszközökben tárolt adatok jelentőségére és védelemben részesítésére az egészségügyi és a hozzájuk kapcsolódó személyi adatok kezelésről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak) már a bevezetésében utal: *„Az Országgyűlés – felismerve azt, hogy az egészségügyi adatokat bizalmi jellegük, valamint a számítástechnika széles körű elterjedése miatt fokozott oltalomban kell részesíteni, ugyanakkor ezen adatok kezelése az egészségügyi ellátás során elengedhetetlenül szükséges, az információs önrendelkezési jogról és az információszabadságról szóló törvény rendelkezéseire tekintettel a következő törvényt alkotja.”*[12]

---

[11] A 2018. május 25-én életbe lépő európai általános adatvédelmi rendelet alapján a genetikai adatot olyan, a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő személyes adatként kell meghatározni, amely az érintett személytől vett biológiai minta elemzésének – különösen kromoszómaelemzésnek, illetve a dezoxiribonukleinsav (DNS) vagy a ribonukleinsav (RNS) vizsgálatának, vagy az ezekből nyerhető információkkal megegyező információk kinyerését lehetővé tevő bármilyen más elem vizsgálatának – az eredménye. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://www.adatvedelmirendelet.hu/wp-content/uploads/2016/07/CELEX3A32016R06793AHU3ATXT.pdf (A letöltés dátuma: 2018. 09. 21.)

[12] 1997. évi XLVII. törvény Eüak., bevezetés

Az Eüak. hatálya kiterjed:

a) minden egészségügyi ellátást nyújtó, valamint annak szakmai felügyeletét, ellenőrzését végző szervezetre és természetes személyre (a továbbiakban: egészségügyi ellátóhálózat), valamint minden olyan jogi személyre, jogi személyiséggel nem rendelkező szervezetre és természetes személyre, amely vagy aki egészségügyi és személyazonosító adatot kezel (a továbbiakban: egyéb adatkezelő szerv),
b) minden, az egészségügyi ellátóhálózattal, valamint az egyéb adatkezelő szervvel kapcsolatba került vagy kerülő, illetve annak szolgáltatásait igénybe vevő természetes személyre, függetlenül attól, hogy beteg-e vagy egészséges (a továbbiakban: érintett), valamint
c) az e törvény előírásai szerint kezelt, az érintettre vonatkozó egészségügyi és személyazonosító adatra.[13]

A hivatkozott törvény 3. paragrafusa az egészségügy specifikussága miatt további fogalommeghatározásokat állapít meg, így például az

- *egészségügyi adat:* az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (például magatartás, környezet, foglalkozás).[14]

Az egészségügyi adatokat, tényeket vagy a páciens közli az orvossal, az ápolóval, vagy – amennyiben ezt már nem tudja valamilyen oknál fogva megtenni – más személy (például közeli hozzátartozó, ismerős vagy például baleset esetén rendőr, tűzoltó, tanú) hozza az orvos, intézmény tudomására. Az informatikai rendszereket érő támadások során kiemelten fontosak lehetnek azok az információk, adatok, amelyeket a beteg ellátása vagy a gyógykezelésük során az orvos, az ápoló, az egészségügyi alkalmazott állapít meg vagy észlel a vizsgálatok alkalmával, illetve amelyek a tudomására jutnak az egyéb beavatkozások, vizsgálatok elvégzése alkalmával. Így ide tartoznak például a labor- és különböző egyéb vizsgálatok eredményei, továbbá a betegfelvétel alkalmával megadott olyan adatok, amelyek alkalmasak a visszaélésekre.

A törvény továbbá kimondja:

- *személyazonosító adat:* a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel (a továbbiakban: tajszám) együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására.[15]

Mind az egészségügyi adat, mind a személyazonosító adat, mint „védendő adat" fontos része az orvosi titoktartásnak, a gyógykezeléssel kapcsolatban megismert egyéb adatokkal együtt is, továbbá az egészségügyi dokumentációban feljegyzés, nyilvántartás vagy bár-

[13] 1997. évi XLVII. törvény Eüak. 2. § a)–c) pont
[14] 1997. évi XLVII. törvény Eüak. 3. § a) pont
[15] 1997. évi XLVII. törvény Eüak. 3. § b) pont

milyen más módon rögzített adatokként is megjelennek az ellátóhálózatban és a törvény hatálya alá tartozó egyéb jogosultnál.

Az egészségügyi ágazatban az egészségügyi és személyazonosító adat kezelésének hatékony védelmét biztosíthatja a bevezetésre kerülő Elektronikus Egészségügyi Szolgáltató Tér (a továbbiakban: EESZT). Ennek az informatikai rendszernek a kiépítése a kormányzat részéről európai uniós támogatással történt (TIOP-2.3.2 / KMOP-4.3.3 projekt A „Nemzeti Egészségügyi Informatikai [e-Health] Rendszer – Elektronikus közhiteles nyilvántartások és ágazati portál fejlesztése" című projekt néven).

Az EESZT-rendszer által egységes informatikai környezetben, a legmagasabb adat- és kibervédelemmel kívánják biztosítani az egészségügyi ágazaton belüli hatékony kommunikációt.

Az EESZT jogintézményét az 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről III/A. fejezetet (35/A–35/N. §) módosító 2015. CCXXIV. törvény 11. §-a iktatta be. E szerint a *„Kormány által rendeletben kijelölt szerv működtetőként ellátja az EESZT, mint az egészségügyi ellátóhálózat informatikai rendszereinek együttműködését biztosító, az e törvényben vagy e törvény felhatalmazása alapján kiadott miniszteri rendeletben meghatározott központi elektronikus szolgáltatásokat megvalósító egészségügyi ágazati informatikai rendszer működtetésével kapcsolatos feladatokat."*[16]

A hivatkozott törvény meghatározta az EESZT-hez informatikai rendszere útján csatlakozásra kötelezetteket:

a) az egészségügyi szolgáltatás nyújtására az egészségügyi államigazgatási szerv által kiadott működési engedély alapján jogosult egészségügyi szolgáltató, aki finanszírozási jelentés benyújtására vagy elektronikus adatszolgáltatásra kötelezett,
b) a gyógyszertár,
c) az állami mentőszolgálat,
d) a miniszter által rendeletben meghatározott államigazgatási szerv és egyéb szervezet.[17]

A törvényben felhatalmazást kapott a miniszter (EMMI), hogy részletes szabályok kerüljenek kidolgozásra az egészségügyi adatok kezelésének, valamint a 15–16/A. § *(Közegészségügyi, járványügyi és munka-egészségügyi célból történő adatkezelés, illetve Népegészségügyi célból történő adatkezelés)* és a 24. § *(Adattovábbítás az egészségügyi ellátóhálózaton kívüli szerv megkeresésére bűncselekmény, gyerekbántalmazás esetén)* szerinti adattovábbítás részletes előírásainak, továbbá a 30. § szerinti kötelező nyilvántartások *(Az egészségügyi és személyazonosító adatok nyilvántartása)* vezetésének szabályai[18] vonatkozásában. Az EESZT működéséről jelenleg a véleményezésre közzétett EMMI-rendelettervezet ismert, amely részletesen felsorolja a rendszerhez történő csatlakozás feltételeit és rendjét, a rendszerben történő felhasználó-azonosítás követelményeit, az adatszolgáltatásra vonatkozó általános szabályokat és az EESZT-szolgáltatásnak leállása esetére vonatkozó szabályokat.

---

[16] 2015. évi CCXXIV. törvény az egyes egészségügyi és egészségbiztosítási tárgyú törvények módosításáról, 11. §. Elérhető: https://mkogy.jogtar.hu/jogszabaly?docid=A1500224.TV (A letöltés dátuma: 2018. 09. 21.)

[17] 1997. évi XLVII. törvény Eüak. 35. § (1) bekezdés

[18] 1997. évi XLVII. törvény Eüak. 15–16/A. §, 24. §, 30. §

A jogi szabályozás és eszközrendszerének kiépítése az egészségügy kritikus infrastruktúrává minősítését igazolja.

Miért veszélyesek az egészségügyet érő kibertámadások?

Az (egészségügyi) adat a 21. században értékesebb, mint az arany.

Az ESET által végzett, egészségügyi adatlopásokkal kapcsolatos felmérés szerint:

- Az egészségügyi adatlopások elszenvedőinek 30%-a észre sem veszi, hogy áldozat lett.
- Átlagosan 3 hónap telik el, amíg felfedezik, hogy egészségügyi adattal kapcsolatos visszaélés történt.
- Átlagosan 3,7 millió forintos számla keletkezik, amikor a csalók a nevünkben különböző műtéteket, orvosi eszközöket, kivizsgálásokat vesznek igénybe az ellopott személyazonosságunk segítségével.
- Átlagosan 200 órányi ügyintézéssel tölti az idejét az adatlopás áldozata, amíg a hatóságok előtt sikerül tisztáznia magát.
- Csak minden tizedik áldozat érzi úgy, hogy az őt ért, orvosi adatokkal kapcsolatos visszaélés számára megnyugtatóan zárul.
- A megkérdezettek 48%-a váltana egészségügyi szolgáltatót, ha elvesznének orvosi adatai vagy visszaélnének azokkal.

Büntetőjogi relevancia

Az egészségügyi intézményekben, kórházakban kezelt adatok jogosulatlan megismerését a hatályos Büntető Törvénykönyv (a továbbiakban: Btk.) 423. §-a az információs rendszer vagy adat megsértésének, valamint a 219. §-a a visszaélés személyes adattal tényállásába ütközteti.[19] Kiemelendő, hogy az egészségügyi intézményeket érő informatikai támadások irányulhatnak az intézmény adatainak (*ergo* a betegekre vonatkozó személyes és egészségügyi adatoknak) a megszerzésére, valamint az adathoz való hozzáférés megakadályozására, illetve az adatok megváltoztatására, továbbá az informatikai rendszerrel vagy berendezéssel működtethető orvosi vagy diagnosztikai berendezések működésének megakadályozására, zavarására.

A számítástechnikai bűnözés hagyományos szabálysértéseket (például csalás, hamisítás és személyazonosság-lopás), tartalmakhoz kapcsolódó szabálysértéseket (például gyermekpornográfia internetes terjesztése vagy fajgyűlöletre uszítás) és csak számítógépekre és információs rendszerekre korlátozódó szabálysértéseket (például információs rendszerek elleni támadások, hozzáférés megtagadása vagy rosszindulatú szoftverek) is magában foglal.[20] Több alkalommal is nyilvánosságot kapott, hogy az Amerikai Egyesült Államok vagy épp hazánk egyik kórházában az információs rendszerhez történő hozzáfé-

[19] 2012. évi C. törvény a Büntető Törvénykönyvről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1200100.TV (A letöltés dátuma: 2018. 09. 21.)

[20] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér. Elérhető: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (A letöltés dátuma: 2018. 04. 17.)

rést megakadályozták, és az elkövetők meghatározott mennyiségű bitcoin megfizetése után engedélyezték a blokkolt adatokhoz történő hozzáférést.[21]

Jelenleg a korlátozott adathozzáférést biztosítja, hogy az ellátóhálózatban a betegek gyógykezelése során „megjelenők" – beleértve az egyetemi hallgatókat és oktatókat is – beosztástól, státusztól függően különböző hozzáférési szintekkel rendelkeznek. Az egészségügyi rendszer az úgynevezett MEDSOL-t használja (e-MedSolution), ez egy *integrált egészségügyi informatikai rendszer,* amelynek célja, hogy magyar nyelvű felületen, egyetlen alkalmazáson belül biztosítsa a fekvő- és a járóbeteg-ellátással kapcsolatosan felmerülő funkcionalitásokat, kiszolgálja a diagnosztikai területek igényeit, és támogassa a gyógyszerellátást.

Az e-MedSolution funkcionális szempontból a betegadminisztrációtól kezdve a vizsgálatok, beavatkozások elektronikus kérésén és leletezésén keresztül az ütemezési, statisztikai funkciókkal bezárólag minden olyan kórházi munkafolyamatot elvégez, amelyet célszerű elektronikus rendszerrel támogatni.[22]

Az informatikai rendszer célja, hogy biztosítsa a felhasználóknak a „határnélküliséget intézményen belül és kívül". PDA-n, tablet PC-n, bluetooth és/vagy GPRS-technológiákkal biztosítja a felhasználók számára az életmentő adatok azonnali elérhetőségét.[23] Ezen rendszer lényege tehát a folyamatos rendelkezésre állás, valamint vészhelyzetben a szükséges adatok tér- és időkorlát nélküli elérése, valamint a betegenkénti nyilvántartások egységesítése, amelyhez csak a jogosultak férnek hozzá.

A személyes adattal való visszaélés

Az egészségügyi intézményeket érő támadások esetében az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. tv. (továbbiakban: Infotv.) 3. § 2. pontja értelmében személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret, valamint az adatból levonható, az érintettre vonatkozó következtetés.[24]

A bűncselekmény elkövetési magatartásai a jogosulatlan vagy a céltól eltérő adatkezelés, az adatok biztonságát szolgáló intézkedés elmulasztása, valamint a tájékoztatási kötelezettség megszegése.

Az adatok biztonságát szolgáló intézkedés elmulasztásával kapcsolatban az adatbiztonság követelményét az Infotv. 7. §-a határozza meg: az adatkezelő – az egészségügyi intézmények esetében, illetve tevékenységi körében az adatfeldolgozó – köteles gondos-

---

[21] Szűcs Péter (2016): Zsarolóvírus ejtette túszul a kórházi rendszert. IT Café. Elérhető: https://itcafe.hu/hir/zsarolovirus_ejtette_tuszul_a_korhazi_rendszert.html (A letöltés dátuma: 2018. 04. 17.)

[22] *Egészségügyi rendszer szolgáltatások* (é. n.). Pécsi Tudományegyetem, Kancellária. Elérhető: http://kancellaria.pte.hu/szervezet/egeszsegugyi%20rendszerek (A letöltés dátuma: 2018. 09. 21.)

[23] *E-MedSolution – Kórházi információs rendszer* (é. n.). T-Systems. Elérhető: http://www.t-systems.hu/megoldasok/alkalmazasok/alkalmazascsomagok/egeszsegugyi-megoldasok/e-medsolution (A letöltés dátuma: 2018. 09. 21.)

[24] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.). Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1100112.TV (A letöltés dátuma: 2018. 09. 21.)

kodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Infotv., illetve az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.[25] Az adatokat megfelelő intézkedésekkel védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az adat biztonságát szolgáló intézkedés jellege az adat fajtájától függ. Az adatkezelők, illetve a személyes adatfajták sokfélesége miatt az ilyen intézkedések kimerítő meghatározása nem lehetséges.

A bűncselekmény csak jelentős érdeksérelem okozásával vagy haszonszerzési céllal követhető el. A jelentős érdeksérelem okozásával megvalósítható személyes adattal visszaélés materiális deliktum, amely csak az eredmény bekövetkeztével válik befejezetté. Csak szándékosan elkövethető bűncselekmény, amelyet adatkezeléssel, illetve adatok feldolgozásával foglalkozó személy követhet el. Az adatok biztonságát szolgáló intézkedés elmulasztásával, illetve a tájékoztatási kötelezettség megszegésével megvalósítható bűncselekmény, amelynek elkövetője olyan személy lehet, akit ilyen kötelezettség terhel.

Súlyosabban büntetendő, aki a személyes adattal visszaélést különleges adatra követi el. A különleges személyes adat fogalma helyett a különleges adat fogalma az információs önrendelkezési jogról szóló törvény 3. § 3. pontjában használt terminológia, mivel a különleges adat szükségszerűen személyes adatnak számít.[26] Ennek értelmében különleges adat a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, a bűnügyi személyes adat. Minősített esetet képez, ha a személyes adattal visszaélést hivatalos személyként vagy közmegbízatás felhasználásával követik el.

Az információs rendszer vagy adat megsértése

Az Európai Parlament és az Európai Unió Tanácsa 2013 augusztusában elfogadta a 2005/222/IB tanácsi kerethatározat felváltásáról és az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelvet, amelynek célja, *„hogy a bűncselekmények tényállására és a vonatkozó szankciókra vonatkozó minimumszabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén”*.[27]

Az irányelv kiemeli a botneteket, és kiemeli a személyazonossághoz kapcsolódó bűncselekményeket, valamint azokat a számítástechnikai környezetben elkövetett deliktumokat, amelyeket alkalmazottak követnek el. Az irányelv továbbá a bűnszervezetben elkövetett kiberbűncselekményeket súlyosabb szankciókkal kívánja büntetni.

A hazai szabályozásban a Btk. 423. §-a – az információs rendszer vagy adat megsértésének tényállása – az, amely a 2013/40/EU irányelv céljait tükrözi, de sajnos nem az

[25] 2011. évi CXII. törvény Infotv. 7. §

[26] 2011. évi CXII. törvény Infotv. 3. § 3. pont

[27] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=fr (A letöltés dátuma: 2018. 09. 21.)

általa előírt kívánalmaknak megfelelően.[28] Így többek között nem minősül súlyosabbnak sem a bűnszervezetben, sem az alkalmazotti minőségben elkövetett, informatikai rendszer felhasználásával elkövetett jogellenes cselekmény.

Az információs rendszer vagy adat megsértését az követi el, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, és vétség miatt két évig terjedő szabadságvesztéssel büntetendő. Azt is szankcionálja a törvény, ha valaki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz. Az elkövetési magatartás az információs rendszer működésének akadályozása, valamint az abban tárolt adat törlése, hozzáférhetetlenné tétele, valamint megváltozása.

Ahogy Nagy Zoltán *Az új számítógépes bűncselekményekről* című tanulmányában kiemeli, szükséges az, hogy az informatikai eszköz vagy az elektronikus információs rendszer

- biztonsági megoldásokkal *védett legyen,* és
- a védelem *aktív legyen,* azaz szükséges legyen a hálózat eléréséhez jelszavak, kódok, más azonosítók használata. Ezek konjunktív feltételek.
- Az elkövető aktív védelemmel ellátott számítógépbe vagy védett hálózatba jogosulatlanul lép be akkor, ha
  - a számítógép vagy hálózat biztonsági rendszerének hiányosságait kihasználva lép be jogosulatlanul, vagy
  - a jogosult felhasználónevével (belépési kódjával), jelszavával vagy a belépést biztosító adat birtokában lép be.[29]

Az Infotv. 3. § 10. pontja szerint adatkezelésnek minősül az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (például ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.[30]

Az egészségügyi intézményekben tárolt adatok is szenzibilis adatoknak minősíthetők, nemcsak azért, mert személyes adatokat lehet megismerni, hanem mert a betegek adatai, a betegségük, egészségügyi állapotuk, az előírt gyógykezelések, gyógyszerek megismerése, hozzáférése többek között visszaélésre adhat lehetőséget, valamint az adatok megváltoztatása, törlése súlyos következményekkel járhat a betegekre nézve.[31]

---

[28] 2012. évi C. törvény a Büntető Törvénykönyvről 423. §

[29] Nagy Zoltán (é. n.): *Az új számítógépes bűncselekményekről (háttér és elemzés).* Kézirat. Elérhető: http://www.mabie.hu/index.php/cikkek-tanulmanyok/95-dr-nagy-zoltan-az-uj-szamitogepes-buncselekmenyekrol-hatter-es-elemzes (A letöltés dátuma: 2018. 09. 21.)

[30] 2011. évi CXII. törvény Infotv. 3. § 10. pont

[31] Az 1997. évi XLVII. törvény 3.§ (1) bekezdés e) pontja szerint *e) egészségügyi dokumentáció:* a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

Az elkövetői magatartás a törvény szerint az információs rendszer vagy adat megsértéséhez és az információs rendszer felhasználásával elkövetett csalás elkövetéséhez szükséges (belépési) jelszó vagy számítástechnikai program készítése, annak átadása vagy hozzáférhetővé tétele, megszerzése, forgalomba hozatala, illetve az ezekre vonatkozó gazdasági, műszaki, szervezési ismeretek mások rendelkezésére bocsátásával valósul meg. A jogellenes cselekményt csak szándékosan lehet elkövetni, amely a Btk. 375. §-ában vagy a 423. §-ában meghatározott bűncselekményt, azaz az információs rendszer felhasználásával elkövetett csalást, vagy az információs rendszer vagy adat megsértésének tényállását valósítja meg.

Abban az esetben tehát, ha a már említett informatikai incidensek érik a rendszert, az elkövetési magatartás lehet:

- olyan program megírása (beletartoznak a vírusok is), amellyel az információs rendszer – e-Medsol – védelmére szolgáló jelszó készítését vagy annak felülírását követően jogosulatlanul lépnek be a rendszerbe;
- a jelszó átadása az adott számítástechnikai rendszer vonatkozásában a program készítőjétől különböző személynek a birtokba adása. Közömbös, hogy ez ingyenesen, visszterhesen, megtévesztéssel vagy más módon történt. A megszerzés módja legfeljebb büntetéskiszabási szempontként értékelhető;
- a hozzáférhetővé tétel a program, a jelszó vagy az adat eljuttatása valamilyen módon, aktív vagy passzív magatartással (több munkatárs által használt informatikai eszközök esetében gyakori, hogy a felhasználók a belépési kódjukat és/vagy jelszavukat egy papírdarabra felírva és azt látható helyen hagyva/ragasztva teszik mások számára hozzáférhetővé). Előfordulhat az is, hogy a jogellenesen megszerzett kódokat pénzért teszik elérhetővé weboldalakon;
- a megszerzés a jelszó vagy program feletti rendelkezés lehetőségét jelenti, a program hordozójának birtokbavétele, ami megvalósulhat nemcsak fizikálisan – főleg a programok, jelszavak immateriális tulajdonságát is figyelembe véve –, hanem a tudomásszerzés által is;
- forgalomba hozatal, amikor több személy számára hozzáférhetővé teszi e programot, akár úgy, hogy saját maga juttatja el a felhasználóknak, akár úgy, hogy egyetlen személynek adja át, ám abban a tudatban, hogy az a személy több személynek adja tovább. A forgalomba hozatal történhet pénzért vagy más ellenszolgáltatásért, de akár ingyenesen is.

Összefoglalás

Életünk során legalább két alkalommal biztosan kapcsolatba kerülünk valamelyik egészségügyi intézménnyel, s ekkor a személyes és egészségügyi adataink mások számára is megismerhetőek lesznek. Az illetéktelenek a megszerzett információkkal visszaélhetnek, nyilvánossá tehetik, valamint – mint egy tárgyat – adhatják-vehetik, és ennek következtében akár a magánszféránkba is betekintést nyerhetnek, vagy akár árucikként értékesíthetik az adatokat egymás között a gyógyszergyárak. Az elkövetők nem minden esetben hackerek és nem minden esetben szándékosan követik el a bűncselekményt, ugyanakkor a hanyagul

kezelt jelszavak, adatok, kódok, valamint az informatikai biztonság ismeretének hiánya, hiányossága jelentős veszélyforrás lehet.

Ahhoz, hogy ezeket a szenzitív adatokat megfelelően kezeljék, tárolják, szükséges az adatkezelőket – az orvosokat, egészségügyi dolgozókat – megfelelő képzésben, folyamatos oktatásban részesíteni.

Felhasznált irodalom

Egészségügyi rendszer szolgáltatások (é. n.). Pécsi Tudományegyetem, Kancellária. Elérhető: http://kancellaria.pte.hu/szervezet/egeszsegugyi%20rendszerek (A letöltés dátuma: 2018. 09. 21.)

E-MedSolution – Kórházi információs rendszer (é. n.). T-Systems. Elérhető: http://www.t-systems.hu/megoldasok/alkalmazasok/alkalmazascsomagok/egeszsegugyi-megoldasok/e-medsolution (A letöltés dátuma: 2018. 09. 21.)

Haig Zsolt – Kovács László (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány. Nemzeti Közszolgálati Egyetem. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (A letöltés dátuma: 2018. 09. 21.)

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér. Elérhető: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (A letöltés dátuma: 2018. 04. 17.)

Nagy Zoltán (é. n.): *Az új számítógépes bűncselekményekről (háttér és elemzés).* Kézirat. Elérhető: http://www.mabie.hu/index.php/cikkek-tanulmanyok/95-dr-nagy-zoltan-az-uj-szamitogepes-buncselekmenyekrol-hatter-es-elemzes (A letöltés dátuma: 2018. 09. 21.)

Orbók Ákos (2013): A kibertér, mint hadszíntér. Elérhető: http://biztonsagpolitika.hu/publikaciok-2013/orbok-akos-a-kiberter-mint-hadszinter-2013-julius-19 (A letöltés dátuma: 2018. 04. 16.)

Szűcs Péter (2016): Zsarolóvírus ejtette túszul a kórházi rendszert. IT Café. Elérhető: https://itcafe.hu/hir/zsarolovirus_ejtette_tuszul_a_korhazi_rendszert.html (A letöltés dátuma: 2018. 04. 17.)

Hivatkozott jogszabályok

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99700047.TV (A letöltés dátuma: 2018. 04. 16.)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.). Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1100112.TV (A letöltés dátuma: 2018. 09. 21.)

2012. évi C. törvény a Büntető Törvénykönyvről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1200100.TV (A letöltés dátuma: 2018. 09. 21.)

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (A letöltés dátuma: 2018. 09. 21.)

2015. évi CCXXIV. törvény az egyes egészségügyi és egészségbiztosítási tárgyú törvények módosításáról, 11. §. Elérhető: https://mkogy.jogtar.hu/jogszabaly?docid=A1500224.TV (A letöltés dátuma: 2018. 09. 21.)

A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (A letöltés dátuma: 2018. 09. 21.)

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Elérhető: https://www.adatvedelmirendelet.hu/wp-content/uploads/2016/07/CELEX3A32016R06793AHU3ATXT.pdf (A letöltés dátuma: 2018. 09. 21.)

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=fr (A letöltés dátuma: 2018. 09. 21.)

Ajánlott irodalom

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A0400079.TV&searchUrl=/gyorskereso%3Fpagenum%3D5 (A letöltés dátuma: 2018. 09. 21.)

Gyaraki Réka (2015): Számítógépes bűncselekmények és az ellenük való védekezés. In Christián László *szerk.*: *Információvédelem.* Budapest, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar. 175–189.

A KONFERENCIA TÁMOGATÓI

A Dialóg Campus Kiadó a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu
www.uni-nke.hu
1083 Budapest, Ludovika tér 2.
Telefon: 06 (30) 426 6116
E-mail: kiado@uni-nke.hu

A kiadásért felel: Petró Ildikó ügyvezető
Felelős szerkesztő: Inzsöl Kata
Tördelőszerkesztés: Corrigendum Kft.
Nyomdai kivitelezés: Stanctechnik Digital Kft.
Felelős vezető: Hermann Nikolett

ISBN 978-615-5920-89-9

Dialóg Campus