infojegyzet

ORSZÁGGYŰLÉS HIVATALA
KÖZGYŰJTEMÉNYI ÉS KÖZMŰVELŐDÉSI IGAZGATÓSÁG
KÉPVISELŐI INFORMÁCIÓS SZOLGÁLAT

2016/44.
2016. szeptember 29.

KIBERFENYEGETÉSEK ÉS KIBERVÉDELEM

A kibertérből származó fenyegetések kivédésére 2016 nyarán a NATO és az Európai Unió két olyan alapvető fontosságú döntést hozott, amelyek a közeljövőben maghatározzák a kibervédelem irányait. Az Infojegyzet ezek kapcsán a kiberfenyegetések és kibervédelem általános területét kívánja bemutatni.

- **„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.” (Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2012)**

- **A kibertér általános jellemzője, hogy globális, folyamatosan bővülő virtuális hálózat, amely decentralizáltságából fakadóan egyedül egyetlen állam által sem szabályozható. Ennek következtében jelentős biztonsági kockázatot jelent minden egyes tagja számára. A virtuális tér nyújtotta lehetőségek ugyanis új bűnözői és hadviselési formák születéséhez vezettek.**

- **A Világgazdasági Fórum éves globális kockázati rangsorában a hagyományos veszélyek – úgymint a háborús konfliktusok, terrorizmus, természeti katasztrófák – mellett a kibertér fenyegetései egyre előrébb sorolódnak. 2014-ben a kibertámadások az 5., 2015-ben a 10. helyen szerepeltek. A tavalyi évben önálló kategóriaként felkerült a top 10-be az adatlopás és a kiberkémkedés kockázata is. (Mapping Global Risk, 2015)**

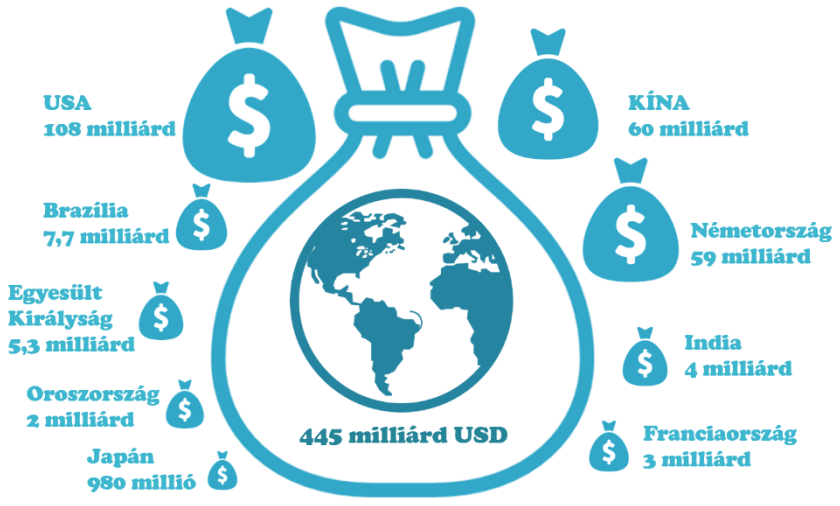
Az infokommunikációs eszközök és szolgáltatások rendkívüli fejlődésével párhuzamban, napjainkban egyre gyakoribbak mind az állami, mind a civil szektort érintő kibertámadások.

Az elmúlt években több nemzetközi szervezet is ajánlásokat, stratégiákat és norma-kereteket fogalmazott meg annak érdekében, hogy a nemzetállamok és a társadalmi-gazdasági szereplők kialakíthassák egyéni kibervédelmi struktúrájukat és lefektessék azokat a minimális feltételeket, melyek a kibertérben való biztonsághoz léthez elengedhetetlenek (ld. többek között: NATO kibervédelmi központja, 2013; az ENSZ Nemzetközi Távközlési Egyesülete (ITU, 2012, 2014), valamint az EU hálózatbiztonságért felelős ügynöksége (ENISA, 2012, 2016).

Mindezek három alapvető és egymásra épülő biztonsági szituációra hívják fel a figyelmet:

- az informatikai és kommunikációs hálózatok minden tagja – legyen az nemzetközi, állami vagy civil szereplő – potenciális áldozata lehet a kibertérből érkező rosszindulatú támadásoknak;
- a kibertámadásoknak komoly nemzetbiztonsági, gazdasági, illetve a társadalom mindennapi életére is veszélyt jelentő következményei lehetnek;
- a veszélyek kivédése a kibertérbe kapcsolódó nemzetközi és nemzetállami, valamint egyéni felhasználói szinten is feladatot jelent a szereplők számára.

A kiberbűnözés által okozott kár a világgazdaságban és egyes országokban, 2014.



Forrás: Infoszolg/McAffee, 2014, Allianz, 2015. Piktogrammok: www.flaticon.com

A KIBERFENYEGETÉSEK TRENDJEI

Az infokommunikációs rendszerek elleni kibertámadások (ld. Cyber Attack – NATO cyber definitions) arra irányulnak, hogy megzavarják vagy gátolják a megtámadott rendszer működését, illetve hogy megszerezzék vagy módosítsák annak adatait. A támadások többségét politikai és vallási aktivisták (ld. „hacktivizmus"), gazdasági-bűnözői csoportok, terrorista szervezetek, illetve egyes államok titkosszolgálatai követik el.

Gazdasági következmények

A kibertámadások gazdasági vetületét vizsgálva: a kiberbűnözés **2014-ben átlagosan 445 milliárd dollár** veszteséget okozott a világgazdaságban, de egyes becslések szerint a kár **meghaladhatja az évi 575 milliárd dollárt** is. (McAffe, 2014.) A világ eddigi legnagyobb bankrablásaként emlegetett akcióját ugyancsak kibertámadások sorozatával hajtották végre. A Carbanak-csoport 2015. évi felfedezéséig két év alatt 30 ország 100 pénzügyi intézetétől több mint egy milliárd dollárt rabolt el.

További jelentős károkat okoznak a cégeknek a **célzott adatlopások** is. Az eddig ismert legnagyobb adatlopásra 2015 februárjában derült fény, melynek során az Anthem amerikai egészségbiztosító cég rendszerének feltörésével több, mint 80 millió ügyfél szenzitív adatát tulajdonították el. A Symantec jelentése szerint az akciót elkövető csoport 2012 óta több más ipari és kormányzati szereplő infokommunikációs rendszereit is megtámadta.

Kritikus infrastruktúrák elleni támadások

A kibertámadások kockázatainak vizsgálata során kiemelhető, hogy 2014-ben az amerikai államok létfontosságú infrastruktúráit érő támadások jelentős növekedést mutattak (OAS-Trendmicro, 2015). A hálózati incidensek tekintetében 53 százalékuk növekményről számolt be, 43 százalékukuk észlelt célzott támadást. Jelentéseik szerint az incidensek leginkább a kormányzati és az energetikai szektort érintették, de növekvő tendenciát észleltek a kommunikációs, a gazdasági és a pénzügyi szférában is.

Az állami infrastruktúrákat ért támadások közül a közelmúltból kiemelhető a lengyel nemzeti légitársaság, az ukrán elektronikai hálózat, illetve a kijevi nemzetközi repülőtér elleni – feltételezett orosz – támadás, de kártékony szoftvert fedeztek fel tavaly egy németországi atomerőmű informatikai rendszerében is.

Kormányok és állami intézmények elleni támadások

Egyes államok kibervédelmi szervei (pl. Egyesült Királyság - UK-Gov Cert, 2015; Németország – BSI, 2015**) növekvő kiberkémkedési aktivitásra hívják fel a figyelmet**. A német szövetségi kormány illetékes szerve szerint egyes titkosszolgálatok részéről az állami intézményeket átlagosan két naponta érik célzott támadások. Az elmúlt évben ilyen volt a Bundestag hálózatát ért – feltételezett orosz – támadás, de további hasonló incidensek érték többek között Svájc állami haditechnikai vállalatát, a Fehér Házat, a Pentagont, illetve az Egyesült Államok személyzeti hivatalát is, melynek során több mint 21 millió alkalmazott – köztük a titkosszolgálatok tagjainak – szenzitív adatait lopták el.

A kormányok mindezek mellett rendszeresen áldozatul esnek az úgynevezett **túlterheléses (DoS) és elosztott szolgáltatásmegtagadásos** (DDoS) támadásoknak is, melyek napokra megbéníthatják weboldalaikat. Ilyen támadásnak esett áldozatul az elmúlt időszakban a finn védelmi minisztérium, az ír kormányzati oldalak egy része, a magyar kormány, legutóbb pedig a riói olimpia nyitónapján több brazil kormányzati honlap is.

A vázolt tendenciákat az ENISA 2016 januári jelentése is alátámasztja. E szerint többek között **a kiberkémkedés, a káros szoftverek, a web-alapú és túlterheléses támadások trendjei** – hasonlóan a 2014-es évhez – **2015-ben tovább növekedtek**.

A NATO és a kibervédelem

A NATO 2007 óta – az Észtország elleni kibertámadást követően – fordít kiemelt figyelmet a kibervédelem és kiberhadviselés területére. 2012-ben a kibervédelem bekerült a szövetség védelmi tervezési folyamatába, 2013-ban pedig létrejött a NATO-hálózatok kibervédelmét ellátó képesség (NATO Computer Incidense Response Capability).

A 2014. évi walesi, illetve a 2016. évi varsói csúcstalálkozó további eredményeket hozott e területen. **A walesi csúcson** a szövetségesek a **kibervédelem területét beemelték a NATO kollektív védelmi feladatai közé**, kiemelt szakpolitikát fogadtak el, egyben deklarálták a NATO kibervédelmi képességeinek fejlesztési célkitűzéseit is (Wales Summit Declaration, 72., 73.). Ezt követően az idei **varsói csúcs záródokumentumában** (Warsaw Summit Communiqué, 70-71.) **az operatív hadviselés területét kiterjesztették a kibertérre**. Elemzések szerint ezzel lehetővé vált, hogy a NATO egy tagországa elleni kibertámadást a szövetség egésze elleni támadásnak tekinthessen és válaszlépéseket tehessen.

Kibervédelem az Európai Unióban

A felmérések szerint az EU lakosságának átlagosan 63 százaléka használja mindennapi szinten otthonában az internetet és 47 százaléka legalább egyszer észlelt már rendszerében káros szoftvert. Ennek ellenére az uniós lakosságnak átlagosan csak 31százaléka használ online felületeken különböző jelszavakat, 27 százaléka cseréli jelszavait rendszeresen és 61 százaléka telepített antivírus-programot készülékére (Eurobarometer, 423/2015.).

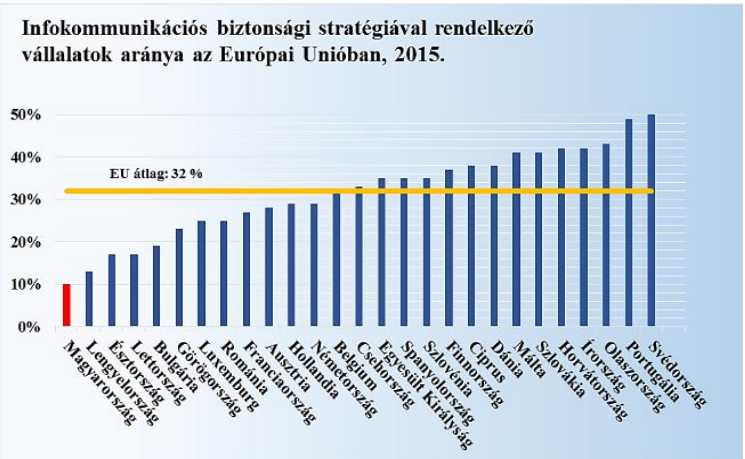
A tagállamok vállalati szektorára vonatkozó elemzés (Eurostat, 2015) szerint 2015-ben az EU vállalatainak átlagosan csak 32 százaléka rendelkezett infokommunikációs biztonsági stratégiával.

Az infokommunikációs hálózatok egységes védelmének kialakítása, a kiberbűnözés visszaszorítása, egyben pedig az EU-állampolgárok biztonsági ismereteinek fejlesztése céljából született meg 2013-ban az Európai Unió kiberbiztonsági stratégiája, az EUROPOL keretében a kiberbűnözés elleni központ, valamint az idén júliusban elfogadott ún. hálózat- és információbiztonsági irányelv (2016/1148).

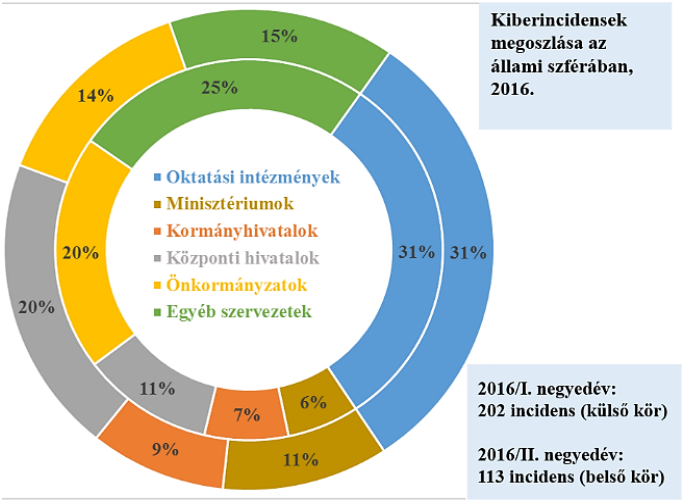
Az irányelv az első átfogó uniós szabályozás, amely közösségi és nemzeti szinteken egyaránt meghatározza a kibervédelem kialakítandó intézményi rendszerét. A jogszabály azért is kiemelkedő fontosságú, mert bár Bulgária, Görögország és Svédország kivételével minden tagállam rendelkezik kibervédelmi stratégiával és számítógép-incidenskezelő szervezetekkel, ezek célrendszere és hatékonysága korántsem egységes, ami közvetve az unió infokommunikációs hálózatait is veszélyezteti.

Az irányelv többek között

- tagállami szinten előírja minimum egy – meghatározott feladatkörű – számítógép-biztonsági incidenskezelő csoport (Computer Security Incident Resoponse Team, CSIRT) felállítását,
- szigorú biztonsági előírásokat és incidensbejelentési kötelezettséget ír elő a társadalom és a gazdaság számára létfontosságú infrastruktúrák, illetve a digitális szolgáltatásokat nyújtó vállalatok számára;
- közösségi szintű szervezetet hoz létre a tagállamok kompetens hatóságai és CSIRT-szervei közötti együttműködésre.



Forrás: Infoszolg / Eurostat



Forrás: Infoszolg/NKI adatszolgáltatás

MAGYARORSZÁG KIBERVÉDELME

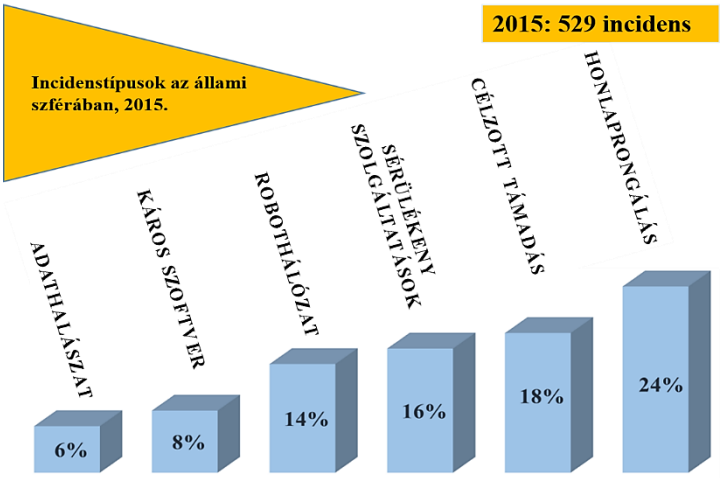
Az EU és a NATO stratégiaalkotási folyamatába illeszkedve a Kormány 2013-ban elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiáját (1139/2013. (III. 21.) Korm. határozat), majd az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.) is, melynek végrehajtása során kialakult az információbiztonság magyarországi szervezeti rendszere.

2015-ben, az Ibtv. módosításával a korábbi széttagolt intézményi rendszer központosításra került. A Nemzetbiztonsági Szolgálatok alárendeltségében létrejött a Nemzeti Kibervédelmi Intézet, melyen belül három szervezeti egység különül el a tevékenységüknek megfelelően:

- a Nemzeti Elektronikus Információbiztonsági Hatóság,
- a Kormányzati Eseménykezelő Központ (az ún. Gov-CERT)
- valamint a Biztonságirányítási és Sérülékenység vizsgálati terület.

Mindezek mellett a honvédelmi terület és a létfontosságú infrastruktúrák infokommunikációs rendszereinek védelméért, valamint a kiberbűnözés elleni küzdelemért külön szervezetek felelősek, de további intézmények (NIIF-CERT; HUN-CERT) védik a civil szféra egyes ágazatainak tagjait is.

A 2013-ban kialakult állami kibervédelmi rendszer alapján az ITU 2014-es kiberbiztonsági rangsorában Magyarországot globálisan a 6. helyre, az európai országok rangsorában pedig a 3. helyre sorolta.



Forrás: Infoszolg/NKI adatszolgáltatás

Források:

- A kiberbiztonság javítása az Európai Unióban – Európai Unió Tanácsa honlapja
- Az Európai Hálózat – és Információbiztonsági Ügynökség honlapja
- A NATO honlapjaA Kormányzati Eseménykezelő Központ honlapja
- Report on Cybersecurity and Critical Infrastructure in the Americas – OAS-Trendmicro, 2015.
- Net Losses: Estimating the Global Cost of Cybercrime – McAffee, 2014
- A Nemzeti Kibervédelmi Intézet adatszolgáltatása

Készítette: Müller Tamás
Képviselői Információs Szolgálat
E-mail: infoszolg@parlament.hu
infoszolg
Internet: www.parlament.hu/infoszolg
Intranet: intra.parlament.hu/infoszolg/
Tel.: (1) 441-4529; (1) 441-6486