DOI: 10.38146/BSZ.2021.12.10

Böröcz Miklós

Az európai IT-biztonság jelenlegi kihívásai

Current challenges for IT security in Europe

Absztrakt

Egy 2020. december 11-én publikált sajtóhír (URL1) nagy visszhangot keltett az információs technológia (IT[1]) világában. Ebben Alaa Abdulridha írta le, hogyan talált komoly sebezhetőségeket a Facebook subdomainjaiban[2]. Mindez azért történt meg, mert a COVID-19 vírus miatti távmunka alatt sok szabadideje maradt, amit „hasznosan" kívánt eltölteni. Érdekesség, hogy a sajtóhírt olvasva a cikkben megjelölt Twitter hivatkozásra (URL2) kattintva egyből üzenetet kaptam, miszerint illetéktelenek hozzáfértek az általam használt fiókhoz, így jelszómódosítást javasoltak. Mindez elegendő motivációt adott számomra ahhoz, hogy a témát mélyrehatóbban kezdjem el vizsgálni.

Kulcsszavak: egységes digitális piac, digitális Európa, kiberfenyegetések, IT-biztonság, kiberreziliencia

Abstract

A press release published on 11 December 2020 has caused a great echo in the IT world. In it, Alaa Abdulridha described how he found serious vulnerabilities in Facebook's subdomains. All of this happened because during home office due to the COVID-19 pandemic, he had plenty of free time left that he wanted to spend productively. Interestingly, while reading the press release, I immediately received a message by clicking on the Twitter link marked in the article that unauthorized people had access to the account I was using, so they suggested to change my password. All of this gave me enough motivation to start exploring the topic in more depth.

1 Information Technology: információs technológia, informatika.
2 Az aldomain a webhely domain nevének egy alacsonyabb szintű része.

Keywords: uniformed digital market, digital Europe, cyber threats, IT security, cyber resilience

Napjaink legjelentősebb IT-kockázatai Európában

A COVID-19 világjárvány ráébresztett bennünket arra, hogy egy ilyen agresszíven terjedő fertőzéssel szemben nemcsak egészségügyi szempontból vagyunk kiszolgáltatottak ebben a globalizált világban, hanem a terjedés visszaszorítására bevezetett otthoni munkavégzésből fakadó kihívások tekintetében is. A kijárási tilalmak, korlátozások jelentette akadályok miatt nemcsak munkafolyamataink, hanem vásárlási szokásaink, ételrendeléseink, társas érintkezéseink is jelentős mértékben áttevődtek a kibertérbe. Ez jelentős mértékű sebezhetőséget okozott, amit az Európai Bizottság *Cybercrime and COVID-19* című publikációja (URL3) szerint rosszindulatú szereplők ki is használnak. Adathalász tevékenységükhöz vírussal kapcsolatos weboldalakat és elérhető dokumentumokat – információknak, tanácsoknak álcázva – készítettek, hogy ezzel fertőzzék meg a számítógépeket. Zsarolóvírusokkal olyan egészségügyi, illetve kutatóközpontokat támadtak, ahol COVID-19 elleni vakcinák fejlesztésén dolgoztak. A sérülékenységeket kihasználva olyan kritikus infrastruktúrákat, illetve nemzetközi szervezeteket támadtak meg, mint például az Egészségügyi Világszervezet (World Health Organization, WHO). Pénzügyi adatok jogtalan kinyerése érdekében olyan applikációkat készítettek, amelyek állítólagosan a vírussal kapcsolatos információk megosztását biztosították. Maszkok, kézfertőtlenítő szerek ígéretével, hamis gyógyszerek árusításával elkövetett csalások modus operandiját dolgozták ki. Kiberbűnözők a nagyvállalatok és egyéb szervezetek rendszereibe a távmunkát végző munkavállalók felhasználói fiókjain keresztül próbáltak – néha sikerrel – bejutni.

A pánik és a társadalmi bizonytalanság elérése érdekében félrevezető információkat és hamis híreket terjesztettek a kormányzati és egészségügyi hatóságok intézkedéseivel kapcsolatban. A fentiek miatt elengedhetetlenné vált a biztonsági intézkedések megerősítése, és egy jóval elővigyázatosabb felhasználói magatartás szükséges, amihez az EUROPOL (European Union Agency for Law Enforcement Cooperation, Európai Rendőrségi Hivatal) szakanyaga is segítséget nyújt (URL4). Hasonló támogatást ad az ENISA (European Union Agency for Cybersecurity, az Európai Unió Kibervédelmi Intézete) *A kibervédelmi ötletek az otthondolgozáshoz* című szakanyagával (URL5).

Ugyanakkor a kihívások – amelyek rohamos léptékkel fejlődnek – igen rugalmasan alkalmazkodnak a hétköznapok újabb és újabb lehetőségeihez.

A Kaspersky[3] szakértői szerint a blackhat hackerek[4] lényegesen több mobiltelefont (42 973 darabot) fertőztek meg a felnőtt-tartalmú platformok használata által 2019-ben, mint az azt megelőző évben, ugyanis 2018-ban ez a szám még csak 19 699 volt. A koronavírus okozta, magánéletre is kiható izoláció megnövelte a felnőtt-tartalmú videókat megosztó oldalak forgalmát, s ezt felismerve a rosszindulatú hackerek valószínűsíthetően több eszköz fertőzését érték el 2020-ban, és fogják elérni 2021-ben (URL6).

Egyéb biztonsági kockázatokra hívja fel a figyelmet az ESET[5] IT-biztonsági szakembereinek elemzése is, amely szerint a kiberbűnözők míg 2015-ben 3 ezer milliárd dollár kárt okoztak világszerte, addig ez a szám 2021-re 6 ezer milliárd dollárra fog emelkedni. A károkba bele kell számítani a váltságdíjfizetést, a termelékenységcsökkenést, továbbá a szükséges technológiai védelmi beruházásokat is. Az elemzés kitért arra is, hogy a bűncselekményeket is könnyebb elkövetni, mivel például a Ranion[6] oldalain már havi vagy éves előfizetéssel is elérhetők zsarolóvírusok. Másik modell, miszerint a vásárlók a kártevőt és az infrastruktúrát ingyen kapják, a beérkezett váltságdíjból pedig részesedést adnak. Kijelenthető, hogy a kiberbűnözők szinte egy iparágat hoztak létre, ami a marketingtől kezdve az ügyfélszolgálatot is magába foglalja, s nemcsak felhasználói kézikönyveket, de frissítéseket is biztosítanak (URL7).

Az EUROPOL 2019-ben kibocsájtott IOCTA[7] jelentése alapján a támadások tekintetében még mindig a zsarolóvírusok jelentették a fő kockázatot. A korábbi tendenciákhoz képest ezek immáron célzottabbak, és a velük okozott gazdasági károk is kiemeltebbek, annak ellenére, hogy számukban csökkenés mutatkozott. A zsarolóvírusok által elkövetett bűncselekmények, a jelentés szerint, továbbra is a leggyakoribb modusok maradnak a közeljövőben, hiszen relatíve könnyű bevételi forrást nyújtanak a kiberbűnözők számára. Ezt követik – a rendészeti szervek és a magáncégek által is megerősítve – a CNP csalások[8], amelyeket leginkább jogtalan adatgyűjtést (például adathalászatot), illetve social engineeringet[9] felhasználva hajtanak végre. Ugyancsak az előbb említett két eszköz igénybevételével valósítják meg a BEC[10] nyújtotta pénzügyi visszaéléseket,

3 A világ élvonalába tartozó, IT-védelemmel foglalkozó cég.
4 Rosszindulatú tevékenységet folytató IT-szakemberek; emellett megkülönböztetünk még whitehat és grayhat hackereket is.
5 Az ESET egy pozsonyi központú, IT-biztonsággal foglalkozó cég.
6 A Ranion az egyik elérhető, nem kimagasló szakmai tudást igénylő zsarolóvírus-csomag.
7 Internet Organized Crime Threat Assessment, a szervezett bűnözés internetes fenyegetését vizsgáló jelentés.
8 Card Not Present – kártya nélküli pénzeszközök jogtalan megszerzése.
9 Magyarul: pszichológiai befolyásolás; a támadó nem a technikai hiányosságokat, hanem a felhasználó megtévesztését használja ki.
10 Business E-mail Compromise – az üzleti e-maileket érintő visszaélések.

amiben az elkövetőket a szegregált vállalati struktúra is segíti. Megemlítendő, hogy a DDoS[11] támadások, illetve az azokkal való fenyegetés továbbra is olyan adatfókuszú fenyegetés, amivel szükséges foglalkozni. Ezek után következnek az ATM-ek[12] elleni bűncselekmények, majd az adathalászat, valamint a távoli asztal kapcsolatok (RDP) sérülékenységeinek kihasználása. Az elkövetők ugyanúgy a sebezhetőségeket keresik, amelyek továbbra is leginkább az üzemeltetői oldal hanyagságára (például nem megfelelő erősségű jelszavak alkalmazása, frissítések elmulasztása) vezethetők vissza. Ugyanakkor a területen egyre jelentősebb kihívást jelentenek a social engineering támadások finomodásai. Az erősödő európai adatvédelmi szabályozásoknak köszönhetően a jogsértések ezen a téren is emelkedést mutatnak (mivel a jogi szigorítások miatt több jogsértés válik ismertté, amelyek korábban látenciában maradtak volna), ami szintén tendenciaként értékelhető. Nem felejtkezhetünk meg azonban a gyermekpornográfia és a SGEM[13] jelenség általi, kiskorúakat érintő bűncselekményekről sem (URL8), de ennek vizsgálatától jelen tanulmányban eltekintek.

Álláspontom szerint vizsgálni szükséges a növekvő jelentőségű kriptovaluták kérdéskörét is, mivel egyre nagyobb számban alkalmazzák például a bitcoint a bűncselekményből származó vagyonok elrejtésére, vagy azokat eszközként használják, illetve illegális tevékenységek céljaként határozzák meg. Fenti álláspontom megegyezik az EUROPOL 2020-as IOCTA dokumentumában (URL9) szereplő, a kriptovalutákra vonatkozó megállapításokkal, miszerint azok továbbra is jelentős szerepet játszanak a kiberbűnözésből származó haszon nyom nélküli eltűntetésének megkönnyítésében. Ebben a kriptovaluták földrajzi érzéketlensége, valamint ismeretlenséget biztosító adottságai jelentős segítséget nyújtanak (Simon, 2018).

Konstans és jelentős kihívásként kell tekinteni a dark weben[14] található illegális piacterekre is, amelyek éves bevétele 860 milliárd USA dollárra tehető. Itt szinte minden elérhető, ami nemcsak a kiberbűnözéssel, hanem annak klasszikus formájával is összefüggésbe hozható (kábítószer, lőfegyver, hackelt szoftver, hackerszolgáltatás, hamis vagy hamisított közokirat, hamis készpénz, banki adat, lopott hitelkártyaadat, gyermekpornográfia stb.). Bár az utóbbi idők bűnüldöző tevékenysége a legnagyobb piacot jelentő, felhasználóbarát Tor környezetét elbizonytalanította, a vásárlói bázis nem pártolt át egyéb alternatív piacokra.

11 Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás, aminek következtében a rendszer összeomolhat, elérhetetlenné válhat vagy csak lelassulhat, ami a felhasználókat megakadályozhatja a tevékenységük végzéséhez szükséges adatok elérésében.
12 Automated Teller Machine – bankautomata.
13 Self-generated Explicit Material – saját magunkról készített kompromittáló fotók.
14 Az úgynevezett sötét web az internet legkisebb, legrejtettebb része.

Amennyiben ez meg is történne, a kereslet miatt hamarosan újabb illegális dark web piac venné át a helyét (Serbakov, 2020).

Fontos szempont, hogy az IT-képességeket nemcsak bűncselekmények elkövetésére használják, hanem a titkosszolgálatok eszköztárát is erősítik; országok belpolitikai eseményeit, így például választásokat is megpróbálnak ezzel befolyásolni. Legutóbb az amerikai elnökválasztás alkalmával – feltehetően orosz hackerek – mintegy 200 olyan szervert támadtak, amelyeknek köze volt a választáshoz (URL10). Az ehhez hasonló támadások már Európát is elérték, hiszen a 2018-as angliai választások napján kibertámadás érte az elektromos hálózatot, a vízellátást és bizonyos feldolgozóipari cégeket. A GCHQ (Government Communications Headquarters, az Egyesült Királyság egyik hírszerző szervezete) nem nevesítette, de sajtóértesülések szerint a támadás hátterében Oroszország állt (URL11). Ezt erősítették azon sajtóhírek is, miszerint Emmanuel Macron elnökválasztási kampányában a GRU-hoz (az orosz katonai hírszerzéshez) köthető hackercsoport[15] adathalászattal, illetve a kampányoldalra malware[16] elhelyezésének szándékával megkíséreltek beavatkozni (URL12).

Kimagasló kockázatot jelentenek és a jövőben több komoly támadás várható az orosz APT-csoportoktól[17] (például: Cozy Bear, Fancy Bear, Sandworm, Silence APT, Turla), amelyek nevéhez köthető a dán Maersk elleni kibertámadás, amihez a NotPetya zsarolóvírust alkalmazták. A számlájukra lehet írni még az áramszünetet okozó, ukrán energiaszektor elleni támadást vagy az amerikai elnökválasztásba való beavatkozást is. Oroszország korán felismerte a kiberműveletekben rejlő kimagasló lehetőségeket, emiatt képességeik nagyarányú fejlesztésébe kezdett, ami mára hackercsoportok komplex struktúráját eredményezte, akik ellen nagyon nehéz felvenni a küzdelmet (URL13).

Jelentős szakirodalom áll rendelkezésre az Európát fenyegető hibrid hadviselés tekintetében. Az újfajta támadásról kijelenthető, hogy egészen addig észrevétlen marad, amíg a megtámadott állam vagy akár az Európai Közösség már képtelen a hatékony reakcióra. A hatalmi eszközök több dimenzióban és szinten történő összehangolása a kulcsmozzanata a hatékony hibrid hadviselésnek (Cullen & Reichborn-Kjennerud, 2019). Ezt az offenzívát indító entitások úgy tudják hatékonyan kifejteni, hogy olyan tevékenységet folytatnak, ami a lakosság ingerküszöbét nem éri el, és az állami szervek – a rendes jogrendből következően – nem folytatnak ellentevékenységet (Somodi & Kiss, 2019).

15 Pawn Storm.
16 Malicious software – rosszindulatú szoftver.
17 Advanced Presistent Threats – fejlett, folyamatos fenyegetés.

A hacktivizmus jelensége is kockázatként értékelendő az EU vonatkozásában. A hacktivista a hacker és az aktivista szavakból tevődik össze, amely olyan személyek gyűjtőfogalma, akik a szólásszabadságért, illetve abból levezetve az internet szabadságáért, illetőleg egyéb társadalmi igazságtalanságok ellen (olykor csupán vélt indokok alapján) küzdenek a kibertérben. Legjelentősebb társulásuk az Anonymous csoport, amelynek kiemelkedő támadásai a szcientológiai egyház ellen vagy a Wikileaks[18] hátráltatását elősegítő pénzintézetek ellen irányultak. Fontos tény azonban, hogy az Anonymous 2015-ben harcot kezdett az Iszlám Állam ellen is, feltörve a terrorszervezet több szerverét, közösségi hálón regisztrált fiókját, amelyeket nyilvánosságra hozott, segítve ezzel a terrorellenes intézkedéseket. A csoport egyebek mellett világméretű pedofilhálózat feltörésében is segítséget nyújtott, így tevékenységük nem értékelhető színtisztán kockázatnak, annak vannak pozitív oldalai is (Berki, 2018).

Fontos kockázatot jelenthet a közeljövőben – az EUROPOL és az ENSZ (United Nations – Egyesült Nemzetek Szervezete) közös jelentése (URL14) alapján – a kiberbűnözők általi, a mesterséges intelligencia (továbbiakban: MI) rosszindulatú felhasználása. A jelentés értelmében az MI jelenlegi deep fake[19] anyagok készítése mellett már megjelentek egyéb felhasználást bizonyító ügyek is. Az MI alkalmazása a zsaroló vírusok esetén olyan gyorsulást eredményezhet, ami képtelenné teszi a rendszereket az időben történő reagálásra. A technológia segíthet olyan vakfoltok felfedezésében is, ahová algoritmusokat rejthetnek anélkül, hogy azok detektálásra kerüljenek (URL15). Másik veszélyforrás az MI jelenlegi infrastruktúrájának támadása lehet, elérve ezzel a folyamatban lévő projektek sikerességének megakadályozását.

Az európai 5G hálózatok kiépítése komoly biztonsági kockázatot fog magában hordozni, ha abban a Huawei eszközeit is felhasználják, állítja az Amerikai Egyesült Államok. A nagyhatalom mindemellett aktívan kampányol amellett, hogy a NATO tagországok mellőzzék a kínai cégekkel való együttműködést (URL16). Azonban az sem zárható ki, hogy a háttérben csupán az USA és Kína között fennálló gazdasági verseny áll. Igaz, hogy nem Európában, hanem a floridai Oldsmar városában, de kibertámadás ért egy víztisztító üzemet, ahol a behatoló megkísérelte az ivóvizet megmérgezni úgy, hogy a nátrium-hidroxid koncentráció normál szintjét több mint százszorosára kívánta emelni (URL17). Ez az eset megmutatta, hogy a kritikus infrastruktúrák elleni, a kibertérben történő offenzíva valós veszéllyé vált hétköznapjainkban, ami hamarosan kontinensünkön

18 Julian Assangehoz köthető nemzetközi nonprofit szervezet, amely kiemelt jelentőségű, jogsértő eseteket leplezett le.

19 A szó jelentése a deep learning és a fake szavakból képződött; egy algoritmus segítségével egy emberi arcot tehetünk például egy másik testre vagy hitelesnek tűnő számla készíthető vele.

is valósággá válhat. Összegezve a fentieket megállapíthatjuk, hogy a kutatott terület rendkívül gyorsan változik, fejlődik és a hétköznapi kihívásokhoz szinte azonnal alkalmazkodik. Az EU által megálmodott egységes európai kibertér biztonságát azonban nemcsak a bűnelkövetők, hanem idegen nagyhatalmak – politikai befolyásolási szándékaik miatt is – napról-napra veszélyeztetik; a hírszerzés fókusza emiatt erre az irányra is kiterjed. A kihívásokra adott megfelelő védelmi stratégia megvalósításához azonban az állami szereplőknek a magáncégekkel együttműködve van egyedül lehetősége a sikerre.

Kiemelt európai IT-támadások a közelmúltban

2018 decemberében, egyfajta adventi naptár formájában, egy 16 ezer követővel rendelkező Twitter-fiókra töltötték fel folyamatosan csaknem ezer német közszereplő személyes adatait és magántitkait, köztük jelentős számban politikusokét is, úgy mint Angela Merkel kancellár és Frank-Walter Steinmar államfőjét is. Az ismeretlen elkövetők a legtöbb esetben kizárólag telefonszámokhoz, e-mail címekhez jutottak hozzá, de körülbelül ötven esetben személyes levelezésekhez és családi fotókhoz is. Az incidens a hatóságoknak hetekig fel sem tűnt (URL18).

2019 szeptemberében hackerek bejutottak az Osztrák Néppárt (ÖVP) informatikai rendszerébe és több hétig információkat szivárogtattak a választásokkal és a párt tevékenységével kapcsolatban. A mintegy 1300 gigabájt adat között kampánytervek, érzékeny tartalmú e-mailek, politikai ellenfelekről készült jelentések is szerepeltek, de az illetéktelen behatolók hamis tartalmú információkat is megkíséreltek feltölteni (URL19).

2020. január 5-én súlyos kibertámadás érte Ausztria külügyminisztériumát, aznap, amikor az Osztrák Zöld Párt koalíciót kötött a konzervatív oldallal. A támadás hátterében újfent Oroszországot sejtik (URL20).

2020 tavaszán hackerek kilencmillió ügyfél adatait lopták el az angol EasyJet diszkont légitársaságtól. A támadók utazási adatokat, e-mail címeket, és kb. 2200 esetben hitelkártya-információkat is megszereztek. Bennfentes források szerint a háttérben kínai hackerek álltak (URL21).

2020 szeptemberében egy düsseldorfi kórházat ért kibertámadás során leállt az intézmény IT-rendszere, így számos tervezett beavatkozást kellett elhalasztani. Köztük volt egy sürgős eset is, melynek során egy beteg – másik egészségügyi intézetbe történő átszállítását követően – életét vesztette, mivel a szükséges segítséget nem tudta időben megkapni. A kibertámadás eredeti célja a Düsseldorfi Egyetemet érintő, zsarolóvírus útján történő jogtalan haszonszerzés volt. Ez az első eset Európában, amely kritikus infrastruktúrát érő kibertámadás alkalmával halált okozott (URL22).

2020 szeptemberében minden eddiginél nagyobb túlterheléses támadást (DDoS) indítottak három magyar pénzintézet, valamint a Magyar Telekom telekommunikációs cég ellen. A több hullámban indított kibertámadás elsősorban Oroszországból, Kínából és Vietnámból indult. Minden eddigi, hasonló jellegű, Magyarországot érintő támadáshoz képest az akció tízszer nagyobb és jóval komplexebb volt (URL23).

2020. december 9-én támadás érte az Európai Gyógyszerügynökséget, amely az illegális akció során éppen a koronavírus-vakcinák forgalomba hozatali engedélyezést végezte. A hackertevékenység eredményeként különböző dokumentumokhoz fértek hozzá (URL24).

A REvil hackercsoport 2020 decemberében az Egyesült Királyság Transform Hospital Group kórházlánctól 900 gigabájtnyi adatot – köztük jelentős számú intim képet – loptak el paciensekről (URL25).

2021 februárjában Franciaországban, a délnyugati Dax és az ország középső részén fekvő Villefranche-sur-Saône kórházakat kibertámadás érte. A zsarolóvírusok lebénították az egészségügyi intézmények IT-rendszereit, amelynek következtében fontos műtéteket kellett elhalasztani, és betegeket átszállítani más egészségügyi intézetekbe.

A helyzetet a COVID-19 pandémia tovább súlyosbítja, a betegadminisztráció jelenleg papíralapon folyik (URL26). A támadások sokszínűsége megmutatja, hogy a kérdést megfelelően csak komplex intézkedésekkel lehet kezelni. Ennek közösségi vetületét a következő fejezetben vizsgálom.

Az EU IT-biztonság érdekében hozott intézkedései

A tanulmány következő részében az Európai Unió jogalkotását (Mezei, 2018), majd egyéb intézkedéseit – köztük különböző szervezetek létrehozását – gyűjtöttem össze, amelyek az előzőkben bemutatott kockázatok leküzdését hivatottak előmozdítani. Az EU első témában megalkotott sarokköve az Európai Tanács 9. (89.) számú ajánlása (Computer-Related Crime, Számítógépekkel kapcsolatos bűncselekmények) volt, amelyben megtalálható lista[20] iránymutatásul szolgált a tagállamoknak az elfogadni kívánt új jogszabályok tekintetében. Az ajánlás – a hatékony eljárások érdekében – egy egyetemes, kötelező erejű jogi norma megalkotását tartja megfelelőnek a tagállamok számára. A jogfejlődés ezen

20 A témában hozott új tagállami jogszabályoknak vagy módosításoknak tartalmazniuk szükséges a listában szereplő meghatározásokat, például számítógépes csalás, hamisítás, szabotázs, jogellenes titokszerzés stb.

szakaszában viszonylag hamar felismerésre került, hogy az anyagi jogi mellett az eljárásjogi szabályok[21] is fejlesztésre szorulnak, ami az Európai Tanács 95. (13.) számú ajánlásához vezetett. Ennek egyik legfontosabb dimenziójának a kölcsönös, határon átnyúló együttműködés tekinthető. Az egyik legnagyobb előrelépést az Európai Tanács 2001. november 23-án, Budapesten kelt Számítástechnikai Bűnözésről szóló Egyezménye (Convention on Cybercrime) jelentette. Az Egyezmény Preambulumában kifejtésre került, miszerint egy olyan közös büntetőjogi politika megteremtését hivatott szolgálni, melynek elsődleges célja – a megfelelő jogszabályok elfogadásával és a nemzetközi együttműködés elősegítésével – a társadalom védelme a számítástechnikai bűnözéssel szemben. A joganyagban újabb jogi kategóriák kerültek meghatározásra, biztosítva ezzel az IT-fogalmak egységes értelmezését. Ugyanakkor nemcsak anyagi, hanem eljárásjogi szabályokat is tartalmaz.

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) elsősorban a felhasználók személyes adatainak és a magánélet tiszteletben tartásához való joguk védelmét hivatott biztosítani a korszerű digitális technológiák által jelentett veszélyekkel szemben. Elsődlegesen a spamek[22] visszaszorítására, a felhasználó előzetes beleegyezést kérő rendszerekre[23] és a cookiek[24] telepítésére határoz meg szabályokat. Ezt később az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.), az úgynevezett „süti" irányelv egészítette ki. A következő fontos szabályozásnak az Európa Tanács az információs rendszerek elleni támadásokról szóló 2005/222/IB (2005. február 24.) kerethatározata tekinthető. A határozat elsődleges célja a tagállamok közötti együttműködés fokozása, amelyet az országok információs rendszerek elleni támadásokra vonatkozó büntetőszabályainak közelítése által lát biztosítottnak. Ebben a szabályozásban már megjelent a kritikus infrastruktúrákat irányító IT-rendszerek elleni támadások egyre növekvő kockázata. Az aggodalmakat akkor még a terrorizmushoz kötötték elsődlegesen, de mára – a hibrid hadviselés fejlődésének köszönhetően – más nagyhatalmak beavatkozása is komoly kihívást jelenthet. Jelentős lépés volt a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint

21 Az elektronikus adatok bizonyítékként történő felhasználásának eljárási rendje, például lefoglalásuk, kezelésük.
22 Kéretlen elektronikus üzenetek.
23 Opt-in.
24 A sütik olyan apró adatrészletek, amelyeket a webhelyek tárolnak a felhasználók számítástechnikai eszközein.

a 2004/68/IB tanácsi kerethatározat felváltásáról szóló Európai Parlament és a Tanács 2011/92/EU irányelve (2011. december 13.). A szabályozás legfőbb indoka, hogy a gyermekpornográfia vagy a gyermekek szexuális bántalmazásának, kizsákmányolásának egyéb súlyos formái az internet használata révén egyre növekvő méreteket öltenek. 2013-ban került elfogadásra az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, az Európai Parlament és Tanács 2013/40/EU irányelve. Az irányelv célja, hogy *„a bűncselekmények tényállására és vonatkozó szankcióikra vonatkozó minimumszabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén, és hogy javítsa a tagállamok illetékes hatóságai, így a rendőrség és az egyéb bűnüldözési szakszolgálatok, valamint az Unió illetékes szakosított ügynökségei és szervei – például az Eurojust, az Europol és annak a számítástechnikai bűnözés elleni európai központja, valamint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) – közötti együttműködést."* A döntéshozók az információs rendszerekre az EU kulcstényezőiként tekintenek a politikai, a társadalmi és a gazdasági dimenziók vonatkozásában. Az irányelv fontos újdonsága, hogy a robothálózatokra[25] vonatkozó tiltott cselekményeket is definiálta és büntetni rendelte. 2014-ben az Európai Parlament és a Tanács a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU számú rendeletet adott ki, amelynek elsődleges célja az online környezet iránti bizalom, valamint a jogbiztonság megteremtése, mélyítése.

2016. július 6-án került elfogadásra az Európai Parlament és a Tanács a hálózati és információs rendszerek biztonságának az egész Európai Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelve (az úgynevezett NIS direktíva), mivel megállapításra került, hogy a rendelkezésre álló képességek nem voltak elégségesek ahhoz, hogy garantálják a hálózati és információs rendszerek magas biztonsági szintjét. A biztonsági kihívások hatékony kezelése globális megközelítést igényel uniós szinten, ezt hivatott biztosítani az irányelv, egyfajta jogi keretet biztosítva.

2017 szeptemberében megszületett az Európa Bizottság nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló 2017/1584 ajánlása, valamint az Európai Parlament és a Tanács az Ellenálló képesség, elrettentés és védelem: az Unió erőteljes kiberbiztonságának kiépítése (JOIN [2017] 450 final) című közös véleménye.

25 A botnet fertőzött informatikai hálózat, amelyet többféle károkozásra is alkalmazhatnak.

Az EU kibervédelmét támogató szervezetei

Az EU 2004-ben létrehozta[26] az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA – továbbiakban: Ügynökség), amely arra volt hivatott, hogy biztosítsa az EU és tagállamai számára a minél sikeresebb felkészülést az információbiztonsági kihívások felderítésében, kezelésében és megelőzésében. Az Ügynökség gyakorlati tanácsokkal látta el az uniós intézményeket, valamint a közösség köz- és magánszektorának képviselőit az információbiztonság területén (URL27). Az Ügynökség feladatköre – már a korábbiakban is említettek szerint – 2018 decemberében kibővült, s az EU hálózat- és információbiztonság európai szakértői központjaként folytatja tevékenységét, Európai Kiberbiztonsági Ügynökség[27] néven (URL28).

2012. december 1-jén megkezdte működését a Szabadságon, a Biztonságon és a Jog Érvényesülésén Alapuló Térség Nagyméretű IT-rendszereinek Üzemeltetési Igazgatását Végző Európai Ügynökség (eu-LISA). A Tallinni székhelyű ügynökség igazgatja a schengeni övezet biztonsága érdekében a Vízuminformációs Rendszert (VIS), a Schengeni Információs Rendszert (SIS II), és az Európai Ujjnyomat-azonosító Rendszert (Eurodac) (URL29).

2013-ban került felállításra az EUROPOL Európai Kiberbűnözés-elleni Központja (EC3), amely arra hivatott, hogy támogassa az EU-ban a bűnüldöző szervek hatékony fellépését a kiberbűnözéssel szemben. Létrehozása óta számos nagy horderejű ügyben volt érintett, több száz sikeres letartóztatáshoz nyújtott helyszíni segítséget, és elemző tevékenysége során több százezer file átvizsgálását hajtotta már végre. Minden évben elkészíti az IOCTA jelentését, amely az adott időszakra a számítógépes bűnözés legfontosabb megállapításait, valamint az új fenyegetéseket is magába foglalja (URL30). A szervezeten belül a Focal Point Cyborg[28] egység hatáskörébe tartozik az elsődlegesen az európai kritikus infrastruktúrákat veszélyeztető high-tech bűncselekmények elleni küzdelem. Az EC3 képességei az igazságügyi informatika szakterületén is kimagasló, ennek a tevékenységnek a támogatására létrehozott laboratóriumában saját IT-kutatást és fejlesztést is folytat.

Szintén 2013-ban került létrehozásra az Európai Tanács Kiberbűnözés Programirodája (C-PROC), amelynek feladata, hogy a jogállami normákkal összhangban támogassa a kiberbűnözésre és az elektronikus bizonyítékokra vonatkozó jogszabályok fejlődését, biztosítsa a bírák, az ügyészek és a rendvédelmi

26 Az Európai Parlament és a Tanács 460/2004/EK rendeletével, amelyet felváltott az Európai Parlament és a Tanács 526/2013 rendelete.
27 EU Agency for Cybersecurity.
28 Kiberbűncselekményekkel foglalkozó fókuszpont az EC3 egyik egysége.

szervek tagjainak képzését. További feladatköre a kooperáció előmozdítása az igazságügy területén, az állami és magánszféra közti párbeszéd mélyítése, és a nemzetközi együttműködés fokozása a kiberbiztonság témakörében. Kiemelt terület a programiroda számára a gyermekek védelme az online szexuális erőszakkal szemben (URL31).

Érdemes röviden bemutatni a 2000-ben létrehozott Trusted Introducer (Megbízható Bevezető – továbbiakban: TI) szolgáltatást, amit az európai CERT (Computer Emergency Response Teams – Számítógépes Vészhelyzeti Reagáló Csoportok) közösség hívott életre. A TI legfontosabb szolgáltatása egy megbízható gerinchálózat biztosítása az eseménykezelő szervezetek számára.

Ugyancsak említést érdemel a Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform – CECSP), amely Magyarország, Lengyelország, Ausztria, Csehország és Szlovákia kiberbiztonsági együttműködési platformja.

Végezetül pedig két nonprofit szervezet tevékenységét érdemes megismerni; az egyik a 2012-ben alapított ENCS (European Network for Cyber Security), amelyet az európai kritikus infrastruktúrák biztonságos támogatására hívtak életre, a másik a 2016-ban létrehozott ECSO (European Cyber Security Organisation), amely az ipari szereplőket képviseli az Európai Bizottság előtt a kiberbiztonság témakörében (Kovács, 2020).

A digitális Európa jövőképe

Tekintettel arra, hogy az EU-ban a kritikus infrastruktúrának számító szektorokban, így a közlekedésben, az energetikában, az egészségügyben és a pénzügyi ágazatban a digitális technológiák fokozatosan átveszik az alapvető tevékenységeket, jelentősebb kockázatok keletkeznek, amelyekre megfelelő válaszokat kell adni. Az Európai Bizottság és az Európai Unió külügyi és biztonságpolitikai főképviselője 2020. december 16-án előterjesztette az új uniós kiberbiztonsági stratégiát. Ez lehetővé fogja tenni, hogy az EU megőrizze vezető szerepét a kibertérrel kapcsolatos nemzetközi normák kidolgozása vonatkozásában, és jelentősen hozzájáruljon a globális, stabil, szabad és nyitott kibertér biztosításához. A stratégia azonban nemcsak az egységes gazdasági térség kiberbiztonságát célozza, hanem a demokratikus értékeken, így az emberi és alapvető szabadságjogokon alapuló jogállamiság teljes érvényesülését is. Az EU elkötelezettségét a témában jól szemlélteti, hogy a 2021–2027 közötti költségvetésében a Digitális Európa Programra 7,5 milliárd EUR összeget különít el (URL32), jelentősen támogatva ezzel a digitális átállás megvalósulását.

Kiemelkedő javaslat az Európai Parlament és Tanács a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelvének (2016. július 6.) felülvizsgálata, ami az állami és magánszektor kiberrezilienciáját hivatott emelni. Ugyanakkor fontosnak tartja kiterjeszteni az Európa Tanács az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvének hatáskörét is.

Az Európai Bizottság egy mesterséges intelligenciával működő műveleti központ kialakítására is javaslatot tett, amely az EU számára egy kiberbiztonsági pajzsot jelentene. Ez egy EU ellen intézett kibertámadást lenne hivatott időben észlelni, és azt biztosítani, hogy a támadást proaktív fellépéssel – még a kár bekövetkezte előtt – elhárítsa. Fontos intézkedésként jelölik a digitális innovációs központok keretében történő kis- és közepes vállalkozások célzott támogatását, valamint a kutatásfejlesztésbe való befektetések ösztönzését. A stratégiában megfogalmazásra került egy új, közös kiberegység felállítása[29], amely az EU szervei és a tagállamok hatóságai közötti együttműködést lenne hivatott előmozdítani, aminek köszönhetően egységesen nőne a kibertámadások elleni megelőzés, elrettentés és válaszadás eszköztára. Az előbbiek erősítésére a főképviselő az EU kiberdiplomáciai eszköztárának bővítésére is javaslatot tett, különös tekintettel arra, ha kritikus infrastruktúrákat, ellátási láncokat vagy demokratikus intézményeket érnének rosszindulatú támadások.

Az Európai Bizottság az ENISA támogatásával arra ösztönzi a tagállamokat, hogy az 5G hálózatok kiberbiztonságról szóló bizottsági ajánlásban (URL33) foglaltak minél szélesebb körben megvalósuljanak. Az Európai Bizottság további célja az EU kiberbiztonsági ipari és technológiai kapacitásának erősítése, amelynek fontos eleme a felhőszolgáltatások, az új generációs processzorok technológiája, a kiemelt biztonságú összeköttetés és a 6G hálózatok területén történő előrelépés (URL34).

Összegzés

Európa lakosságának 87,1 százaléka használt internetet 2020 negyedik negyedévében, nála Észak-Amerika mutat egyedül magasabb arányszámot 89,9 százalékkal. A világ összlakosságának 63,2 százaléka élt a vizsgált időszakban a világháló nyújtotta lehetőségekkel (URL35). Ennek ellenére a svájci székhelyű Nemzetközi Távközlési Egyesület (ITU) Globális Kiberbiztonsági

29 Joint Cyber Unit

Indexe Európát a legbiztonságosabb régiónak értékeli évek óta. A rangsor kialakításában a jogszabályalkotást, technikai, szervezeti, kapacitásfejlesztési és együttműködési intézkedéseket veszik elsődlegesen figyelembe (URL36). Tekintettel arra, hogy az EU fejlődésének fő irányvonala az egységes digitális piac megteremtése, szükséges is ez a kimagasló teljesítmény a kiberreziliencia szavatolása érdekében. Ugyancsak ezt szorgalmazza az a tény, miszerint az információs és kommunikációs technológia vált az Európai Közösség gazdasági növekedésének gerincévé. Ugyanakkor erre a fejlődési irányvonalra a külföldi nagyhatalmak – leginkább titkosszolgálataik segítségével – vissza nem térő lehetőségként tekintenek.

A kibertérre nemcsak mint a modernkori hírszerzés új irányára, hanem egyéb operációk, műveletek új, kedvezőbb helyszínére tekintenek. Oroszország Ukrajnával szemben vezetett hibrid hadviselése is megmutatta, hogy napjainkra a rendelkezésre álló eszközök kombinatív alkalmazása a leghatékonyabb módja egy sikeres katonai konfliktusnak. Nem szabad figyelmen kívül hagyni, hogy a bűnözés is folyamatosan alkalmazkodik a gazdasági fejlődés nyújtotta lehetőségekhez. A digitális piac kiépítése nemcsak az uniós állampolgárokat, hanem a nagyvállalatokat is az újgenerációs bűnözők célpontjává teszik. Mindemellett a hacktivizmus és a terrorizmus kibertérben (Besenyő, 2017) történő megjelenése is komoly kihívásokat jelenthetnek a jövőben. Álláspontom szerint az EU megfelelő válaszokat ad a jogszabályi keretek és a szervezeti struktúra alakításában, de a védelmi ipari kutatás, fejlesztés, innováció területén folyamatos előrelépéseket kell tennie, mivel az euroatlanti szövetségen kívülről származó technikai eszközök biztonsági kockázatot jelenthetnek. Paradigmaváltás szükséges abban a tekintetben, hogy a biztonságra proaktív módon kell gondolni, amire olykor jelentős összegeket kell fordítani, mert az esetleges kibertámadásokra adandó reakciók már nem képesek az elvárt rehabilitációra. Fontosnak tartom továbbá az uniós állampolgárok és a közösség gazdasági szereplőinek képzését, valamint annak elérését, hogy felismerjék a biztonságtudatos viselkedés jelentőségét. Hiszen csupán a technikai megoldások sosem fognak elégséges védelmet nyújtani a kibertámadásokkal szemben.

Felhasznált irodalom

Berki G. (2018). A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. *Nemzetbiztonsági Szemle*, *6*(3), 5-21.

Besenyő J. (2017). Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. *Strategic Impact, 62*(1), 83-100.

Fekete-Karydis K. & Lázár B. (2019). A kibervédelmi stratégiák fejlődése, kibervédelmi kihívások, aktualitások (2.). *Honvédségi Szemle*, *147*(4), 38-49.

Kovács Z. (2020). Kibervédelem és biztonság. In Kiss T. (Szerk.), *Kibervédelem a bűnügyi tudományokban* (pp. 65-90). Dialóg Campus Kiadó.

Mezei K. (2018). Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. *JURA*, *24*(1), 349-360.

Cullen P. & Reichborn-Kjennerud E. (2019). Understanding Hybrid Warfare. In Monaghan, S. (EDS.), *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare* (pp. 13–16). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Serbakov M. (2020). Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. *Büntetőjogi Szemle*, *1*, 91-107.

Simon, B. (2018). Kriptovaluták – rendészeti válaszok. *Belügyi Szemle, 66*(10), 71-87. https://doi.org/10.38146/BSZ.2018.10.5

Somodi Z. & Kiss Á. (2019). A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle*, *147*(6), 22-28. https://doi.org/10.35926/HSZ.2019.6.2

A cikkben található online hivatkozások

URL1: *How I hacked Facebook: Part One.* https://medium.com/bugbountywriteup/how-i-hacked-facebook-part-one-282bbb125a5d

URL2: *Alaa Abdulrida*. https://twitter.com/alaa0x2

URL3: *Cybercrime and COVID-19*. https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

URL4: *Make your home a cyber safe stronghold.* https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

URL5: *Tips for cybersecurity when working from home.* https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

URL6: *2019-ben megduplázódtak a pornónak álcázott mobil-fenyegetések.* https://computerworld.hu/ceginfo/kaspersky-2019-ben-megduplazodtak-pornonak-alcazott-mobil-fenyegetesek-280342.html

URL7: *Pénzben alig kifejezhető, ésszel alig felfogható nagyságú károkat okoznak a kiberbűnözők.* https://www.digitalhungary.hu/e-volution/Penzben-alig-kifejezheto-esszel-alig-felfoghato-nagysagu-karokat-okoznak-a-kiberbunozok/8237/

URL8: *Internet Organised Crime Threat Assessment 2019.* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

URL9: *Internet Organised Crime Threat Assessment 2020.* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

URL10: *Russian Hackers Have Targeted 200 Groups Tied to U.S. Election, Microsoft Says.* https://www.wsj.com/articles/russian-hackers-have-targeted-200-groups-tied-to-presidential-election-microsoft-says-11599763502?mod=hp_lead_pos2
URL11: *Russians hacked energy companies on election day, GCHQ claims.* https://www.telegraph.co.uk/news/2017/07/18/russians-hacked-energy-companies-election-day-gchq-claims/?utm_source=POLITICO.EU&utm_campaign=a83b139846-EMAIL_CAMPAIGN_2017_07_19&utm_medium=email&utm_term=0_10959edeb5-a83b139846-189703869
URL12: *Macron campaign was target of cyber attacks by spy-linked group.* https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200
URL13: *Ki kicsoda az orosz kiberkémkedésben?* https://nki.gov.hu/it-biztonsag/hirek/ki-kicsoda-az-orosz-kiberkemkedesben/
URL14: *UN and Europol Warn of Growing AI Cyber-Threat.* https://www.infosecurity-magazine.com/news/un-and-europol-warn-of-growing-ai/
URL15: *Malicious Uses and Abuses of Artificial Intelligence.* https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf
URL16: *Huawei labelled as security threat to the EU's 5G network*. https://www.brusselstimes.com/news/eu-affairs/135929/huawei-zte-eu-european-union-5g-threat-security-high-risk-digital-network-thierry-breton-margrethe-vestager/
URL17: *Az ivóvízkészlet-mérgezési incidens tanulságaira figyelmeztet az FBI.* https://nki.gov.hu/it-biztonsag/hirek/az-ivovizkeszlet-mergezesi-incidens-tanulsagaira-figyelmeztet-az-fbi/
URL18: *German politicians targeted in mass data attack*. https://www.bbc.com/news/world-europe-46757009
URL19: *Austrian People's Party calls alleged hack an 'attack on democracy'*. https://www.irishtimes.com/news/world/europe/austrian-people-s-party-calls-alleged-hack-an-attack-on-democracy-1.4010308
URL20: *'Serious cyber-attack' on Austria's foreign ministry*. https://www.bbc.com/news/world-europe-50997773
URL21: *EasyJet admits data of nine million hacked*. https://www.bbc.com/news/technology-52722626
URL22: *A murderous cyber-attack is only a matter of time*. https://www.economist.com/the-world-ahead/2020/11/17/a-murderous-cyber-attack-is-only-a-matter-of-time
URL23: *Példátlan hackertámadás érte Magyarországot tegnap*. https://www.portfolio.hu/uzlet/20200925/peldatlan-hackertamadas-erte-magyarorszagot-tegnap-450324
URL24: *Hacker greifen Daten von Biontech ab*. https://www.tagesschau.de/ausland/pfizer-biontech-ema-cyberattacke-101.html
URL25: *Hackers threaten to leak plastic surgery pictures.* https://www.bbc.com/news/technology-55439190
URL26: *Cyber attacks hit two French hospitals in one week*. https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week

URL27: *European Union, European Union Agency for Cybersecurity (ENISA).* https://www.enisa.europa.eu/about-enisa
URL28: *European Union Agency for Cybersecurity, Homepage.* https://www.enisa.europa.eu/
URL29: *EULISA.* https://eulisa.europa.eu/
URL30: *EUROPOL, European Cybercrime Centre - EC3*. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
URL31: *Council of Europe, Cybercrime Programme Office (C-PROC).* https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-
URL32: *European Commission, Press release, Commission welcomes political agreement on €7.5 billion Digital Europe Programme.* https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2406
URL33: *A BIZOTTSÁG (EU) 2019/534 AJÁNLÁSA (2019. március 26.) az 5G hálózatok kiberbiztonságáról*. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019H0534&from=EN
URL34: *Közös közlemény az Európai Parlamentnek és a Tanácsnak. Az EU kiberbiztonsági stratégiája a digitális évtizedre.* https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020JC0018&from=EN
URL35: *Internet World Stats.* https://www.internetworldstats.com/stats.htm
URL36: *ITU Publications, Global Cybersecurity Index (GCI) 2018.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

A cikk APA szabály szerinti hivatkozása

Böröcz M. (2021). Az európai IT-biztonság jelenlegi kihívásai. *Belügyi Szemle*, *69*(12), 2227-2243. https://doi.org/10.38146/BSZ.2021.12.10