KIBERBIZTONSÁG AZ EURÓPAI UNIÓBAN ÉS MAGYARORSZÁGON

A Cloudflare 2023-ban több mint 4200 cég és szervezet körében végzett felmérést, amely szerint:

- **az európai piacokon a cégek és szervezetek 40%-a szenvedett el kibertámadást;**
- **a támadások fő célja 53%-ban kémprogram telepítése, 48%-ban haszonszerzés volt;**
- **a cégek és szervezetek 29%-a érzi védettnek magát egy jövőbeli támadással szemben.**

Az Eurobarometer (2024) felmérése szerint

- **az európai vállalatok 74%-a nem nyújt kiberbiztonsági képzést az alkalmazottainak;**
- **a vállalatok 76%-a szerint nincs szükség kiberbiztonsági képzésekre és figyelemfelkeltésre;**
- **a vállalatoknál a kiberbiztonsággal kapcsolatos munkakörökben dolgozók 76%-a nem rendelkezik hivatalos képesítéssel vagy tanúsított képzéssel.**

Az EU kiberbiztonsági ügynöksége 2023 júniusa és 2024 júliusa között több mint 11 ezer incidenst regisztrált (ENISA 2024) amelyek:

- **41%-a elosztott szolgáltatásmegtagadásos támadás (DDOS),**
- **26%-a zsarolóvírus-támadás (ransomware),**
- **19%-a adatlopás/szivárgás volt.**

A kormány T/9716 számú törvényjavaslatának célja, hogy megerősítse Magyarország kiberfenyegetésekkel szembeni ellenállóképességét, s egyúttal átültesse az európai hálózati és információs rendszerek egységesen magas szintű kiberbiztonságát garantáló (EU) 2022/2555 irányelv (NIS2) rendelkezéseit.

A 2000-es évek első évtizedeiben az emberiség a negyedik, globális ipari forradalom időszakába lépett, amely példanélküli gyorsasággal változtatja meg a társadalmi és gazdasági struktúrákat. E forradalmat olyan technológiák fúziója jellemzi, amelyek elmossák a határokat a fizikai, a digitális és a biológiai szféra között. A digitalizáció, az egyre gyorsabbá váló internet- és mobilhálózatok, az okoseszközök – főként az Internet of Things (IoT), vagyis a Dolgok Internete –, a nagyméretű digitális adathalmazok és az ezekre épülő mesterséges intelligencia, az automatizálás, az autonóm rendszerek, a kvantuminformatika, és egyéb forradalmi technológiák láthatatlan, összekapcsolódó fonalai életünk szinte minden területét behálózzák. Átalakítják az üzleti és gazdasági modelleket, a munkahelyeket, a termelést, az oktatást, és a magánéletünket is (Schwab, 2016; Krasznay, 2022). Ennek következtében a digitális technológiákhoz adaptálódó jelenkori társadalmat egyes tudósok immár nem az elterjedt információs vagy digitális, hanem hálózati társadalomként definiálják, vagyis olyan társadalmi struktúraként, amelynek kereteit a mikroelektronikán és a digitális számítógépes hálózatokon alapuló információs és kommunikációs technológiák által működtetett hálózatok jelentik (Castells, 2018). E hálózatok által formált, összekapcsolt, decentralizált, s egyre növekvő elektronikus információs rendszerek alkotta térben – a kibertérben – az infokommunikációs eszközök nemcsak a mindennapi életünk, hanem egyenesen az államok és társadalmak működéséhez elengedhetetlen infrastruktúrák alkotóelemeivé váltak.

Amint azonban a negyedik forradalom példátlan gyorsasággal alakítja át társadalmi struktúráinkat, úgy a kiberbűnözők is hasonló gyorsasággal adaptálják az új technológiák előnyeit, s használják ki a kibertér alkotórészeinek, hálózatainak és résztvevőinek sérülékenységeit, gyengeségeit. E globális, összekapcsolt környezetben azonban a kiberbiztonsági incidensek nemcsak az egyénekre, hanem akár egész demokráciákra, államokra, szervezetekre, vagy a belső piacok határain átlépve teljes ellátási láncokra is káros hatással lehetnek. A kibertámadások veszélyeit felismerve az Európai Unió a 2010-es évek elejétől kiemelt figyelmet fordít a tagállamok kibervédelmi és kiberbiztonsági képességeinek fejlesztésére, a kibertudatosság növelésére, az ellátási láncok és termékek biztonságának megerősítésére, a fenyegetések jobb észlelésére, valamint az egyre kifinomultabbá és egyre nagyobb gazdasági kárt okozó kiberbűnözés elleni küzdelemre.

AZ EU KIBERFENYEGETETTSÉGE

Az Európai Bizottság a Biztonsági Unióra vonatkozó stratégia (COM(2020) 605 final) végrahajtásáról szóló 7., 2024. évi jelentésében kiemeli, hogy az EU-ban a kiberfenyegetettség helyzete jelentősen romlott az elmúlt években, amit leginkább az ellátási láncok elleni támadások drámai növekedése, valamint a szoftverek, a mobileszközök vagy éppen a személyi számítógépek operációs rendszerei és a virtuális magánhálózatok sebezhetőségeinek kihasználása mutat (COM(2024) 198 final). E folyamatban az elmúlt évek technológiai újításai mellett a COVID-19 világjárvány a katalizátor szerepét játszotta. A pandémia időszaka rávilágított, hogy a társadalmak és a gazdasági szektor mennyire függenek az információs és kommunikációs hálózatoktól, valamint az összekapcsolt termékektől, s ezáltal a középpontba helyezte e hálózatok kiberbiztonságának és ellenállóképességének fontosságát is.

Az Europol szerint a világjárvány a társadalmi és gazdasági működés kibertérbe való eltolódásával visszafordíthatatlanul és alapjaiban alakította át a bűnözést is. A technológiai fejlődés gyors ütemével párhuzamban, a feltörekvő technológiai újítások kihasználásával a kiberbűnözők is gyorsan alkalmazkodnak a 4. ipari forradalom által átalakuló társadalmi és gazdasági környezethez. Támadásaik ezáltal nemcsak egyre nagyobb kárt okoznak, de egyre inkább kifinomultabbá is válnak, amely komoly kihívások elé állítja mind a bűnüldözői, mind a kiberbiztonsági terület szakértőit (Europol, 2021).

Az Europol Kiberbűnözés Elleni Központja (EC3) legújabb elemzésében kiemeli, hogy a mesterséges intelligencián és gépi tanuláson alapuló eszközök és szolgáltatások egyre inkább a kiberbűnözők általános eszközeivé válnak, s hatékonyan csökkentik e bűnözési terület belépési korlátait. Az EC3 kiemeli, hogy részben ennek, részben a potenciális támadási felületet kiszélesítő digitális infrastruktúra növekvő összetettségének, és az ehhez kapcsolódó felhasználók alacsony biztonságtudatossági szintjének köszönhetően a kiberbűnözők száma jelentős ütemben növekszik. A bűnelkövetők számát növeli, hogy a tiltott weboldalakon egyes szereplők immár szolgáltatásként árulják kiépített kiberbűnözői eszköztárukat. Mindezek következtében az EU-ban naponta több millió áldozatot érintenek az online támadások sokszínű formái, a zsarolóvírus-csoportok pedig egyre inkább a kis- és középvállalkozásokat veszik célba, mivel ezek kibervédelme egyelőre alacsonyabb (Europol: IOCTA, 2024).

Az Európai Unió kiberbiztonsági ügynöksége – az ENISA – az elmúlt években folyamatosan feltérképezte az Unió kiberfenyegetettségi helyzetét. Értékeléseik szerint a kibertámadások száma évről évre egyre növekszik, amelyek a magánszemélyek mellett leginkább a nehézipart, az információs szolgáltatásokat, a kormányzatot, az egészségügyet, a közlekedési és banki szektort célozzák. A támadások típusai között az adatlopások mellett a túlterheléses támadások és a zsarolóprogramok – immár nem csak a támadások száma, hanem a bűnbandák és a geopolitikai érdekek által vezérelt háttérszereplők növekvő összejátszása következtében – kiemelt és növekvő veszélyt jelentenek. Emellett az ENISA kiemeli, hogy Oroszország Ukrajna ellen indított háborúja következtében tovább növekedett az információmanipuláción és az online befolyásoláson alapuló, illetve a létfontosságú és ipari infrastruktúrák elleni támadások száma is (ENISA, 2023; 2024).

AZ ENISA ÁLTAL VIZSGÁLT KIBERINCIDENSEK FŐBB TÁMADOTT SZEKTOROK SZERINT, 2023.VII.–2024.VI.

Forrás: Infoszolg/ENISA, 2024.

Az EU kiberbiztonsági szabályozása

A dinamikusan változó, egyre növekvő és összetettebb fenyegetettségre reagálva az EU az utóbbi években minden korábbinál fokozottabb figyelmet szentelt a kibertámadások elleni európai ellenállóképesség kiépítésére és erősítésére, az elavult kiberbiztonsági szabályok felülvizsgálatára, valamint a kiberbiztonság részterületeinek átfogó szabályozására. Ennek során az EU 2019-ben az ENISA-ról, valamint az infokommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelettel [(EU) 2019/881] hatályon kívül helyezte a 2013-ban elfogadott első átfogó uniós kiberbiztonsági rendeletet.

A Bizottság 2020-ban a Biztonsági Unióra vonatkozó stratégia [(COM(2020) 605 final] pillérévé tette a digitális infrastruktúrák kiberbiztonságát és a kiberbűnözés elleni küzdelmet, emellett a digitális évtizedre vonatkozóan uniós kiberbiztonsági stratégiát is elfogadott [(JOIN(2020) 18 final]. E stratégia felülvizsgálatára az EU Tanácsa – az EU jövőbeni kiberbiztonságának növeléséhez szükséges lépések sorában – idén májusban kérte fel a Bizottságot (10133/24).

2021-ben a Tanács és a Parlament irányelvet fogadott el a pénzügyi ágazat digitális működési rezilienciájáról [(EU) 2022/2554], átdolgozta és hatályon kívül helyezte a 2016-ban elfogadott információ- és hálózatbiztonsági jogszabályt [(EU) 2022/2555, NIS2 irányelv], valamint új irányelvet fogadott el a kritikus szervezetek ellenállóképességéről is (CER irányelv, [(EU) 2022/2557].

2023-ban az Unió digitális igazgatásának biztonsága érdekében új szabályozás került elfogadásra az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságáról (EU, Euratom) 2023/2841]. Emellett a Bizottság a kiberbiztonsági készségek és a képzett szakemberek számának növelésére 2023-ban elindította a Kiberképességek Akadémiáját. A kibertámadások számának növekedése ugyanis – amint arra a legutóbbi Eurobarometer felmérés és az ENISA is rávilágít – kapcsolatban van a kiberbiztonsági szakemberek hiányával és képzettségbeli hiányosságaikkal is (Eurobarometer, 2024; ENISA foresight, 2024).

A Bizottság 2023-ban egy úgynevezett kiberszolidaritási javaslatot is előterjesztett (COM(2023)209 final). A jogalkotási folyamat utolsó fázisában lévő tervezet fő célja, hogy egy európai kiberbiztonsági riasztóhálózat, valamint reagálási mechanizmus létrehozásával megerősítse a jelentős fenyegetések és támadások észlelésére, illetve a felkészülésre és reagálásra szolgáló kapacitásokat.

Részben az adathalász támadások visszaszorítása és a digitális egységes piac megbízhatóságának növelése érdekében 2024-ben módosításra került a digitális személyazonosságról szóló rendelet is [(EU) 2024/1183]. Emellett 2024 októberében elfogadták az úgynevezett kiberrezilienciáról szóló rendeletet, amelynek célja, hogy a digitális elemeket tartalmazó – például IoT – termékek az ellátási lánc egészében, teljes életciklusuk alatt biztonságosak legyenek.

A felsorolt jogszabályok közül az Országgyűlés a (EU) 2019/881 rendelet intézkedéseit 2023-ban ültette át a magyar jogrendbe, megteremtve a magyar kibertanúsítási rendszer alapjait (Csiky, 2023). Az erről szóló 2023. évi XXIII. törvény részben már tekintettel volt a NIS2 egyes előírásaira is. A NIS2 irányelv teljes implementációját a Kormány a most benyújtott javaslattal kívánja elvégezni.

A NIS2 irányelv

A 2016-ban bevezetett hálózat- és információbiztonságról szóló irányelv [(EU) 2016/1148, továbbiakban NIS-irányelv] konkrét célja az volt, hogy a tagállamok körében egységes, magas szintű kiberbiztonságot érjen el. A jogszabály felülvizsgálata azonban rámutatott, hogy a nem egyértelmű szabályozás miatt annak végrehajtása nem teljes körű. A vizsgálat rámutatott továbbá, hogy bár a NIS-direktíva növelte a tagállamok kiberbiztonsági képességeit, de továbbra is jelentős különbségek mutatkoznak az egyes tagállami kiberbiztonsági szintek és kapacitások között.

Emellett az irányelv születését követően a felgyorsult digitalizáció és az összekapcsoltság megnövekedett mértéke következtében szükségessé vált, hogy további ágazatok kerüljenek be a NIS-irányelv hatálya alá (SWD/2020/345 final).

A NIS 2 irányelv [(EU) 2022/2555] új ágazatokra és szervezetekre terjeszti ki hatókörét, ezáltal az új szabályok az EU valamennyi, kritikus ágazatokban tevékenykedő ipari és nem ipari szervezetét, valamint azok beszállítóit is érintik. Emellett megerősíti a kockázat- és incidenskezelést, a szervezetek incidensbejelentési kötelezettségét, illetve az eseménykezelő szervezetek uniós szintű együttműködését is (CSIRT-hálózat). Az irányelv célul tűzi ki továbbá a nagyszabású kiberbiztonsági eseményekre való közös válságreagálás céljából egy Kiberválságügyi Kapcsolattartó Hálózat létrehozását is (EU-CyCLONe).

A követelmények betartására a NIS2 szigorúbb szankciókat vezet be annak érdekében, hogy az EU-ban az egységes, magas szintű kiberbiztonság mielőbb létrejöhessen (EUR-LEX: NIS2 összefoglaló).

Az irányelv végrehajtásához kapcsolódó bizottsági rendelet 2024. október 17-én került kiadásra (C(2024)7151).

Magyarország kiberbiztonsága

Az uniós szabályozás kialakulásával párhuzamban 2013-ban a Kormány elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiáját (1139/2013. (III. 21.) Korm. határozat). Ezen stratégia mentén került kidolgozásra az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), majd került felállításra az információbiztonság szervezetrendszere. 2015-ben, az Ibtv. módosításával az intézményi rendszer egy része központosításra került. A Nemzetbiztonsági Szolgálatok alárendeltségében létrejött a Nemzeti Kibervédelmi Intézet, amely az információ- és hálózatbiztonsági terület központi – s így a digitális szolgáltatókért felelős illetékes – hatóságként működik, és egyben átvette a korábbi kormányzati eseménykezelő központ (GOV-Cert) feladatait is. Az NKI emellett az EU kiberbiztonsági együttműködési csoportjában a nemzeti kapcsolattartó szervezet szerepét is betölti. Az NKI mellett speciális szervezetek védik továbbá a katonai rendszerek (KNBSZ, MH Kiber- és Információs Műveleti Központ), valamint az állami létfontosságú infrastruktúrák (BM OKF) kiberbiztonságát. A kiberbiztonsági eseménykezelő központok és szervezetek működésének részletes szabályait a 271/2018. (XII. 20.) Korm. rendelet tartalmazza.

A korábbi, 2016-os NIS-direktíva következményeként 2018-ban megszületett a 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról, amely az új és dinamikusan változó kiberfenyegetésekre kívánt reagálni.

A Kormány kiberbiztonsági stratégiai szemléletét és céljait Magyarország Nemzeti Biztonsági Stratégiája tartalmazza (163/2020. (IV. 21.) Korm. határozat).

Források:

- Az Európai Unió kiberbiztonsági politikái – Az Európai Bizottság honlapja
- A hálózati és információs rendszerek kiberbiztonsága (2022) – EUR LEX összefoglaló
- Mar Negreiro: The NIS2 Directive: A high common level of cybersecurity in the EU, EPRS, 2023.
- ENISA: Threat Landscape 2024
- Europol: Internet Organised Crime Threat Assessment (IOCTA), 2024

Készítette: Baranyi-Müller Tamás
Képviselői Információs Szolgálat
E-mail: infoszolg@parlament.hu

infoszolg

Internet: www.parlament.hu/infoszolg
Intranet: intra.parlament.hu/infoszolg/
Telefon: (1) 441-6486