TERTÁK ELEMÉR - KOVÁCS LEVENTE

Kiberbiztonság – kibertér

TERTÁK ELEMÉR - KOVÁCS LEVENTE

Kiberbiztonság – kibertér

MAGYAR BANKSZÖVETSÉG

Magyar Bankszövetség

Budapest, 2025

TERTÁK ELEMÉR - KOVÁCS LEVENTE

Kiberbiztonság – kibertér

Magyar Bankszövetség

Tartalom

Tartalom

Bevezető

A mindennapi pénzügyek terén az informatikai és kommunikációs technológiáknak a múlt század végén beindult hatalmas fejlődése forradalmi változásokat hozott. A bankolás gyakorlata a vállalatok és az egyének számára egyaránt hatalmasat változott: Egyfelől nagymértékben csökkent, egyszersmind tartalmilag is módosult a hagyományos bankfiókok és a banki dolgozók szerepe, feladata. Másfelől lehetővé vált a bankszámlák éjjel-nappal való elérhetősége szinte bárhonnan; önkiszolgálóvá vált a személyes bankszámlákról történő utalás, lehetővé vált az utalások és a bevételek jóváírásának az úgyszólván azonnali végrehajtása. Mindez lehetővé tette a határokon belüli és túli e-kereskedelmet, hiszen a megrendelt áruk ellenértékének kiegyenlítése valós időben megtörténhetett, emiatt az eladónak nem kellett a vevőt személyesen ismernie, hitelképességét megvizsgálnia, hiszen mindezt az azonnali fizetés lehetősége szükségtelenné tette. A „hálózatosítással" – azaz a számítógépek és a mobileszközök sűrű szövésű, világméretű hálózatba történt szerveződésével – hatalmas költségcsökkenés és óriási időmegtakarítás vált lehetővé, aminek előnyeiből a pénzügyi szolgáltatók és az ügyfeleik egyaránt részesültek. Noha a hagyományos készpénz használata nem szorult ki még a pénzforgalomból, a termelők, a fogyasztók és a kereskedők közötti fizetéseken belül jócskán megnőtt a digitális fizetés részaránya.

A technológia fejlődésével megnyílt innovatív pénzügyi megoldások az alacsonyabb költségek, a gyorsabb lebonyolítás és a nagyobb kényelem miatt gyorsan elterjedtek, annál is inkább, mert a fogyasztók oldalán az elektronikus bankoláshoz szükséges eszközre – döntően az okostelefonra – más igények és szükségletek kielégítéséhez is szükség volt. Ráadásul az okostelefonok napjainkra már a kispénzű rétegek számára is elérhetővé váltak. Napjainkban a világ 8 milliárdos lakosságának már 95%-a rendelkezik mobiltelefonnal, és a lakosság mobiltelefóniás lefedettsége 2022-ben meghaladta a 97%-ot, a nagysebességű 5G hálózati lefedettség pedig 2024-ben elérte az 51%-ot.

A mobiltelefónia széles elterjedtsége – ami az emberek közötti kapcsolatteremtésre és kapcsolattartásra is óriási hatást gyakorolt – rövid idő alatt hatalmas adattömeget generált, amelynek jelentős hányada tartósan tárolódik a kommunikációs szolgáltatók – tehát a mobiltelefon-szolgáltatók, a kommunikációs vállalkozások, a szociális média vállalkozások, a kereskedők és a bankok, valamint a hatóságok – adatbázisaiban. Ezt az összetett és gyorsan növekvő méretű adathalmazt nevezi a szakmai zsargon big datá-nak (vagyis nagy adatbázisnak), melynek feldolgozására és elemzésére a hagyományos adatkezelési módszerek már nem alkalmasak; ehhez nagysebességű számítógépekre, hatalmas kapacitású szerverekre és nagy átvitelképességű hálózatokra van szükség. A big data adattömegének elemzése alapján a vállalkozások és a szervezetek jobban tudják követni és elemezni a piaci folyamatokat, az ügyfelek viselkedését és további más releváns információt, ami segíti őket az irányításban és döntéshozatalban. A big data

olyan innovációk forrásává válik, melyek új piacokat tárnak fel és új üzleti lehetőségeket teremtenek. A hatalmas adatmennyiség feldolgozását technikailag a nanotechnológia eredményei, módszertanilag pedig az adatbányászat (data mining), a mesterséges intelligencia (artificial intelligence – AI), a prediktív elemzés (predictive analysis) és a gépi tanulás (machine learning – ML) módszerei teszik lehetővé. Napjainkra a big data felhasználásának korszakába érkeztünk, amelyben újabb forradalmi változások mennek végbe a szolgáltatások szinte teljes spektrumában, köztük a pénzügyek terén is. Így például az ügyfélszolgálati teendők egyre nagyobb hányada már automatizált, de kiterjedt és összetett irányítási és vezérlési feladatok is – köztük például a járművek vezetése– automatizálhatóvá válnak, sőt élethűnek tűnő, ám hús-vér szereplők nélküli filmek és hangjátékok is készülhetnek.

Amilyen óriási kényelmet és hatékonyságnövelést tett lehetővé a közelmúltban a társadalmaknak a technológiai, média- és telekommunikációs (TMT) szektor fejlődése, napjainkban pedig a big data hasznosítása, ugyanolyan nagyarányú függőséget és kiszolgáltatottságot is teremtett. Egyfelől a korszerű vezérlési rendszerek használata nélkülözhetetlenné vált a mindennapi életben. Másfelől az egyre több feladatot ellátó rendszerek és adatközpontok működtetéséhez növekvő mennyiségű villamos energiára van szükség a szerverek, a hűtőrendszerek és a kapcsolódó infrastruktúra energiaszükséglete miatt: világviszonylatban ez a teljes villamosenergia-termelés 1,5-3%-át teszi ki. Ez a részarány az első pillantásra csekélynek tűnhet, ám 2025 tavaszán Spanyolországban és Portugáliában emberek milliói kényszerültek megtapasztalni, hogy az energiaellátás akár átmeneti kiesése is milyen nagy mértékben bénithatja meg egész országrészek működését. Az elektromos hálózat összeomlása miatt az ibériai félsziget jelentős részében teljesen megszűntek a digitális szolgáltatások, köztük a digitális fizetés is, Ezen pedig többnyire még a hagyományos készpénzes fizetés lehetősége sem tudott segíteni, hiszen az áramszolgáltatás hiányában a boltok pénztárgépei sem működtek.

Az említett hatalmas technológiai változások azonban nem csupán a társadalmak növekvő kiszolgáltatottságához vezettek, de nem hagyták érintetlenül a társadalmakat és az egyéneket fenyegető bűnözést sem. A bűnözés indítékai az emberiség fejlődése és a technológiai haladás során ugyan mit sem változtak, azonban a bűncselekmények elkövetési módszerei és eszközei gyorsan követték a végbement hatalmas technikai változásokat. E változások nyomán a bűnözés terén csökkent a fizikai erőszak alkalmazása, viszont a bűnelkövetés hatótávolsága már kiterjed a világ egészére. Emellett személytelenné vált az elkövetés; a távoli elkövetőknek az áldozataikat még látásból sem kell ismernie, sőt az áldozat fizikai közelsége, esetleges elesettsége miatt korábban érzett bűntudat visszatartó ereje is megszűnt. Az országhatárokon átnyúló „távolsági" számítógépes bűnözés – szakzsargonban kiberbűnözés – ráadásul megnehezíti a tettesek azonosítását és felelősségre vonását is, hiszen ez a feladat nemzeti szintről áttevődik a nemzetközi szintre.

A kiberbűnözés térnyerése szédítő ütemű, az általa okozott károk pedig napjainkra csillagászati magasságba szöktek. Az előrejelzések szerint a globális kiberbűnözés által

okozott károk értéke 2025-ben több ezermilliárd dolláros nagyságrendet ér el, és az évtizedünk elejeihez képest jelentős növekedést mutat. A károk összege immár megközelíti a világ két legnagyobb gazdasági hatalmának – az Egyesült Államoknak és Kínának – az éves GDP-jét. Ám a károsultak száma sem csekély: becslések szerint évente körülbelül 550 millió áldozata van a számítógépes bűnözésnek világszerte, vagyis átlagosan a Föld minden 15. lakója a kiberbűnözés áldozatául esik.

A technológiai, média- és telekommunikációs szektorban jószerint naponta megjelenő újdonságok miatt szinte lehetetlen a gyorsan elharapódzó kiberbűnözés teljes körű leírása. Átfogó pillanatképet lehetne ugyan készíteni, ám az csakhamar belül idejétmúlttá válna. Ezért – noha a szerzők a kiberbiztonságot fenyegető veszélyeket konkrét példákkal is illusztrálják –, didaktikai megfontolásból is inkább arra törekedtek, hogy olyan módszertanokat ismertessenek meg az olvasókkal, amelyek segítségével ők is követni tudják a kibertérben felmerülő kockázatok terén végbemenő változásokat. Olyan tömör kézikönyvet kívántak megalkotni – egyes elemeiben az AI segítségével –, amely vezérfonalként tud szolgálni a kibertér szüntelenül változó kockázatainak felismeréséhez, és a megfelelő hatékony védekezés kidolgozásához. A kockázatok, a veszélyek bekövetkezését teljességgel már csak azért sem lehet kizárni, mert véletlenek és emberi tévedések bármikor bekövetkezhetnek. A kockázatok időben történő felismerésével és azok megfelelő kezelésével azonban nagymértékben csökkenthető a károk bekövetkezése, illetve mérsékelhető az elszenvedett károk nagysága. A szerzők remélik, hogy e kompendium mindezekben hasznos segítséget tud nyújtani az olvasók számára.

E kézikönyv egy terjedelmes lexikális részt is tartalmaz, mert a kibertér kialakulása, valamint az ott alkalmazott eszközök és szolgáltatások megjelenése először az Egyesült Államokban ment végbe, ennél fogva a szakkifejezések és az ezekből képzett mozaikszavak is angol nyelven születtek meg és terjedtek el. Bár nyelvművelési és nyelvápolási szempontból kívánatos volna az idegen szakszavak, szakkifejezések sokaságát magyarítani, ám ez a már említett szakadatlan műszaki fejlődés miatt soha véget nem érő feladat lenne. Az idegen szavak használatának ennél jóval nyomatékosabb oka pedig az, hogy a kibertér, s így a kibertér kockázatai, valamint a kiberbűnözés egyaránt átfogják az egész világot, ami szükségessé teszi az egyértelmű kommunikációt az egyes nyelvek és országok között. Ennek kézenfekvő „közvetítőnyelve” az angol. A kézikönyv fogalomtára ezért abban is kíván segíteni, hogy a magyar olvasók megismerhessék és alkalmazhassák a világszerte elterjedt és használt angol kifejezések és mozaikszavak értelmét, ugyanakkor bemutatja azok esetleges magyar megfelelőit is.

S ha már a nyelvhasználat került szóba, a szerzők egy rövid etimológiai kitérőre invitálják az olvasót. Egyre többször lehet találkozni a hírekben a kiberbűnözés (cybercrime), a kibertámadás (cyberattack) vagy a kiberháború (cyberwar) kifejezésekkel, továbbá a médiában a különféle informatikai támadásokat egyre többször emlegetik „kiber”-előtaggal. De vajon mit is jelent, és honnan származik a „cyber” („kiber”) előtag? Ez az előtag először a szabályozás, vezérlés, információfeldolgozás, adattovábbítás általános törvényeit vizsgáló tudományág, a kibernetika nevében fordult elő. Ezt a szót e

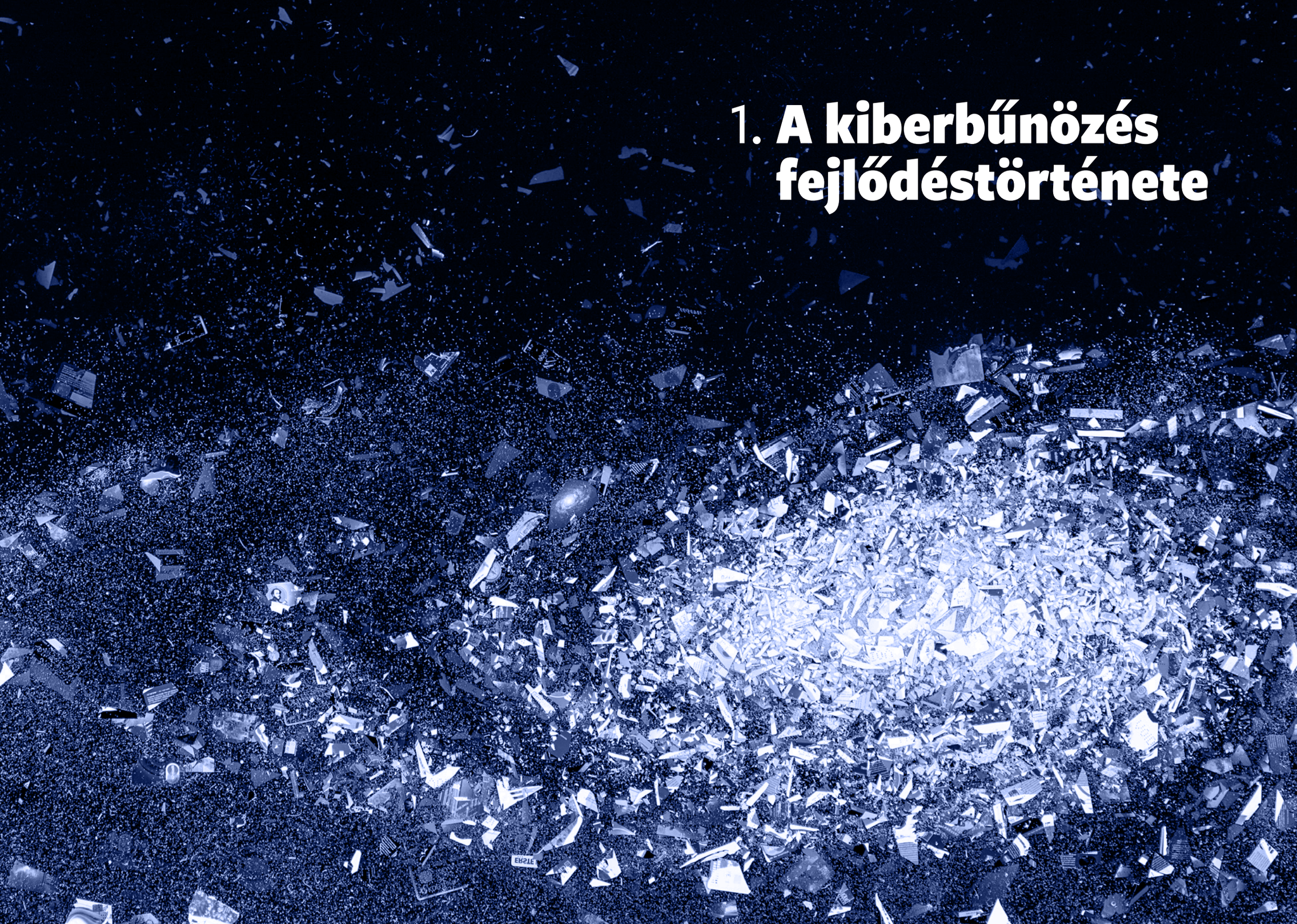
tudományág első jeles művelője, az amerikai Norbert Wiener matematikus alkotta meg a görög kübernétész (kormányos) szóból, a „Kibernetika, avagy irányítás és kommunikáció az állatban és a gépben” címmel 1948-ban megjelent könyvében. William Gibson, amerikai születésű kanadai sci-fi író pedig a nyolcvanas évek közepén megjelent, magyar nyelvre is lefordított egyik regényében egy olyan világot ábrázolt, amelyet egy hatalmas számítógép-hálózat sző át, amit ő kibertérnek (cyberspace) nevezett el.

A szerzők köszönetet mondanak mindazoknak, akik bátorították és segítették e könyv megszületését. Külön köszönettel tartozunk Kerényi Ádámnak a lektorálásért, Sütő Ágnesnek a hazai és nemzetközi kiber-aktualitásokban való kalauzolásért, Vincze Erzsébetnek az anyanyelvi lektorálásért, Németh Dánielnek a nyomdai előkészítésért, továbbá a Kiberpajzs munkájában részt vevő szakembereknek a javaslatokért.

Reméljük, hogy az olvasók e könyvet haszonnal tudják forgatni.

A SZERZŐK

1. A kiberbűnözés fejlődéstörténete



Az elmúlt évtized során a kiberbűnözés hatalmas vállalkozássá nőtte ki magát – egy olyan iparággá, amely évente több ezermilliárd dolláros bevételt generál, és amelyben bűnszervezetek egész hálózata működik. A 2020-as évek közepére a kiberbűnözés széles körű „munkamegosztást" hozott létre: egyes szervezetek például a zsarolóvírusokat terjesztő bűnözők számára kínálnak technikai támogatást fizetett szolgáltatásként (ransomware-as-a-service – RaaS), sőt a legelvetemültebbek a dark weben még nyilvánosan is hirdetik az ilyen szolgáltatásaikat. Ha az egyéni hackerektől kezdve egészen az államilag támogatott hackercsoportokig valamennyi szereplőt figyelembe veszünk, akkor bizony egy nagyon széles és jól felkészült támadói körrel szemben kell a szakadatlanul táguló kibertér biztonságát megvédeni.

Noha a kiberbűnözés az évezred első évtizedének vége óta lendült fel igazán, a kiberbűnözés korántsem tekinthető új jelenségnek, gyökerei ugyanis egészen a korszerű távközlés megszületéséig vezethetők vissza. (Sőt, ha a bizalmas információk csalárd módszerekkel történő megszerzését – vagyis lényegében a kémkedést – is a kiberbűnözés egyik válfajának tekintjük, akkor ezen bűncselekmény gyökerei már az ókorra nyúlnak vissza.)

A korszerű távközlés lényegét a hálózatok jelentik, melyekben az információt fizikai úton továbbítják a végpontok között. Kezdetben az információt optikai úton, fényjelekkel továbbították, ezt követte a távirati és távbeszélő hálózatok vezetékkel összekötött végpontjai és központjai közötti elektromos jelátvitel. Majd a műsorsugárzás és a vezeték nélküli telefónia területén az információt elektromágneses hullámok segítségével, hálózatba kapcsolt adók és átjátszók rendszere közvetíti. Az első távközlési hálózat elleni támadást 1834-ben – vagyis még jóval az internet feltalálása előtt – követték el Franciaországban. Közel két évszázaddal ezelőtt a támadók az akkor még optikai jeltovábbításon alapuló francia távírórendszerhez hozzáférkőzve szereztek meg fontos és bizalmas pénzügyi piaci információkat. (Az optikai távközlési hálózat „feltörését" Alexandre Dumas részletesen leírta a XIX. század közepén megjelent Monte Cristo grófja című regényében. A regény főhőse a távíróhálózaton továbbított üzleti célú dezinformációval döntötte romba egyik árulójának bankját.) A távközlési hálózatok „megcsapolása", valamint az azokon manipulált információk terjesztése a kezdetekben mégis főleg a hírszerzés területén vált elterjedtté.

A távközlés köztörvényes bűnözésre történő felhasználása jóval később, a XX. század végén kezdett gyorsan elterjedni. A távközlés terén is végbement digitális forradalom során ugyanis a kiberbűnözők a digitális technológiák korai alkalmazóivá váltak, akik az ebből eredő előnyüket, valamint szakmai felkészültségüket kiaknázva újabb és újabb fondorlatos módszereket találtak ki, hogy megfosszák az embereket és a vállalatokat bizalmas adataiktól és a pénzüktől. Innentől kezdve a kiberbűnözés szinte exponenciális ütemben nőtt, amit a taktikák, a technikák és az eljárások (Tactics, Techniques, and Procedures, – TTP) gyors fejlődése jellemez – mindezt rosszindulatú haszonszerzés céljából.

Napjainkra a kiberbűnözés kiterjesztette ökoszisztémáját, tele kiszivárogtató oldalakkal, „szolgáltatási" modellekkel, jövedelmező támadásokkal; például üzleti e-mail-fiókok feltörésével, vagy zsarolóvírusok telepítésével évről évre egyre több pénzt tudnak eltulajdonítani vagy kicsikarni szervezetektől és magánszemélyektől.

1. ÁBRA: A kiberbűnözés szereplőinek megkülönböztetett csoportjai

	„Amatőrök"	Hacktivisták	Szervezett bűnözés	Államilag támogatott hackerek
Erőforrás:	Korlátozott technikai erőforrások	Kiterjedt hálózat Erős érzelmi elkötelezettség	Jelentős technikai erőforrások	Csak az állami költségvetés korlátozza
Motiváció:	Hírnév és ismertség szerzése, esetenként személyes sérelemért bosszúállás	Közszereplési lehetőség, zavarkeltés	Gazdasági haszonszerzés	Politikai befolyásszerzés, ellenséges ország közvéleményének vagy pártjainak manipulálása, illetve szolgáltatásainak megbénítása.
Felkészültség:	Nem professzionális. Ismert szoftverhibák kihasználása	Néha alacsony felkészültség, de kíméletlen és célzott támadás	Professzionális, kiforrott bűnszervezet	Nagyon felkészült, türelmes, kreatív, kitartó.

Forrás: Swiss Re Economic Research and Consulting.

A kiberbűnözés főbb mérföldkövei

A továbbiakban időrendben bemutatott esetek a kiberbűnözés történelmi változásának felvázolásán túl azt is tanúsítják, mennyire különböző indítékok vezérlik a kiberbűnözést, milyen gyorsan képes a technológiai haladás az eredményeit a maga hasznára fordítani, végső soron pedig azt is mutatják, milyen mértékben járult hozzá a bűnözők „sikereihez" az áldozatok óvatlansága, felkészületlensége vagy naivitása.

1962. A számítógépes bűnözés modern története akkor kezdődött, amikor Allen Scherr kibertámadást indított a bostoni Massachusetts Institute of Technology (MIT) számítógépes rendszere ellen, és lyukkártya segítségével jelszavakat lopott el az egyetem adatbázisából.

1971. Az első számítógépes vírust Bob Thomas hozta létre kutatási célokra a bostoni BBN Technologies (eredetileg Bolt, Beranek and Newman) cégnél, és megjósolta a vírusok jelentős jövőbeli károsító hatását a számítógépes rendszerekben. A Creeper Virus (kúszónövény vírus) néven emlegetett, önmagát sokszorozó programot 1971-ben észlelték az internet elődjén, az ARPANET-en. Kárt egyáltalán nem okozott a terjesztésével, mert a vírus csupán látványosan kiírta a képernyőre, hogy: "I'm the creeper, catch me if you can!" („Én vagyok a kúszónövény, kapj el, ha tudsz!")

1981. A magát Captain Zap-nak nevező amerikai Ian Murphy volt az első ember, akit elítéltek számítógépes bűncselekmény elkövetéséért, mégpedig az ATT távközlési cég számlázórendszerének megváltoztatásával okozott bevételkiesés és a cég üzleti hírnevének rombolása miatt.

1988. Az első nagyobb internetes kibertámadásra Robert Morris, a new york-i Cornell egyetem hallgatójának „jóvoltából” került sor. A „Morris Worm” („Morris féreg”) a világháló debütálása előtti évben csapott le, amikor az internet még elsősorban az akadémiai kutatók által használt szolgáltatás volt. Megfertőzte többek között a Stanford, a Harvard, a Princeton, a Johns Hopkins és a kaliforniai Berkeley egyetemek, továbbá a NASA, valamint az 1952-ben multidiszciplináris állami kutató- és fejlesztőközpontként létrehozott Lawrence Livermore National Laboratory számítógépes rendszereit. A vírus az akkoriban az internetre csatlakozott összesen 60 ezer számítógép 10%-át érte el és kényszerítette leállásra mindössze 24 óra alatt.

1989. Ebben az esztendőben jelent meg az első ransomware, vagyis az első zsarolóvírus. A zsarolóvírusok első törzsét – az AIDS Trojan, más néven PC Cyborg vírust – még könnyű volt eltávolítani és hatástalanítani. Napjaink gyakorlatától eltérően a zsarolóvírusok terjesztése akkoriban még flopilemezeken történt: a vírus kifejlesztője, Joseph Popp biológus 20 ezer vírussal fertőzött floppyt osztott szét az Egészségügyi Világszervezet montreali AIDS-konferenciájának résztvevői között.

Az 1990-es évek: az új technológiák megteremtik az újfajta bűnözést

Az 1990-es években született meg az emberiség által ismert legjelentősebb kommunikációs technológia, amely forradalmi változást hozott: az internet, ami különböző kommunikációs hálózatokon keresztül összekapcsolta az embereket, bárhol is legyenek a hálózattal átszőtt világon.

Ám ez a fejlődés nem csupán kedvező változásokat eredményezett, ugyanis az új technológiák használatával elterjedt a kiberbűnözés is és gyors fejlődésnek indult. A hackerek és más rosszindulatú szereplők kihasználták, hogy az új technológiák fejlesztése és bevezetése kezdetén még feltétel nélküli bizalom uralkodott a részvevők között, ezért biztonsági intézkedések és ellenőrzések bevezetésére még nem került sor.

A kiberbiztonság ekkoriban még egy nem létező fogalom volt, nemhogy aktív szakterület. Ezeknek az éveknek a fókuszában a gyors kommunikáció és az üzleti hatékonyság úttörő alkalmazásainak létrehozása állt. Időközben azonban a bűnözés is felfedezte az új technológiák haszonszerzésre fordítható potenciálját akár bizalmas információk megszerzése útján, akár különböző számítógépes vírusok zsarolásra történő felhasználásával.

Az AOL, az évtized vezető amerikai internetszolgáltatójának hálózata, akaratlanul is a kibertámadások helyszínévé vált, mivel ott a kiberbűnözők adathalász támadásokat indítottak, ellopták a felhasználókat hitelesítő adatokat, és kéretlen, tömeges e-mailekkel árasztották el a többi AOL-felhasználót, hogy ezzel zsarolhassák a céget.

A kiberbűnözés gyors terjedése azt jelezte, hogy a bűnözők hamar megtalálták a lehetőséget, hogy jogosulatlanul behatolhassanak különböző kommunikációs rendszerekbe, hozzáférjenek az ott tárolt adatokhoz, vagy akár manipulálják azokat.

Az 1990-es évtized néhány figyelemre méltó kiberbűncselekménye

1994. A magát Datastream Cowboy-nak nevező 16 éves brit iskolás fiú és „Kuji” nevű bűntársa egy „jelszó-szippantó” programot használt ahhoz, hogy támadássorozatot indítson, amivel megbénították az amerikai légierőnek a georgiai Rome-ban lévő laboratóriumát, és ellopták a harci repülőgépek támadási utasításaiként használt adatokat.

1995. Vladimir Levin volt az első ismert hacker, aki megpróbált kirabolni egy bankot – méghozzá mindjárt egy óriás bankot. Feltörte a Citibank hálózatát, és számos csalárd tranzakciót hajtott végre. Mindent összevetve több mint 10 millió dollárt utalt át a világszerte nyitott különböző bankszámláira.

1995. Kevin Mitnick – az egyik leghírhedtebb hacker – volt az első, aki úgy jutott be a nagy hálózatokba, hogy pszichikailag manipulálta az embereket, és így megszerezte tőlük a kódokat többek között a Motorola, Sun Microsystems és a Nokia szervereibe történő behatoláshoz.

1998. Max Butler, számítástechnikai biztonsági tanácsadó, aki az FBI informátora volt, megtévesztő ürügyek segítségével feltörte az amerikai kormányzat több weboldalát is. E tetteiért 18 hónapos börtönbüntetést kapott. Később egy újabb illegális támadásért visszaesőként 13 évre ítélték, ami a hackerek esetében rekordnak számít.

1999. A számítógépes vírusok viszonylag sokáig ismeretlenek maradtak a nagyközönség számára egész addig, amíg a Melissa nevű vírus 1999 márciusában le nem csapott. Az internetre feltöltött, felnőtt videókhoz való hozzáférést ígérő dokumentum vírusa átvette az irányítást az egyének Microsoft Word alkalmazása felett, innen átterjedt a Microsoft Outlook levelezőprogramra, és különféle e-mail fiókokba küldve terjesztette magát. Becslések szerint 80 millió dolláros kárt okozott, és az egyik első nagy vírus volt, amelyik túllépett az AOL hálózatán.

Az új évezred: a kiberbűnözés térnyerése

Ahogy az új évezred első évtizedében a pénz- és a fizetési forgalom lebonyolítása egyre inkább átterelődött a távközlési hálózatokra, egyre felkészültebb támadások indítására került sor, továbbá számos fejlett állandó fenyegetés (Advanced Persistent Threat – APT) is született, amelyek kifejlesztését esetenként egyes országok is szponzorálták. A kiberbűnözés fejlődése egyre több számítástechnikai vírus megjelenéséhez vezetett, amelyek bevetése jelentős károkat okozott a globális, digitális gazdaság kritikus ágazataiban.

Az évtized végére a kiberbiztonság fenyegetettsége már mindenhol aggodalomra adott okot a számítógép-felhasználók – mindenekelőtt a kormányzati szervek és a nagyvállalatok – körében, mert ez a fenyegetettség számukra egyre inkább egzisztenciális, illetőleg politikai és rendszerstabilitási kockázatot is jelentett.

Az új évezred első évtizedének a legjelentősebb kiberbűncselekményei

2000. Egy 15 éves kanadai hacker, Michael Calce, aki a „Mafiaboy” álnevet használta, elosztott szolgáltatásmegtagadási (DDoS) támadások sorozatát indította a világ legnagyobb kereskedelmi webhelyei ellen, mint például az Amazon, a Yahoo, a CNN és az eBay ellen. A támadás esetenként órákra is megbénította e cégek weboldalait, és ezzel becslések szerint 1,2–1,7 milliárd dollárnyi kárt okozott a vállalkozásoknak.

2000. Egy jelentős adathalász támadás történt az ILOVEYOU elnevezésű vírus terjesztésével, amelyet gyakran Lovebug (szerelembogár) vagy Loveletter (szerelmeslevél) vírusnak is neveztek. Ez a vírus több mint 10 millió személyi számítógépet fertőzött meg világszerte. A felhasználók által véletlenül megnyitott spam e-mailként terjedt, és a Windows egy hibáját kihasználva a teljes operációs rendszerhez hozzáfért. Az Onel de Guzman, egy Fülöpszigeteki amatőr hacker által útjára indított fertőzés milliárdos károkat okozott szerte a világon. Tíz nap alatt több mint ötvenmillió fertőzést jelentettek, és becslések szerint a világon az internetre csatlakozott számítógépek 10%-a volt érintett. A károk főként a fertőzéstől való megszabadulással és a fájlok biztonsági másolatokból való helyreállításával töltött időt és erőfeszítést jelentik. Abban az időben ez volt a világ egyik legpusztítóbb számítógépes katasztrófája.

2005. Egy amerikai kiskereskedőnél keletkezett biztonsági rés a HSBC Bank 1,4 millió bankkártya-tulajdonos ügyfele adatainak kiszivárgását tette lehetővé.

2006. Megjelenik az első olyan zsarolóvírus-törzs, amely fejlett RSA titkosítást[1] használ, az Archievus. Az RSA-titkosítás, vagy a nyilvános kulcsú titkosítás ettől kezdve a legtöbb zsarolóvírus-támadás alapértelmezettje lett.

2008. A valaha volt egyik legnagyobb jogsértés során a Heartland Payment Systems fizetési rendszert SQL[2]-injektálás, jelszó-szippantók és rosszindulatú programok kombinációjával támadták meg, ami 134 millió felhasználó adatait veszélyeztette.

2010-es évek: a kibertámadások robbanásszerű megjelenése

2010 és 2019 között robbanásszerű növekedésnek indult a kiberbűnözés, aminek következtében a kezdetben kisipari módon űzött tevékenység hatalmas, globális méretű vállalkozássá vált. A bűnözők számtalan új, rosszindulatú támadó programot és technikát fejlesztettek ki, amelyek növelték a kiberbűnözés arányát és a napi támadások számát. Az ezek által okozott károk pedig ezer milliárd dolláros nagyságrendet értek el.

Az évtized folyamán különösen a zsarolóvírusos támadások erősödtek fel, jórészt annak betudhatóan, hogy a mobileszközök, az új operációs rendszerek és a sötét web

1 Az RSA nyilvános kulcsú titkosító rendszer, az egyik legrégebben széles körben használt biztonságos adatátviteli rendszer. Az „RSA” rövidítés Ron Rivest, Adi Shamir és Leonard Adleman vezetékneveiből származik, akik 1977-ben nyilvánosan leírták az algoritmust.

2 A Structured Query Language (SQL) egy programozási nyelv, amelyet relációs adatbázisokban tárolnak és dolgoznak fel információkként. A relációs adatbázisok táblázatos formában tárolják az információkat, ahol a sorok és oszlopok a különböző adat-attribútumokat és az adatértékek közötti különféle kapcsolatokat jelölik.

elterjedése, továbbá a kriptovaluták megjelenése új utakat nyitott és új erőforrásokat teremtett a zsarolásos támadásokhoz. A következő ábra szemléletes áttekintést nyújt arról, hogyan alakult a kiberbűnözés ebben az évtizedben:

2. ÁBRA: A kibertámadások fejlődése 2000 és 2020 között

Év	Jellemző kibertámadási módszer
2011	A jelentős adatvédelmi incidensek állandósulnak
2012	A támadások terjedése más, nem PC-alapú platformokra – például mobileszközökre, közösségi platformokra stb.
2013	Fejlett online banki fenyegetések jelennek meg, pl. Zeus’Zbot
2014	Sokrétű, széles körben elterjedt kibertámadások
2015	Nagy botnetek pl. BeeBone leállítása
2016	Elterjedtek a zsarolóvírusok és az online zsarolások
2017	A zsarolóvírusok globális terjedése megbénítja a vállalatok, az önkormányzatok és egyéb szervezetek működését.
2018	„Álhírek”, kiberpropaganda, kriptovaluta-bányász kártevők, valamint a dolgok internetéhez (IoT) tartozó eszközökön keresztüli támadások
2019	A zsarolóvírusok továbbra is megbénítják a szervezeteket és a kormányokat. Az üzleti e-mailek feltörése egyre gyakoribb.
2020	Adathalász és szociális manipulációs támadások a világjárvány idején.

Forrás: IMF

A kiberbűnözés gyors elterjedése szervezett védekezési intézkedéseket indított el. A vállalkozások és intézmények egyre nagyobb számban alkalmaztak kiberbiztonsági szakembereket, és egyre több beruházást hajtottak végre a kiberfenyegetések kockázatának leküzdésére, mivel a kiberbűnözés terjedése szertefoszlatta a digitális tér biztonságába vetett addigi hitet és egyre nagyobb mértékű veszteségeket okozott. Az adatbiztonság iránti megnövekedett igény eredményeként pedig kialakult egy új tevékenység, az etikus hackelés is, amelynek egyetlen célja a számítástechnikai rendszerek és programok sebezhetőségek felfedezése és kijavítása még azelőtt, hogy azokat rosszindulatú bűnözők kihasználhatnák. A kiberbűnözés által okozott károk növekedése kiváltotta a bűnüldözéssel foglalkozó állami szervezetek – így a rendőrség, az elhárítás, az ügyészség és a bíróságok fokozott figyelmét –, ami a kiberbiztonság védelmére szakosított egységek, illetőleg csoportok létrehozásához vezetett.

Az évtized végére a különböző típusú kiberfenyegetések egyre kifinomultabbá válása, továbbá a támadások gyorsan növekvő száma elbizonytalanította a vállalatokat és az intézményeket az ellenük való védekezés eredményességét illetően, ami gyengítette a védekezést célzó erőfeszítéseket és óhatatlanul a bűnözők malmára hajtotta a vizet.

Az elmúlt évtized legkártékonyabb támadásai

2010. A Stuxnet elnevezésű rosszindulatú számítógépes féreg – amelyet a világ első „digitális fegyverének” is neveztek – megtámadta és súlyosan károsította az iráni urándúsító létesítményeket. A vírust a fehérorosz „VirusBlokAda” cég fedezte fel Iránban, a bushehri atomerőmű egyik számítógépén. A feltételezések szerint az USA-ban és/vagy Izraelben államilag szponzorált hackercsoport által az „Olimpiai Játékok” nevű titkos hadművelet keretében kifejlesztett vírus Iránban mintegy 45 ezer irányítási feladatot ellátó számítógépet és szervert fertőzött meg, súlyosan visszavetve az ország saját atombomba előállítására irányuló erőfeszítéseit.

2010. A Zeus trójai vírust a bűnözők e-mailben terjesztették az egész világon a pénzügyi szolgáltató szervezeteket célba vevő támadások során. A több mint 100 fős bűnözői hálózatnak, amelynek központját az Egyesült Államokban találták meg, e vírus alkalmazásával több mint 70 millió dollárt sikerült ellopnia amerikai bankoktól. A Zeus vírus (vagy Zeus Trojan malware) egy olyan rosszindulatú szoftver, amely a Microsoft Windows rendszert támadja, és amelyet pénzügyi adatok ellopására alkalmaznak. Az először 2007-ben észlelt Zeus trójai vírus, vagy más néven Zbot, a világ egyik legsikeresebb botnet-szoftvere lett, amely számítógépek millióit fertőzte meg, és számos hasonló kártevő-változat kifejlesztését is ihlette. Míg a Zeus vírus jelentette fenyegetés mérséklődött, amikor létrehozója 2010-ben állítólag nyugdíjba vonult, a vírus forráskódjának nyilvánosságra kerülése után rövidesen több új mutáció is megjelent a színen, így ez a rosszindulatú program ismét relevánssá és veszélyessé vált.

2010. Az Aurora hadművelet egy kínai katonai hackercsoportnak tulajdonított kibertámadás-sorozat volt, amely amerikai nagyvállalatokat célzott meg. A támadók célzott adathalász hadjáratot indítottak, amelynek révén feltörték a Yahoo, az Adobe, a Dow Chemical, a Morgan Stanley, a Google és még legalább két tucatnyi további amerikai nagyvállalat hálózatait, hogy megszerezzék üzleti titkaikat.

2011. A Sony Corporation áprilisban bejelentette, hogy néhány nap leforgása alatt a hackerek a PlayStation Network 77 millió felhasználójának tették lehetetlenné a hálózat elérését. Az ellopott információk a játékosok felhasználónevét és jelszavát, születési dátumát, a biztonsági kérdésekre adott válaszokat és még sok egyéb mást tartalmaztak. A rendszer helyreállítása és a fenyegetés elhárítása 23 napot vett igénybe.

2013. Minden idők talán legnagyobb horderejű adatlopását Edward Snowden leplezte le, amikor nyilvánosságra hozta, hogy az Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) PRISM titkos megfigyelési programjával több külföldi kormánytól és magánszemélytől lopott el bizalmas adatokat és információkat. Az Oroszországban menedéket kért Snowdenre a történészek úgy fognak emlékezni, mint a történelem egyik legnagyobb hatású leleplezőjére (whistleblower[3]-jére), aki sokak számára vált hőssé, míg mások szemében árulóvá. Tettéről több film is készült.

3 A whistleblower (magyarul: sípfúvó) kifejezés onnan ered, hogy az angol rendőrség régebben sípszóval hívta fel a figyelmet egy folyamatban levő bűncselekményre.

2013. Az amerikai Target kiskereskedelmi vállalat mintegy 100 millió ügyfelének hitelkártya-adatait lopták el egy adathalász támadás során, ami az Egyesült Államok eddigi történetének egyik legjelentősebb adatvédelmi incidense. Az ellopott vásárlói adatokat a „kártyaboltoknak” nevezett online feketepiaci fórumokon kínálták eladásra. Az amerikai szenátus Kereskedelmi Bizottsága 2014 márciusában arra a következtetésre jutott, hogy a Target cég elmulasztotta a lehetőségeket az ilyen katasztrofális kimenetelű jogsértés megakadályozására, mivel a cég biztonsági szolgálata már a betörés előtt aggodalmának adott hangot értékesítéshelyi terminál-rendszereik (POS-rendszereik) ismert sebezhetősége miatt, ám a cég vezetői nem tettek lépéseket a jelzett problémák megoldására. Független források becslése szerint az ellopott hitelkártyaadatokból eredő költségek 250 millió és 2,2 milliárd dollár között mozognak. A Target cég ellen eddig több mint 80 kártérítési pert indítottak.

2013. Egy kutató felfedezte, hogy a finn Nokia távközlési cég lényegében közbeékelődéses támadást hajtott végre okostelefonjainak felhasználói ellen azáltal, hogy egy információátviteli protokollal adatcsomagokat küldött a szerverein keresztül, majd visszafejtette azok adattartalmát. A vállalat azzal védekezett, hogy ezzel elősegítette az adatok tömörítését, ezáltal pedig a hálózathasználati díjak csökkentését.

2013. A CryptoLocker, az első zsarolóprogram, amelyet botnet terjesztett, demonstrálta mind a kiberbűnözőknek, mind a kiberbiztonsági szakma képviselőinek, hogy egy zsarolóvírus (ransomware) valójában milyen könnyen terjeszthető és veheti át a megtámadott rendszerek irányítását.

2013. Egy mára hírhedtté vált és azóta is gyakran emlegetett adatsérelem során 38 millió Adobe-felhasználó adatai, köztük hárommillió hitelkártya adatai szivárogtak ki az interneten. Az Adobe cég informatikai biztonságért felelős vezetője egy interjúban kijelentette, hogy a felhőben történő tárolásra való áttérés tette sebezhetővé az Adobe-t a fenyegetés szereplőivel szemben.

2014. A „Celebgate” botrány során bűnözők szerezték meg több híresség feltört iCloud-fiókjából a meztelen és intim fotókat, majd azokat kiszivárogtatták az interneten. A szakértők a kezdetben úgy vélték, hogy az Apple iCloud felhőszolgáltatás vagy az iCloud API biztonsági hibája miatt tudtak a hackerek hozzáférni a képekhez. Az Apple egy későbbi sajtóközleményben azonban azt állította, hogy a tettesek a fiókokhoz való hozzáférést lándzsás adathalászattal szerezték meg. A lándzsás adathalászat egy olyan új csalási technika, amely során a támadók személyre szabott üzenetekkel próbálják tőrbe csalni a potenciális áldozatot. Ez a hack új figyelmet irányított a jelszóhigiéniára és a mobileszközök biztonságára.

2015. Az amerikai védelmi minisztérium fontos célpontjai ellen, személyre szabott e-mailek felhasználásával végrehajtott sikeres orosz adathalász támadás 4 000 olyan katona és polgári alkalmazott adatainak megszerzéséhez vezetett, akik az egyesített vezérkari főnökségnél dolgoztak. A támadás arra kényszerítette a Pentagont, hogy leállítsa levelezőrendszerét.

2015. Az Impact Team néven ismert számítógépes bűnözői csoport kiszivárogtatta az Ashley Madison, félrelépések közvetítésére szakosodott, 37 millió regisztrált felhasználóval rendelkező fizetős társkereső oldal belső adatbázisát. A csoport kezdetben váltságdíjat követelt és az oldal bezárását szorgalmazta, majd miután az Ashley Madison ellenállt a zsarolásnak, az adatbázist a bűnözők nyilvánosságra hozták. Ez a bűncselekmény rávilágított az adatbiztonság fontosságára, különösen a felhasználói adatok védelme tekintetében, mivel a webhely archiválta és megőrizte a korábbi felhasználók személyes adatait, beleértve a hitelkártya-adatokat és a valódi nevüket.

2016. Megjelent a TeleCrypt orosz eredetű ransomware, amely internetes online játékok résztvevőit támadta meg. Szerencsére a Malwarebytes kutatói gyorsan létrehoztak egy ingyenes visszafejtő eszközt.

2016. A Petya elnevezésű zsarolóvírus-változattal történő támadás elsősorban Ukrajna kormányzati, pénzügyi és infrastrukturális rendszereire irányult, de gyorsan tovább terjedt. (A Petya az „Aranyszem" /Golden Eye/ című, 1995-ös James Bond film két atombombát szállító műholdja egyikének a neve.) A hagyományos zsarolóprogramokkal ellentétben, amelyek fájlok titkosításával akarnak pénzt kicsikarni az áldozatoktól, Petya valódi célja az adatok megsemmisítése volt. Visszafordíthatatlanul törölte az adatokat a fertőzött rendszerekről, így szinte lehetetlenné tette a helyreállítást ott, ahol nem készítettek rendszeresen biztonsági mentéseket. A támadást geopolitikai jellege miatt egyes körökben az orosz állam által támogatott kiberszereplőknek tulajdonítják, főként azért, mert súlyosan érintette Ukrajnát. A feltételezések szerint a Petya/NotPetya kísérlet lehetett az ukrán infrastruktúra megzavarására, talán az Oroszország és Ukrajna közötti tágabb konfliktus részeként.

2016. Egy osztrák repülőgépipari cégtől, a FACC AG-tól lándzsás adathalász támadással közel 50 millió eurót csaltak ki, mégpedig úgy, hogy megtévesztéssel vették rá a cég pénzügyeit intéző alkalmazottját arra, hogy a pénzt a kiberbűnözők által megadott bankszámlákra utalja. A történtek miatt a részvényesek kirúgták a cég vezérigazgatóját.

2017. Talán a legalattomosabb ransomware törzs, a WannaCry több százezer Windows-os számítógépet fertőzött meg 150 országban. A vírus nem csupán veszélyes volt, de halált okozó is, amennyiben az Egyesült Királyság Nemzeti Egészségügyi Szolgálatának kórházai is a támadás áldozataivá váltak, és ennek következtében a rendszerek megbénulása miatt életmentő műtétek is elmaradtak. Egyes szakértők azt feltételezik, hogy a támadás mögött észak-koreai hackerek álltak.

2017. Alig egy hónappal később, a WannaCry sikerére támaszkodva a NotPetya, a korábbi ransomware törzs frissített változata támadott. Olyan nagy szervezeteket bénított meg, mint a dán Maersk tengeri konténerszállítmányozó óriás, vagy a német Merck multinacionális gyógyszergyártó cég.

2017. Egy litván kiberbűnöző ázsiai gyártónak adta ki magát, hogy megtévessze a Google és a Facebook alkalmazottjait, akikkel több mint 100 millió dollárt utaltatott nyomonkövethetetlen offshore bankszámlákra. A tettest a támadás után két évvel sikerült elfogni. A Google azt állította, hogy sikerült visszaszereznie az ellopott pénzt.

2018. Az eddigi legnagyobb DDoS-támadás során a GitHub – egy népszerű fejlesztői platform – másodpercenként 1,3 terabájt forgalmat észlelt, ami leállította az összes műveletet a szerverein. A GitHub ugyan már korábban számos biztonsági intézkedést vezetett be, jóval többet, mint a legtöbb vállalat, de a támadás puszta mérete így is túlterhelte.

2018. 2018 tavaszán a kiberbűnözők Georgia állam fővárosa, Atlanta városházának több számítógépes hálózatát is feltörték, és SamSam elnevezésű zsarolóvírussal fertőzték meg. A kiberbűnözők megakadályozták a hozzáférést számos önkormányzati online platformhoz és adatbázishoz, a helyreállítás fejében pedig jelentős összegű váltságdíjat követeltek. (A kiberbűnözők feltehetően azért vették célba Atlantát, mert a város közlekedési és gazdasági központként betöltött nemzetközi jelentőségének köszönhetően a támadás széles körű figyelmet kapott.) Atlanta város vezetése azonban nem volt hajlandó kifizetni váltságdíjat. Emiatt a rendszerek helyreállítása több hónapig is eltartott, ami hosszabb időre elérhetetlenné tett különböző önkormányzati szolgáltatásokat, és több millió dolláros kárt okozott. Ez az incidens az egyik legköltségesebb, önkormányzatot ért kibertámadás volt.

2018. A Coinhive kriptovaluta-bányász szolgáltatást több kiberbiztonsági cég is a webfelhasználókra leselkedő egyik legrosszindulatúbb fenyegetésként azonosította. A Coinhive egy olyan kriptovaluta-bányász szolgáltatás, amelyet idegen webhelyekre történő rátelepülésre terveztek. A Coinhive a weboldalát felkereső látogatók számítógépei teljesítményének egy részét (de sokszor egészét) alattomos módon kriptovaluta bányászására használja. A kiberbűnözők 15 hónapon keresztül alkalmazták a rosszindulatú programot eszközök millióinak megfertőzésére, ezáltal számítógépes teljesítményük megcsapolására.

2019. Az amerikai Capital One Financial Corporation a banktörténet egyik legnagyobb adatsértésének áldozata lett, amikor kiberbűnözők több mint 100 millió hitelkártya-kérelemhez férkőztek hozzá, és több ezer társadalombiztosítási és bankszámlaszámot másoltak le. A Capital One banknak mintegy 150 millió dollárt kellett a keletkezett károk enyhítésére fordítania.

2020. Azt követően, hogy az Egyesült Államok 2008-ban javasolta Ukrajna és Grúzia felvételét a NATO-ba, megszaporodtak az amerikai kormányzati intézmények elleni orosz kibertámadások. Ezek közül a legsúlyosabb egy texasi cég elleni támadás volt. A SolarWinds cég az Orion elnevezésű népszerű hálózatkezelő rendszeréhez tett elérhetővé egy szoftverfrissítést az ügyfelei számára. Ezt a rutinszerű szoftverfrissítést használták fel az Orosz Föderáció külföldre irányuló polgári hírszerző szervezete, az SzVR (Szluzsba Vnyesnyej Razvedki) irányítása alatt álló hackerek arra, hogy rosszindulatú kódot csempésszenek az Orion szoftverébe. Ezáltal az orosz hackerek sikeresen hatolhattak be a szoftvert alkalmazó mintegy 100 nagyvállalat és egy tucatnyi kormányzati szerv számítástechnikai rendszerébe. A cégek között volt a Microsoft, az Intel és a Cisco; a megtámadott állami szervek pedig a legfontosabb minisztériumok voltak. Ezt követően az amerikai kormányzat szigorú szankciókat jelentett be Oroszország ellen, amelyeket a SolarWinds behatolására adott „látható és láthatatlan" válaszként jellemzett.

Kiberbűnözés: 2021-től napjainkig

Elveszett dollármilliárdok

Ha a 2010-es évek voltak azok az évek, melyek során a kiberbűnözés jelentős méreteket öltött, akkor 2020-as évek során az ökoszisztémát átalakítva s magát megújítva vált minden korábbinál veszélyesebbé. Ebben az évtizedben a kiberbűnözésnek két fő forrása van: az egyik a kiberbűnözés általános térnyerése, ami egyfelől a technológiai fejlődésből, másfelől egyes országokban végbemenő társadalmi-gazdasági fejlődés sajátosságaiból táplálkozik. A másik fő forrás pedig az egyes végpontok, valamint a globális terjeszkedésre törekvő szervezetek növekvő felhőhasználata jelenti, amelyet a kiberbűnözők kiaknáznak, mivel a felhőszolgáltatók és felhasználóik kiberbiztonsági intézkedései gyakran csak késedelmesen valósulnak meg, ami lehetőséget teremt a sikeres támadásokra.

Mi ment végbe a XXI. század második évtizedének első felében a kiberbűnözés terén?

- A kiberbűnözés napjainkra már ezer milliárd dolláros nagyságrendű „iparággá” vált.
- A kiberbűnözés lett az egyik legsúlyosabb globális üzleti kockázat.
- A jogsértések többsége a felhőn keresztüli adatforgalomra irányul.
- Az adathalászat és a hitelesítő adatok feltörése a kiberbűnözés két legfontosabb támadási módszerének az egyike.
- A másik támadási módszer a zsarolóvírusok fokozott „bevetése”: 2024-ben ez tette ki a támadások hozzávetőleg egynegyedét.
- A kiberbűnözők a pénzügyi szektor mellett egyre gyakrabban vesznek célba nem pénzügyi vállalatokat. Mindenekelőtt az egészségügyi szolgáltatásokat, mert ezen a téren lehet – érthető okokból – a leghatásosabban zsarolni. Ezen túl, az utóbbi években jócskán megszaporodtak a kisebb oktatási szervezetek elleni támadások is, elsősorban alacsony kiberbiztonsági költségvetésük, de még inkább a birtokukban lévő érzékeny hallgatói és alkalmazotti információk miatt. Néhány esztendeje a kiberbűnözők világszerte egyre több iskolát céloztak meg, értékes személyi adatokhoz jutottak hozzá, és olyan súlyos működési zavarokat okoztak, amelyek kedvezőtlenül hatottak a diákokra és az oktatókra egyaránt.

Mint a tények és az adatok mutatják, ebben az évtizedben is folytatódott a kiberbűnözés térnyerése, bár egyes szakértők szerint némiképpen lassult az üteme. Noha a kiberbiztonság megszilárdítása terén gyors fejlődés indult, a kiberbűnözéssel folytatott szakadatlan harcban egyelőre túlterhelt, sokszor létszámhiányos és gyakran nem kellően magasan kvalifikált munkatársakkal rendelkező kiberbiztonsági szervezeteknek kell helytállnia.

2021. Május elején egy feltehetően orosz hackercsoport ransomware támadással több mint három napra működésképtelenné tette a Colonial Pipeline cég üzemanyag-vezetékrendszerét. Mivel az USA keleti partvidékén a Colonial Pipeline biztosítja a jármű- és repülőgép-üzemanyag-ellátás 45%-át, ez súlyos gondokat okozott. Az üzemanyagárak országszerte felszöktek, egyes benzinkutak készlete teljesen kimerült, késtek a közúti szállítások, egyes helyekről pedig benzinfelhalmozásról is érkeztek jelentések.

2021. A hírhedt REvil (Ransomware Evil; más néven Sodinokibi) egy oroszországi vagy oroszul beszélő személyek tulajdonában lévő, zsarolóvírust szolgáltatásként értékesítő (RaaS) hackercsoport zsarolóvírussal támadta meg a floridai székhelyű Kaseya szoftverszolgáltatót, és 70 millió dollárnyi váltságdíjat követelt bitcoinban. Ez a támadás öt kontinens szervezeteit sújtotta: kikényszerítette például több új-zélandi állami iskola és egy svédországi nagy élelmiszerbolt-lánc bezárását, az Egyesült Államokban pedig több száz vállalat működését zavarta meg.

2021. Az esztendő egy „nulladik napi” támadás lehetőségéről szóló beszámolóval zárult, ami hatalmas hullámokat keltett a kiberbiztonsági iparban. Biztonsági kutatók ugyanis közzétették a távoli kódfuttatás („Remote Code Execution” - /RCE/) általi sebezhetőség bizonyítékát a Log4j-ben, egy Java naplózási könyvtárban, amelyet számos internetes alkalmazásban használnak. A következő hetekben a vállalkozások világszerte nagy erőfeszítéssel dolgoztak ennek a sebezhetőségnek a kiküszöbölésén: biztonsági szakemberek és szakértők javításokat és ellenőrző eszközöket tettek elérhetővé, továbbá útmutatást adtak a szervezeteknek az ilyen fajta támadások elleni leghatásosabb védekezéshez.

2022. A kiberbűnözők emberek életét és megélhetését is veszélyeztető támadásainak egyik legijesztőbb megnyilvánulása volt a Costa Rica-i társadalombiztosítási ügynökség május végi ransomware támadása, amely megbénította a közép-amerikai ország teljes egészségügyi ellátó rendszerét. Ráadásul a támadás következményei országszerte más intézményekre is átterjedtek, ami szükségállapot kihirdetését vonta maga után.

2022. Egy szeptemberi hackelés feltűnő mennyiségű adatot tulajdonított el a játékipar egyik titánjától. A Rockstar Games cég Grand Theft Auto 6 játékának várva várt piaci megjelenése komoly nehézségekbe ütközött, amikor a „teapotuberhacker” néven ismert hacker feltörte a Rockstar egyik belső csatornáját, és 90 folyamatban lévő játékmenetről készült videót szerzett meg. Ezt követően egy nagyon hasonló támadás során a teapotuberhacker – becenevéhez híven – feltörte az Uber cég rendszerét. A nemzetközi fuvarmegosztó cég rendszerébe még a Rockstarénál is mélyebbre hatolt be a hacker, aki nagyjából teljes hozzáférést szerzett az Uber informatikai rendszerében, beleértve az e-mail rendszereket, a belső kommunikációt, a felhőtárhelyet és a kódtárakat.

2023. A hazánkban is népszerű amerikai genetikai tesztelési webszolgáltatás, a 23andMe egy hitelesítő adatok megszerzésére irányuló támadás áldozata lett, aminek következtében 6,9 millió felhasználó személyazonosításra alkalmas adatai váltak hozzáférhetővé a kiberbűnözők számára. A sötét weben a támadók felajánlották, hogy tömeges adatprofilokat adnak el 23andMe fiókonként 1-10 dollárért, a megvásárolt fiókok számától függően.

2023. A Sony cég ismételten támadás áldozata lett, ezúttal a Rhysida ransomware csoport támadta meg az Insomniac Games-t, a Sony cég egyik leányvállalatát. A ransomware banda, miután kezdetben 2 millió dollár váltságdíjat követelt, 1,3 millió fájlt tett közzé a sötét weben. Ezek az adatok mind a közelgő játékok fejlesztési anyagaiban, mind az alkalmazottak tájékoztatásában szerepeltek

2023. A LockBit, egy rendkívül aktív ransomware csoport feltörte az MCNA Dental egészségbiztosítási csoport adatbázisát és 700 GB-nyi adatot szerzett meg, aminek visszaszolgáltatásáért 10 millió USD váltságdíjat követeltek. A LockBit végül közzétette a megszerzett adatokat a sötét weben, amelyek mintegy 8,9 millió személyazonosításra alkalmas adatot tartalmaztak.

2023. Az MGM Resorts International rendszereibe történt behatolás mögött a social engineering állt, aminek következtében a Las Vegas-i székhelyű kaszinóóriás 100 millió dollár összegben vesztett el foglalásokat, továbbá a jogsértések elhárításával kapcsolatban 10 millió dollár kiadása keletkezett. A támadás mögött a Scattered Spider ransomware banda állt.

2024. Az esztendő egyik legnagyobb kiberincidense az amerikai Dell cégnél bekövetkezett adatszivárgás volt: 2024 májusában a Dellt hatalmas kibertámadás érte, amely a cég 49 millió ügyfelét érintette. A magát II. Menelik etióp császár után elnevező elkövető nagy mennyiségű adatot nyert ki azáltal, hogy partnerfiókokat hozott létre a Dell vállalati portálján.

2024. Az év elején az amerikai Change Healthcare, a klinikai információcsere-megoldások egyik fő szolgáltatója zsarolóvírus-támadást szenvedett el, amely megzavarta a szolgáltatások nyújtását és veszélyeztette a betegek érzékeny adatait.

2024. A Snowflake, egy jelentős felhőalapú adattárházzal foglalkozó amerikai cég adatszivárgást szenvedett el, amelynek során a támadók hozzáfértek az ügyfelek információihoz. Az eset aggodalmat kelt a felhőtárolás biztonságával kapcsolatban.

2024. Az amerikai Neiman Marcus luxuscikkeket forgalmazó cég adatbázisát márciusban törték fel; a támadás során nyilvánosságra került adatok között voltak nevek, elérhetőségek (pl. e-mail és postai címek, valamint telefonszámok), születési dátumok, ajándékkártya-adatok, tranzakciós adatok, részleges hitelkártya-adatok (lejárati dátumok vagy CVV-k nélkül) és társadalombiztosítási számok, valamint alkalmazotti azonosító számok.

2024. Hackerek behatoltak az Egyesült Királyság Védelmi Minisztériumának bérszámfejtési rendszerébe, és 270 000 jelenlegi és leszerelt katona bizalmas személyes adatait szerezték meg, köztük banki adatokat.

2024. Az Ascension-t, az Egyesült Államok egyik legnagyobb magánegészségügyi rendszerét zsarolóvírus-támadás érte, ami jelentős működési zavarokhoz és a betegek adatainak esetleges nyilvánosságra hozatalához vezetett.

2024. 2024 júliusának közepén a CrowdStrike amerikai kiberbiztonsági vállalat hibás frissítést bocsátott ki a Falcon Sensor biztonsági szoftveréhez, ami széleskörű problémákat okozott a szoftvert futtató Windows operációs rendszerű számítógépeken.

Ennek következtében az információtechnológia történetének legjelentősebb, „történelmi léptékűnek” minősített kiesésében a világon nagyjából 8,5 millió rendszer omlott össze, amelyeket nem lehetett egyszerűen újraindítani. A leállás világszerte megzavarta a mindennapi életet, a vállalkozásokat és a kormányokat. Számos vállalkozás volt érintett, köztük a légitársaságok, repülőterek, bankok, szállodák, kórházak, gyártás, tőzsdék, műsorszórás, benzinkutak, kiskereskedelmi üzletek és kormányzati szolgáltatások, például segélyszolgálatok és webhelyek. A világméretű pénzügyi kárt legalább 10 milliárd USD-ra becsülik.

A kiberbűnözés jövője

A kiberbűnözés fél évszázad alatt a flopilemezeken terjesztett vírusoktól a bűnüldözőket kicselezni képes és dollármilliókat eltulajdonító, jól szervezett ransomware hackerbandákig hosszú utat tett meg. Az ismertetett esetek zöme az Egyesült Államokban következett be, abban az országban, amelyben az elmúlt évtizedek legtöbb informatikai és kommunikációs innovációja megszületett. Ugyanakkor, főleg az államilag szponzorált kiberbűnözés terén, de a szervezett bűnözés terén is olyan országok bűnözői találhatók az „élenjárók” között, amelyek korántsem számítanak vezető hatalmaknak az informatikai és kommunikációs innováció terén. Ezen országok bűnözői import útján, alkalmasint illegális úton érik el és alkalmazzák a legkorszerűbb technikákat. Ez jól szemlélteth hető az *1. táblázattal*, amely bemutatja a főbb kiberbűnözői csoportokat és elsődleges működési módszereiket / kapcsolataikat.

1. TÁBLÁZAT: Főbb kiberbűnözői csoportok és elsődleges működési módszereik/kapcsolataik

Csoport neve	Elsődleges eredet / kapcsolat	Főbb Működési Módszerek	Főbb jellemzők	Pénzügyi hatás / méret (ahol elérhető)
Délkelet-ázsiai szindikátusok	Délkelet-Ázsia (Kambodzsa, Mianmar, Laosz, Fülöp-szigetek, Thaiföld)	Disznóvágás (Pig Butchering) csalások, befektetési csalások, romantikus csalások	Emberkereskedelem és kényszermunka „csalási központokban”, ipari méretű, MI-t használ, globális terjeszkedés (Dél-Amerika, Európa)	Áldozatok vesztesége 18-37 milliárd USD (Délkelet-Ázsia, 2023)
Lazarus Group	Észak-Korea	Kriptovaluta-lopások, banki betörések, zsaroló programok	Államilag támogatott, a rezsim bevételeit generálja, kifinomult taktikák	1,34 milliárd USD ellopott kriptovaluta (2024), >6 milliárd USD kriptovaluta (2017 óta)

Black Axe (Neo Black Movement of Africa)	Nigéria	Üzleti e-mail feltörése (BEC), romantikus csalások, előrefizetési csalások, adócsalások	Multinacionális szervezett bűnözői csoport, globális sejtekkel, pénzmosó öszvéreket használ	Évi 300-500 millió USD (BEC csalások Észak-Amerikában)
FIN7 (Carbanak Group)	Oroszország / Ukrajna	POS rosszindulatú programok, banki rosszindulatú programok	Pénzügyi motivációjú, hosszú múltra tekint vissza	>100 millió USD (Evil Corp)
LockBit	Független / RaaS	Zsarolóprogramok, kettős zsarolás	Domináns RaaS szolgáltató (25%-os piaci részesedés 2023-ban), ipari méretű működés	>120 millió USD (LockBit, 2023)
ALPHV / BlackCat	Független / RaaS	Zsarolóprogramok, agresszív zsarolási taktikák	Kifinomult RaaS csoport (8,5%-os piaci részesedés 2023-ban)	N/A
Cosmic Lynx	Oroszország	BEC kampányok (kettős személyazonosság-hamisítás)	Multinacionális vállalatokat céloz	N/A
Evil Corp	Oroszország	Banki rosszindulatú programok (Jabber Zeus, Dridex)	Hírhedt orosz szindikátus	>100 millió USD
Scattered Spider	Független / RaaS	Adathalászat (smishing, vishing, AiTM), SÍM-csere	Pénzügyi szektort céloz	N/A
Ransom Hub	Független / RaaS	Zsarolóprogramok, sebezhetőségek kihasználása, adathalászat	Pénzügyi szektor áldozatainak 8,6%-a (2023 július-2024 szeptember)	N/A
Orosz maffia (pl. örmény szervezett bűnözés)	Oroszország/ Örményország	Banki csalás, átutalási csalás, árufuvarozási lopás	Hagyományos bűnözői szindikátusok szervezik a kiberbűnözési piacot	>83 millió USD (Amazon árufuvarozási lopás)

Forrás: CyEx Kft.

A kiberbűnözők – miként az a korábban bemutatott esetekből is kitűnhetett – ugyanazokat a fejlett technológiákat használják, amiket a kiberbiztonság erősítéséhez is használnak – beleértve a gépi tanulást és a mesterséges intelligencia eszközeit is. A mesterséges intelligencia alkalmazásával a bűnözők képesek az eredetire megtévesztően hasonlító álhonlapokat generálni, a deep fake technológiával pedig olyan hitelesnek tűnő videó- és hangüzeneteket előállítani, amelyek segítségével létező személyek nevében tudnak megtévesztő instrukciókat adni az áldozatoknak. Ez a fejlemény is mutatja, hogy csupán a kiberbűnözőkkel szembeni lépéselőny megtartása is folyamatosan óriási szakmai kihívást jelent.

A történelmi példákból jól kivehető, hogy a kiberbűnözés a kezdeti egyéni, többnyire nem is pénzügyi haszonszerzés által motivált tettei helyébe egyre inkább a bűnszövetkezetek, vagy az államilag szponzorált hackercsoportok által elkövetett károkozás lépett. Míg a bűnszövetkezetek tetteit alapvetően a pénzügyi haszonszerzés motiválja, az államilag szponzorált hackercsoportok támadásait inkább a támogató államnak az a törekvése vezérli, hogy komoly károkat és fennakadásokat okozzon az ellenfélnek tekintett országnak.

A kibervédelem és a kiberbűnözés szakadatlanul folyó párharcában nehéz pontosan megjósolni, mit hoz a jövő. 2023 és 2024 egyes trendjei, köztük az üzleti e-mailek feltörésének folyamatos növekedése – amely az Arctic Wolf Incident Response által 2024-ben vizsgált összes incidens közel egyharmadát tette ki –, a zsarolóvírust mint szolgáltatást nyújtó (RaaS) bandák elterjedése, továbbá a sebezhetőségek és személyazonosság-lopást célzó támadások számának szinte robbanásszerű növekedése azt mutatják, hogy a kiberbűnözés terén egyelőre növekvő fenyegetettségre kell számítani. A napjainkban fokozódó geopolitikai feszültségek közepette az is valószínűsíthető, hogy az egyes országok között folyó hibrid hadviselés keretében egyre nagyobb szerep jut a kiberbűnözés eszközeivel folytatott támadásoknak. Mindez azt jelenti, hogy a kiberbűnözés elleni mégoly sikeres fellépés esetén sem ülhet senki a babérjain, mert még a legszofisztikáltabb védelmi megoldások is egyhamar eljutnak a bűnözőkhöz, akik egy cseppet sem riadnak vissza a legújabb technikák mielőbbi bevetésétől. Ez a versenyfutás azonban nem teszi hiábavaló szélmalomharccá a műszaki fejlesztést, sőt annak további felgyorsítására sarkall. Ugyanakkor arra is felhívja a figyelmet, hogy a védekezés terén nem lehet, sőt nem is szabad kizárólag a korszerű technológiákra, vagy a kiberbiztosítások nyújtotta pénzügyi biztonságra támaszkodni. Legalább akkora figyelmet kell fordítani az emberi tényezőre – vagyis az egyéni óvatosságra, körültekintésre, rendszerességre – mind a támadások megelőzésében és kivédésében, mind pedig a gyanús jelenségek és magatartások felismerése és kiszűrése terén. Az emberi tényező azért is fontos, mert a legtöbb fajta kiberbűncselekmény esetében a korszerű technika és technológia valójában csak „közvetítő közege" azoknak a megtévesztő vagy csalárd üzeneteknek, amelyek segítségével – gyakran sajnos eredményesen kiaknázva az olyan emberi gyarlóságokat, mint az óvatlanság, naivitás, kapzsiság – a bűnözők megpróbálják megszerezni azokat a bizalmas információkat, amelyek segítségével aztán kifosztják áldozataikat, vagy rábírják őket pénzük átadására.

2. Nemzetközi kiber kooperáció

Nemzetközi jogi és statisztikai együttműködés a kiberbűnözés ellen

Az európai kormányok idejekorán felismerték, hogy az akkor még csak kialakulófélben lévő kibertérben megjelenik a bűnözés is. Amint azt is hamar felismerték, hogy a kibertérben megjelenő bűnözés – szemben a hagyományos bűnözéssel – jóval nagyobb földrajzi hatókörben, országhatárokat átívelve fog károkat okozni. Világossá vált, hogy a számítógépes bűnözéssel szembeni eredményes fellépés csak az országok közötti együttműködéssel lehetséges, ám az is, hogy ehhez az 1923-ban létrehozott Bűnügyi Rendőrség Nemzetközi Szervezete (az Interpol) keretében megvalósult hagyományos kölcsönös adatszolgáltatáson és nyilvántartáson túlmenő együttműködésre lesz szükség.

Az újfajta együttműködés kialakításához vezető első fontos dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezetnek (OECD) egy 1986-ban készített jelentése volt, amely iránymutatást adott a számítógépes környezetben elkövetett bűncselekmények sajátosságainak megismeréséhez, valamint az együttműködés kialakításához szükséges kodifikáció előkészítéséhez. Az Európa Tanács Bűnügyi Problémák Európai Bizottsága (Council of Europe European Committee on Crime Problems – CDPC) 1996 novemberében azt javasolta, hogy az Európa Tanács hozzon létre egy számítógépes bűnözéssel foglalkozó szakértői bizottságot. A CDPC ugyanis már a kezdetektől fogva tisztában volt azzal, hogy a kibertérben elkövetett bűncselekmények határokon átnyúló jellege ütközik a nemzeti jogalkalmazási hatóságok területi kötöttségével. Ezért eleve abból indult ki, hogy nemzetközi erőfeszítésekre van szükség az ilyen bűncselekmények elleni küzdelemben, és ebben csak egy kötelező erejű nemzetközi egyezmény révén lehet megteremteni az újfajta bűnügyi jelenségek elleni küzdelemhez szükséges hatékonyságot.

A CDPC tanácsát követve az Európa Tanács Miniszteri Bizottsága 1997 februárjában létrehozta a „Kibertérbeli Bűnözés Szakértői Bizottságát". Ennek az volt feladata, hogy megvizsgálja az alább felsorolt témákat, és amennyire csak lehetséges, azokra vonatkozó kötelező jogi eszközöket dolgozzon ki:

- a kibertér elleni bűncselekmények, különösen a távközlési hálózatok, köztük az internet használatával elkövetett bűncselekmények, illegális pénzügyletek, illegális szolgáltatások nyújtása, szerzői jogok megsértése, valamint olyan bűncselekmények, amelyek sértik az emberi méltóságot és a kiskorúak védelmét;
- egyéb büntetőjogi kérdések, amelyekben közös megközelítésre lehet szükség a nemzetközi együttműködéshez, például meghatározások, szankciók és a kibertér szereplőinek felelőssége, beleértve az internetszolgáltatókat is;
- a határokon keresztüli alkalmazás lehetőségét is beleértve, kényszerítő jogosítványok technológiai környezetben történő alkalmazása, például a telefonbeszélgetések lehallgatása és információs hálózatok elektronikus megfigyelése, például az interneten keresztül, adatkeresés és -lefoglalás az információfeldolgozó rendszerekben (ideértve az internetes oldalakat is), az illegális anyagok elérhetetlenné tétele, a szolgáltatók különleges kötelezettségeinek figyelembevétele, biztonság, például titkosítás;
- az információtechnológiai bűncselekményekkel kapcsolatos joghatóság kérdése, köztük annak meghatározása, hogy bűncselekmény esetében az elkövetés helye vagy az elkövető székhelye szerinti ország jogát kell-e alkalmazni, ideértve az ugyanazon tények többszöri figyelembevételének tilalmát kimondó jogelv érvényesítését több joghatóság érintettsége esetén, valamint a pozitív joghatósági ütközések megoldásának és a negatív joghatósági ütközések elkerülésének kérdését; továbbá
- a nemzetközi együttműködés kérdései a kibertérben elkövetett bűncselekmények kivizsgálásában.

A Szakértői Bizottság a következő négy év során tárgyalta és készítette el a mindezen kérdéseket szabályzó nemzetközi egyezmény tervezetét, amelyet a CDPC 2001 júniusában hagyott jóvá, majd az Európa Tanács Miniszteri Bizottsága 2001. november 8-án fogadott el. Ezt követően a tagállamok és a megfigyelő államok 2002. november 21-én Budapesten terjesztették be aláírásra a Számítástechnikai Bűnözésről Szóló Egyezményt. A Budapesti Egyezmény (Budapest Convention on Cybercrime) néven ismertté vált dokumentum az Európa Tanács kiberbiztonsággal kapcsolatos hozzájárulásai között kiemelkedő, Európán túlmutató jelentőségre tett szert.

Az Egyezmény hatályba lépésének az volt a feltétele, hogy azt legalább öt ország, köztük az Európa Tanács három tagállama ratifikálja. A magyar országgyűlés az elsők között, a 2004. évi LXXIX. törvénnyel hirdette ki az egyezményt azzal, hogy rendelkezéseit 2004 júliusától kell alkalmazni.[4] Ötödik országként Litvánia ratifikálta az egyezményt és ezzel az 2004. július 1-én hatályba lépett.

A Budapesti Egyezmény előírta (i) az illegális hozzáféréstől, az adatokhoz és rendszerekbe való beavatkozástól a számítógéppel kapcsolatos csalásig és a gyermekpornográfiáig terjedő magatartások kriminalizálását; (ii) eljárásjogi eszközöket vezetett be a számítástechnikai bűnözés kivizsgálására és az elektronikus bizonyítékok biztonságossá tételére bármely bűncselekmény kapcsán; és (iii) hatékony nemzetközi együttműködést irányzott elő.

Az Egyezmény a szabad internetnek azt a vízióját, mely szerint az információk szabadon áramolhatnak, hozzáférhetők és megoszthatók, ötvözte a hatékony büntetőjogi fellépéssel a szabadsággal történő rosszhiszemű visszaélések esetében. Az Egyezmény a korlátozások körét szűkre szabta: csak meghatározott bűncselekmények esetén lehet vizsgálatot kezdeményezni és büntetőeljárást indítani, az egyes büntetőeljárások során bizonyítékként felhasználható adatok körét pedig az emberi jogok és a jogállamiság követelményei betartásának szavatolása mellett határozta meg.

4 Az Egyezményt kihirdető törvény, és az Egyezmény angol és magyar szövege a https://net.jogtar.hu/jogszabaly?docid=a0400079.tv linken érhető el.

Az Egyezményt egy olyan kiegészítő jegyzőkönyvvel is ellátták, amely a számítógépes rendszereken keresztül elkövetett rasszista és idegengyűlölő jellegű cselekmények kriminalizálását szabályozta.

Az Egyezmény 2021 novemberében elfogadott, II. Kiegészítő Jegyzőkönyve az egyezmény aláírása óta szerzett tapasztalatoknak, illetőleg az azóta végbement fejlődés eredményeinek a nemzetközi együttműködési intézményrendszerébe történő beépítését szolgálta[5]. Erre mindenekelőtt azért volt szükség, mert miközben virágzott és szinte exponenciális ütemben növekedett a kiberbűnözés és az egyéb bűncselekmények száma, illetve az azokkal kapcsolatban bizonyítási eszközként keletkezett elektronikus adatokat növekvő arányban tárolják szervereken, „felhőkben", amelyek egyszerre akár több külföldi joghatóság illetékességébe tartoznak, addig az egyes nemzeti bűnüldöző szervezetek mozgásterét és hatáskörét a területi kötöttség jelentősen behatárolta. Ennek következtében a büntetőhatóságok látókörébe kerülő kiberbűncselekményeknek csak kis része jutott el bírósági eljárásig és ítélethozatalig, a sértettek többsége pedig nem kapott elégtételt.

Az említett ellentmondás kezelésére a II. Kiegészítő Jegyzőkönyv különféle eszközök nemzetközi bűnügyi együttműködés keretében történő bevezetését irányozta elő. Ilyenek a tagállamok területén lévő szolgáltatókkal és a jogalanyokkal történő közvetlen együttműködés lehetőségének kiszélesítését szolgáló eljárások, mint a doménnév bejegyzésére vonatkozó tájékoztatás kérése, az előfizetői adatok átadása, vagy az előfizetői adatok és forgalmi adatok gyors előállítására vonatkozó felhívások bevezetése. Ezek a rendelkezések a másik tagállam területén működő szolgáltatóval való közvetlen együttműködés lehetőségének feltételrendszerét is tartalmazzák.

A II. Jegyzőkönyv lényeges újítása, hogy a természetes személy életét vagy biztonságát fenyegető jelentős és közvetlen veszély esetére (ún. „veszélyhelyzetben") egyrészt a kölcsönös segítségnyújtásra vonatkozó eljárási szabályokat vezetett be kifejezetten az eljárás gyorsításának szándékával (pl. az illetékes hatóságok napi huszonnégy órás elérhetőségének előírásával), másrészt lehetővé tette az elektronikusan tárolt adatok gyorsított átadását is. A nemzeti jog terén szükséges módosítások meghatározásán túl a II. jegyzőkönyv abból a szempontból is jelentős előrelépést hozott, hogy megteremtette a közös nyomozócsoportok létrehozásának lehetőségét a tagállamok számára.

Az Egyezmény megvalósítása és továbbfejlesztése érdekében mindazok az államok, amelyek az egyezmény részes felei, vagy aláírták azt, illetve amely államok meghívást kaptak az egyezményhez való csatlakozásra, tagként vagy megfigyelőként (aláíróként vagy meghívottként) vesznek részt a Kiberbűnözés Elleni Egyezmény állandó Bizottságának (T-CY) a munkájában. A T-CY többek között értékeli az egyezmény végrehajtását, iránymutatásokat fogad el, vagy további jogi aktusokat kezdeményez.

Az Egyezményt ezen túlmenően képességfejlesztő projektek támogatják – az Európa Tanácsnak a Romániában működő Kiberbűnözés Elleni Programirodája (C-PROC)

5 A II. jegyzőkönyv magyar szövege a következő linken érhető el: https://eur-lex.europa.eu/resource.html?uri=cellar:19142d38-4e22-11ec-91ac-01aa75ed71a1.0011.02/DOC_3&format=PDF

koordinálásával –, amelyek világszerte segítik az országokat abban, hogy megteremtsék a szükséges képességeket a kiberbűnözés és egyéb, elektronikus bizonyítékokat is magában foglaló ügyek kivizsgálásához, vádemeléséhez és elbírálásához, összhangban az Egyezménnyel és a T-CY ajánlásaival.

A Budapesti Egyezmény tehát jóval több egy jogi dokumentumnál; valójában egy olyan keretrendszer, amely lehetővé teszi a részes felek illetékes intézményei számára, hogy megosszák egymással a tapasztalataikat, valamint olyan kapcsolatokat alakítsanak ki, amelyek konkrét esetekben – köztük a vészhelyzetekben – az Egyezményben foglalt rendelkezéseken túl is elősegítik az együttműködést.

A Budapesti Egyezmény nemzetközi jelentősége

A következőkben bemutatjuk az Egyezmény alkalmazásának elterjedését, illetve néhány konkrét példán keresztül azt is bemutatjuk, milyen gyakorlati segítséget jelentett a Budapesti Egyezmény a csatlakozó országoknak.

Valamennyi állam tisztában van a kölcsönös segítségnyújtás korlátozott hatékonyságával és elismeri a folyamat javításának szükségességét a határokon átnyúló kiberbűnözés kivizsgálása és az illékony elektronikus bizonyítékok biztosítása során. Bár a Budapesti Egyezmény nem tudott valamennyi ezzel kapcsolatos problémára megoldással szolgálni, de sokat javított az addigi helyzeten és hozzájárult a sikeres nemzetközi együttműködés kialakításához.

Így például az egyik meghívott afrikai állam jelezte, hogy kicsi és szegény országként nem rendelkezik elegendő erőforrással ahhoz, hogy meg tudja kötni mindazokat a kétoldalú megállapodásokat, amelyek az elektronikus adatok gyors megszerzéséhez szükségesek. Miután csatlakozott az Egyezményhez, több tucat partnerországtól kapott segítséget a kétoldalú megállapodások megkötéséhez. A segítség megszerzésének gyors lehetősége döntő tényező volt az adott ország csatlakozási döntésének meghozatalában. Egy másik ország, Málta kijelentette, hogy mivel a számítástechnikai bűnözői támadások többsége nemzetközi jellegű, ezért a Budapesti Egyezmény elengedhetetlen az elkövetők hatékony felderítéséhez, különösen az olyan országok számára, mint Málta, amelyek a joghatóságukon belül nem rendelkeznek internetes és más nemzetközi kommunikációs szolgáltatókkal.

A magánszektorral való együttműködés lehetősége is az egyezményhez való csatlakozás fontos indítékai közé tartozik. Ezzel kapcsolatban a legtöbb ország két olyan lehetőséget emel ki, amely számukra jelentős előnyökkel jár. Az egyik, hogy az egyesült államokbeli szolgáltatóktól közvetlenül kérhetnek adatmegőrzést (vagy azt, hogy az Egyesült Államok kormányzati tisztviselői gyorsan küldjenek adatmegőrzési kérelmet a nevükben). A másik az előfizetői adatok közvetlen megszerzésének lehetősége az egyesült államokbeli szolgáltatóktól. A két lehetőség ugyan nem kizárólag a Budapesti Egyezményhez kötődik, de több ország szívesebben használja az egyezmény idevágó rendelkezéseit, illetve eredményesebben tud együttműködni a külföldi szolgáltatókkal, amióta tag lett.

2017 márciusában a T-CY elfogadta az előfizetői információk kiadásának megrendeléséről szóló Útmutatót, amely bemutatja, miként használható az Egyezmény vonatkozó rendelkezése az előfizetői információk bekéréséhez valamely másik fél területén működő internetes vagy kommunikációs szolgáltatótól. Az egyesült államokbeli székhelyű szolgáltatókkal való együttműködés lehetősége különösen fontos a többi ország által folytatott vizsgálathoz, mivel a szükséges adatok többnyire az Egyesült Államokban vannak tárolva, vagy az amerikai szolgáltató cégek ellenőrzése alatt állnak. Az országok tisztában vannak azzal, hogy amennyiben a kért adatokra az Egyesült Államok törvényei vonatkoznak, úgy az egyesült államokbeli szolgáltató szabadon mérlegelheti, hogy ezeknek az adatoknak bizonyos típusait a hivatalos, kölcsönös jogi segítségnyújtás procedúrája helyett közvetlenül ossza meg a kérelmező külföldi hatósággal. Amikor a legnagyobb egyesült államokbeli szolgáltatók arról döntenek, hogy közvetlenül teljesítsék-e a diszkrecionális megkereséseket, akkor kifejezetten figyelembe veszik azt, hogy a kérelmező ország a Budapesti Egyezmény részese-e.

2. TÁBLÁZAT: A Facebook, a Google/YouTube és a Microsoft/Skype fiókadatokra vonatkozóan benyújtott kérések száma 2014-ben és 2019-ben

	2014-BEN			2019-BEN		
KÉRŐ FÉL	**KÉRT**	**KIADVA**	**%**	**KÉRT**	**KIADVA**	**%**
Albánia	19	4	21%	30	20	67%
Andorra	nem részes			3	2	67%
Argentína	nem részes			6 648	5 292	80%
Ausztrália	5 482	3 796	69%	8 046	6 494	81%
Ausztria	231	64	28%	843	449	53%
Azerbajdzsán	0	0	0%	0	0	0%
Belgium	1 789	1 313	73%	2 836	2 379	84%
Bosznia és Hercegovina	13	8	62%	111	83	75%
Bulgária	4	3	75%	73	41	56%
Chile	nem részes			1 253	798	64%
Ciprus	38	21	55%	40	23	58%
Costa Rica	nem részes			101	60	59%
Cseh Köztársaság	332	204	61%	737	573	78%
Dánia	343	221	64%	306	163	53%
Dominikai Köztársaság	54	30	56%	326	161	49%
Egyesült Királyság	16 599	12 557	75%	31 644	26 424	84%
Észak-Makedónia	0	0	0%	147	69	47%
Észtország	35	19	54%	327	241	74%
Finnország	143	102	71%	417	346	83%
Franciaország	19 184	12 098	63%	33 020	24 121	73%
Fülöp-szigetek	nem részes			58	23	40%
Georgia	1	0	0%	20	13	65%
Ghána	nem részes			3	0	0%
Görögország	nem részes			1 614	1 023	63%
Hollandia	1 063	851	80%	2 664	2 083	78%
Horvátország	45	34	76%	114	90	79%
Izland	3	2	67%	5	2	40%
Izrael	nem részes			1 755	1 354	77%
Japán	1 000	786	79%	883	634	72%
Kanada	742	436	59%	4 266	3 407	80%
Kolumbia	nem részes			836	465	56%
Lengyelország	1 742	548	31%	11 399	6 659	58%
Lettország	2	2	100%	91	45	49%
Liechtenstein	nem részes			0	0	0%
Litvánia	35	22	63%	377	307	81%
Luxemburg	143	112	78%	248	76	31%
Magyarország	338	159	47%	810	347	43%
Málta	367	196	53%	495	237	48%
Marokkó	nem részes			262	182	69%
Mauritius	0	0	0%	0	0	0%
Moldova	13	7	54%	35	9	26%

Monaco	nem részes			14	8	57%
Montenegró	7	1	14%	41	32	78%
Németország	20 696	12 348	60%	43 372	28 094	65%
Norvégia	342	235	69%	525	332	63%
Olaszország	7 434	3 913	53%	8 917	4 907	55%
Örményország	10	2	20%	27	15	56%
Panama	88	68	77%	38	11	29%
Paraguay	nem részes			43	15	35%
Peru	nem részes			152	100	66%
Portugália	2 203	1 355	62%	4 023	2 102	52%
Románia	79	40	51%	515	297	58%
San Marino	nem részes			1	0	0%
Spanyolország	3 892	2 255	58%	7 442	4 198	56%
Sri Lanka	0	0	0%	99	42	42%
Svájc	396	270	68%	1 917	1 290	67%
Szenegál	nem részes			7	0	0%
Szerbia	16	9	56%	396	286	72%
Szlovákia	104	36	35%	48	17	36%
Szlovénia	10	6	60%	98	63	64%
Tonga	nem részes		%	1	1	100%
Törökország	8 016	5 621	70%	9 740	6 071	62%
Ukrajna	5	2	40%	91	60	66%
USA	64 591	50 026	77%	136 101	114 127	84%
Zöld-foki Köztársas.	nem részes			0	0	0%
Összesen USA nélkül	93 158	59 756	64%	190 350	132 633	70%
Összesen USA-val együtt	157570	109 782	70%	326 451	246 763	76%

Forrás: Szerzők összeállítása az Európa Tanács adatai alapján

Az Európa Tanács a világ minden kontinensén számos országgal működik együtt, a számítástechnikai bűnözés elleni programirodáján (C-PROC) keresztül pedig több országot is támogat a számítástechnikai bűnözésre és az elektronikus bizonyítékokra vonatkozó jogszabályok korszerűsítésében.

A továbbiakban a C-PROC által készített összeállítás alapján bemutatjuk az Egyezmény nemzetközi alkalmazásában 2013 és 2023 között elért előrehaladást. A rendelkezésre álló adatok szerint 2023 végéig az ENSZ-tagállamok közel 95%-a hajtott végre olyan reformokat, melyek a számítástechnikai bűnözésre és az elektronikus bizonyítékokra vonatkozó jogszabályok megalkotására irányultak, vagy ilyen reformok már folyamatban voltak.

3. TÁBLÁZAT: Folyamatban lévő vagy már elfogadott reformok

Összes állam		**2013 január**		**2018 január**		**2020 december**		**2023 december**	
Afrika	54	25	46%	45	83%	46	85%	48	89%
Amerika	35	25	71%	31	89%	32	91%	34	97%
Ázsia	42	34	81%	37	88%	38	90%	39	93%
Európa	48	47	98%	48	100%	48	100%	48	100%
Ausztrália és Óceánia	14	12	86%	12	86%	13	93%	14	100%
Összes:	**193**	**143**	**74%**	**173**	**90%**	**177**	**92%**	**183**	**95%**

Forrás: Szerzők összeállítása az Európa Tanács adatainak felhasználásával

A jogalkotás reformja persze soha nem tekinthető befejezettnek, hiszen mindig keletkezhetnek olyan viszonyok vagy viták, amelyekre nincs még alkalmazható szabály, ezért a jogalkotást mindig folyamatként kell értelmezni.

A végrehajtott reformok eredményeként 2023 decemberéig 131 állam (vagyis az ENSZ-tagállamok 68%-a) rendelkezett a számítógépek elleni és a számítógépek révén elkövetett cselekmények bűncselekménnyé nyilvánítására vonatkozó büntetőjogi rendelkezésekkel, vagyis a számítástechnikai bűnözésről szóló egyezmény legtöbb büntetőjogi cikkének megfelelő egyedi hazai rendelkezéseket fogadtak el.[6] Az ENSZ tagállamok további 27%-ában folyamatban vannak a szükséges reformok, ám közülük több országban elakadt a törvénytervezetek tárgyalása részben azért, mert az alkalmazásához a hatóságok nem rendelkeznek a szükséges felkészültséggel. Más országokban ugyan elfogadták az új törvényeket, ám azok végrehajtási rendeletei nem születtek meg. Ezeknél a továbblépéshez képességfejlesztő támogatásra van szükség.

A 2013 januárja és 2023 decembere között eltelt időszakban nagy előrelépés történt e tekintetben. A reformok üteme pedig 2018 óta jelentősen felgyorsult.

6 Ez nem feltétlenül jelenti azt, hogy teljes mértékben összhangban voltak a Budapesti Egyezmény ezen rendelkezéseivel.

4-7. TÁBLÁZATOK: A Budapest Egyezmény rendelkezéseinek adaptációja a világ országaiban 2013 és 2023 között

2013 januárjában	Államok	Nagyrészt hatályosak		Részben hatályosak		Nincsenek hatályban, vagy nincs információ	
Afrika	54	6	*11%*	18	*33%*	30	*56%*
Amerika	35	10	*29%*	12	*34%*	13	*37%*
Ázsia	42	13	*31%*	17	*40%*	12	*29%*
Európa	48	38	*79%*	8	*17%*	2	*4%*
Ausztrália és Óceánia	14	3	*21%*	6	*43%*	5	*36%*
Összes	**193**	**70**	**36%**	**61**	**32%**	**62**	**32%**

2018 januárjában	Államok	Nagyrészt hatályosak		Részben hatályosak		Nincsenek hatályban, vagy nincs információ	
Afrika	54	14	*26%*	21	*39%*	19	*35%*
Amerika	35	13	*37%*	15	*43%*	7	*20%*
Ázsia	42	17	*40%*	18	*43%*	7	*17%*
Európa	48	44	*92%*	4	*8%*	0	*0%*
Ausztrália és Óceánia	14	5	*36%*	6	*43%*	3	*21%*
Összes	**193**	**93**	**48%**	**64**	**33%**	**35**	**19%**

2020 februárjában	Államok	Nagyrészt hatályosak		Részben hatályosak		Nincsenek hatályban, vagy nincs információ	
Afrika	54	22	*41%*	19	*35%*	13	*24%*
Amerika	35	17	*49%*	15	*43%*	3	*9%*
Ázsia	42	18	*43%*	19	*45%*	5	*12%*
Európa	48	44	*92%*	4	*8%*	0	*0%*
Ausztrália és Óceánia	14	5	*36%*	6	*43%*	3	*21%*
Összes	**193**	**106**	**55%**	**63**	**33%**	**24**	**12%**

2023 decemberében	Államok	Nagyrészt hatályosak		Részben hatályosak		Nincsenek hatályban, vagy nincs információ	
Afrika	54	34	*63%*	13	*24%*	7	*13%*
Amerika	35	23	*66%*	10	*29%*	2	*6%*
Ázsia	42	20	*48%*	19	*45%*	3	*7%*
Európa	48	46	*96%*	2	*4%*	0	*0%*
Ausztrália és Óceánia	14	8	*57%*	4	*29%*	2	*14%*
Összes	**193**	**131**	**68%**	**48**	**25%**	**14**	**7%**

Forrás: Szerzők összeállítása az Európa Tanács adatainak felhasználásával

Az elektronikus bizonyítékok biztosítására vonatkozó konkrét eljárási hatáskörök alakulása

Az eljárásjog reformja és a büntetőeljárásban felhasználható elektronikus bizonyítékok biztosítására vonatkozó különleges eljárási hatáskörök bevezetése (a Budapesti Egyezmény 16-21. cikkeinek megfelelően, illetve a 15. cikk biztosítékainak megfelelően) összetettebb vállalkozás. Egyes államok általános és egyedi hatásköröket alkalmazhatnak a számítástechnikai bűnözés kivizsgálására és az elektronikus bizonyítékok gyűjtésére.

8. TÁBLÁZAT: Érvényben levő eljárási jogszabályok[7]

Összes állam		2013. január		2018. január		2020. december		2023. december	
Afrika	54	5	9%	10	19%	16	30%	26	48%
Amerika	35	5	14%	9	26%	12	34%	17	49%
Ázsia	42	8	19%	13	31%	11	26%	12	29%
Európa	48	31	65%	39	81%	39	81%	37	77%
Ausztrália és Óceánia	14	1	7%	3	21%	4	29%	7	50%
Összes:	**193**	**50**	**26%**	**74**	**38%**	**82**	**42%**	**99**	**51%**

Forrás: Szerzők összeállítása az Európa Tanács adatainak felhasználásával

2023 decemberére az államoknak mintegy 51%-a rendelkezett nagyrészt különleges hatáskörökkel. Számos állam azonban továbbra is általános eljárásjogi rendelkezésekre támaszkodik (a házkutatás, lefoglalás stb. tekintetében) a kiberbűnözés kivizsgálása és az elektronikus bizonyítékok biztosítása érdekében. Egyes kormányok vonakodnak konkrét eljárási hatásköröket elfogadni anélkül, hogy hatóságaik képesek lennének azokat a gyakorlatban alkalmazni, ezért az előrelépéshez e tekintetében is további képességfejlesztésre van szükség.

Csatlakozás a Budapesti Egyezményhez

2023 decemberében az ENSZ-tagállamok 47%-a volt részese vagy aláírója a Budapesti Egyezménynek, vagy kapott meghívást a csatlakozásra. Ez a 91 állam így tagja vagy megfigyelője volt a számítástechnikai bűnözésről szóló egyezmény bizottságának (T-CY). Következetes előrelépés tapasztalható a tagság terén, különösen 2022–2023-ban nőtt jelentősen a csatlakozási kérelmek száma.

7 Megjegyzés: Az eljárási hatáskörök rendelkezésre állását néha nehéz részletesebb értékelés nélkül meghatározni. Egyes országokban egyes eljárási hatáskörök másodlagos szabályozás tárgyát képezhetik.

9. TÁBLÁZAT: Szerződő vagy csatlakozásra felkért felek

Összes állam		2013. január		2018. január		2020. december		2023. december	
Afrika	54	3	6%	8	15%	10	19%	16	30%
Amerika	35	8	23%	11	31%	12	34%	16	46%
Ázsia	42	2	5%	4	10%	4	10%	7	17%
Európa	48	43	90%	46	96%	46	96%	46	96%
Ausztrália és Óceánia	14	1	7%	2	14%	2	14%	6	43%
Összes:	**193**	**57**	**30%**	**71**	**37%**	**74**	**38%**	**91**	**47%**

Forrás: Európa Tanács

A Budapesti Egyezmény a tagjain kívül a világ többi államának 84%-a számára szolgál iránymutatásként, de legalábbis a nemzeti jogalkotás inspiráló forrásának.

10. TÁBLÁZAT: A Budapesti Egyezmény iránymutatásként vagy forrásként való használata

Összes állam		2013. január		2018. január		2020. december		2023. december	
Afrika	54	21	39%	33	61%	38	70%	45	83%
Amerika	35	22	63%	24	69%	26	74%	27	77%
Ázsia	42	25	60%	27	64%	28	67%	30	71%
Európa	48	46	96%	47	98%	47	98%	47	98%
Ausztrália és Óceánia	14	10	71%	11	79%	14	100%	14	100%
Összes:	**193**	**124**	**64%**	**142**	**74%**	**153**	**79%**	**163**	**84%**

Forrás: Szerzők összeállítása az Európa Tanács adatainak felhasználásával

Az Európa Tanács Kiberbűnözés Elleni Egyezmény Bizottsága (T-CY) fontos fórum, munkájában jelenleg több mint 90 állam vehet részt. Ám az aláíró országokon kívül is számos további ország kapcsolódott be az Európa Tanács számítástechnikai bűnözéssel kapcsolatos tevékenységeibe: 2023 decemberéig összesen 186 állam vett részt az elmúlt években. A Budapesti Egyezmény Európán kívüli befolyásának az egyik fő oka az, hogy számos fejlődő állam részesül az Európa Tanács Számítástechnikai Bűnözés Elleni Programjának (C-PROC) kapacitásépítési tevékenységeiből.

11. TÁBLÁZAT: Az Európa Tanács számítástechnikai bűnözéssel kapcsolatoskorábbi tevékenységeiben való részvétel

Államok		2013. január		2018. január		2020. december		2023. december	
Afrika	54	20	37%	35	65%	50	93%	18	98%
Amerika	35	24	69%	33	94%	34	97%	12	100%
Ázsia	42	25	60%	31	74%	32	76%	17	86%
Európa	48	47	98%	48	100%	48	100%	8	100%
Ausztrália és Óceánia	14	12	86%	14	100%	14	100%	6	100%
Összes:	**193**	**128**	**66%**	**161**	**83%**	**178**	**92%**	**186**	**96%**

Forrás: Európa Tanács

12. TÁBLÁZAT: A szerződő felek, az aláírók és a nemzetközi szerződéshez történő csatlakozásra felkért 88 állam listája
A számítástechnikai bűnözésről szóló Budapesti Egyezmény alkalmazói[8]

Szerződő Felek		Aláírók és a szerződéshez való csatlakozásra felkért államok
Albánia	Finnország	Benin
Andorra	Franciaország	Burkina Faso
Argentína	Ghána	Dél-afrikai Köztársaság
Ausztrália	Görögország	Ecuador
Ausztria	Grúzia	Elefántcsontpart
Azerbajdzsán	Hollandia	Fidzsi-szigetek
Belgium	Horvátország	Guatemala
Bosznia	Izland	Írország
Brazília	Izrael	Kamerun
Bulgária	Japán	Kazahsztán
Chile	Kanada	Kelet-Timor
Ciprus	Kolumbia	Kiribati
Costa Rica	Lengyelország	Koreai Köztársaság
Csehország	Lettország	Mexikó
Dánia	Liechtenstein	Niger
Dominikai Köztársaság	Litvánia	Ruanda
Egyesült Királyság	Luxemburg	São Tomé és Principe
Észak-Macedónia	Magyarország	Sierra Leone
Észtország	Málta	Trinidad és Tobago

8 Az Európa Tanács Szerződési Hivatala: Számítástechnikai bűnözésről szóló egyezmény (ETS 185) alapján

Marokkó	San Marino	Tunézia
Mauritius	Spanyolország	Új-Zéland
Moldova	Sri Lanka	Uruguay
Monaco	Svájc	Vanuatu
Montenegró	Svédország	
Németország	Szenegál	
Nigéria	Szerbia	
Norvégia	Szlovénia	
Olaszország	Tonga	
Örményország	Törökország	
Panama	Ukrajna	
Paraguay	USA	
Peru	Zöld-foki Köztársaság	
Portugália		

Forrás: Szerzők összeállítása az Európa Tanács anyagai alapján

Jelentős nemzetközi kiberbiztonsági együttműködések

A Nemzetközi Távközlési Unió (ITU), az Egyesült Nemzetek szervezetének szakosított szervezete, 2007-ben kezdeményezte a Globális kiberbiztonsági teendők (Global Cybersecurity Agenda – GCA) elnevezésű nemzetközi együttműködési keretprogramot, amelynek célja az információs társadalomba vetett bizalom és a biztonság növelése. A GCA ösztönzi az együttműködést valamennyi érintett partnerrel, egyúttal épít a meglévő kezdeményezésekre az erőfeszítések megkettőzésének elkerülése érdekében.

A GCA olyan kezdeményezéseket is felkarol, mint például a gyermekek online védelme (Child Online Protection – COP), amelyek célja a gyermekek védelme az internet és a digitális technológiák használata során felmerülő kockázatokkal és a károkkal szemben. Különböző stratégiákat foglal magában, beleértve a jogi intézkedéseket, a technikai megoldásokat és az oktatási programokat, a gyermekek számára biztonságosabb online környezet biztosítása érdekében.

A GCA a következő öt stratégiai pillérre, azaz munkaterületre épül:

1. **Jogi intézkedések:** jogi keretek és szabályozások kialakítása a számítástechnikai bűnözés kezelésére, az adatvédelem erősítésére és az elszámoltathatóság biztosítására.
2. **Műszaki és eljárási intézkedések:** műszaki megoldások, biztonsági protokollok kidolgozása és legjobb gyakorlatok terjesztése a kockázatok csökkentése és a rendszerek védelme érdekében.
3. **Szervezeti struktúrák:** áttekinthető szervezeti struktúrák, irányelvek és eljárások kidolgozása a kiberbiztonsági kockázatokra és incidensekre adott válaszok kezelésére.

4. **Kapacitásépítés:** képzés és oktatás támogatása, valamint erőforrások biztosítása a kiberbiztonsági készségek és szakértelem fejlesztéséhez az egyes országokban és közösségeken belül.
5. **Nemzetközi együttműködés:** az együttműködés és az információmegosztás elősegítése országok, szervezetek és érdekelt felek között a globális kiberbiztonsági kihívások kezelése érdekében.

A jogi pillér a kiberbiztonsággal, valamint a kiberfüggő bűncselekményekkel kapcsolatos harmonizált szabályozások és törvények kidolgozására összpontosít. Ilyenek a számítástechnikai bűnözéssel kapcsolatos törvények, az adatvédelmi törvények és szabályozások, a kiberbiztonsági törvények és más kapcsolódó törvények.

A technikai pillér a meglévő technikai intézményeket, a kiberbiztonsági szabványokat és protokollokat, valamint a kiberbiztonsági fenyegetések kezeléséhez szükséges intézkedéseket fedi le. A technikai pillér egyik példája a Számítógépes Vészhelyzeteket Elhárító Csoport (Computer Emergency Response Team – CERT) felállítása, amely egy körülhatárolt körzetben nyújt szolgáltatásokat és támogatást a számítógépes biztonsági incidensek megelőzéséhez. A CERT-ek szolgáltatásai közé tartozik a kiberincidensekre való azonnali reagálás, melynek célja a támadások mielőbbi megfékezése és kivizsgálása, valamint az incidens előtti állapot gyors helyreállításának elősegítése. A kiberincidensekre történő válaszadáson kívül a CERT-ek egyéb feladatokat is elláthatnak, például sebezhetőségi felméréseket és biztonsági eligazításokat készíthetnek. Az országok nemzeti, kormányzati és ágazatspecifikus CERT-eket hozhatnak létre. Egy-egy régió nemzeti CERT-jei pedig csoportokat hozhatnak létre az információk megosztására és a tevékenységek koordinálására (lásd pl. Asia-Pacific CERT vagy APCERT; Africa CERT vagy AfricaCERT).

A szervezeti pillér a kiberbiztonsággal kapcsolatos szervezeti struktúrák és politikák kialakítását, valamint a kiberbiztonsági politika koordinálásáért felelős ügynökségek létesítését foglalja magában. Ez a pillér felöleli a nemzeti kiberbiztonsági stratégiákat és nemzeti kiberbiztonsági keretrendszereket, valamint az ezek végrehajtását felügyelő szabályozó testületeket (pl. Izlandon a Kiberbiztonsági Tanácsot; a németországi Szövetségi Információbiztonsági Hivatalt; a Kiberbiztonsági és Információbiztosítási Hivatalt az Egyesült Királyságban).

A kapacitásépítési pillér a kiberbiztonsági tudatosság, az oktatás és a képzés előmozdítására irányuló erőfeszítéseket fedi le. Ilyenek például a lakossági figyelemfelkeltő kampányok, a kiberbiztonsági kutatás és fejlesztés, a szakmai képzés, valamint a nemzeti oktatási programok és tantervek. Például a Dominikai Köztársaságban az Információs Társadalom és Tudás Nemzeti Bizottságának (CNSIC) hivatalosan elismert nemzeti tudatosító programja van, amely előmozdítja azokat a normákat, értékeket és társadalmi

viselkedésmódokat, amelyek hozzájárulnak az integritáshoz, a kreativitáshoz és az innovációhoz a kibertérben való navigáció során. Más országok is indítottak kapcsolódó kiberbiztonsági figyelemfelkeltő és oktatási kampányokat. A kiberbiztonsági figyelemfelkeltő és oktatási kampányokon kívül az ITU eszközöket biztosít a tagországoknak a kapacitásépítési erőfeszítéseikhez. Ezeket az eszközöket arra tervezték, hogy felmérjék az országot célzó konkrét fenyegetéseket (Honeypot Research Network /„Mézesbödön Kutatási Hálózat"/, vagy rövidítve HORNET), valamint összesítsék és megosszák a releváns incidensadatokat (Abuse Watch Alerting and Reporting Engine /Visszaélésfigyelő Riasztási és Jelentési Gépezet/ vagy rövidítve AWARE).

Az együttműködési pillér az ügynökségek közötti és a köz-magán partnerségekre, az információmegosztó hálózatokra és az együttműködési megállapodásokra összpontosít. Ilyen például Ausztrália Nemzetközi Kiberelkötelezettségi Stratégiája, amelynek célja a köz- és a magánszektor együttműködésének, valamint az egyes országok közötti együttműködés elősegítése. További példák az országok partnerségei és információcseréje az ITU-val, az Európai Unió Hálózat- és Információbiztonsági Ügynökségével (ENISA), az Európai Biztonsági és Együttműködési Szervezettel (EBESZ) és az Észak-atlanti Szerződés Szervezetével (NATO), valamint az együttműködési megállapodások, mint például az Európa Tanács 2001. évi számítógépes bűnözésről szóló egyezménye, a Független Államok Közösségének számítógépes együttműködési megállapodása. Az Arab Államok Liga 2010. évi arab egyezménye az információs technológiai bűncselekmények elleni küzdelemről, valamint az Afrikai Unió 2014. évi kiberbiztonsági és személyes adatok védelméről szóló egyezménye, hogy csak néhányat említsünk.

Az átfogó és hatékony nemzeti kiberbiztonsági stratégia kidolgozásához az ITU 2018-ban egy Útmutatót tett közzé, amelyben a következő tematikus területek bevonását ajánlotta: kockázatkezelés, vagyis a fenyegetések azonosításának, értékelésének, ellenőrzésének és/vagy megszüntetésének folyamata; a felkészültség és az ellenálló képesség növelése; a kritikus infrastrukturális szolgáltatások és az alapvető szolgáltatások védelme; kapacitás- és kapacitásbővítés és tudatosságfejlesztés, valamint a nemzetközi együttműködés fejlesztése.

Statisztikai együttműködés

2015-ben az Egyesült Nemzetek Statisztikai Bizottsága (UNSC) és az Egyesült Nemzetek Bűnmegelőzési és Bűnüldözési Igazságszolgáltatási Bizottsága (UN-CCPCJ) jóváhagyták a bűnözés nemzetközi statisztikai célú osztályozását (International Classification of Crime for Statistical Purposes – ICCS), összhangban az ENSZ BT, valamint a Gazdasági és Szociális Tanács idevonatkozó határozataiban elfogadott elvekkel. Az ICCS a bűncselekmények meghatározásának és osztályozásának nemzetközi szabványa a bűnözésre és a büntető igazságszolgáltatásra vonatkozó statisztikai adatok előállítása és terjesztése terén.

Azóta világszerte megnőtt az érdeklődés a nemzeti bűnügyi statisztikáknak az ICCS-szel történő összehangolása iránt, amihez az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatalának (UNODC), valamint más nemzeti és nemzetközi érdekelt felek figyelemfelkeltő és technikai segítségnyújtási tevékenysége is hozzájárult. Az ICCS-hez történő igazodás létfontosságú a bűnözésre és a büntető igazságszolgáltatásra vonatkozó jó minőségű, összehasonlításra alkalmas statisztikai adatszolgáltatáshoz. Számos ország már jelentős előrelépést tett az ICCS végrehajtását szolgáló szervezeti feltételek megteremtésében, valamint nemzeti bűnügyi kategóriáinak vagy büntető törvénykönyvének az ICCS-vel történő összehangolásában. A nemzeti bűnügyi statisztikáknak az ICCS-hez való igazítására irányuló erőfeszítések eredményeként egyre inkább elérhetővé válnak a nemzeti, regionális és globális szinten összehasonlítható adatok.

Az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala által 2024 decemberében közzétett végrehajtási kézikönyv célja, hogy útmutatással szolgáljon az ICCS bevezetéséhez az országok számára. A kézikönyv konkrét lépéseket ismertet az ICCS átvételének elősegítésére, a megvalósítás hatókörének meghatározására, megfelelési táblázat létrehozásához és az ICCS szerinti adatok előállítására.

Az ICCS kifejlesztésének indokoltsága

A bűnözési és büntető igazságszolgáltatási adatok célirányos gyűjtése és statisztikai formába történő rendezése nélkülözhetetlen a bizonyítékokon alapuló döntéshozatali folyamatokat megalapozó információk előállításához. A megbízható, kellő részletezettségű adatok segítségével a büntető igazságszolgáltatási rendszer, a döntéshozók és a közvélemény nyomon követhetik a bűnözés tendenciáiban és mintáiban végbemenő változásokat, figyelemmel kísérhetik az egyes államoknak a bűnözésre adott válaszait, értékelhetik a bűnmegelőzési stratégiákat, és képessé válnak a bűnözés különböző aspektusainak különféle összefüggésekben történő alaposabb megértésére. A statisztika minden társadalom információs rendszerének nélkülözhetetlen alapeleme, amelynek pártatlan módon kell összegyűjtenie és hozzáférhetővé tenni az adatokat, miközben tiszteletben tartja a polgároknak a nyilvános információkhoz való jogát és a személyes adataik védelmét.

A bűnügyi statisztikát készítő szervezetek számára az adatok időbeli vagy földrajzi adatsorának elemzése azonban gyakran nagy kihívást jelent, mivel még nincsenek olyan világszerte elfogadott szabványosított fogalmak és ismérvek, amelyek lehetővé tennék az adatok érdemi összehasonlítását. Az egyes országok büntető igazságszolgáltatási rendszerei ugyanis eltérő módszereket, különböző definíciókat és különböző fogalmakat használnak a bűnözés és a büntető igazságszolgáltatás adatainak meghatározására és rendszerezésére, ráadásul inkább jogi szempontok, mint statisztikai elvek alapján. Ahhoz például, hogy egy bűncselekmény támadásnak minősüljön, az egyik országban az áldozat és a támadó között fizikai érintkezésnek kell történnie, míg egy másik országban ez nem szükséges előfeltétel.

Az adatoknak a statisztikai elvek mellett a jogszabályi rendelkezésekkel, például a büntető törvénykönyv cikkeivel összhangban tovább rendszerezhetőknek és kategorizálhatóknak kell lenniük, és tükrözniük kell az adatrögzítő szervezet működési fókuszát. A jogszabályok és a statisztikák közötti szoros és összefüggő kapcsolat megteremtése gyakran elemzési problémákhoz vezet. A rendelkezésre álló adatok ugyanis nem mindig relevánsak a politikai döntéshozatal számára, illetve nem mindig hasznosíthatók hatékonyan az elemzések során, továbbá, gyűjtésük és tárolásuk módja sem mindig igazodik az adatok megosztásának lehetőségeihez és az adatok felhasználási céljaihoz.

Az időbeli és a joghatóságok közötti összehasonlíthatóságot hátráltathatják továbbá a jogszabályok elkerülhetetlen változásai, valamint az a tény, hogy ugyanaz a cselekmény országonként sokszor meglehetősen eltérő jogi rendelkezések alapján minősül büntethetőnek. A jogi heterogenitás miatt nehéz objektíven összehasonlítani a büntető igazságszolgáltatás vagy a közösségi biztonság eredményeit az egyes joghatóságok között.

Az ICCS ezeknek a problémáknak a megoldásával foglalkozik azáltal, hogy nemzetközileg elfogadott fogalmakon, meghatározásokon és elveken alapuló közös keretrendszert teremt statisztikai célokra. Fontos, hogy amint azt az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala által közzétett kézikönyv is részletesebben kifejti, az osztályozás elvégzése ne tegye szükségessé a hatályos büntetőjog módosítását, továbbá kizárólag statisztikai célokat szolgáljon. A bűncselekményeket az ICCS érthető és szisztematikus módon csoportosítja, ami javítja a bűnözési és büntető igazságszolgáltatási statisztikák összegyűjtésének, előállításának, terjesztésének és felhasználásának lehetőségét a nyilvánosság tájékoztatásához, valamint tágítja a politikák és programok testreszabásának lehetőségét a bűnmegelőzés, a jogállamiság és a büntető igazságszolgáltatás reformja terén.

Az ICCS olyan átfogó keretet biztosít a nemzetközileg elfogadott bűnözési fogalmak és definíciók számára, amelyek a bűnözésre vonatkozó statisztikai adatok gyűjtésének, előállításának, terjesztésének és felhasználásának javítását szolgálják. Ezen túlmenően, az ICCS megkönnyíti további adatok gyűjtését, például a bűncselekmények, az áldozatok és az elkövetők jellemzőiről, valamint az elkövetés indítékairól, egy sor szelekciós változó segítségével.

Az osztályozás a kialakult statisztikai elvekre épül:

- Hierarchikusan felépítés – az ICCS négy összesítési szinttel rendelkezik, felül a legáltalánosabb kategóriákkal, és alul a legrészletesebb kategóriákkal. A legrészletesebb kategóriák összesíthetők az általánosabb kategóriákba (például a „súlyos támadás” és a „kisebb támadás” a 4. szintű kategóriába tartoznak, amelyek egyaránt a 3. szintű „támadás” kategóriába sorolhatók).
- Egymást kizáró kategorizálás – A minősítés azonos szintjén minden bűncselekmény hatókörét úgy kell meghatározni, hogy kizárja a kétértelműséget és az átfedést. Az ICCS-ben elvileg minden bűncselekményt csak egy kategóriába szabad besorolni.

- Teljeskörűség – Az osztályozás a bűncselekmények olyan átfogó jegyzékén alapul, amelyben minden olyan cselekmény vagy esemény rögzítésre kerül, amelyekről általában tudott, hogy megfelelő számú országban bűncselekménynek minősülnek. Ez lehetővé teszi a lehető legtöbb fajta bűncselekmény megfelelő besorolását.

Mindemellett az ICCS arra is törekszik, hogy univerzálisan alkalmazható legyen. A besorolás kategóriái ezért inkább magatartás szempontú megközelítésen alapulnak, nem pedig a büntetőjog szigorú jogi előírásain. A büntetőjogban meghatározott bűncselekmények jellemzően olyan cselekményekhez vagy viselkedési és kontextuális jellemzőkhöz kapcsolódnak, amelyek általánosan bűncselekménynek minősülnek (például egy személy szándékos megsebesítése, vagy vagyon elvétele a tulajdonos hozzájárulása nélkül). A magatartás alapú megközelítés alkalmazása elkerüli a jogi részletezettség okozta problémákat, ezáltal egyszerűsített és globálisan alkalmazható osztályozást eredményez, kevesebb kétértelműséggel. Úgy is lehet fogalmazni, hogy könnyebb minősíteni azokat a bűncselekményeket, amelyeket magatartások és cselekedetek határoznak meg, nem pedig jogi definíciók és szándékok. Ez a megközelítés teszi lehetővé az országok, intézmények és jogrendszerek közötti következetes alkalmazást, függetlenül a nemzeti büntetőjog sajátosságaitól. Az ICCS tehát alapvető eszköz az adatok minőségének, összehasonlíthatóságának és részletességének javításában a nemzeti büntető igazságszolgáltatási rendszerek valamennyi érintett szereplője számára. Mivel az ICCS-t több országban alkalmazzák, az ebből eredő megnövekedett statisztikai összehasonlíthatóság várhatóan javítja az elemzési lehetőségeket nemzeti, regionális és nemzetközi szinten egyaránt.

Közös statisztikai terminológia

Az ICCS-t a bűnözés és a büntető igazságszolgáltatás statisztikai célú rendszerezésére és harmonizálására fejlesztették ki. Az osztályozás hatálya kiterjed a bűncselekmények valamennyi fő típusára, és mint ilyen, átfogó definíciós keretet ad a nemzeti bűnügyi statisztikák készítéséhez. A statisztikai fogalmak és definíciók alapján az ICCS átfogó, hosszú távú perspektívát nyújt a nemzeti bűnügyi statisztikai rendszer kiépítése vagy felülvizsgálata számára, mivel úgy alakították ki, hogy ne legyen érzékeny a nemzeti jogszabályok és szabályozási keretek változásaira. A bűncselekményi kategóriák szabványosítása elősegíti és koordinálja a büntető igazságszolgáltatási szervek és a különböző adatforrások közötti adatcserét, beleértve az adminisztratív nyilvántartásokat és a statisztikai felméréseket.

Ezenkívül az ICCS lehetővé teszi a büntető igazságszolgáltatási rendszer különböző szakaszai közötti adatkapcsolatok feltárását is. Ha valamennyi érintett adatelőállító következetesen alkalmazza, az ICCS felhasználható a büntető igazságszolgáltatási rendszer különböző szakaszai közötti áramlások mérésére is. Például összefüggések állapíthatók meg egy adott bűncselekmény feljegyzett száma, az azonos típusú bűncselekmények

miatti letartóztatások száma, valamint az egyes személyeknek azonos típusú bűncselekmények elkövetése miatt visszaesőként történő felelősségre vonása, elítélése között. Az ICCS tehát közös nyelvet biztosít a statisztikai információk kommunikációjához és cseréjéhez, lehetővé téve a bűnözéssel kapcsolatos nemzeti helyzet és a büntető igazságszolgáltatási folyamatok hatékony megértését.

Nagyobb részletezettség

Az ICCS lehetővé teszi a bűncselekményekkel kapcsolatos részletes adatok gyűjtését, és jól alkalmazható a büntető igazságszolgáltatási eljáráshoz kapcsolódó események és körülmények, például a letartóztatások, a vádemelések és az ítélethozatalok számszerűsítésére. Ráadásul a lebontható változók gyűjtése révén az ICCS rávilágíthat a bűnözés számos aspektusára, és képes a politikai döntéshozatalhoz szükséges rendkívül részletes bűnözési és büntető igazságszolgáltatási információk előállítására is. Az ICCS-ben használt lebontható változók készlete kontextuális információkat nyújt a bűncselekményekről, támogatva az adott bűncselekmények kifinomultabb, mélyebb elemzését. Az ilyen adatok gyakran kulcsfontosságúak a bűnözési trendek jobb megértéséhez.

A nemzetközi összehasonlíthatóság elősegítése

Nemzetközi szinten az ICCS a fogalmak és definíciók szabványosításával, az adatok szisztematikus gyűjtésének, előállításának és terjesztésének elősegítésével, továbbá a nemzetközi bűnözéssel kapcsolatos mélyreható kutatások és elemzések iránti megnövekedett igények kielégítésével javítja az országok közötti bűnözési statisztikák összehasonlíthatóságát. A következő fejezetben láthatjuk az adatok korlátozott összehasonlíthatóságából eredő nehézségeket.

A szervezett – különösen a transznacionális jellegű – bűnözés utáni nyomozás során a bűnügyi válaszlépések hatékonyságát hátráltathatja e bűncselekmények összetett jellege, valamint az a tény, hogy a szervezett bűnözési csoportok utáni nyomozás gyakran átnyúlik az intézményi és az országok közötti határokon. Az Egyesült Nemzetek Szervezete által a transznacionális szervezett bűnözés ellen 2000-ben elfogadott egyezmény (A/RES/55/25) egyebek között hangsúlyozza, hogy a részes államoknak közös definíciókat, szabványokat és módszereket kell kialakítaniuk a szervezett bűnözés természetének jobb megértése érdekében. Az ICCS hozzájárul ennek a célkitűzésnek az eléréséhez azáltal, hogy a bűncselekmények szabványosított osztályozását és szakpolitikai szempontból releváns, lebontható változókat kínál.

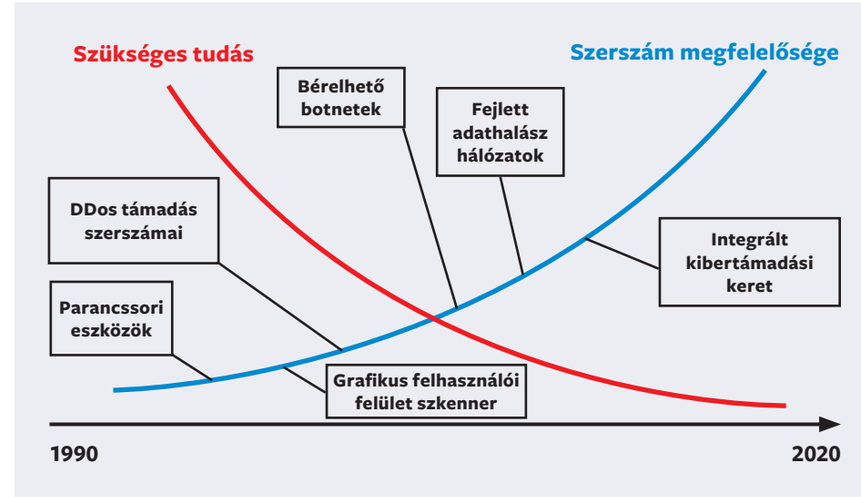
Ezen túlmenően az ICCS az egyik elsődleges eszköz a 2030-ig terjedő időszakra szóló Fenntartható Fejlődési Keretrendszer keretében a jó minőségű adatok gyűjtését célzó nemzeti erőfeszítések támogatására. A közbiztonság, az emberkereskedelem, a korrupció és az igazságszolgáltatáshoz való hozzáférés területéhez kapcsolódó számos, a Fenntartható Fejlődési Célok keretében alkalmazott meghatározás összhangban van az ICCS-vel. Az ICCS bevezetése így lehetővé teszi az országok számára, hogy jó minőségű

adatokat állítsanak elő a fenntartható fejlődési célok mutatóinak kimunkálásához. Például a 16.5-ös cél (a korrupció és a vesztegetés minden formájának jelentős csökkentése) két mutatójának nyomon követéséhez az országoknak pontos, az ICCS-ben meghatározott korrupciós adatokra van szükségük a lakosság és a vállalkozások körében. Ezen túl a mutatók további, például életkor és nem szerinti bontást követelnek meg, amely változókat az ICCS tartalmazza.

Egyéb nemzetközi erőfeszítések a kiberbűnözéssel kapcsolatos statisztikák és szabályozások egységes értelmezésére

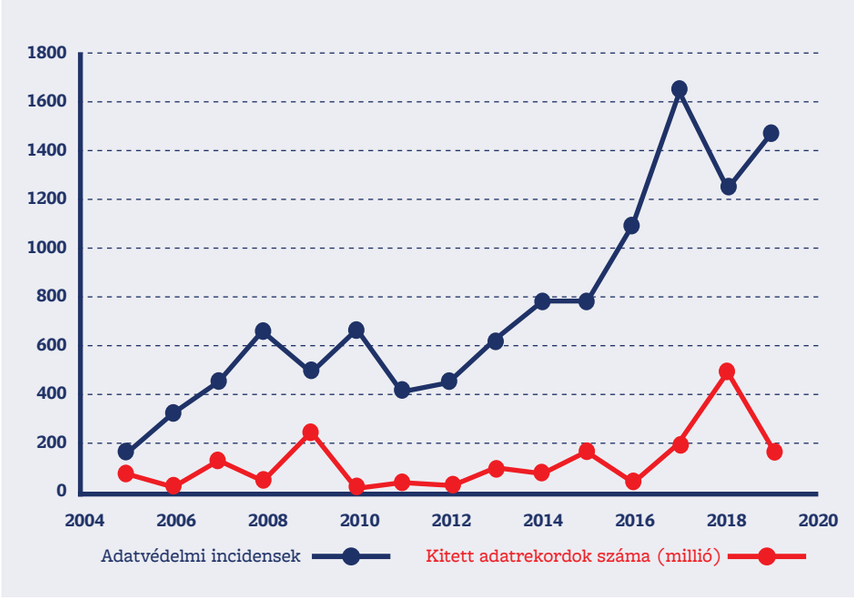
Az információs és kommunikációs technológiai rendszerek elleni támadások (kibertámadások) száma világszerte növekszik, ezek körében pedig a pénzügyi szolgáltatások a leggyakrabban megcélzott ágazat. A kiberbűnözés egyre kiterjedtebbé válik, aminek többnyire az a fő oka, hogy egyelőre a büntetőeljárásoknak viszonylag alacsony a kockázata, ugyanakkor széles körben érhetők el a könnyen használható támadási eszközök és a kiberbűnözést támogató szolgáltatások. A technológia fejlődése egyelőre nem csupán a pénzintézetek és a többi megcélzott ágazat számára teremt további lehetőségeket a kockázat megelőzésére és mérséklésére, hanem a bűnözők számára is, amint azt a kiberbűnözésről szóló fejezetben már bemutattuk. A hackelésre használt eszközök és szoftverek például az elmúlt két évtized során ugyancsak sokat fejlődtek, és napjainkban már viszonylag alacsonyan képzett támadók is könnyen használhatják azokat a korábbi költségek töredékéért. Ez a kiberincidensek és adatszivárgások számának meredek növekedéséhez vezetett (*3. ábra*).

3. ÁBRA: A kiberkockázatok alakulása a pénzügyi szektorban



Forrás: Adelmann et al., 2020. p.7. Carnegie Mellon University utánközlés

4. ÁBRA: Az adatfeltörések száma és a veszélyeztetett adatok száma az Egyesült Államokban



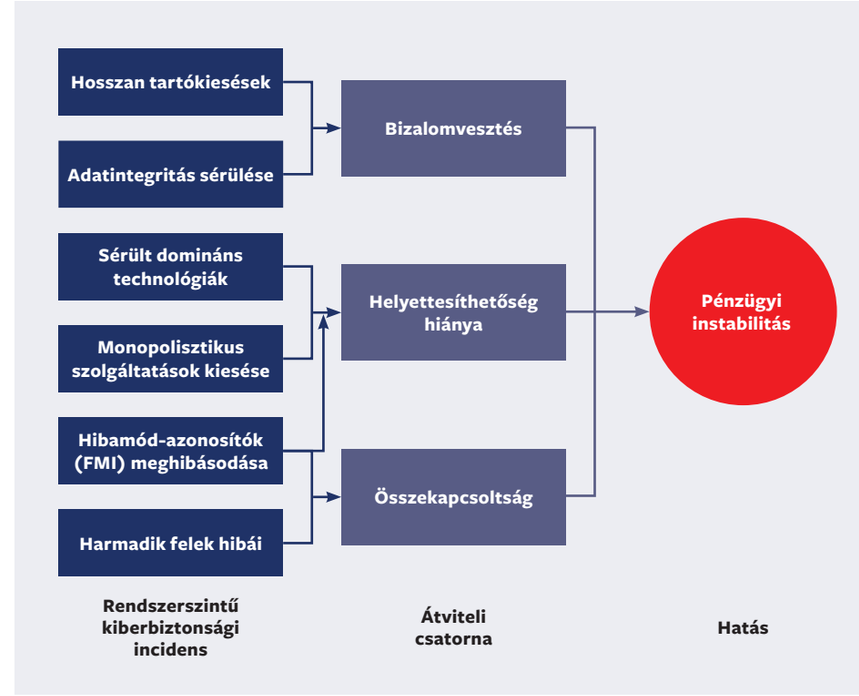
Forrás: Identity Theft Resource Center.

A kiberfenyegetések egyre kifinomultabbá váltak, és gyakran több joghatóságra is kiterjednek, így nagyobb kihívást jelent a nyomozás és a vádemelés. A kibertámadások „iparosodtak", számos művelet esetében nemzetközi munkamegosztás jött létre; a hackelési szolgáltatásoknak, a sebezhetőségi cseréknek, a speciális szolgáltatásoknak és az outsourcing szolgáltatásoknak önálló piacai alakultak ki (Cybercrime-as-a-service). A támadók olyan fokú agilitást mutatnak a határokon átnyúló aktivitásban, amelyet a hatóságok nehezen tudnak megragadni.

Míg a legtöbb támadás pénzügyi indíttatású, a növekvő geopolitikai feszültségek megnövelik a stratégiai indíttatású incidensek kockázatát is. A pénzügyi szolgáltatások a támadók széles körével szemben kiszolgáltatottak, a magányos hackerektől a kifinomult szervezeteken át egészen a nemzetállami kiberhadviselési egységekig. A pénzügyi szektor adatoktól való függése növeli a kiberbiztonság sebezhetőségét és összetettségét. Az adatsérülés – amelyet néha „adatmérgezésnek" is neveznek – egy olyan új típusú fenyegetés, amikor a kibertámadás hibás vagy félrevezető adatokat táplál be a rendszerekbe. Ennek legsúlyosabb következménye a bizalom megingása, hasonlóan ahhoz, ahogy a dezinformáció az „álhíreken" révén aláássa a közbizalmat. A gépi tanulás és a mesterséges intelligencia megjelenése még komolyabbá teszi ezt a kockázatot, különösen, ha a feltört adatokat az algoritmusokba táplálják és felhasználják a döntéshozatal befolyásolására.

A kiberkockázat a bizalomvesztés, a helyettesíthetőség hiánya és a fokozott összekapcsolódás révén befolyásolhatja a pénzügyi stabilitást. Az *5. ábra* szemlélteti a kibertámadástól a gazdasági instabilitásig vezető ok-okozati láncot, kiemelve a leggyakoribb kiváltó okokat és a valószínű átviteli csatornákat. (Természetesen alternatív kombinációk is lehetségesek.) Megfigyelhető, hogy – néhány figyelemre méltó kivételtől eltekintve – a legtöbb sikeres kibertámadás csak egy adott intézményt érint, és korlátozott károkat okoz. Egy olyan sikeres támadás viszont, amely kellő technikai háttérrel rendelkezik egy kulcsfontosságú intézmény megbénításához vagy megzavarásához, vagy a rendszeren képes terjedni, az rendszerszintű eseménnyé válhat. A kiberbűnözés történetéről szóló fejezet legutóbbi évekről szóló részében számos példa található a rendszerkockázatú támadásokra, többek között a 2021-es Colonial Pipeline és a 2024-es CrowdStrike elleni incidensekre.

5. ÁBRA: A kibertámadástól a gazdasági instabilitásig vezető ok-okozati lánc



Forrás: Adelmann et al., 2020. p.10.

A pénzügyi szektornak az egyes nemzetgazdaságok vérkeringésében, valamint a világkereskedelemben betöltött stratégiai szerepe miatt a pénzügyi szektor – valamint néhány más, ugyancsak stratégiai jelentőségű szektor, mint az energetika, a hírközlés és az egészségügy – kiberbiztonságának védelme kiemelt fontosságú kormányzati feladat. Ebből adódóan a pénzügyi szektor stabilitásáért felelős nemzeti szervek és nemzetközi

szervezetek külön erőfeszítéseket tesznek a pénzügyi szektor kiberbiztonsága nemzetközi szabványainak, szabályainak és terminológiájának összehangolására.

A pénzügyi szektor rendszerszintű stabilitásának megőrzése és a kiberreziliencia – azaz a kibertámadások elleni védekezőképesség – fokozása érdekében a Pénzügyi Stabilitási Tanács (Financial Stability Board) koordinálásával olyan szervezetek, mint a BIS, az IMF, a FATF, az IOSCO, a BCBS, az ECB, valamint az Európai Unió ágazati szakhatóságai és a bűnüldözéssel foglalkozó nemzetközi szervezetek összehangoltan dolgoztak ki irányelveket, iránymutatásokat, szabványokat, vizsgálati módszertanokat és az egységes fogalomhasználatot elősegítő dokumentumokat. Ennek az együttműködésnek egyik fontos „terméke" a Pénzügyi Stabilitási Tanács (FSB) által 2018-ban kidolgozott Kiberlexikon, aminek az volt a rendeltetése, hogy támogassa az FSB, a szabványalkotó testületek (SSB-k) és más nemzetközi szervezetek munkáját a pénzügyi szektor kiberbiztonságával és kiberellenállásával kapcsolatban. Az első közzétételt követően a Kiberlexikont 2023-ban frissítették, hogy naprakész maradjon a gyorsan változó kiberkörnyezetben és a folyamatosan fejlődő információs technológiák területén. A lexikon frissítése során ugyanazokat a befogadási és kizárási kritériumokat alkalmazták, mint az első kiadás elkészítésekor, ezzel biztosítva a tartalom folyamatos következetességét. A felülvizsgálat során az FSB több mint 80, a magánszektor és a nemzeti hatóságok által javasolt kifejezést vizsgált meg, miközben figyelembe vette a nyilvános konzultációk és a magánszektorral folytatott együttműködés tapasztalatait is.

A kiberfenyegetettségekkel kapcsolatos fejlemények mérlegelése alapján a „kibertámadás", a „bennfentes fenyegetés", az „adathalászat", a „zsarolóvírus" és a „nulladik napi sebezhetőség" kifejezések elég fontosnak tűntek a lexikonba történő felvételhez. Ezen kívül a „biztonsági műveleti központ" kifejezést számos olyan pénzügyi intézmény alapvető funkciójának tekintették, amelyek kulcsszerepet töltenek be a kiberincidensek felderítésében és kezelésében. Ezért indokoltnak tűnt a fogalom felvétele, hogy tovább támogassa a kiberellenállóság erősítését célzó törekvéseket.

A szerkesztők elengedhetetlennek tartották a következő definíciók felülvizsgálatát is: „kiberriasztás", „kiberincidens", „kiberincidens-reagálási terv", „információs rendszer", „penetrációs tesztelés" és „sebezhetőség-értékelés". A „kiberincidens" definíciójával kapcsolatban megoszlottak az álláspontok abban a tekintetben, hogy a meghatározásnak elég tágnak kell-e lennie ahhoz, hogy magában foglalja-e mind a rosszindulatú, mind a nem rosszindulatú tevékenységekből eredő eseményeket. Tekintettel arra, hogy a legtöbb pénzügyi hatóság tágabb értelemben használta ezt a kifejezést politikáiban, szabályzataiban és útmutatásaiban, az FSB úgy döntött, hogy a tágabb definíciót alkalmazza a konvergencia előmozdítása érdekében.

A kiberlexikon kidolgozásának célja, hogy támogassa az FSB munkáját az ágazati szabályalkotó szervezetek – beleértve a Bázeli Bankfelügyeleti Bizottságot (BCBS), a Fizetési és Piaci Infrastruktúrák Bizottságát (CPMI), a Biztosításfelügyeletek Nemzetközi Szövetségét (IAIS) és az Értékpapír-felügyeletek Nemzetközi Szervezetét (IOSCO), – továbbá a magánszektor szereplői, például pénzügyi intézmények és nemzetközi szabványügyi szervezetek munkáját, hogy eredményesebben foglalkozzanak a pénzügyi szektor kiberbiztonságával és kiberellenállóságával. A lexikonnak ugyanakkor nem célja, sem és feladata semmilyen nemzetközi megállapodás vagy magánszerződés jogi értelmezése.

A lexikon hasznos segítséget nyújthat a munkafolyamatok támogatásában, különösen az alábbi területeken:

- A releváns kiberbiztonsági és kiberellenállósági terminológia ágazatokon átívelő közös értelmezése. A lexikon elősegítheti a megfelelő kiberbiztonsági és kiberellenállósági terminológia közös és egységes értelmezését a pénzügyi szektorban, beleértve a bankszektort, a pénzügyi piaci infrastruktúrákat, a biztosítást, a tőkepiacokat és más releváns iparágakat. A pénzügyi szektorban – ide értve a hatóságokat és a magánszektorbeli szereplőket is – az egységes fogalomhasználat elősegítheti a kiberbiztonság és a kiberellenállóság erősítését az ágazat egészében. Tágabb értelemben pedig a közös lexikon elősegítheti a közös megértést más iparágakkal, és támogathatja a megfelelő együttműködést a kiberbiztonság és a kiberellenállás erősítése érdekében.
- A kiberkockázati forgatókönyvek pénzügyi stabilitási kockázatainak felmérése és nyomon követése. Mivel az FSB és tagjai a kiberincidensekhez kapcsolódó pénzügyi stabilitási kockázatok felmérésén és nyomon követésén dolgoznak, erőfeszítéseiket támogathatja egy olyan lexikon, amely elősegíti a kiberkockázatokkal kapcsolatos terminológia közös megértését. Például, a globális pénzügyi rendszer sebezhetőségeinek rendszeres értékelése részeként az FSB időszakonként mérlegeli, hogy a működési kockázatok, köztük a kiberkockázatok milyen sokkokat válthatnak ki, amelyek átterjedhetnek a pénzügyi rendszer egészére.
- Adott esetben információmegosztás. Egy olyan lexikon, amely elősegíti a közös megértést a pénzügyi szektorban, beleértve a köz- és magánszereplőket, valamint a különböző joghatóságokat is, hasznosnak bizonyulhat a szükséges információk megosztása és cseréje során.
- A lexikon hasznos lehet az FSB és/vagy az ágazati szabályozók munkájában, azáltal is, hogy útmutatást nyújt a kiberbiztonsággal és a kiberellenállósággal kapcsolatban, beleértve a bevált gyakorlat azonosítását. Elősegítheti például a hatékony szabályozási megközelítéseket, miközben csökkenti a párhuzamos és esetlegesen ellentmondó szabályozási követelményekből eredő kockázatot.

A 21 oldal terjedelmű lexikon a https://www.fsb.org/2023/04/cyber-lexicon-updated-in-2023/ linken érhető el.

Az Európai Unió kiberbiztonsági szabályai

13. TÁBLÁZAT: Az EU kiberbiztonsági irányítási és intézményi mechanizmusának áttekintése

Intézmény	Jogszabályi háttér
Computer Emergency Response Team (CERT-EU) – Az uniós intézményeknél és szerveknél dolgozó informatikai biztonsági szakértők csoportja	EU, Euratom 2023/2841
Európai Kiberbiztonsági Kompetenciaközpont (ECCC)	EU 2021/887
Európai Védelmi Ügynökség (EDA)	EU 2015/1835
Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA)	EU 2019/881
Európai Kiberpajzs	EU 2025/38
Európai Kiberbiztonsági Tanúsító Csoport (European Cybersecurity Certification Group – ECCG)	ECCG EU 2019/881
NIS együttműködési csoport	EU 2022/2555
Intézményközi Kiberbiztonsági Tanács (Interinstitutional Cybersecurity Board – IICB)	EU, Euratom 2023/2841
Intézményközi Információbiztonsági Koordinációs Csoport	2022/0084 COD
Nemzeti Koordinációs Központok Hálózata	EU 2021/887
Computer Security Incident Response Team (EU-CSIRT) - Számítógépes biztonsági esemény-elhárítási csoportok európai hálózata	EU 2022/2555
Európai kiberválságügyi kapcsolattartó szervezetek hálózata – EU European Cyber Crisis Liaison Organisation Network	EU 2022/2555
Uniós kiberbiztonsági tartalék	EU 2025/38
Európai kiberbiztonsági riasztórendszer	EU 2025/38

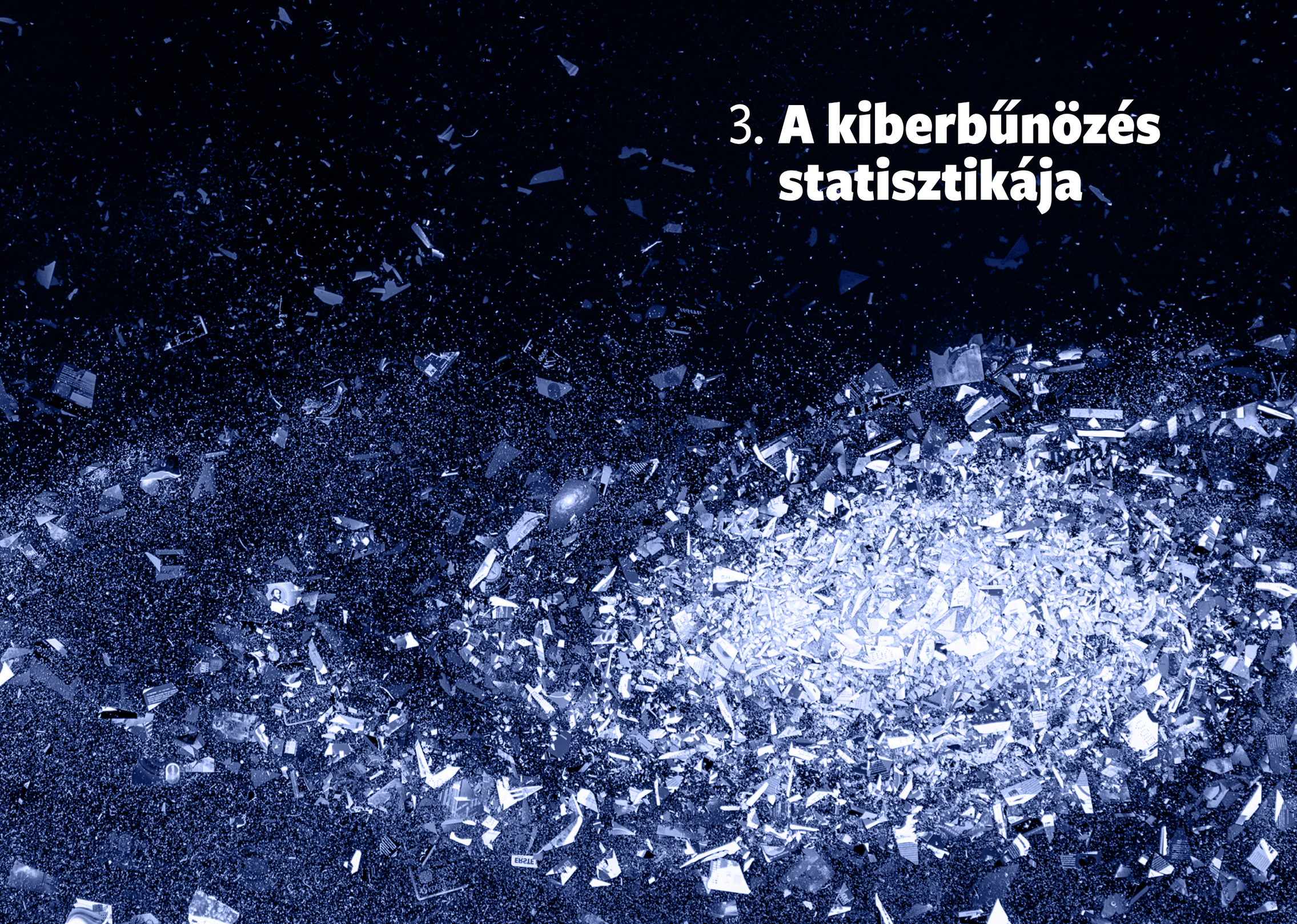
Forrás: Szerzők összeállítása az Európai Bizottság adatközlése alapján

14. TÁBLÁZAT: Az EU kiberbiztonsággal kapcsolatos jogszabályai

Jogszabály
(EU) 2019/881 rendelet az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről
(EU) 2021/887 rendelet az Európai Kiberbiztonsági Kompetenciaközpont létrehozásáról
(EU) 2022/2555 irányelv az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
(EU) 2023/2841 rendelet a kiberbiztonságról
(EU) 2024/2847 rendelet a kiberbiztonsági ellenállóképességről
(EU) 2025/38 rendelet a kiberszolidaritásról
(EU) 2022/0084 (COD) rendelet az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

Forrás: Szerzők összeállítása az Európai Bizottság adatközlése alapján

3. A kiberbűnözés statisztikája



Világszerte egyre nagyobb aggodalomra ad okot a kiberbűnözés, mert áldozatainak száma évről-évre növekszik, miközben jelentős anyagi veszteségeket is okoz.

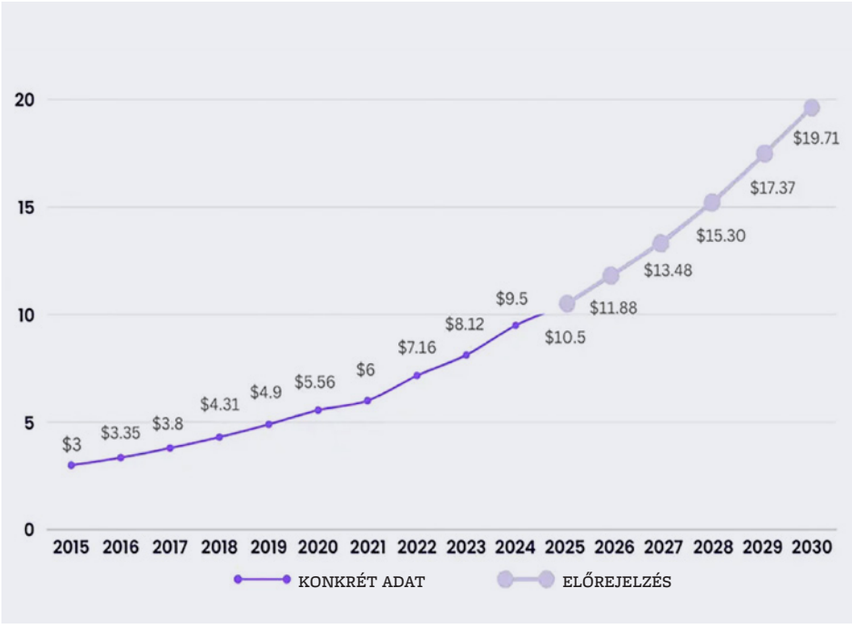
Az angol Comparitech kiberbiztonsági kutatócég 2023-ban tüzetesen elemezte a világ 100 legnagyobb GDP-jével rendelkező országból rendelkezésre álló kiberbűnözési jelentéseket és statisztikákat (Bischoff, 2023). Közülük 77 ország esetében állnak rendelkezésre részletes adatok, ám csak 16 esetben találhatók információk az okozott károk értékéről. A 100 országról készített összeállítást a *15.sz. táblázat* mutatja be.

A rendelkezésre álló adatok szerint a legnagyobb veszteséget elszenvedő országok a következők:

- Egyesült Államok: 5,3 millió áldozat, 42,9 milliárd dollár veszteség,
- Egyesült Királyság: 5 millió áldozat, akik 40,1 milliárd dollárt veszítettek,
- Oroszország: 3,5 millió áldozat, 28,1 milliárd dollár veszteség,
- Kína: 3,1 millió áldozat, 25 milliárd dollár veszteség,
- Spanyolország: 2,5 millió áldozat, a veszteség 20,2 milliárd dollár.

A kutatók becslése szerint 100 000 emberre számítva évente 1096 fő válik kiberbűnözés áldozatává, ami a világ 8,072 milliárd lakosára vetítve 88,5 millió áldozatot jelent világszerte. Az egyes bűncselekmények átlagosan 8069 dolláros költsége pedig évente közel 714 milliárd dollár veszteség elszenvedését jelenti.

6. ÁBRA: Globális kiberbűnözés okozta költség 2015–2030 (billió USD)



Forrás: (Salgado, 2024)

15.A TÁBLÁZAT: A kiberbűnözés által legfenyegetettebb 10 ország

Rang-sor	Ország	Basel pénzmosási index	Kiber-biztonsági kitettségi index	Nemzeti kiber-biztonsági index	Digitális fejlettségi szint	Globális kiber-biztonsági index	Kiber-bűnözési kockázati pontszám
1	Panama	5,81	5,69	4,32	5,16	3,35	**4,86**
2	Belarusz	5,21	6,14	3,51	4,34	3,86	**4,61**
3	Chile	4,03	4,69	5,07	4,11	2,98	**4,18**
4	Costa Rica	4,58	4,38	4,68	3,77	2,49	**3,98**
5	Grúzia	4,64	3,83	5,58	4,64	0,81	**3,90**
6	Egyesült Arab Emirátusok	5,70	3,59	5,97	3,11	0,00	**3,68**
7	Thaiföld	5,80	4,45	4,00	3,08	0,08	**3,48**
8	Szaúd Arábia	5,28	3,90	4,08	2,92	0,00	**3,24**
9	Uruguay	4,07	3,48	3,92	3,15	0,53	**3,03**
10	Mauritius	5,03	2,00	3,75	3,99	0,00	**2,95**

Forrás: (Salgado, 2024)

15.B TÁBLÁZAT: A kiberbűnözésnek legkevésbé kitett 10 ország

Rang-sor	Ország	Basel pénzmosási index	Kiber-biztonsági kitettségi index	Nemzeti kiber-biztonsági index	Digitális fejlettségi szint	Globális kiber-biztonsági index	Kiber-bűnözési kockázati pontszám
1	Finnország	2,88	0,11	1,56	1,73	0,00	**1,26**
2	Franciaország	3,52	0,23	0,91	2,00	0,10	**1,35**
3	Svédország	3,12	0,21	1,56	1,85	0,07	**1,36**
4	Dánia	3,56	0,12	1,43	2,17	0,00	**1,45**
5	USA	4,32	0,15	1,58	1,58	0,01	**1,53**
5	Egyesült Királyság	3,63	0,21	1,56	2,27	0,00	**1,53**
6	Norvégia	3,50	0,13	1,17	2,78	0,30	**1,58**
7	Kanada	4,25	0,21	1,25	2,15	0,68	**1,71**
8	Spanyolország	3,88	0,21	3,25	1,98	0,03	**1,87**
8	Németország	4,21	0,24	2,50	1,79	0,62	**0,62**

Forrás: (Salgado, 2024)

Már a Comparitech számai is csillagászati nagyságrendet képviselnek, ám ha összehasonlítjuk más becslésekkel, amelyek szerint 2024-ben az áldozatok száma elérte az 556 milliót, vagyis a föld lakosságának több mint 6%-át, továbbá, ha figyelembe vesszük, hogy létezik olyan becslés is (Computer Crime Research Center, 2024), miszerint a kiberbűnözés globális költsége 2025-ben elérheti akár a 12 ezer milliárd dollárt, akkor a Comparitech által számított adatok akár szerénynek is mondhatók.

Egy másik becslés az alábbi adatokat tette közzé a kiberbűnözés összegszerű nagyságáról a 2023-2025. évekre:

16. TÁBLÁZAT: Összeállítás a 2023-2025. évek kiberbűnözéséről

Év	Összes globális kiberbűnözés becsült költsége	FBI IC3-hoz bejelentett veszteségek	Becsült Illegális kriptovaluta forgalom	Átlagos adatszivárgás költsége	Kifizetett váltságdíjak átlagos összege
2023	9,5 ezer milliárd USD (becslés)	12 milliárd USD	46,1 milliárd USD	4,5 millió USD	1,5 millió USD
2024	9,5 ezer milliárd USD	16 milliárd USD	40,9 milliárd USD (becsült 51 milliárd)	4,9 millió USD	2,7 millió USD
2025	10,5 ezer milliárd USD (előrejelzés)	N/A	N/A	N/A	57 milliárd USD (összes zsarolóprogram)

Forrás: (Frész, 2025)

A kiberbűnözés alakulásáról az utóbbi időben egyre több adat látott napvilágot. Ezek ugyan tükrözik a kiberbűnözés terjedését és profilját, ám alapos elemzéshez, összehasonlításokhoz csak korlátozottan használhatók fel. Az okok többfélék. Mindenekelőtt az adatok gyűjtése, feldolgozása és kiértékelése sok országban egyelőre nem teljes körű és sokszor időigényes folyamat, ezért a rendelkezésre álló publikus adatok gyakran már idejét múltak. Ezekről a problémákról részletesebben is írunk a Nemzetközi jogi és statisztikai együttműködés című fejezetben. Ezen túlmenően a rendelkezésre álló adatok sem tekinthetők mindig teljes körűnek. A tapasztalatok szerint ugyanis a kiberbűnözést a rendőrség és a kormányzati szervek többnyire alul jelentik, és az okozott károk valós összegét sem ismerik. Egyrészt azért, mert reputációs okokból gyakran maguk a károsultak sem jelentik be az elszenvedett támadást, de a bűnüldöző szerveknek sem áll mindig érdekében, hogy a tudomásukra jutott valamennyi támadást regisztrálják. (Ezt tükrözi az *16. táblázatban* a jelentett és a becsült esetek száma közötti különbség.) A bejelentett támadásokra vonatkozó adatok tartalma, illetve az adatok megbízhatósága is meglehetősen egyenetlen, csakúgy, mint az adatok feldolgozásának módszertana. Így például egyes országokban csak a kiberincidensek által közvetlenül okozott kárt mérik fel. Másutt viszont a közvetett károkat (pl. a termeléskiesést, az ügyfelek elvesztését) is számításba veszik.

A széles sávban szóródó adatok, illetve becslések jól mutatják, hogy a kiberbűnözés gyors terjedése ellenére számos ország még nem rendelkezik részletes és megbízható adatokkal sem a kiberbűnözésről, sem pedig a kibertámadások által okozott károk összegéről. A kárérték megállapítása is meglehetősen ingatag alapokon áll, főleg mivel a támadás másodlagos, „tovagyűrűző" hatásait és következményeit nehéz megragadni. Sokszor azért is, mert azok csak jóval a támadás időpontja után válnak nyilvánvalóvá és mérhetővé. A napvilágra kerülő nemzeti adatok összehasonlítását és elemzését az is nehezíti, hogy az egyes kiberbűncselekmények jogi meghatározása és statisztikai feldolgozásának módszere országonként jelentősen eltérhet egymástól, továbbá, mert az ilyen bűncselekmények által okozott károk fogalmi meghatározása és értéke

megállapításának módszertana sem kiforrott. Ezek a nehézségek magyarázzák, hogy az ENSZ statisztikai szervezete csak 2024 végére tudott egy olyan kézikönyvet közzétenni, amely egységes módszertanra és értelmezésre épülve, nagymértékben növeli a nemzetközi összehasonlítások megbízhatóságát (UNODC, 2024). A Nemzetközi jogi és statisztikai együttműködés című fejezetben erről is bővebben írunk.

Az előbb említett okok miatt a továbbiakban bemutatott adatokat és jelzőszámokat kellő óvatossággal kell kezelni, és azokat csak korlátozott mértékben szabad egymással összehasonlítani.

Az adatok azonban az említett fenntartások és korlátozások ellenére is rendkívül tanulságosak; segítenek bemutatni a kiberbűnözés terjedését, megismerni a különböző kiberbűncselekmények megoszlását, gyakoriságát, valamint feltárni azoknak az egyes országok társadalmára és gazdaságára gyakorolt hatását. A továbbiakban elsősorban a pénzügyi szektorra vonatkozó adatokat mutatjuk be, de – ahol a tendenciák szemléltetése indokolja – szélesebb körű adatokat is ismertetünk.

Most pedig következzen néhány további adat és jelzőszám a kiberbűnözésről:

- Adatsértések: 2021-ben a jogellenes adathozzáférésnek világszerte óránként átlagosan 97 áldozata volt. Egy-egy adatsértés 2024-ben átlagosan 4,88 millió dollárt kárt okozott.
- Kibertámadások: becslések szerint naponta közel 4000 új kibertámadás történik, és eddig 560 000 rosszindulatú programot – zsarolóvírust, vagy védelmet sértő programot – észleltek.
- A legnagyobb szervezeti (vállalati, intézményi) kiberkockázatot egyelőre a zsarolóprogramok jelentik, de jelentősen megnőtt a mesterséges intelligencia (artificial intelligence – AI) segítségével generált adathalász e-mailek száma.
- Kibertámadások célpontjai: eddig a feldolgozóipart érte a legtöbb kibertámadás, és számuk 2019 óta jelentős növekedést mutat. A kiberbűnözők azonban egyre gyakrabban veszik célba az olyan kulcsfontosságú ágazatokat is, mint például az egészségügy.
- A kiberbiztonsági piac növekedése: a globális kiberbiztonsági piac a 2023-as 190,4 milliárd dollárról 2028-ra várhatóan 298,5 milliárd dollárra nő.

2023-ban világszerte 3348 bejelentett kiberincidens történt a pénzügyi szektorban, szemben az előző évi 1829-cel. Ezen belül az elmúlt években nőtt az adatszivárgások száma, a 2021-es 690-ről 2023-ra 1115-re. Ezek a számok ugyan első pillantásra nem tűnnek magasnak, csakhogy a pénzügyi szektor vállalatainak, főleg a bankoknak számos ügyfele van, ezért a bankok feltört adatbázisai gyakran sok-sok ezer károsultat jelentenek. Mivel pedig a pénzintézetek a kibertámadások elsődleges célpontjai, a védekezést szolgáló befektetéseket folyamatosan növelni kell. Ezek becsült piaci értéke 2021-ben elérte a 38,7 milliárd dollárt, ám az előrejelzések szerint az évenkénti átlag 22,4%-os növekedési ütemmel 2029-ben várhatóan 195,5 milliárd dollárt tesz ki.

Országonkénti kiberbiztonsági rangsorok

Érthető módon az embereket, a vállalkozásokat és a kormányokat egyaránt az érdekli, vajon hol nagyobb a kiberbiztonság, s az e téren fennálló különbségeknek milyen konkrét okai vannak. A kiberbiztonság mérésére több mérőszámot is kidolgoztak. A továbbiakban a két legtöbbször idézettet mutatjuk be.

Az egyik a Nemzeti Kiberbiztonsági Index (National Cyber Security Index – NCSI). Ez egy olyan globális jelzőszám, amely 2018 óta évente mutatja be a világ országainak felkészültségét a kiberfenyegetések megelőzésére és a kiberincidensek kezelésére. Az indexet az e-Kormányzati Akadémia [e-Governance Academy (eGA)], egy 2002-ben Észtországban alapított olyan civil szervezet és alapítvány teszi közzé, amely kiválósági központként kívánja elősegíteni a társadalmak a digitális átalakulását. Az index kiszámítása egy nyilvánosan elérhető, ellenőrzött adatokat tartalmazó adatbázis segítségével történik. Az NCSI azt méri, hogy egy ország képes-e megelőzni a kiberfenyegetéseket és kezelni a kiberincidenseket. Az NCSI a kormányzat által megvalósított kiberbiztonság mérhető szempontjaira összpontosít:

1. Hatályos kibervédelmi jogszabályok – jogszabályok, irányelvek, szabványok stb.
2. Létrehozott kibervédelmi egységek – meglévő szervezetek, szervezeti egységek stb.
3. Ezek együttműködési formája – bizottságok, munkacsoportok stb.
4. Eredmények – irányelvek, gyakorlatok, technológiák, weboldalak, programok stb.

Az NCSI pontszám egy adott ország pontszámának százalékos arányát jelzi a mutató legmagasabb, 100 pontos értékéhez viszonyítva. A közzétett táblázatban az NCSI pontszám mellett a digitális fejlettségi szint (Digital Development Level – DDL) indexe is szerepel. A DDL-t az e-kormányzás fejlettségi mutatója (e-Government Digital Indicator – EGDI) és a hálózati készenlét mutatója (Networked Readiness Index – NRI) alapján számítják ki. A hálózati készenlét egy ország azon képességét jelzi, mennyire képes hasznosítani az információs és kommunikációs technológiákat (Information and Communication Technologies – ICT) a gazdasági és társadalmi fejlődés érdekében. Lényegében azt mutatja be, mennyire felkészült egy ország a digitális technológiák adta lehetőségek kiaknázására. A DDL azt az átlagos százalékos arányt mutatja, amelyet az ország elért mindkét index legmagasabb 100 pontos értékéhez viszonyítva. A különbség oszlop az NCSI pontszám és a DDL közötti összefüggést mutatja. A pozitív előjel azt jelzi, hogy az ország kiberbiztonsági fejlettsége azonos vagy magasabb a digitális fejlettségénél. A negatív előjel pedig azt mutatja, hogy az adott ország digitális társadalma fejlettebb, mint a kiberbiztonsági tere.

A tavalyi rangsort a *17. táblázat* mutatja be:

17. TÁBLÁZAT: National Cyber Security Index – NCSI 2024

	Ország	Nemzeti Kiberbiztonsági Index (NCIS)	Digitális fejlettség indexe (DDI)	Különbség		Ország	Nemzeti Kiberbiztonsági Index (NCIS)	Digitális fejlettség indexe (DDI)	Különbség
1	Csehország	98,33	72,93	25,40	33	Marokkó	70,00	57,17	12,83
2	Kanada	96,67	78,14	18,53	34	Tunézia	68,33	55,46	12,87
3	Finnország	93,33	85,76	7,57	35	Észak-Macedónia	66,67	58,31	8,36
4	Lengyelország	92,50	73,21	19,29					
5	Belgium	92,50	73,55	18,95	37	Grúzia	64,17	63,61	0,56
6	Olaszország	88,33	73,58	14,75	36	Montenegró	64,17	60,85	3,32
7	Észtország	88,33	82,56	5,77	38	Ghána	63,33	53,56	9,77
8	Ausztrália	87,50	82,60	4,90	39	Bahrein	60,83	72,73	–11,90
9	Albánia	85,00	62,34	22,66	41	Chile	60,00	70,84	–10,84
10	Litvánia	85,00	75,53	9,47	43	Kína	60,00	77,94	–17,94
11	Ausztria	85,00	78,35	6,65	40	Kirgizisztán	60,00	58,66	1,34
12	Szingapúr	85,00	86,93	–1,93	42	Uruguay	60,00	71,73	–11,73
13	Portugália	84,17	72,94	11,23	44	Benin	59,17	40,70	18,47
14	USA	84,17	85,46	–1,29	45	Szaúd-Arábia	59,17	77,39	–18,22
15	Koreai Köztársaság	83,33	85,82	–2,49	48	Argentína	58,33	67,36	-9,03
					47	Banglades	58,33	54,63	3,70
16	Horvátország	82,50	70,07	12,43	46	Nigéria	58,33	41,51	16,82
17	Moldova	81,67	62,66	19,01	49	Panama	55,83	59,30	–3,47
18	Hollandia	81,67	84,66	–2,99	51	Új-Zéland	55,00	79,24	–24,24
19	Szlovákia	80,83	67,55	13,28	50	Üzbegisztán	55,00	62,43	–7,43
20	Ukrajna	80,83	71,87	8,96	52	Togo	54,17	19,60	34,57
21	Lettország	79,17	73,10	6,07	53	Bhután	51,67	32,56	19,11
22	Írország	77,50	78,79	–1,29	54	Egyiptom	50,83	55,71	–4,88
23	Ciprus	76,67	71,44	5,23	55	Omán	50,00	69,64	–19,64
24	Egyesült Királyság	75,00	84,67	–9,67	56	Botswana	49,17	47,86	1,31
					57	Costa Rica	48,33	66,77	–18,44
26	Azerbajdzsán	73,33	61,08	12,25	58	Ruanda	47,50	50,58	–3,08
25	Jordánia	73,33	57,77	15,56	59	Jamaica	41,67	54,64	–12,97
27	Szerbia	72,50	70,05	2,45	60	Katar	40,83	69,88	–29,05
28	Svájc	72,50	81,88	–9,38	61	Mexikó	38,33	64,41	–26,08
29	Dominikai Köztársaság	71,67	57,70	13,97	62	Comoros	37,50	12,93	24,57
					63	Vanuatu	37,50	27,14	10,36
30	Brazília	71,67	69,62	2,05	64	Kuvait	37,50	63,71	–26,21
31	Törökország	71,67	70,89	0,78	65	Trinidad és Tobago	35,83	53,11	–17,28
32	Kazahsztán	70,83	70,31	0,52					

	Ország	Nemzeti Kiberbiztonsági Index (NCIS)	Digitális fejlettség indexe (DDI)	Különbség
66	Kiribati	33,33	22,86	10,47
67	Bosznia-Hercegovina	33,33	53,25	–19,92
68	Uganda	30,83	38,77	–7,94
69	Sierra Leone	30,00	26,93	3,07
70	Mozambik	30,00	27,56	2,44
71	Bahamák	30,00	35,72	–5,72
72	Honduras	23,33	42,48	–19,15
73	Líbia	21,67	27,33	–5,66
74	Suriname	21,67	31,83	–10,16
75	Mianmar	21,67	50,01	–28,34
76	Nicaragua	20,83	40,83	–20,00
77	Libanon	20,83	54,49	–33,66
78	Tonga	20,00	25,82	–5,82
79	Mauritánia	19,17	31,04	–11,87
80	Guatemala	19,17	46,95	–27,78
81	Antigua és Barbuda	18,33	30,72	–12,39
82	Zimbabwe	18,33	37,57	–19,24
83	Angola	17,50	33,37	–15,87
84	Tádzsikisztán	15,83	28,03	–12,20
85	Türkmenisztán	14,17	23,79	–9,62
86	Nauru	13,33	22,27	–8,94
87	Saint Kitts és Nevis	12,50	31,53	–19,03
88	Mali	11,67	30,44	–18,77
89	Irak	10,00	22,86	–12,86
90	Saint Lucia	8,33	26,28	–17,95
91	Mikronézia	5,83	16,18	–10,35
92	Haiti	4,17	10,59	–6,42
93	Salamon szigetek	4,17	18,41	–14,24
	Koszovó*	40,00		
	Magyarország**	67,53	64,25	3,28

Forrás: https://ncsi.ega.ee/ncsi-index/
Megjegyzés: * Csak a Nemzeti Kiberbiztonsági Index értéke áll rendelkezésre, ** Magyarország adatai – adatközlés hiányában – nem szerepeltek a 2024. évi táblázatban, ezért „vonal alatt" a 2023. évi táblázat adatait tüntettük fel.

Az 2024. évi rangsorban Magyarország – adatközlés hiányában – nem szerepel, de a 2023. éviben igen. Minthogy azonban a két esztendő rangsorában nem következett be jelentős átrendeződés, továbbá, mert a vizsgált szempontok alapján Magyarországon sem történt 2023-hoz képest nagy változás, ezért hazánk a 2024. évi sorrendben bizonyára a 34.-35. helyre került volna. Ez a helyezés arra utal, hogy a kiberbiztonság terén még bőven akad teendő Magyarországon.

Az ENSZ szakosított szerve, a Nemzetközi Távközlési Unió (ITU) 2-3 évente ugyancsak készít és közzétesz egy rangsort – a Global Cybersecurity Index-et (GCI) – a tagországok kiberbiztonság iránti elkötelezettségéről. A GCI a következő öt – pillérnek nevezett – tényező alapján értékeli az országokat:

1. jogi,
2. technikai és
3. szervezeti intézkedések, valamint
4. képességfejlesztés és
5. együttműködés.

Bár a Nemzeti Kiberbiztonsági Index és GCI értékelési szempontjai meglehetősen hasonlóak, az egyes országok helyezése az eltérő módszertan és súlyozás alapján különbözik. Az ITU 2024. évi felmérése (Global, 2024) szerint például az élenjáró országok közé tartozott az Egyesült Államok, Kanada, Ausztrália és Malajzia, míg az NCSI rangsorának élén ezek közül csak Kanada és Ausztrália található. A teljesítményszintek alapján végzett csoportosítás terén azonban nincs lényeges különbség a két index között.

Hazánk az ITU által készített rangsor szerint sem tartozik az éllovasok közé: a T2-es, azaz a haladó országok csoportjában szerepel. Ennek az az oka, hogy míg jogi, műszaki és szervezeti szempontból magas pontokat kapott Magyarország, addig főleg a képességfejlesztés terén csupán a közepesnél valamivel jobbat. Ez konkrétan azt jelenti, hogy a közvéleményt tájékoztató kampányok, a kiberbiztonsági szakemberek minősítésére és akkreditálására szolgáló keretrendszerek, a kiberbiztonsággal kapcsolatos szakmai képzések, oktatási programok vagy tudományos tantervek terén le vagyunk maradva más országokhoz képest. Az ITU megítélése szerint ugyanis a kiberbiztonság kérdésével erős társadalmi-gazdasági és politikai vonatkozásai dacára a kiberbiztonság kérdésével nálunk eddig inkább csak technológiai szempontból foglalkoztak. A humán és az intézményi képességek fejlesztése azonban elengedhetetlen a társadalom ellenálló képességének erősítéséhez. Ebben a vonatkozásban szerencsére – különösen a pénzügyek terén – mostanában kedvező változások kezdődtek.

A kiberbűnözés globális jelenléte

2021-ben a világon az ázsiai szervezetek szenvedték el a legtöbb kibertámadást. A szervezetek elleni támadások százalékos aránya kontinensenként 2021-ben a következő volt:

- Ázsia (26%),
- Európa (24%),
- Észak-Amerika (23%),
- Közel-Kelet és Afrika (14%),
- Latin-Amerika (13%).

2020 és 2021 májusa között az ázsiai térségben a kiberbűnözés 168%-kal nőtt. Egyedül Japánban 2021 májusában 40%-kal nőtt a kibertámadások száma az év korábbi hónapjaihoz képest.

Ázsia magas kitettsége főleg abból adódik, hogy e kontinens lakossága a föld lakóinak mintegy 58%-át teszi ki, az ott előállított bruttó társadalmi termék folyó áron a világ GDP-jének közel 37%-át, vásárlóerő-paritáson pedig megközelítően 48%-át adja. A kiberbűnözés intenzitása és az említett két mutatószám közötti kapcsolat persze meglehetősen laza, hiszen az intenzitást egyéb tényezők is befolyásolják. Így például demográfiai jellemzők, a nyelvhasználat, továbbá a digitális fejlettség és a bűnüldözés eredményessége is hatással van arra, amilyen erőteljes a kiberbűnözés. A népsűrűségnek és az urbanizációnak, továbbá az angol nyelv használatának (minthogy a csalás és a megtévesztés leginkább nyelvi kommunikáció segítségével történik) bizonyára szerepe

van abban, hogy az internethasználók számához mérten az Egyesült Államokban és az Egyesült Királyságban jóval több áldozata van a kiberbűnözésnek, mint más országokban. A nagy népsűrűségű térségekben, azon belül különösen a megapoliszokban ugyanis a bűnözőknek könnyebb a bűnüldöző szervek elől elrejtőznie. Ugyanakkor például az Egyesült Államokkal szomszédos Kanadában, ahol – noha a népesség 87%-a beszél angolul – az alacsony népsűrűség és az urbanizáció kisebb foka is hozzájárulhatott ahhoz, hogy az áldozatok száma ezer főre vetítve mindössze a nyolcada volt az USA-belinek.

Kontinensenként a vállalkozásokat ért kibertámadások fajtáját illetően is eltéréseket láthatunk:

- Az Ázsiában tapasztalt elsődleges támadástípus a szerverekbe történő behatolás volt, a megfigyelt támadások 20%-ával. Ezt követte a zsarolóvírusok alkalmazásának 11%-os és az adatlopásoknak 10%-os aránya.
- Európában a zsarolóvírusok jelentették az elsődleges támadási típust, amely a kontinensen elkövetett támadások 26%-át tette ki. A szerverekbe történő behatolás (12%) és az adatlopás (10%) volt a következő leggyakoribb támadási típus.
- Észak-Amerikában az elsődleges támadástípus ugyancsak a zsarolóvírus volt, a támadások 30%-ával. Ezt követték az üzleti e-mail szerverek feltörései (12%) és a szerverhozzáférési támadások (9%).
- A Közel-Keleten és Afrikában a fő megfigyelt támadástípus a szerverhozzáférés volt, ami a támadások 18%-át jelentette.
- Latin-Amerikában a fő támadási típus a zsarolóvírus volt, amely a támadások 29%-át adta. Ezt követte az üzleti e-mailek feltörése és a hitelesítő adatok ellopása (mindkettő a támadások 21%-ában fordult elő).

A kiberbűnözés regionális különbségeit mutatja egy másik megközelítésben a következő táblázat:

18. TÁBLÁZAT: Főbb kiberbűnözői csoportok és elsődleges működési módszereik/kapcsolataik

Csoport neve	Elsődleges eredet / kapcsolat	Főbb Működési Módszerek	Főbb jellemzők	Pénzügyi hatás / méret (ahol elérhető)
Délkelet-ázsiai szindikátusok	Délkelet-Ázsia (Kambodzsa, Mianmar, Laosz, Fülöp-szigetek, Thaiföld)	„Disznóvágás” (Pig Butchering) csalások, befektetési csalások, romantikus csalások	Emberkereskedelem és kényszermunka „csalási központokban” ipari méretű, MI-t használnak, globálisan terjeszkednek (Dél-Amerika, Európa)	Áldozatok vesztesége 18-37 milliárd USD (Délkelet-Ázsia, 2023)
Lazarus Group	Észak-Korea	Kriptovaluta-lopások, banki betörések, zsarolóprogramok	Államilag támogatott, a rezsim bevételeit generálja, kifinomult taktikák	1,34 milliárd USD ellopott kriptovaluta (2024), >6 milliárd USD kriptovaluta (2017 óta)

Black Axe (Neo Black Movement of Africa)	Nigéria	Üzleti e-mail feltörése (BEC), romantikus csalások, előrefizetési csalások, adócsalások	Multinacionális szervezett bűnözői csoport, globális sejtekkel, pénzmosó öszvéreket használ	Évi 300-500 millió USD (BEC csalások Észak-Amerikában)
FIN7 (Carbanak Group)	Oroszország / Ukrajna	POS rosszindulatú programok, banki rosszindulatú programok	Pénzügyi motivációjú, hosszú múltra tekint vissza	>100 millió USD (Evil Corp.)
LockBit	Független / RaaS	Zsarolóprogramok, kettős zsarolás	Domináns RaaS szolgáltató (25%-os piaci részesedés 2023-ban), ipari méretű működés	>120 millió USD (LockBit, 2023)
ALPHV / BlackCat	Független / RaaS	Zsarolóprogramok, agresszív zsarolási taktikák	Kifinomult RaaS csoport (8,5%-os piaci részesedés 2023-ban)	N/A
Cosmic Lynx	Oroszország	BEC kampányok (kettős személyazonosság-hamisítás)	Multinacionális vállalatokat céloz	N/A
Evil Corp	Oroszország	Banki rosszindulatú programok (Jabber Zeus, Dridex)	Hírhedt orosz szindikátus	>100 millió USD
Scattered Spider	Független / RaaS	Adathalászat (smishing, vishing, AiTM), SÍM-csere	Pénzügyi szektort céloz	N/A
Ransom Hub	Független / RaaS	Zsarolóprogramok, sebezhetőségek kihasználása, adathalászat	Pénzügyi szektor áldozatainak 8,6%-a (2023 július-2024 szeptember)	N/A
Orosz maffia (pl. örmény szervezett bűnözés)	Oroszország/Örményország	Banki csalás, átutalási csalás, árufuvarozási lopás	Hagyományos bűnözői szindikátusok szervezik a kiberbűnözési piacot	>83 millió USD (Amazon árufuvarozási lopás)

Forrás: Frész Ferenc substack blogja

Az említett módszerek mellett a vállalkozásokkal és egyéb szervezetekkel szemben alkalmazott egyik legelterjedtebb, az üzletmenetet romboló veszélyforrás a túlterheléses – szakzsargonban a Distributed Denial of Service (DdoS), azaz az elosztott szolgáltatásmegtagadással járó – támadás. Ez a támadási módszer általában zsarolással társul: ha a megtámadott vállalkozás nem fizet, akkor előfordulhat, hogy másodpercenként akár 500 Gbps forgalommal, több mint 200 ezer forrásból küldött adatcsomaggal próbálják megbénítani a támadók a célba vett intézmények vagy szolgáltatók rendszereit, amelyek ezért képtelenek fogadni vagy feldolgozni az ügyfelek által indított tranzakciókat.

Ugyancsak elterjedtek az online fizetési csalások: az előrejelzések szerint ezek 2023 és 2027 között 343 milliárd dollárjába kerülnek a vállalkozásoknak.

Az Egyesült Államok számítógépes bűnözési statisztikái

Becslések szerint 2022 első felében 53,35 millió amerikai állampolgárt érintett valamilyen módon a kiberbűnözés. Ezzel az Egyesült Államok volt a kibertámadásoknak leginkább kitett ország: a világszerte regisztrált támadások 46%-át szenvedte el.

Az FBI internetes bűnügyekkel foglalkozó panaszirodájához, az Internet Crime Complaint Centerhez (IC3) 2024-ben mintegy 860 ezer bejelentés érkezett, a bejelentett károk összege pedig 16,6 milliárd dollárt tett ki, ami 33%-kal haladta meg az előző évi kár összegét. A bejelentett károk nagy részét a csalások okozták, és ismét a zsarolóvírusok jelentették a kritikus infrastruktúrát sújtó legelterjedtebb fenyegetési formát. Csoportként a 60 év felettiek szenvedték el a legtöbb veszteséget, és ők tették a legtöbb panaszt is.

A veszteségek növekedése azért volt különösen aggasztó, mert az előző évben az FBI jelentős lépéseket tett annak érdekében, hogy megnehezítse és költségesebbé tegye a rosszindulatú szereplők garázdálkodását. Komoly csapást mértek a LockBitre, a világ egyik legaktívabb zsarolóvírust terjesztő csoportjára. 2022 óta pedig az FBI már több ezer visszafejtési kulcsot ajánlott fel a zsarolóvírusok áldozatainak, ami lehetővé tette, hogy több mint 800 millió dolláros összegben mentesülhessenek a zsarolási pénz kifizetésétől.

Az FBI-nak 2024 folyamán tett bejelentések számát és a bejelentett károk összegét a *19. táblázat* mutatja be. Az áldozatok korát tekintve 23%-uk volt 60 év feletti – ez magasabb részarány, mint e korcsoportnak a népesség egészében való részesedése –, ugyanakkor ők szenvedték el a károk közel 42%-át.

19. TÁBLÁZAT: Az FBI-IC3-nál bejelentett kiberbűncselekmények

Bűnelkövetés módja	Panaszok száma	Megoszlás	Kár (USD)	Megoszlás
Adathalászat/ adathamisítás	193 407	30,29%	70 013 036	0,44%
Zsarolás	86 415	13,53%	143 185 736	0,89%
Személyes adatok eltulajdonítása	64 882	10,16%	1 453 296 303	9,03%
Nem fizetés / nem kézbesítés	49 572	7,76%	785 436 888	4,88%
Befektetési csalás	47 919	7,50%	6 570 639 864	40,84%
Technikai támogatás	36 002	5,64%	1 464 755 976	9,10%
Üzleti e-mail feltörése	21 442	3,36%	2 770 151 146	17,22%
Személyazonosság-lopás	21 403	3,35%	174 354 745	1,08%
Foglalkoztatási csalás	20 044	3,14%	264 223 271	1,64%
Bizalommal visszaélés/romantika	17 910	2,80%	672 009 052	4,18%
Kormányzati megszemélyesítés	17 367	2,72%	405 624 084	2,52%
Hitelkártya /csekkcsalás	12 876	2,02%	199 889 841	1,24%
Zaklatás/ követés	11 672	1,83%	10 611 223	0,07%
Ingatlan	9 359	1,47%	173 586 820	1,08%
Előleggel kapcsolatos csalás	7 097	1,11%	102 074 512	0,63%
Gyermekek elleni bűncselekmények	4 472	0,70%	519 424	0,00%
Szerencsejáték/ sorsolás/ öröklés	3 690	0,58%	102 212 250	0,64%
Adatszivárgás	3 204	0,50%	364 855 818	2,27%
Zsarolóvírus	3 156	0,49%	12 473 156	0,08%
Túlfizetés	2 705	0,42%	21 452 521	0,13%
SzT*/Szerzői jog és hamisítás	1 583	0,25%	8 715 512	0,05%
Erőszakkal való fenyegetés	1 360	0,21%	1 842 186	0,01%
SIM csere	982	0,15%	25 983 946	0,16%
Robothálózat	587	0,09%	8 860 202	0,06%
Rosszindulatú szoftver	441	0,07%	1 365 945	0,01%
Egyéb			280 278 325	1,74%
Összesen	**638 565**	**100,00%**	**16 088 411 782**	**100,00%**
Leíró Kriptovaluta**	**149 686**	**23,44%**	**9 322 335 911**	**57,94%**

Megjegyzések: *SzT: Szellemi tulajdonjogok, ** Ez a leíró arra a médiumra vagy eszközre vonatkozik, amelyet a bűncselekmény elkövetése során használnak, és amit az IC3 csak nyomkövetés céljára használ. Csak a bűncselekmény típusának kiválasztása után használható leíróként.
Forrás: FBI-IC3: Internet Crime Report 2024, 2025. 05. 12

Az egyes bűncselekményfélékre vonatkozó adatokat szemügyre véve tanulságos, hogy a bejelentések 30%-a adathalászat és adathamisítás miatt futott be, ugyanakkor az okozott károknak alig fél százaléka volt ezeknek betudható. Ezzel szemben a kárérték döntő része – közel 41%-a – befektetési csalásokból származott, miközben ezek az esetek a beérkezett panaszoknak mindössze 7,5%-át tették ki. Ezekből az adatokból egyebek között akár az a következtetés is levonható, hogy a bűnüldözési kapacitások korlátozott volta miatt az erőforrásokat a fajlagosan nagy kárt okozó bűncselekményekre indokolt összpontosítani, míg a csekélyebb károk tekintetében erőteljesebben kell fókuszálni a megelőzést szolgáló képzésre és a felvilágosító munkára.

Figyelemre méltó az is, hogy az IC3-hoz befutott panaszok közel negyedénél, az elkövetési értéknek pedig háromötödénél kérték, illetve követelték a bűnözők kriptovalutában az áldozatoktól a pénzt. Ennek a magyarázata abban rejlik, hogy a kriptovalutában teljesített átutalások, illetve az abban tárolt pénzkészlet a blokklánc technológia sajátosságai miatt csak nehezen követhetők nyomon.

A vállalkozások számára a zsarolóvírusok jelentik a legnagyobb biztonsági fenyegetést, a sikeres zsarolóvírus-támadások ugyanis az amerikai szervezetek 60%-ának adatait tették átmenetileg elérhetetlenné. Az ilyen támadások orvoslásának költsége 2021-ben átlagosan 1,08 millió dollár volt.

Védettek-e az amerikai szervezetek a kiberfenyegetésekkel szemben?

Az amerikai kkv-k jelentős hányada nincs megfelelően védve a kiberfenyegetésekkel szemben. Egyfelől az általuk használt számítástechnikai eszközök védettsége meglehetősen gyenge és korszerűtlen, másfelől a költségviselő-képesség korlátozott volta miatt többségük nem rendelkezik kellően felkészült és tapasztalt IT szakemberekkel.

Az amerikai szervezetek mindössze 60%-a bír teljes körű kiberbiztosítással. További 28%-uk ugyan rendelkezik valamilyen korlátozott kiberbiztosítással, azonban ezek sok esetben nem nyújtanak fedezetet bizonyos támadástípusok vagy kizárt kockázatok következményeire. A legnagyobb problémát az jelenti, hogy a szervezetek több mint egytizede egyáltalán nem rendelkezik kiberbiztosítással, így egy sikeres kibertámadás nagy valószínűséggel a pénzügyi összeomlásukat okozza. A kiberbiztosítás szerepéről a „Mit tehetnek a vállalatok a kibervédelmük sikeres és költséghatékony megszervezése érdekében?" című fejezetben szólunk részletesebben.

Kiberbűnözés Európában

Az Europol, az Európai Unió bűnüldözési együttműködési ügynöksége, melynek célja a tagállamok közötti rendőrségi együttműködés fokozása a bűnözés elleni küzdelemben, különösen a súlyos nemzetközi és szervezett bűnözés, a kiberbűnözés és a terrorizmus területén, rendszeresen készít beszámolót az internetes szervezett bűnözés fenyegetettségéről. Az Europol legutóbbi értékelése (Internet Organised Crime Threat Assessment – IOCT) szerint 2023-ban továbbra is a zsarolóprogramok támadásai, a gyermekek szexuális kizsákmányolása (CSE) és az online csalások voltak a kiberbűnözés legveszélyesebb megnyilvánulásai az Európai Unióban. A kiberbűnözők köre továbbra is változatos maradt, széles körű szakértelemmel és képességekkel rendelkező magányos szereplőket és bűnözői hálózatokat egyaránt magában foglalva. Az EU-t célzó kiberbűnözők egy része az EU-n belül tevékenykedett, míg mások inkább külföldről támadtak.

A digitális rendszerek védelmét célzó szabályozási keretek folyamatosan igazodnak a változó környezethez és bűnügyi praktikákhoz, ám a kibervédelem terén továbbra is az emberi tényező a leggyengébb láncszem. A többrétegű zsarolási modellek egyre gyakoribbak a kiberbűnözéssel kapcsolatos fenyegetések teljes spektrumában.

A mesterséges intelligencia (AI) alapú technológiák még veszedelmesebbé teszik a social engineeringet, vagyis az olyan pszichológiai manipulációt, amivel a kiszemelt áldozatokat érzékeny adatok átadására kívánják rábírni. Kialakult a bűnözési szolgáltatások (Crime-as-a-Service – CaaS) piaca, amely megszervezi és működteti az ellopott adatokkal történő kereskedést. Ennek a piacnak fontos eszközévé válik a nagy nyelvi modellek (Large Language Models – LLM-ek) rosszindulatú felhasználása. A bűnözők által használt sötét vagy láthatatlan weben már kínálnak olyan szolgáltatásokat, amelyek segíthetik az online csalókat a támadásra bevethető utasítássorozatok fejlesztésében vagy adathalász e-mailek létrehozásában. A mélyhamisítások (deep fake) használata további aggodalomra ad okot, mivel erőteljesen kiegészíti a kiberbűnözők eszköztárát.

Az Eurostat szerint 2023-ban minden ötödik uniós vállalkozás (21,54%) tapasztalt IKT-val kapcsolatos olyan biztonsági incidenst, amelynek következtében elérhetetlenné váltak az IKT-szolgáltatások, zárolt adatok semmisültek meg, vagy bizalmas adatok kerültek illetéktelenek birtokába. Ezeket a biztonsági incidenseket a vállalaton kívülről vagy belülről érkező rosszindulatú támadások egyaránt okozhatják, de bekövetkezhetnek például hardver vagy szoftver meghibásodásából, vagy az alkalmazottak nem szándékos tevékenysége miatt is. 2023-ban a vállalkozások gyakrabban számoltak be arról, hogy IKT-szolgáltatásaikat vagy adataikat nem szándékos rosszindulatú incidensek károsították. Az IKT biztonsági incidensek által okozott, leggyakrabban jelentett következmény az IKT-szolgáltatások hardver- vagy szoftverhiba miatti elérhetetlenné válása volt (a vállalkozások 18%-a). Összehasonlításképpen: az IKT-szolgáltatások külső támadások (például zsarolóvírus általi támadások, vagy szolgáltatásmegtagadási támadások) miatti elérhetetlenségét a vállalkozások 3%-a jelentette. Hardver- vagy szoftverhiba miatti adatmegsemmisülésről vagy megsérülésről a vállalkozások 4%-a számolt be. Összehasonlításképpen, a rosszindulatú szoftverekkel való fertőzés vagy az illetéktelen behatolás a vállalkozások 2%-ánál vezetett az adatok megsemmisüléséhez vagy megsérüléséhez. A leggyakrabban a vállalkozások behatolás, adathalász vagy pharming[9] támadás, illetve alkalmazottaik szándékos cselekedete (2%) vagy nem szándékos tevékenysége (1%) miatt számoltak be a vállalkozások bizalmas adatok nyilvánosságra hozataláról.

A kiberbűnözők az európai pénzügyi szektort többnyire adatlopással támadják. Az elkövetők egy zsarolási kampány részeként leginkább az ellopott adatok kiszivárogtatásával fenyegetik meg az áldozattá vált pénzintézetet. Ezzel a pénzintézetet tárgyalások megkezdésére ösztönzik, hogy elkerüljék jó hírnevük sérelmét vagy a szabályozási szankciókat. A támadók az ellopott adatokat ezenkívül további adatlopáshoz használhatják fel, például célzott adathalász kampányok révén. Adatlopással támadják egyre gyakrabban az egészségügyi ágazatot is, hogy hallgatási pénzt zsarolhassanak ki (Zettl-Schabath et al., 2024).

Számítógépes bűnözés a szovjet utódállamokban

Oroszországnak és több más szovjet utódállamnak a kiberbűnözéssel kapcsolatos álláspontja meglehetősen kétértelmű és összetett. Ezt támasztja alá az a tény is, hogy Oroszország és néhány más utódállam sem csatlakozott az Európa Tanács Budapesti Egyezményéhez; miközben 193 ország csatlakozott. (Erről az egyezményről bővebben a „Nemzetközi jogi és statisztikai együttműködés" c. fejezetben szólunk.) A rendelkezésre álló információk szerint az utódállamok kormányai bár határozottan fellépnek a kiberbűnözés ellen, és erős eltökéltséget mutatnak a kriptovaluták szabályozására (amelyeket a kiberbűnözők előszeretettel használnak a pénzmosás elleni szigorú

9 A pharming az adathalászathoz hasonló olyan visszaélés, mely egy csalárd módon felépített weboldalt használ az adatok megszerzésére úgy, hogy valamilyen rosszindulatú szoftver vagy kémszoftver segítségével az eredeti oldalról egy másik, hamisított weboldalra téríti el a felhasználót.

szabályok kijátszására), mégis számos jel utal arra, hogy egyes hackercsoportokkal párhuzamosan félhivatalos kapcsolatokat ápolnak, hogy elérjék saját stratégiai céljaikat a kibertérben.

Oroszországban a rendelkezésre álló adatok szerint az elmúlt években a pénzügyi számítógépes bűnözés meglehetősen elterjedt. Oroszországban csak 2022 első negyedévében 42,92 millió adatsértés történt. Bár ez a szám 2022 második negyedévében jelentősen csökkent, ám egyértelmű, hogy a kiberbűnözés komoly fenyegetést jelent Oroszországban. Évente átlagosan több mint 249 000 digitális csalás történik. Egyetlen nap alatt 8 milliárdnál is több adathalász e-mailt küldtek orosz címekről.

Az Oroszországban működő hackercsoportok pontos számát nehéz megállapítani, mert azok gyakran válnak szét, majd sokszor újra egyesülnek. Rosszindulatú műveletek lebonyolítása érdekében az oroszországi kiberbűnözői közösség online platformokat használ „szolgáltatásaik" és „termékeik" népszerűsítésére vagy akár értékesítésére. Az oroszországi kiberbűnözői csoportok az „önkéntesség elvén" működnek együtt. A bűnözői csoport típusától és kiterjedtségétől függően az egyes csoportok vezetői vagy „személyzetet" alkalmaznak, vagy szabadúszókat foglalkoztatnak, pontosabban dolgoztatnak egyes feladatok elvégzésében. Ezekben a csoportokban nélkülözhetetlen szereplők az úgynevezett „teherhordó öszvérek", akiket azért fizetnek meg, hogy az ellopott pénzt a bűnözők számláira továbbítsák. A bűnözői csoportok három nagyobb kategóriába sorolhatók: államilag támogatott szereplők, nem állami csoportok és egyéni elkövetők. Ezek közül a nagy, azon belül pedig az államilag támogatott csoportok a legveszélyesebbek és a legpusztítóbbak.

Oroszország az államilag támogatott és a földalatti kiberbűnözés jelentős kiinduló pontja, kifinomult kibertámadásokkal és virágzó kiberbűnözői ökoszisztémával. Ide tartoznak a kémkedésben, pénzügyi csalásban és a kritikus infrastruktúrák elleni kibertámadásokban részt vevő csoportok. A kiberbűnözés történetét bemutató fejezetben több olyan támadás is szerepel, amelyeket igazolhatóan Oroszországból, de legalábbis orosz „munkanyelvű" szervezetek követtek el. Az orosz kiberfenyegetés összetett, állami szereplőket, nem állami csoportokat és egyéneket egyaránt magába foglal, közöttük gyakran változó kapcsolatokkal és átfedésekkel. Oroszországban az állam a legfelső szintű kiberhatalom, amely felkészült támadó csoportokkal rendelkezik. A jelentős kiberbűnözői tevékenység nagyrészt az egykor erős, reál-orientált szovjet oktatási rendszerre, valamint a COCOM-korlátozások megkerülésére kiépített szovjet ipari kémkedésre vezethető vissza, emellett az IT-szakemberek számára kedvezőtlen gazdasági környezet és a kiberbűnözés alacsony büntetési tételei is hozzájárultak kialakulásához.

Bár világszerte minden régióban találhatók aktív kiberbűnözői csoportok, az Orosz Föderáció és néhány más posztszovjet ország az elmúlt években a számítógépes szervezett bűnözés központjaivá váltak. Az Oroszországban alapított, de 2019-ben Szingapúrba áttelepült Group-IB kiberbiztonsági vállalat becslése szerint az orosz ajkú bűnözők bevétele 2011-ben elérte a 4,5 milliárd dollárt, míg a csak egyéni kiberbűnözőknek számító orosz állampolgárok bevétele 2,3 milliárd dollárra rúgott.

Az orosz ajkú kiberbűnözési üzletágnak a világgazdaság stagnálása ellenére növekvő gazdasági sikerei jól demonstrálják az elmúlt néhány év evolúciós tendenciáját. A korábbi évek kaotikus kiberbűnözési piaca helyett napjainkra egy jól szervezett struktúra alakult ki olyan bűnözői csoportokkal, amelyek tevékenysége a nyugati nagyvállalatok működését követi és világos célokkal is rendelkezik (Paganini, 2012). A posztszovjet térségben kialakult kiberbűnözés potenciálisan veszélyes következményekkel járhat a jövőben, mivel támadásaik egyre kifinomultabbá válnak.

A világ legveszélyesebb rosszindulatú szoftverei legalább egyharmadának származási helyeként Oroszországot azonosították. Szakértők szerint a rosszindulatú programok fejlett típusai tekintetében Oroszország az élen jár. Hasonlóképpen Vitalij Kamluk orosz kiberelemző szerint „ha a rosszindulatú támadások mennyiségét nézzük, akkor Kína, Latin-Amerika és Kelet-Európa járnak az élen. Minőségi szempontból azonban minden bizonnyal Oroszország a vezető" (De Carbonnel, 2013). Troels Oerting, az Europol Kiberbűnözés Elleni Európai Központjának (EC3) vezetője ugyancsak megerősítette az orosz ajkú számítógépes bűnözés elterjedtségét, amikor kijelentette, hogy az Europol által feltárt támadások jelentős hányadának Oroszország a kiinduló pontja.

Kiberbűnözés Magyarországon

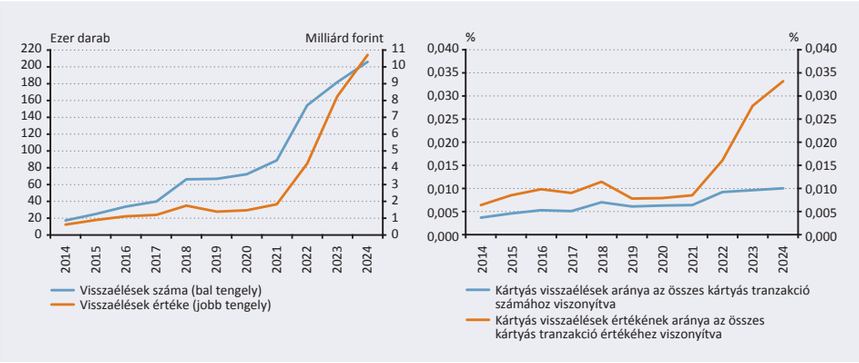
A kibercsalások száma szerte a világban emelkedik, ám a növekedés üteme Magyarországon az elmúlt néhány évben az átlagosnál magasabb volt, főleg a koronavírus járvány következtében felgyorsult digitalizáció következtében. Emiatt a csalárd ügyletek aránya a jelenlegi teljes bankkártyás forgalom 0,03-0,04 százalékát teszi ki – azaz 1 millió forintnyi bankkártyás forgalomból 300-400 forint – ami az európai középmezőnybe helyezi hazánkat.

A Magyar Nemzeti Bank szerint 2024-ben több mint 226 ezer bankkártyás és átutalást érintő visszaélés történt Magyarországon 41,9 milliárd forint értékben; ebből 31 milliárd a lakossági ügyfeleket érintő kár volt. Noha a legutóbbi adatok szerint az eddigi növekvő trend ugyan megtört, de a visszaélések száma és értéke az elért magas szinten stagnál.

A pénzügyi kibercsalások jellege az elmúlt évtizedben jelentősen megváltozott. Míg korábban a fizikai bankkártyák ellopása és lemásolása volt jellemző, ma már sokkal inkább az adathalászat, a pszichológiai manipuláció, a hamis befektetési ajánlatok és a webshopmásolatok dominálnak. Az öt leggyakoribb visszaélési forma közé tartozik a hamis befektetés, a hamis banki vagy webáruházi oldalak, a csomagküldős csalások, az „unokázós" módszer és a romantikus csalások.

Míg korábban a bankok viselték a kár nagy részét, addig napjainkban az átutalásos csalások esetében az ügyfelek több mint 98%-ban, kártyás csalásoknál pedig 72%-ban viselik a veszteségeket. Ennek oka leggyakrabban az ügyfél súlyos gondatlansága, ugyanis a csalások hátterében általában az ügyfelektől csalárd módon megszerzett személyes adatok állnak, és nem a banki rendszerek sérülékenysége. 2025 elején egy jól szervezett külföldi – vélelmezetten ukrán – bűnszervezet célzott kibertámadása nyomán magánszemélyek, egyesületek, kis- és középvállalkozások tucatjai estek áldozatul egy olyan megtévesztő és szisztematikus online csalássorozatnak, amelynek

7. ÁBRA: Visszaélések számának és az okozott kár értékének alakulása (bal oldali ábra), illetve ezek aránya a kártyakibocsátó bankok oldalán az összes fizetési kártyás forgalomhoz képest (jobb oldali ábra)



Forrás: (MNB, 2025a, p. 50.)

során akár egy-két rossz kattintás is elég volt ahhoz, hogy több millió forint tűnjön el a bankszámlákról. A csalók szinte az összes hazai bank ügyfeleit támadták, de többnyire a legnagyobb szolgáltatók ügyfeleivel tudtak visszaélni, mivel jó eséllyel minden negyedik ember ezeknek a bankoknak az ügyfele. A legutóbbi időszak csalássorozatában nagy szerepet játszottak az egyes külföldi bűnözői csoportok által a Google-keresőn meghirdetett hamis, ám megtévesztő banki oldalak. A kár bekövetkeztében ugyan a károsultak gondatlansága is közrejátszhatott, azonban egyre több esetben vetődött fel az is, hogy a bankok és a banki rendszerek sem reagáltak kellő gyorsasággal vagy érzékenységgel az ilyen típusú csalásokra. Az említett csalási módszerrel szemben ugyanis a bankok is fel tudnának lépni, elutasítva például a webkeresőkről indított bejelentkezéseket, vagy keresztazonosítási rendszerrel igazolhatnák az ügyfélnek, hogy valóban a számlavezető bankjának ügyintézőjével beszél. Ha ilyen üzenet nem jelenik meg a mobiltelefonján, akkor az ügyfél rögtön tudhatja, hogy a bank nevével visszaélve egy csaló hívta fel.

Az MNB a visszaélések számának növekedése és a pénzügyi rendszerbe vetett bizalom csökkenése miatt átfogó intézkedéscsomagot hirdetett meg „öt csapás” néven 2025 júniusában. A kormány pedig arról döntött, hogy a kiberbűncselekmények megfékezésére külön munkacsoport hoz létre.

Kiberbűnözés földrajzi koncentrációja

Mint a már bemutatott adatokból is egyértelműen kitűnt, a kiberbűnözés komoly kihívást jelent az egész világ számára, az általa okozott károk becsült költségei pedig ezer milliárd dolláros nagyságrendig is terjedhetnek. A növekvő fenyegetettség ellenére a kiberbűnözés meglehetősen láthatatlan, megfoghatatlan jelenség maradt. Bár a kiberbűnözési támadások földrajzi szempontból jól dokumentáltak, hiszen a támadások helyszínéről, azok áldozatairól, az alkalmazott módszerekről és az okozott károkról meglehetősen sok – igaz gyakran pontatlan – adat áll rendelkezésre, addig a támadók

tartózkodási helyéről és nemzetiségéről csak meglehetősen hiányos ismeretek vannak. A kibertérben végrehajtott támadások során ugyanis az elkövetők gyakran elfedik fizikai tartózkodási helyüket azáltal, hogy technikai védelem mögé bújnak és félrevezető online álneveket használnak. Ez azt jelenti, hogy a rendelkezésre álló technikai adatok többnyire nem alkalmasak az elkövetők személyének és tényleges tartózkodási helyének megállapítására. Emiatt a kiberbűnözés földrajzával kapcsolatos ismeretek is korlátozottak. Az oxfordi egyetem kutatói ezért 2021 márciusa és októbere között nagyszabású szakértői megkérdezést szerveztek. Ehhez a világ minden tájáról meghívták a számítástechnikai bűnözés elleni hírszerzés és nyomozás vezető szakértőit, hogy vegyenek részt a kiberbűnözők földrajzi elhelyezkedését vizsgáló anonimizált, online felmérésben. A felmérés készítői arra kérték a résztvevőket, hogy vegyék figyelembe a kiberbűnözés öt fő kategóriáját, nevezzék meg azokat az országokat, amelyekről úgy vélik, hogy a kiberbűnözés legjelentősebb központjai, majd rangsorolják ezeket az országokat az elkövetők hatása, professzionalizmusa és technikai felkészültsége alapján. A felmérés eredménye a World Cybercrime Index, a kiberbűnözés globális mérőszáma lett, amely a számítógépes bűnözés öt fő típusát öleli fel. Az eredmények azt mutatják, hogy viszonylag kevés országban összpontosulnak a legnagyobb kiberbűnözői fenyegetések. Az eredmények részben lerántják az anonimitás fátylát a kiberbűnök elkövetőiről a bűnüldözők és a politikai döntéshozók számára a kiberfenyegetések elleni hatékonyabb fellépés érdekében, továbbá hozzájárulhatnak a kiberbűnözés mint földrajzi jelenség jobb megértéséhez.

A helymeghatározás feladatát mindazonáltal megnehezíti az, hogy a kiberbűnöző nem feltétlenül odavalósi, ahonnan a kibertámadásait indítja. Így például egy román illetőségű elkövető egy az Egyesült Államokban található botnet révén irányíthatja a zombikat, amelyek spameket küldhetnek a világ országaiba, kínai adathalász oldalakra mutató linkekkel. A nemzeti határok tehát egyáltalán nem korlátozzák a kiberbűnözők hatókörét.

A kiberbűnözők gyakran proxy szolgáltatásokat is alkalmaznak IP-címeik elrejtésére, az országhatárokon átnyúló támadások végrehajtására, továbbá világszerte támaszkodnak bűnözési szolgáltatókkal (CaaS) való együttműködésre és a különböző országokban elérhető infrastruktúrára. A témával foglalkozó kutatók (Lusthaus, 2018) ezért arra a következtetésre jutottak, hogy a kiberbűnözés országokra lebontott indexének technikai adatok alapján történő összeállítására tett kísérletek hitelességi problémával küzdenek. Érvelésük szerint: „Ha ezek az adatok bárminek a mértékét is tükrözik, akkor az a kibertámadások intenzitásának földrajzi megoszlása, de nem az elkövetők származási helye és a támadások kiindulópontja.”

A nem technikai adatok jóval alkalmasabbnak tűnnek az eredet megállapítására. A bírósági jegyzőkönyvek, vádiratok és egyéb nyomozati anyagok többet mondanak az elkövetőkről, és részletesebb információkkal szolgálnak a tartózkodási helyükről. Ezek az adatok jól használhatók a mikroszintű elemzésekhez és az esettanulmányokhoz, azonban alapvető aggályok merülnek fel e kis minták reprezentativitása miatt. Először is, minden minta csak azokat az eseteket rögzíti, amelyek kapcsán a kiberbűnözőket büntetőeljárás alá tudták vonni, de nem tartalmaznak elegendő és megbízható információt

a szabadlábon maradt tettestársakról. Másodszor, az adatgyűjtés célja többnyire a számítógépes bűnözéssel kapcsolatos büntetőeljárások országonkénti számának megállapítása. Ebben az esetben az adatok tükrözhetik azt, mennyire veszik komolyan az egyes országok a számítógépes bűnözés elleni védekezést, vagy mekkora erőforrást szántak annak felderítésére; nem mutatják viszont az egyes országokon belüli kiberbűnözés tényleges szintjét. Emiatt a bűnügyi statisztika sem szolgál elegendő támponttal az elkövetők származásáról és működési helyéről.

A szakértői felmérés szervezői arra kérték a felkért résztvevőket, hogy vegyék figyelembe a számítógépes bűnözés öt fő jellegzetességét: (1) műszaki termékek /szolgáltatások; (2) támadások és zsarolás; (3) adat- és személyazonosság-lopás; (4) csalások; és (5) pénzbehajtás /pénzmosás; továbbá nevezzék meg azokat az országokat, amelyeket az egyes kiberbűnözési típusok legjelentősebb kiindulási helyének tartanak. A résztvevők ezután az egyes országokat az ott elkövetett bűncselekmények hatása (súlya), valamint az ott székhellyel rendelkező elkövetők professzionalizmusa és technikai készsége alapján értékelték. A szakértői válaszok felhasználásával a kutatók pontszámokat generáltak a számítógépes bűnözés minden típusára, amelyeket a kiberbűnözés országonkénti átfogó mérőszámába egyesítettek és így kapták meg a World Cybercrime Index-et (WCI), amelyet a *20. táblázat* mutat be.

20. TÁBLÁZAT: A kiberbűnözés világindexe: a 15 vezető ország

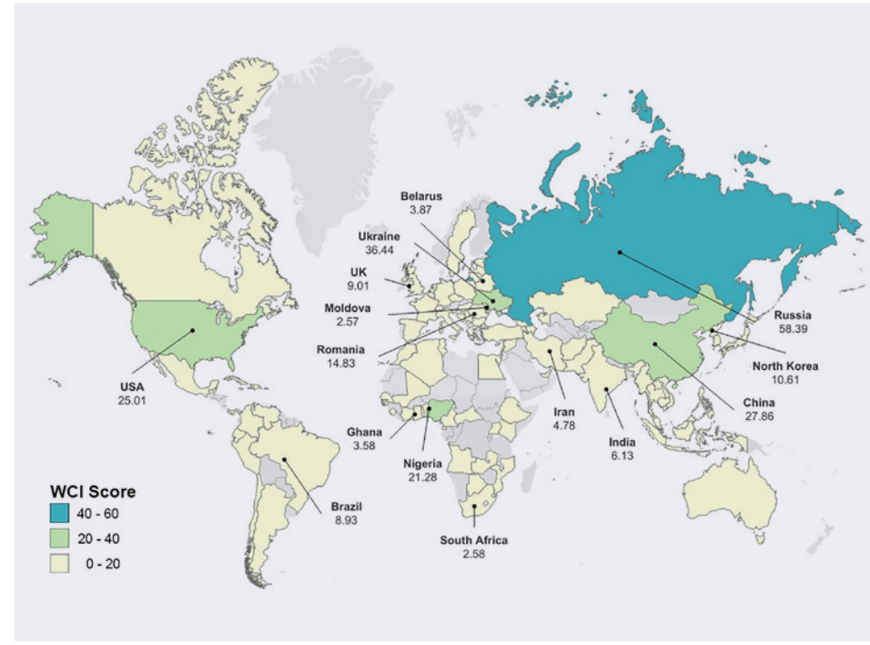
Sorrend	Ország	I	P	TS	WCI	tech	támadás	adat	csalás	készpénz
1	Oroszország	8,96	8,81	8,73	**58,39**	82,17	81,34	65,18	21,70	41,56
2	Ukrajna	8,37	8,29	8,24	**36,44**	52,97	50,76	36,01	11,20	31,27
3	Kína	8,22	7,70	7,81	**27,86**	40,22	24,24	34,89	15,83	24,13
4	USA	7,99	7,21	7,21	**25,01**	27,64	17,68	30,36	22,72	26,63
5	Nigéria	8,25	6,49	5,80	**21,28**	7,93	8,41	23,04	52,17	14,86
6	Románia	7,12	7,04	7,15	**14,83**	17,83	9,17	22,50	13,15	11,49
7	Észak-Korea	7,91	7,23	7,38	**10,61**	8,66	25,33	13,01	2,17	3,88
8	Egyesült Királyság	7,86	7,21	6,75	**9,01**	5,04	4,75	5,80	7,86	21,63
9	Brazília	6,90	6,35	6,32	**8,93**	13,70	8,77	10,29	7,28	4,64
10	India	7,90	6,60	6,65	**6,13**	4,46	3,62	6,81	12,75	3,01
11	Irán	6,88	6,45	6,64	**4,78**	8,62	10,00	3,59	0,94	0,72
12	Belarusz	6,84	7,20	7,32	**3,87**	11,92	5,58	1,85	–	–
13	Ghána	8,57	6,83	6,09	**3,58**	1,23	0,76	2,97	10,36	2,57
14	Dél-Afrika	6,95	5,35	5,50	**2,58**	1,20	0,65	0,58	7,17	3,30
15	Moldova	7,38	7,19	7,56	**2,57**	6,70	0,98	2,43	0,83	1,88

I = Hatás; P = Professzionalizmus; TS = Műszaki készség, Műszaki = Műszaki termékek/szolgáltatások, Támadások = Támadások és zsarolás, Adatok = Adat-/személyazonosság-lopás, Készpénz = Készpénzfelvétel és pénzmosás. I, P és TS 10-ből pontozódik. A „WCI Score" és az azt követő oszlopok 100-ból kerülnek pontozásra. Az egyes országok legjobb pontszáma az összes kiberbűnözési típusban sötétebb színű.
Forrás: https://doi.org/10.1371/journal.pone.0297312.t001

A táblázatból néhány fontos összefüggés derül ki. Először is, a számítógépes bűnözés nem általánosan elterjedt. Egyes országok a kiberbűnözés központjainak tekinthetők, míg mások nem játszanak különösebb szerepet a kiberbűnözés terén. Másodszor, a kiberbűnözés egyes központjai a számítógépes bűnözés bizonyos típusaira „szakosodtak". Ez azt jelenti, hogy annak ellenére, hogy néhány ország a kiberbűnözés központjának tekinthető, jelentős eltérések mutatkoznak közöttük mind a bűnelkövetési módok, mind pedig a hatás, a professzionalizmus és a technikai készségek terén. Harmadszor, az eredmények szerint a kiberbűnözés terén „élenjáró" országok listája hosszabb, mint amennyit általában a kiberbűnözés földrajzáról szóló publikációk felsorolnak.

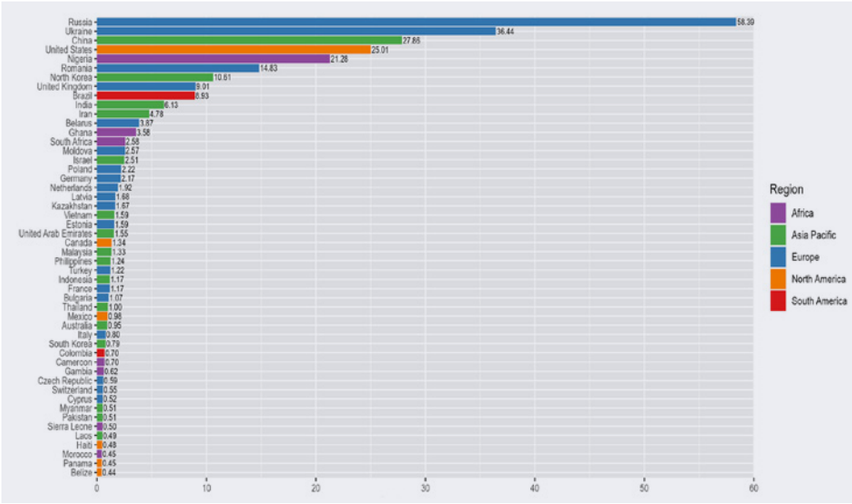
A központok specializációjának vizsgálatához a kutatók kiszámították a WCIoverall index első 15 országára vonatkozó „technikai felkészültség pontszámát" vagy „T-pontszámot". A számítógépes bűnözés minden típusához 2 és –2 közötti értéket rendeltek, hogy megjelöljék a technikai összetettség szintjét. A technikai termékek/szolgáltatások jelentik a technikailag legösszetettebb típust (2), ezt követi a támadások és zsarolás (1), az adat-/személyazonosság-lopás (0), a csalások (–1), végül a készpénzfelvétel és a pénzmosás (–2), amelynek a technikai összetettsége meglehetősen alacsony. Ezután megszorozták az egyes országok WCI-pontszámát az egyes kiberbűnözési típusokra vonatkozóan a hozzárendelt értékkel.

8. ÁBRA: Világtérkép a WCIoverall-index első 15 országáról Az OpenStreetMap és az OpenStreetMap Foundation alaptérképe és adatai



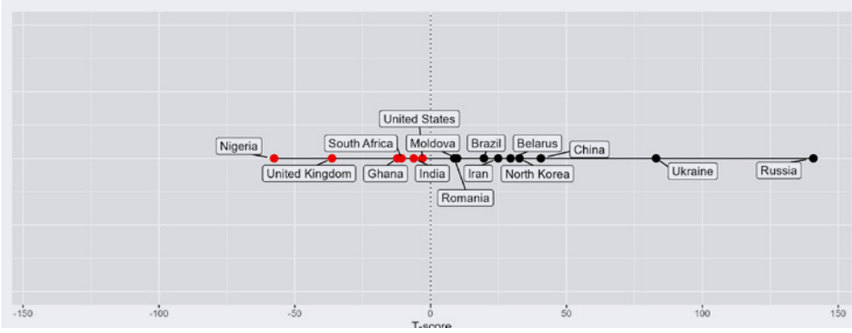
Forrás: https://doi.org/10.1371/journal.pone.0297312.g001

9. ÁBRA: Az 50 legjobb ország a WCI összesített pontszáma szerint



Forrás: https://doi.org/10.1371/journal.pone.0297312.g001

10. ÁBRA: Az első 15 WCI-ország technikai vagy T-pontszáma



Forrás: https://doi.org/10.1371/journal.pone.0297312.g001

A negatív értékek az alacsonyabb, a pozitív értékek pedig a magasabb technikai felkészültségnek felelnek meg.

A bűnszervezetek globális jelenléte

A nemzetközi bűnüldöző szervek – így az INTERPOL, az Europol, az FBI és több nagy elemzőház, mint a Palo Alto Networks és a Chainalysis – által közzétett adatok alapján az online banki csalások világszerte elterjedtek, de az elkövetők nem korlátozódnak egyetlen országra, térségre. E források szerint országonként, illetve térségenként a legnagyobb ismert bűnszervezetek, amelyek kiterjedt online csalási műveleteket működtettek az elmúlt években a következők:

- **Oroszország**: A REvil (Ransomware Evil) és a Conti (korábban Wizard Spider) olyan hírhedt kiberbűnöző csoportok, amelyek több milliárd dolláros károkat okoztak ransomware és banki trójai támadássorozattal.
- **Nyugat-Afrika (főként Nigéria):** A Black Axe, Airlords és más ún. „cultist" bűnbandák főként romantikus átverésekkel, adathalászattal és vállalati e-mailes csalásokkal (BEC) károsítanak meg áldozatokat világszerte.
- **Románia:** Több csoport, köztük a Florian Tudor által vezetett hírhedt szervezet Dél-Amerikában és Európában is kiterjedt ATM- klónozási és pénzmosási tevékenységet folytatott.
- **Ukrajna:** Ukrajnában is működnek kiberbűnöző hálózatok, amelyek jelentős károkat okoztak. A legismertebbek közé tartozik a Zeus és SpyEye banki trójaiak mögött álló fejlesztői közösség, amely főként az Egyesült Államok és Nyugat-Európa pénzügyi rendszereit célozta meg. Emellett 2022-ben egy olyan ukrán bűnszervezetet számoltak fel, amely több mint 400 hamis phishing weboldalt működtetett, több mint 3 millió dolláros kárt okozva. Az ukrán esetek volumene, földrajzi irányultsága és szervezettségi szintje elmarad az orosz, a nyugat-afrikai vagy a román hálózatokhoz képest. A nemzetközi bűnüldöző szervek nyilvántartásai alapján Ukrajna ugyan nem tartozik a legnagyobb kibercsalási gócpontok közé, de egyes „célországokban", így például Magyarországon annak számíthat.

Nemzetközi elfogatóparancsok alapján

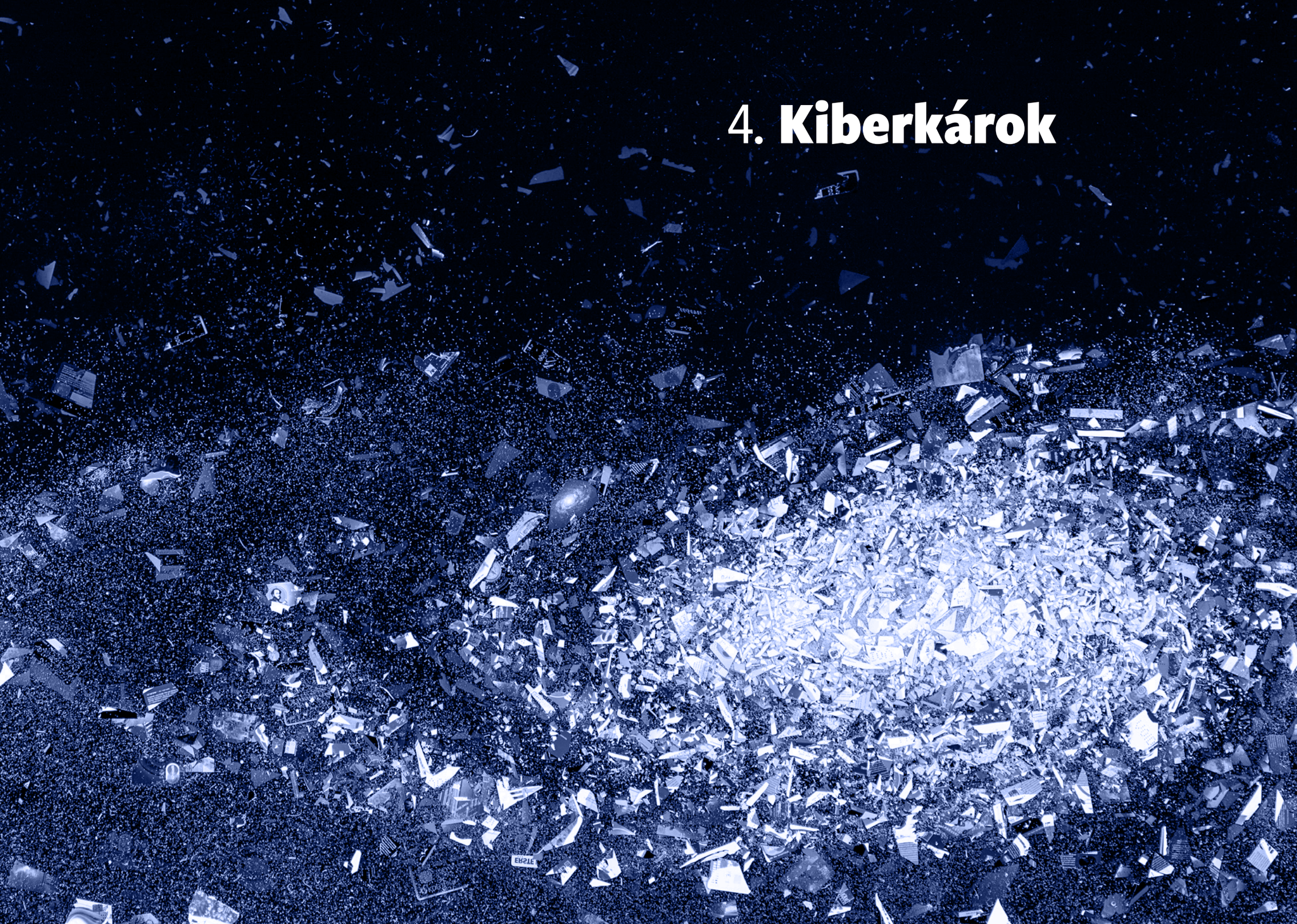
A 2024-2025 között kibocsátott több mint 500 nemzetközi elfogatóparancs alapján az online csalásokkal kapcsolatos körözések java része orosz, nigériai és román állampolgárokhoz köthető. Ezeket követték kisebb számban más kelet-európai és délkelet-ázsiai elkövetők.

Néhány példa a nemzetközi bűnüldözési szervek által elért eredményekre:

- A 2024-2025-ös időszakban a nemzetközi bűnüldöző szervek jelentős eredményeket értek el az online csalások elleni harcban. Az INTERPOL által koordinált Operation HAECHI V például több mint 5 500 letartóztatást eredményezett, és 400 millió dollár értékű vagyont foglaltak le (INTERPOL HAECHI V).
- Az Europol Operation Endgame nevű akciója több ezer káros domént semmisített meg, és számos elfogatóparancsot adott ki (Reuters: Europol Operation Endgame).
- Szintén 2024-ben, az Operation First Light keretében 61 ország közreműködésével közel 4 000 gyanúsítottat tartóztattak le, és több ezer bankszámlát zároltak csalások gyanúja miatt (INTERPOL Operation First Light).

Mind a WCI, mind a bűnüldöző szervek statisztikái szerint a legtöbb kiberbűnözőnek Oroszországban, Ukrajnában, Romániában és Kínában vannak a gyökerei, de számottevő az egyesült államokbeli és az egyesült királyságbeli kiberbűnözők száma is. Természetesen az egyes bűnözői csoportok „műveleti terepe" eltér, ezért az egyes országokban érzékelt/észlelt támadások kiindulási pontjai is eltérőek lehetnek.

4. Kiberkárok



Figyelemmel a pénzügyi szektornak a digitalizáció következtében végbemenő viharos ütemű átalakulására, egyre fontosabb, hogy megértsük a kiberincidensek gazdasági hatását a kibertér megfelelő védelme kialakításának és fenntartásának érdekében. A kiberincidensek – a hálózatok vagy a rendszerek szándékos, rosszindulatú megsértése által okozott működési fennakadások és veszteségek – komoly veszélyt jelentenek a társadalmak gazdasági és politikai struktúráira. A kötetnek ez a fejezete áttekintést kíván adni a számítógépes incidensekből származó költségekkel kapcsolatos eddigi kutatásokról, felvillantva a kiberincidensekhez kapcsolódó gazdasági költségek és potenciális kockázatok széles körét, különbséget téve a közvetlen költségek – a kézzelfogható, azonnali gazdasági veszteségek, például váltságdíjak –, és az olyan közvetett költségek között, mint például az áttételes és utóhatások.

A kiberbiztonságba történő befektetések mérlegelése során mind a köz-, mind a magánszektor számára komoly kihívást jelent a várható/elvárt nettó haszon becslésének nehézsége. A kiberbűncselekmények valószínűségének, valamint az általuk okozott károk potenciális értékének meghatározása ugyanis több, összetett tényező nehéz számszerűsíthetőségétől függ (Gordon et al., 2020). E fejezetnek egyik célja az eddigi költségbecslések bemutatása azért, hogy jobban meg lehessen érteni a kiberincidensekből eredő károk fajtáit, a veszteségbecsléshez használt módszereket, valamint a kiberbiztonsági incidensekre vonatkozóan elérhető adatforrásokat. Az eddigi tapasztalatokból ugyanis azt lehet leszűrni, hogy a kiberincidensek gazdasági költségeinek mélyebb megértése elengedhetetlen a hatékonyabb döntéshozatalhoz és a megfelelő védekezés kialakításához (CISA, 2020).

A Világbank munkatársai nemrégiben több mint 50 tudományos dolgozatot és különféle „sűrűn idézett” iparági jelentést dolgoztak fel, bemutatva, hogy a kiberincidensek közvetlen költségei az országok gazdasági teljesítményének akár jelentős hányadát is elérhetik, és hozzátéve, hogy a közvetett költségek ehhez hasonló nagyságrendet is kitehetnek. Különösen azért, mert a kiberincidensek kockázatot jelenthetnek az egyes államok makrogazdasági stabilitására, például rendszerszintű zavarokat okozhatnak a pénzügyi piacokon és jelentős veszteségeket okozhatnak a részvénypiacokon is (Cobos - Cakir, 2024).

Ennek a fejezetnek két fő célja van. Először is, rá kíván mutatni a megbízható adatok szűkösségére és a szabványosított kiberbiztonsági definíciók hiányára. Ez a két hiány jócskán megnehezíti a megbízható költségbecslések és hatékony védekezés kidolgozását, annál is inkább, mert a kiberbűnözést jelentős hányadban határokon át elkövetett bűncselekmények jellemzik. Ezért elengedhetetlen a fokozott nemzetközi együttműködés a kiberincidensek globális megfigyelése és az így nyert adatok egységes értelmezése érdekében. Másodszor, rá kíván mutatni a kormányok aktívabb szerepvállalásának fontosságára a kiberincidensekből és a kiberbiztonsági piac kudarcaiból eredő közvetett költségek megállapításában, hangsúlyozva azonban, hogy a kormányzati szerepvállalás növelése a kiberbiztonság terén nem csökkenti a gazdasági szereplők egyéni és közös felelősségét.

A kiberincidensek közvetlen költségei

A kiberincidensekkel kapcsolatos közvetlen költségek magukban foglalják az áldozatok által elszenvedett, kimutatható pénzügyi veszteségeket és károkat, valamint az ilyen események kapcsán felmerülő kiadásokat. E költségeknek a kiberbűnözők által jogellenesen szerzett pénzügyi haszon csupán egy részét teszi ki, mert a járulékos károk és veszteségek akár jóval magasabbak is lehetnek, mint a bűnözők zsákmánya.

A Világbank idevágó vizsgálatai tizenöt, 2017 és 2023 között közzétett kiemelkedő iparági jelentés adatait gyűjtötték össze, hogy világosabb képet lehessen alkotni a kiberbiztonsági incidenseknek tulajdonítható közvetlen költségekről. Fontos azonban felhívni a figyelmet egy jelentős korlátra: a felhasznált iparági jelentésekből gyakran hiányzik az átláthatóság az alkalmazott becslési módszerek és az adatforrások tekintetében, ami akadályozza pontosságuk alátámasztását.

A 21. táblázat a legtöbbször idézett iparági jelentésekben szereplő számítógépes incidensek éves globális költségeire vonatkozó összesített becslések széles skáláját mutatja be. Míg a kiberbiztonsági szakma gyakran idézi ezeket a számokat, az alkalmazott módszerek érvényessége nem értékelhető.

21. TÁBLÁZAT: Az összes kiberbiztonsági incidens éves globális költségére vonatkozó összesített becslések

Jelentés és a megjelenés éve	Módszertan	Korlátozás	Összesített globális éves költségbecslés (milliárd USD)	a globális GDP %-a
IC3 (2017) *	Nem elérhető	Az adatforrás az IC3-hoz érkezett panaszok, amelyek az Egyesült Államokban történt incidensek töredékét képezik.	1,42	0,00%
Norton (2017)	Online felmérés 21 539, 18 év feletti személy részvételével, 20 országban	Csak a fogyasztók veszteségeit rögzíti	172	0,21%
McAfee és CISS (2018)	Szakirodalomból összeállítja a közvetlen és közvetett veszteségbecsléseket számos országra vonatkozóan, és összesíti azokat egy nem elérhető módszertannal.	Az adatok mérési hibának vannak kitéve	522,5	0,60%
eSentire és kiberbiztonság Ventures (2019)	Nem elérhető	A becslések a kiberbűnözés történeti arányán alapulnak.	6000	6,90%
IC3 (2019) *	Nem elérhető	Az adatforrás az IC3-hoz érkezett panaszok, amelyek az Egyesült Államokban történt incidensek töredékét képezik.	2710	0,03%

IC3 (2020)*	Nem elérhető	Az adatforrás az IC3-hoz érkezett panaszok, amelyek az Egyesült Államokban történt incidensek töredékét képezik.	3500	0,04%
Európai Bizottság (2021)*	Nem elérhető	Az adatforrások nem állnak rendelkezésre.	6070	6,90%
eSentire és kiberbiztonság Ventures (2022)	Nem elérhető	A becslések a kiberbűnözés történeti arányán alapulnak.	8000	8,00%
eSentire és kiberbiztonság Ventures (2022)	Nem elérhető	A becslések a kiberbűnözés történeti arányán alapulnak.	10500	9,10%

Megjegyzés: Ezek az összesített becslések nem tesznek különbséget a kiberbiztonsági incidens súlyossága vagy típusa között. Az eredmények becslésére használt módszereket a fejezet szerzői nem validálták. *Összehasonlítás céljából hozzáadtuk az ugyanabból az időszakból származó, de nem feltétlenül az iparági érdekelt felektől származó jelentéseket. A globális nominális GDP (USD-ben) forrása az IMF.
Forrás: Szerzők összeállítása

A költségbecslések töredékessége ellenére ezek az iparági jelentések egyértelműen tanúsítják, hogy a kiberbűnözés által okozott költségek világszerte folyamatosan emelkednek, beleértve az adatlopásokat, a zsarolóvírus-támadásokat, valamint a nagyvállalatoknál és a kis– és középvállalkozásoknál tapasztalható biztonsági incidenseket. Az elkövetkező évekre vonatkozó iparági előrejelzések a kriptográfiai bűnözést és a zsarolóprogramok támadásait helyezik a leggyorsabban növekvő számítógépes incidensek élére; a globális költségbecslések szerint a károk 2025-ben elérik az évi 30 ezer milliárd USD-t, 2031-re pedig a 265 ezer milliárd USD-t.

A kiberincidensek közvetett költségei

A számítógépes incidensekből eredő közvetett költségeket nehéz számszerűsíteni, ráadásul sokszor figyelmen kívül is hagyják őket, jóllehet komoly, hosszú távú hatásuk lehet a gazdaságra (Campbell et al., 2003). A közvetett költségek ugyanis gyakran akár nagyobbak is lehetnek, mint a közvetlen költségek. Kibertámadást elszenvedő cégek esetében végzett felmérések (Kamiya et al., 2021) szerint a közvetlen költségek, mint például a vizsgálati és kárelhárítási költségek, a jogi szankciók és szabályozói szankciók nagyságrenddel kisebbek voltak, mint a részvényesek által elszenvedett teljes vagyonveszteség egy adatvédelmi incidens bejelentését követően.

Az Accenture multinacionális tanácsadó vállalat és az amerikai Ponemon Intézet 2019. évi becslése szerint a cégeknek azzal a kockázattal kellett szembesülnie, hogy 2024-ig a kibertámadások következtében mintegy 5,2 ezer milliárdnyi USD értékteremtési lehetőséget veszítettek el, ami majdnem megegyezik Franciaország, Olaszország és Spanyolország együttes GDP-jével.

Tőzsdei reakciók a kiberincidensekre és a hírnévre gyakorolt hatásokra

Számos eddigi kutatás irányult annak feltárására, hogy egy kibertámadás elszenvedésének bejelentése milyen hatással van az érintett cég tőzsdei értékére. Az évezredforduló táján végzett empirikus vizsgálatok még kevés bizonyítékot találtak arra vonatkozóan, hogy a sajtóban közzétett hírek komolyan befolyásolták volna a tőzsdére bevezetett amerikai vállalatok nyilvánosan kibocsátott értékpapírjainak árfolyamát; csupán a bizalmas adatokhoz való jogosulatlan hozzáféréssel járó jogsértések esetén észleltek jelentős hatásokat. Ezzel szemben a legutóbbi vizsgálatok a jogsértés bejelentésének nagy és jelentős káros tőzsdei hatásait állapították meg (pl. Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018; Piccotti - Wang, 2022).

A szakirodalom azt is feltárta, hogy egy-egy kiberincidens bejelentésére a támadás típusától függően meglehetősen eltérő tőzsdei reakciókat lehetett megfigyelni. Garg et al. (2003) úgy találták, hogy bár az IT-biztonsági incidensek mindegyik típusa árfolyamveszteséget okozott, a piac eddig leginkább a hitelkártya-információk ellopására (9-15%) és a DoS incidensekre (1-4%) reagált. Akey et al., (2021) vizsgálódásai pedig azt mutatták, hogy a cégek értéke jobban csökken az ügyfelek adatainak ellopása esetén, mintha az alkalmazottakét szerezték volna meg a támadók. Végül Piccotti és Wang (2022) kimutatta, hogy a négyféle jogsértés közül (i) hackelés vagy rosszindulatú programok, (ii) elveszett, kiselejtezett vagy ellopott papírdokumentumok, (iii) elveszett, kiselejtezett vagy ellopott adathordozók, és (iv) a hordozható eszközök feltörése útján elkövetett jogsértések mind jelentős negatív hatást gyakoroltak a tőzsdei hozamra.

Amellett, hogy árfolyamveszteségeket okoznak, a kibertámadások bejelentése a cég értékét azáltal is befolyásolhatja, hogy maradandóan csökkenti a márka (goodwill) értékét. Így például egy, a 2002 és 2018 közötti cégszintű adatok felhasználásával készült vizsgálat (Makridis, 2021) úgy találta, hogy a nagy adatszivárgások a pozitív cégérték (goodwill) 5-9%-os csökkenésével jártak. A részvényárfolyamok csökkenése a kibertámadások bejelentését követően a fogyasztók és a befektetők bizalmának jelentős visszaesését tükrözi a vállalat iránt.

Az ellátási lánc, a rendszerszintű kockázatok és a tovagyűrűző hatások

A kiberincidensek miatt a cégek nem csupán értékes információkat veszíthetnek el, hanem komoly hírnévromlást szenvedhetnek el és hatalmas jogi költségeket kell viselniük. A kibertámadások azonban az említetteken túlmenően rövid és hosszú távon egyaránt nehezíthetik a cég működését és csökkenthetik az árbevételét. A megtámadott cégek árbevételének összehasonlítása a hasonló, támadástól nem sújtott cégekével azt mutatta, hogy az értékesítés jelentősen visszaesett a támadást követő 3 évben. Más vizsgálatok pedig azt is kimutatták, hogy a kereslet visszaesése a támadás által közvetlenül érintett cégekről óhatatlanul átterjed a beszállítókra is, megsokszorozva ezzel a kezdeti profitcsökkenést.

A kiberincidensek fertőző hatásokkal is járhatnak, különösen a pénzügyi szektorban. Kotidis és Schreft (2022) egy többnapos kibertámadás hatását tanulmányozták egy amerikai technológiai szolgáltatóra (Technological Service Provider – TSP), és arra a következtetésre jutottak, hogy a kibertámadás rontotta a szolgáltató banki ügyfeleinek fizetőképességét is, ami miatt fennállt a veszélye annak is, hogy nem tudják maradéktalanul teljesíteni ügyfeleik fizetési megbízásait. Kamiya et al., (2021) azt is kimutatták, hogy egy támadás nyilvánosságra hozatala hátrányosan érinti az áldozattal azonos szektorban működő cégeket. Ez megerősítette a szerzők azon feltételezését, miszerint egy kibertámadás nyilvánosságra hozatala különösen akkor káros, ha megváltoztatja a befektetők megítélését az adott iparág kockázati kitettségéről. De más vizsgálódások is azt mutatták, hogy a vállalati szintű kockázat a pénzügyi piacokon rendszerkockázat forrása lehet. A szakirodalom a céget listázó tőzsdéken bizonyítékot talált a rendszerszintű fertőzésre az érintett cégek részvényárfolyamának az ingadozásán keresztül. Négy fertőző csatornát azonosítottak, amelyeken át a kiberkockázat cégek és piacok között hat: (i) technológiával kapcsolatos csatornák, (ii) korrelált kockázati csatornák, (iii) hálózati fertőzési csatornák és (iv) összetett működési környezetek.

A késedelmes bejelentésből eredő költségek

Tapasztalatok szerint a kiberincidensek bejelentése általában késedelemmel történik. Egy felmérés (IBM, 2021) szerint a kibertámadások észlelése és bejelentése között sokszor hetek is eltelnek. E késedelemnek persze vannak objektív okai, nevezetesen a kár és a következmények felmérése időbe telik, viszont a késedelem a bűntett közvetlen költségeinek felhalmozódásához is vezethet a jogsértés megszüntetéséig, sőt olyan közvetett veszteségeket is okozhat, amelyek a cég ügyfeleit és befektetőit is sújtják.

A cégek vezetése (az igazgatóság és a menedzsment) sokszor abban érdekelt, hogy stratégiailag aluljelentse az elszenvedett károkat, netán késleltesse a kiberincidens bejelentését (Amir et al., 2018). A kibertámadások késleltetett bejelentése és/vagy a károk alulbecslése ugyanis opportunista időablakokat teremt bennfentes kereskedésre. Kutatók (pl. Ashish Garg) bizonyítékot találtak arra, hogy a kiberincidensről tájékozott bennfentesek shortolták a cég papírjait. Más vizsgálatok (pl. Piccotti - Wang, 2022) pedig úgy találták, hogy a hackerek vagy zsarolóvírusok terjesztői sokszor már hónapokkal azelőtt belevágtak a bennfentes kereskedésbe, hogy megtámadják a kiszemelt áldozatot és az bejelentette a kiberincidenst. Az ilyenfajta bennfentes kereskedést nehéz leleplezni, ugyanakkor persze, ha a bűnözők nagyban próbálkoznak ezzel a lehetőséggel élni, akkor könnyen magukra terelik a gyanút.

Válaszköltségek

A reagálási költségek az incidens hatásainak kezelésével és mérséklésével kapcsolatos kiadások, amelyek a közvetlen védelmi intézkedésektől a széles körű közvetett költségekig terjednek, és tükrözik a kiberincidensek cégekre gyakorolt sokrétű következményeit. A kiberincidensek különféle válaszadási költségekkel járhatnak. Sok cég, amikor

egy kiberincidenssel szembesül, például egy incidenskezelő csapatot bíz meg a támadás kivizsgálásával és a károk enyhítésével. Ezek a speciális csoportok segítenek az igazságügyi vizsgálatok lefolytatásában, elemzik az érintett rendszereket és hálózatokat, hogy azonosítsák az incidens okát, továbbá bizonyítékokat gyűjtenek a lehetséges jogi lépésekhez. Ezeknek a költsége általában 30 000 és 150 000 USD között mozog. A kiberincidensek által érintett szervezeteknél felmerülhetnek a jogi és szabályozási kötelezettségekkel kapcsolatos költségek is. Az ilyen típusú válaszköltségek magukban foglalják a jogi tanácsadók igénybevételét, az adatvédelmi incidens bejelentési kötelezettségének való megfelelést, továbbá a meg nem felelés esetén kiszabható pénzbírságokat vagy szankciókat. Burgard (2021) becslése szerint az ügyvédi költségek legalább mintegy 25 000 USD-ba kerülnek, amely összeg persze exponenciálisan növekedhet, ha a cég pert indít, vagy a károsult ügyfelek indítanak pert a céggel szemben.

A szakirodalom szerint az áldozattá vált cégek többet tesznek annál, hogy csupán jogi lépéseket tegyenek válaszul a számítógépes incidensre; úgy alakítják viselkedésüket, hogy ellensúlyozzák a jó hírnevük károsodását. Felmérések azt mutatták, hogy a megtámadott cégek jelentősen megnövelték a vállalati társadalmi felelősségvállalásba eszközölt befektetéseiket, hogy mérsékeljék a reputációs veszteségüket. A vállalati társadalmi felelősségvállalásba és a vezetői változásokba való fokozott befektetés rávilágít a kiberincidensek súlyosságára és arra is, milyen mértékben készek és képesek a cégek ellensúlyozni ezek káros hatásait. Azt is tapasztalni, hogy az Egyesült Államokban egy nagyobb kiberincidenst követően mind az érintett cégek és beszállítóik, mind pedig a nem érintett, hasonló jellegű cégek hajlamosak megnövelni készpénzállományukat. Ez kollektív választ sugall a pénzügyi stabilitás megerősítésére a kiberkockázatokkal szemben.

Azok a cégek, amelyek adatszivárgással/lopással szembesültek, általában többet fektetnek be a kutatásba és fejlesztésbe (K+F) is, ami azt jelzi, hogy hosszú távú elkötelezettséget vállalnak biztonsági intézkedéseik javításán túl is. Főleg a megtámadott cégeknél nagyobb a valószínűsége annak is, hogy lecseréljék vezérigazgatójukat és technológiai igazgatójukat (Lending et al., 2018).

A kiberkockázatból eredő költségek

A kiberbiztonsági kockázat fontos szempont a befektetési döntéseknél. A kiberkockázat jelenléte közvetett költségekkel járhat a gazdaságban azáltal, hogy befolyásolja az erőforrások allokációját és megnehezíti egyes, kiberkockázatnak kitett ágazatok fejlődését. A vállalatvezetők a kiberincidenseket tartják a legnagyobb működési kockázatnak (World Economic Forum, 2022). Florackis et al., (2023) pedig azt mutatták ki, hogy a kiberbiztonsági kockázatot a részvényárakban beárazzák.

A kiberkockázat számszerűsítése a befektetésben és a vállalati értékteremtésben betöltött jelentősége miatt még nagyobb kihívást jelent, mint az adatgyűjtés, mivel meg kell becsülni a sikeres és sikertelen támadások bekövetkezési valószínűségét (Woods – Moore, 2019). A meglévő kiberkockázati indexeket és eszközöket, valamint

a szakirodalmat áttekintve az tapasztalható, hogy a kiberkockázatról szóló irodalom meglehetősen szűkös, és nem tartalmaz konzisztens adatokat és módszereket a kiberkockázat felmérésére. Ezeknek a korlátoknak a felismerése arra késztette a kutatókat és az érdekelt feleket (például biztosítótársaságokat), hogy új vagy összetettebb módszereket alkalmazzanak a kiberkockázat számszerűsítésére.

Mint az a kiberbűnözés fejlődéstörténetéről szóló fejezetben ismertetett esetekből is kitűnhetett, a pénzügyi piacokon a vállalati szintű kiberbiztonsági kockázat akár rendszerkockázat forrása is lehet. Ez abból fakad, hogy egy-egy pénzügyi vagy logisztikai szolgáltató kiberkockázatának jelentős, a cégen túlterjedő külső hatásai is lehetnek. A hálózati hatások megsokszorozhatják az egyetlen cégnél előforduló incidens hatását és ezért nagy zavarokat okozhatnak az egész pénzügyi rendszerben.

A kiberbiztonsági kockázat összetett természete azonban megnehezíti a magánszektor számára a kibertér megfelelő védelmét. Az externáliák és a hálózati hatások jelenléte rávilágít a kiberbiztonság közjóként való elismerésének fontosságára.

A kiberincidensek költségei tanulmányozásának kihívásai

A jelentősebb kiberincidensekre vonatkozó adatok többsége a közzétételi kötelezettségek betartásából vagy a kiberbiztonságért felelős hírszerző ügynökségek munkájából származik. Ezekben az adatokban is gyakran előfordulhatnak alul- vagy felülbecslési problémák (Howell és Burrus, 2020), ami az elemzés hatókörét olyan fejlett országokra korlátozza, mint az Egyesült Államok, ahol több és jobb minőségű adat áll rendelkezésre (pl. Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Lending et al., 2018, Tosun, 2021). Például a Privacy Rights Clearinghouse (PRC) nyílt adatokat szolgáltat az Egyesült Államok kormányzati szervei által 2004 óta nyilvánosságra hozott összes számítógépes jogsértésről, amelyek a terület legbefolyásosabb lapjairól tájékoztattak (Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021), Wang, 2022; Lin et al., 2020, Tosun, 2021). Népszerű, de az egész világon elérhető bizalmas adatállományt képez a svájci székhelyű ORX – a pénzügyi szolgáltatási szektor legnagyobb működési kockázatkezelési egyesülete – által szolgáltatott konzorciumi adatok, amelyek azonban csak a pénzintézetek működési kockázatait fedik le. Az egyesületet 2002-ben alapították a veszteség adatokat megosztani kívánó pénzügyi cégek.

Legalább öt oka van annak, hogy amiért kihívást jelent a kiberincidensek rögzítése, összesítése és mérése. Először is, a kiberbiztonsági fogalmak (például kiberincidensek és rendszerszintű kiberbiztonsági kockázat) nem szabványosított definícióit találjuk. Például egyesek úgy határozzák meg a kiberincidenseket, mint az információs kommunikációs technológia (IKT) felhasználásával előidézett hagyományos bűncselekményeket, valamint olyan új bűncselekményeket, amelyek a számítási alapú technológiák megjelenésével jelennek meg (Ho – Loung, 2022). Mások a kiberincidenseket az általános működési kockázati események alosztályaként határozzák meg (Aldasoro et al., 2020). Megint mások olyan iparági eseményekként határozzák meg azokat, amelyek a

technológiai eszközöket érinthetik (Biener et al., 2015). A kiberincidensek meghatározásáról szóló nemzetközi megállapodás lehetővé tenné a szükséges kiberbiztonsági intézkedések, például a rendszerszintű kiberbiztonsági kockázat helyes azonosítását. A kiberincidens legátfogóbb definíciója egyelőre az, hogy minden emberi kísérlet a kibertér megzavarására rosszindulatú vagy káros gazdasági szándékkal, ahol a kibertér az 'információ tárolására, módosítására és közlésére használt összes digitális hálózatból' álló tartomány, amely gazdasági veszteségeket eredményezhet, vagy nem. Mások szerint a számítástechnikai bűnözés az, amely magában foglalja az IKT-kon keresztül elkövetett hagyományos bűncselekményeket és az elektronikus hálózatokra jellemző bűncselekményeket, például a DDoS-t, a hackelést és a rosszindulatú programokat.

Másodszor, a kibertámadások nyilvánosságra hozatalára vonatkozó előírások és más kiberbiztonsági előírások régiónként és időben egyaránt eltérőek. Például az Európai Unió általános adatvédelmi rendelete (GDPR) előírja a cégeknek, hogy 72 órán belül felfedjék a jogsértéseket. Az Egyesült Államok Értékpapír- és Tőzsdefelügyelete arra kötelezi a nyilvános részvénytársaságokat, hogy az észlelését követő 96 órán belül jelentsék a kiberincidenseket. Míg az európai országok 99%-a rendelkezik adatvédelmi jogszabályokkal, az afrikai országoknak csak 65%-a hozott ilyen intézkedéseket. Hasonlóképpen, míg az európai országok 85%-a, addig az amerikai kontinens országainak csupán 34%-a alkalmaz szabálysértési eljárást a bejelentési kötelezettség elmulasztása esetén. Az ázsiai és csendes-óceáni országok 42%-a, Afrikában pedig az országok 43%-a alkalmazott ilyen jogszabályokat (The Digital, 2021).

Harmadszor, a polgárokat érintő számítógépes incidenseket nem jelentik rendszeresen, és még nehezebb nyomon követni azokat. Az egyének elleni támadásoknak jelentős fizikai és nem fizikai költségei lehetnek, mint például a számítógépek és telefonok károsodása, valamint az alapvető dokumentumok és személyes adatok, a figyelem és a termelékenység elvesztése.

Negyedszer, általában időbe telik, amíg egy entitás észreveszi, hogy kibertámadásnak van kitéve, ami megnehezíti az esemény bekövetkezése pontos időpontjának megállapítását. Tapasztalatok szerint az adatvédelmi incidensek azonosítása és megszüntetés között jellemzően több hónap telik el. Ez azt jelenti, hogy még akkor is, ha léteznek a kiberbiztonsági incidensek közzétételére vonatkozó szabályok, továbbra is bizonytalan marad a jogsértés pontos időpontja.

Végül Amir et al., (2018) szerint a cégek stratégiai aluljelentést tanúsítanak a kibertámadások feltárása terén. Facchinetti et al., (2020) vizsgálatai azt sugallják, hogy a cégek aluljelentése megakadályozásának egyik kézenfekvő módja az lenne, hogy csak a támadás súlyosságára vonatkozó információk jelentését követeljék meg tőlük ahelyett, hogy a támadás veszteségeinek számszerűsítésére kelljen összpontosítaniuk, mivel csak a támadás súlyosságának bejelentése csökkenti a cég jogi és helyreállítási költségeit a jogsértés észlelését követően. Ezért a cégek jelentősebb ösztönzést kapnának a gyors bejelentésre, ha nem kellene a hatóságokat tájékoztatniuk a veszteségek pontos összegéről.

Következtetések és szakpolitikai ajánlások

Ez a fejezet bemutatta a kiberincidensek gazdasági költségeit, amelyeket az iparág és a kormány érdekelt feleitől származó 15 kiemelkedő, globális kiberbiztonsági jelentés, valamint a kiberbiztonság gazdasági kérdéseivel foglalkozó vezető tudósok több mint 50 tudományos közleménye rögzít. Megállapítottuk, hogy a kiberteret érő fenyegetés gazdasági költségei jóval meghaladják a kiberbűnözés közvetlen költségeit, és olyan közvetett költségeket okoznak, amelyek ugyanolyan fontosak lehetnek, mint a korábbi és folyamatos válaszadási költségek.

A nem tudományos irodalom a kiberincidensek összköltségére vonatkozó összesített becslések széles skáláját mutatta be, amelyek a 2017-es 172 milliárd USD-től a 2021-es 8,0 ezer milliárd USD-ig terjedtek, és 2025-re akár 10,5 ezer milliárd USD-t is elérhetnek (a globális GDP körülbelül 9,1%-a). Ezeknek a költségbecsléseknek a hitelessége nem ellenőrizhető, mivel számos forrás nem támasztja alá megállapításait jól megmagyarázott módszerekkel. Ez pedig téves döntések meghozatalhoz vezethet, mivel a költségbecsléseknek alapvető szerepe van a költség-haszon elemzések kiindulópontjaként (CISA, 2020). Ezen túlmenően az elemzésekből az is kiderült, hogy a kiberincidensek gazdasági veszteségei meghaladják az azonnal számszerűsíthető költségeket, mivel a kiberincidensek gyakran olyan közvetett költségekkel járnak, amelyeket eddig általában nem szoktak mérni. Az elemzések azt is feltárták, hogy a gyakorlatban a kiberincidensek rendszerszintű kockázatot is jelenthetnek a pénzügyi piacokon, mivel hatásuk átterjedhet az ugyanabban a szektorban működő más cégekre is, és volatilitást okozhatnak a hazai és a globális részvénypiacokon egyaránt. Mivel azonban nem állnak rendelkezésre nyílt, pontos és megbízható adatok sem a nyilvánosságra hozott, sem a rejtett kiberincidensekről, jelenleg még nem létezik megalapozott és hiteles becslés a kiberincidensek tényleges globális költségeiről.

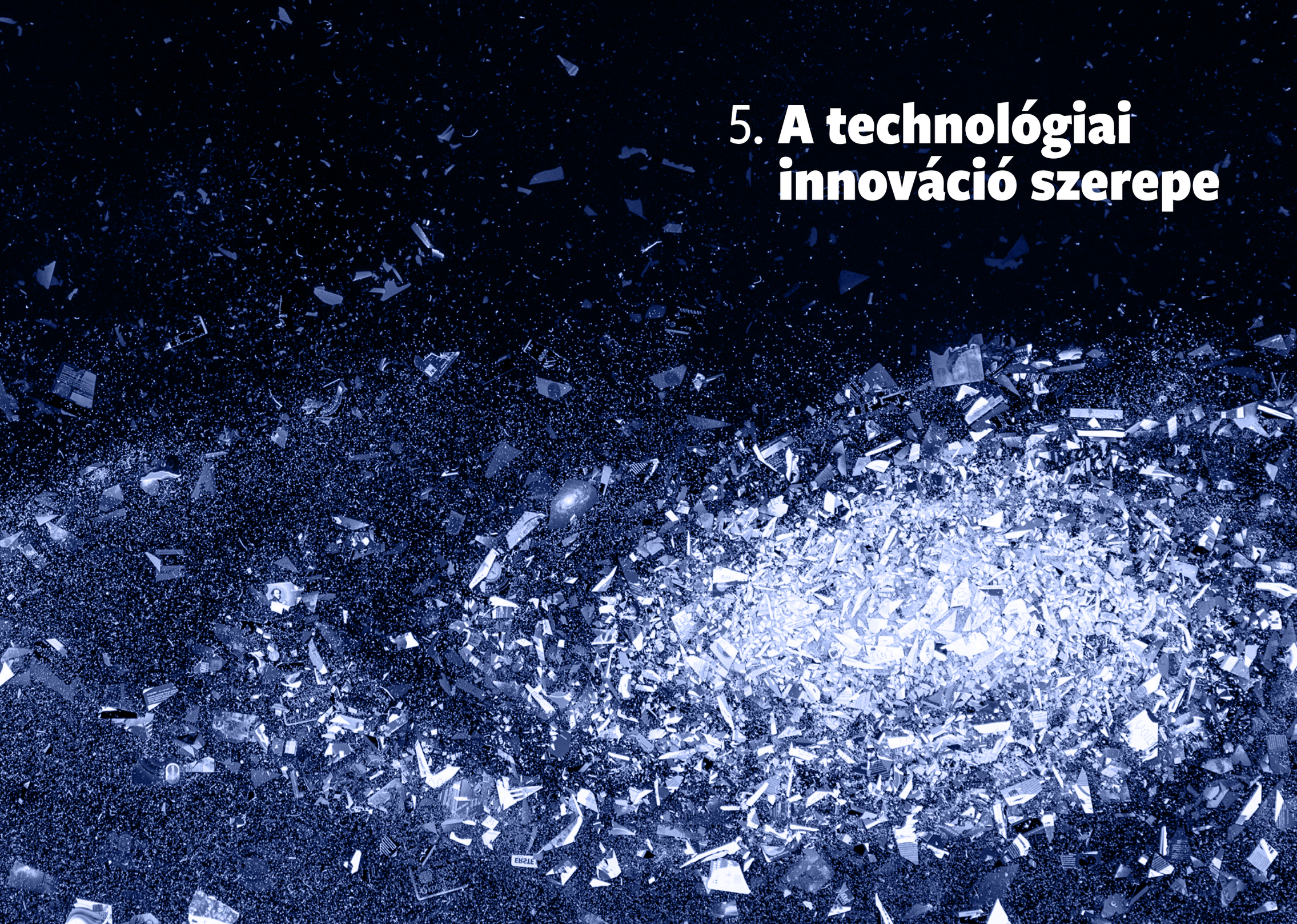
A hiteles becslések problémája mellett az is komoly problémát okoz, hogy jelentős hiányosságok tapasztalhatók a fejlődő országok kiberbiztonsági ismereteiben. A rendelkezésre álló szakirodalom több mint 90%-a a fejlett országokra, főként az Egyesült Államokra összpontosít. Ez a kiegyensúlyozatlanság óhatatlanul torzítja a kiberincidensek tényleges gazdasági költségeire és a kapcsolódó szakpolitikai következményekre vonatkozó elemzési eredményeket. A probléma megoldásához további adatokra, eszközökre és továbbfejlesztett elemzési megközelítésekre volna szükség ahhoz, hogy jobban meg lehessen érteni a kiberincidenseknek a világgazdaság egészére gyakorolt hatását.

A szakpolitikai vonatkozások tekintetében a szakirodalmi áttekintés két jelentős problémát azonosít. Az elsődleges tényező a kiberincidensekre vonatkozó megbízható adatok hiánya, amely megnehezíti, hogy pontos becsléseket lehessen kapni a kiberincidensek gazdasági hatásairól. A meglévő adatbázisok (pl. az Egyesült Államok KNK-adatbázisa) csak a fejlett országok meghatározott iparágaira vonatkozóan jelentenek nyilvánosságra hozott incidenseket, s főként az ezeket az adatállományokat használó tudományos tanulmányok adnak hiteles becsléseket a kiberbiztonsági incidensek egyes fontos aspektusairól, így például a tőzsdei hatásokról. Mindazonáltal

ezek a tanulmányok sem elegendőek ahhoz, hogy bemutassák a kiberincidensek teljes gazdasági hatását. Különösen kevés információ áll rendelkezésre a fejlődő országokban bekövetkezett kiberincidensek hatásairól, mivel a rendelkezésre álló adatállományok nem tartalmazzák ezeket az eseteket. Ezért nemzetközi együttműködésre van szükség a kiberincidensek jelentésére és osztályozására szolgáló rendszerek globális szabványosítása érdekében.

Másodszor, a kiberbiztonság egyes aspektusainak közjószágként való elismerése kiemelten fontos a kiberincidensek rendszerszintű kockázatai miatt, amelyek a pénzügyi rendszerekre, az ellátási láncokra és a kritikus infrastruktúrákra is kiterjednek. Ezen túlmenően a kiberbiztonsághoz kapcsolódó piaci hiányosságok, mint például a megcélzott cég által ügyfeleikkel és beszállítóikkal szembeni externáliák, egyértemű rámutatnak arra, hogy a kiberbiztonságot közjószágként kellene elismerni. Világszerte a kormányok vannak abban a helyzetben, hogy a jelenleginél erősebb kiberbiztonsági eredményeket mozdítsanak elő. A biztonságos technológiák létrehozásának ösztönzésével, továbbá a köz– és nemzetbiztonságba történő befektetéssel lehet szavatolni a társadalom és a gazdaság működéséhez létfontosságú infrastruktúra megfelelő védelmét.

Összefoglalva, az eddig végzett felmérések és elemzések aláhúzzák egy átfogó, empirikus és multidiszciplináris, szabványosított adatokon alapuló megközelítés szükségességét a kiberincidensekkel kapcsolatos gazdasági költségek megértéséhez, méréséhez és mérsékléséhez. Cégek és országok szintjén továbbra is felmerül a kérdés: Honnan tudhatjuk, hogy vajon jó befektetés-e a számtalan lehetőség közül az, amelybe potenciálisan beruházhatunk? Hogyan javíthatunk olyan hiteles mérőszámok kidolgozásán, amelyek segítségével a testületek megalapozottabb döntéseket hozhatnak? Az okadatolt tényeken alapuló mérőszámok és a kockázatalapú megközelítés elfogadásával az érdekelt felek jobban megérthetik a kiberbiztonsági befektetések megtérülését.



5. A technológiai innováció szerepe

Vállalatok a kibervédelemben

A technológiai innováció napjainkban viharos ütemben alakítja át a pénzügyi szektort mindenekelőtt annak komplexitását növelve. A technológiai innováció, valamint az általa indukált szabályozási változások gyors iramban mennek végbe, ami a szolgáltatókat és a felhasználókat egyaránt nagy kihívások elé állítja, és szakadatlan tanulást és alkalmazkodást kíván meg tőlük.

A 2008-ban kirobbant globális pénzügyi válságot megelőző időszakot a financializáció – vagyis a pénzügyi tevékenységeknek, a pénzügyi piacoknak és a pénzügyi intézményeknek a gazdaságban betöltött növekvő szerepe –, valamint a pénzügyi termékek innovációja jellemezte. Az elmúlt másfél évtized során viszont a fejlődés súlypontja a technológiai innováció felé tolódott el.

Az új technológiák alkalmazása a pénzügyi szektor számos területén hozott hatalmas – mondhatni szinte forradalmi – változásokat: a hagyományos pénzügyi szolgáltatásokat gyorsabbá, elérhetőbbé és hatékonyabbá tette, miközben csökkentette azok helyhez, illetőleg bankfiókokhoz való kötöttségét, valamint visszaszorította az ügyletek papíralapú lebonyolítását. Egyes területeken, így különösen a mesterséges intelligencia alkalmazása terén pedig még csak most kezdjük ízlelgetni a megnyíló új lehetőségek széles spektrumát.

Ám a viharos fejlődés új kockázatokat is hoz magával. Miért? Főként az elterjedés már-már követhetetlen gyorsasága és kiterjedése miatt, valamint egyes olyan szolgáltatások, mint például az adatok felhőalapú tárolása és feldolgozása terén, vagy a kulcsfontosságú szolgáltatók körében zajló koncentráció miatt. Mindezek mellett a kibertámadások elszaporodása és technológiai fejlődése is új kockázatokat teremtett.

Az új technológiák alkalmazása olyan új kölcsönhatásokat hoz létre, amelyek révén egyfelől széles körben válnak elérhetővé a haladás gyümölcsei/eredményei, másfelől azonban felgyorsulhat a gazdasági és pénzügyi válságok kibontakozásának és terjedésének üteme is, így tágítva a válságok társadalmi és földrajzi hatókörét és erejét. A kiberbűnözés történetéről szóló fejezetben ismertetett néhány kirívó eset is jól példázza, hogy akár pusztán egy zsarolóprogram vagy egy rosszindulatú vírus nem csupán a közvetlenül megtámadott szervezetet sújtja, hanem az ellátási láncokon keresztül meglehetősen széles körben képes létfontosságú szolgáltatások működését megbénítani, vagy vállalatok működőképességét és üzleti lehetőségeit korlátozni, gyakran akár hosszabb időre is.

Nem véletlen, hogy számos ország, valamint az Európai Unió az NIS (network and information systems, hálózati és információs rendszerek) kiberfenyegetéseknek való fokozott kitettsége miatt szabályokat és kötelező szabványokat alkotott annak érdekében, hogy megerősítse ezen rendszerek felhasználóinak és más érintett személyeknek védelmét a kiberbiztonsági eseményekkel és fenyegetésekkel szemben. Az Európai Unió 2016-ban fogadta el az első idevágó irányelvet, amelyet hat évvel később a 2022/2555 irányelv, más néven a NIS2 irányelv váltott fel, tükrözve az időközben végbement technológiai változásokat.

A NIS2 a szélesebb hatály, az egyértelműbb szabályok és a szigorúbb felügyeleti eszközök révén növeli az EU-ban a kiberbiztonsággal kapcsolatos közös ambíciószintet. Előírja a tagállamok számára, hogy javítsák kiberbiztonsági felkészültségüket, kockázatkezelési intézkedéseket és jelentéstételi követelményeket vezessenek be több ágazat szervezetei számára, továbbá szabályokat állapítsanak meg az együttműködésre, az információmegosztásra, a felügyeletre és a kiberbiztonsági intézkedések végrehajtására vonatkozóan.

Az irányelv előírja, hogy minden tagállamnak olyan nemzeti kiberbiztonsági stratégiát kell elfogadnia, amely magában foglalja az ellátási lánc biztonságára, a sebezhetőségek kezelésére, valamint a kiberbiztonsági oktatásra és tudatosságra vonatkozó szakpolitikákat. A tagállamoknak össze kell állítaniuk és rendszeresen frissíteniük kell az alapvető szolgáltatásokat nyújtó szereplők jegyzékét, biztosítva, hogy ezek a szervezetek megfeleljenek az irányelv követelményeinek.

Az irányelvet a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (röviden a Kibertan törvény) emelte be a magyar jogrendbe. A törvény a legfontosabb ágazatok szereplőinek kiberbiztonságát, vagyis azt, hogy az érintett cégek rendszerei biztonságosan működnek-e, rendszeres – kétévente megújítandó – kiberbiztonsági audit segítségével kívánja megállapítani.

A törvény hatálya alá tartozó cégeket alacsony, jelentős vagy magas kockázati osztályba kell sorolni attól függően, hogy mennyire veszélyeztetettek. A törvény végrehajtásával megbízott Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) 2024 júniusában tette közzé, melyik osztály auditálásához milyen követelményeknek kell megfelelni. A kiberbiztonsági szakma általános egyetértéssel fogadta, hogy a rendszeres monitorozás révén nagyobb hangsúly kerül a kiberbiztonságra, és sokan azt is pozitívumnak tartják, hogy az auditálást csak szakmailag megfelelően felkészült személyek és szervezetek végezhetik majd.

Amint az a törvény nevéből is kitűnik, a törvény végrehajtásának két pillére van; a rendszeres kiberbiztonsági tanúsítás és a kiberbiztonsági felügyelet.

- A tanúsítás lényege, hogy egy adott infokommunikációs termék vagy szolgáltatás, amelyet felhasználók vagy cégek igénybe vesznek, megfelel-e az előírt biztonsági követelményeknek. Ennek igazolását az SZTFH által felhatalmazott tanúsító vagy megfelelőségértékelő szervezetek végezhetik el – erre példa a pénzügyi szervezetek kiberbiztonsági tanúsítása.
- A felügyelet nem termékekre vagy szolgáltatásokra irányul, hanem azon cégek biztonságának és felkészültségének ellenőrzésére, amelyek kockázatos vagy kiemelten kockázatos ágazatokban működnek. Az érintett szervezetek informatikai rendszereinek biztonságát az SZTFH által felhatalmazott auditorok ellenőrzik.

A NIS2, illetve a Kibertan törvény tehát azt hivatott elősegíteni, hogy a kockázatos ágazatok szereplői kellőképpen fel legyenek készülve a kiberfenyegetések elleni védekezésre.

Kikre vonatkozik a NIS2? Az alanyi hatálynak két rendezőelve van: a cégek mérete és a tevékenységük jellege. Fő szabály szerint azok a közép- és nagyvállalatok (azaz ötvennél több főt foglalkoztató vagy tízmillió eurónál nagyobb éves árbevételű cégek) az érintettek, amelyek alapvető vagy a digitalizáció szempontjából nélkülözhetetlen szolgáltatásokat nyújtanak. Ezeket a törvény két kategóriába sorolja:

- Kiemelten kockázatos ágazatok: energetika, közlekedés, egészségügy, víziközmű, hírközlési szolgáltatások (telekommunikációs és internetszolgáltatók), digitális infrastruktúra (felhőszolgáltatók, adatközpontok, doménnyilvántartók stb.), valamint űralapú szolgáltatások.
- Kockázatos ágazatok: postai és futárszolgálatok, élelmiszercégek, hulladékgazdálkodás, vegyipar, egyes gyártási ágazatok, digitális szolgáltatók (keresők, közösségi média, doménszolgáltatók), valamint egyes kutatóhelyek.

Mikro- és kisvállalatokra csak akkor vonatkoznak az előírások, amennyiben elektronikus hírközlési szolgáltatást, bizalmi szolgáltatást vagy valamilyen doménszolgáltatást nyújtanak. (A törvény értelmében elektronikus hírközlési szolgáltatóknak minősülnek a telekomcégek és netszolgáltatók, viszont az online médiacégek nem.)

Milyen követelményeknek kell a cégeknek megfelelniük? Ezt a Miniszterelnöki Kabinetirodának a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK sz. rendelete állapította meg. A rendelet három biztonsági osztályt határozott meg aszerint, amekkora kárt okozhat az adott szervezetnél egy kiberincidens. Minden érintett szervezetnek be kell sorolnia a saját rendszereit alap, jelentős vagy magas biztonsági osztályba, majd az annak az osztálynak megfelelő követelményeket kell teljesítenie.

Hány vállalkozás érintett Magyarországon? Erről eltérő becslések vannak. Az SZTFH szerint mintegy 2500 hazai cég lehet érintett, de egyes szakértők szerint az érintett vállalkozások száma ennél akár 800-zal is több lehet.

Mikortól lesz mindez hatályos? Részben már most is az, de a java még hátra van:

- 2025 januárjától kezdődött el azoknak a szervezeteknek a nyilvántartásba vétele, amelyeket érint a NIS2.
- Az érintett szervezeteknek 2025. október 18-tól már alkalmazniuk kell a Miniszterelnöki Kabinetiroda által jegyzett rendeletben a biztonsági osztályukra meghatározott konkrét védelmi intézkedéseket, s ettől kezdve felügyeleti díjat is kell majd fizetniük az SZTFH-nak.
- Legkésőbb 2025. december 31-ig szerződniük kell egy nyilvántartásba vett auditorral, aki tanúsítja, hogy a rendszereik kellően biztonságosak.
- Az első auditot legkésőbb 2025. december 31-ig kell elvégeztetni.

A szabályozás szakmai tartalmát méltató, döntően pozitív piaci visszajelzésekből azonban az is kitűnt, hogy az érintettek szerint az audit határidejének felülvizsgálata nagyban elősegítené a kötelezettségek megfelelő teljesítését. Erre figyelemmel az SZTFH és az MKIK közösen azt javasolta a Kabinetirodának, hogy a kiberbiztonsági audit teljesítésének határideje fél évvel későbbre, azaz 2026. június 30-ra módosuljon.

Az SZTFH álláspontja szerint az auditoroknak nem az lesz a feladata, hogy pálcát törjenek az átvilágított cégek felett; ehelyett egy skálán értékelik a vizsgált cégek felkészültségét. Ezen a skálán – hasonlóan az iskolai osztályozáshoz – lesz egy „megfelelt" szint, amit legalább teljesíteniük kell a cégeknek. A következő audit alkalmával már a hármas szintet várják el, aminek teljesítéséhez az éppen csak megfelelt cégeknek valószínűleg egy cselekvési tervre is szükségük lesz. A felügyelet számára persze egyértelmű, hogy nem lehet a nagy, ipari rendszerekkel működő, jól automatizált cégeket olyan kicsi cégekkel összehasonlítani, amelyek – ha a szolgáltatásuk miatt érintettek is, de – méretüknél fogva nem jelentenek nagy kockázatot.

A Kibertan törvénynek ugyan nem a szankcionálás a célja, mindazonáltal kiterjeszti a kiberbiztonsági hatóságok szankcionálási lehetőségeit. A jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok nemteljesítése vagy be nem tartása esetén többféle jogkövetkezménnyel lehet számolni a felügyeletet ellátó SZTFH részéről:

- Figyelmeztetés, határidő megállapítása, felszólítás, illetve az SZTFH elnöke által kiadott rendeletben meghatározottak szerint információbiztonsági felügyelő kirendelése a szervezet költségére.
- További szankcióként bírság is kiszabható, melynek mértékét kormányrendelet határozza meg.
- Szankcióként kezdeményezhető még a tevékenységi engedély vagy tanúsítás ideiglenes felfüggesztése, illetve a vezető tisztségviselő legfeljebb öt évre szóló eltiltása, amennyiben a kiberbiztonsági kötelezéseknek nem tett eleget.
- Emellett az SZTFH a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységektől is eltilthatja az érintett szervezeteket.

A kiberbiztonsági incidensek kezelésében is változások várhatóak. A nemzeti incidenskezelő központ, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet mellett – feltehetően – létrejönnek majd az egyes ágazatokon belüli kiberbiztonsági incidenskezelő központok is. E központokon túlmenően bármely szervezet az őt ért kiberbiztonsági incidensek kezelésére megbízhat – az SZTFH elnökének rendeletében előírt szakértelemmel és infrastrukturális feltételekkel rendelkező – gazdálkodó szervezetet, amely szerepel az SZTFH által vezetett nyilvántartásban.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet immár közel két évtizede aktívan részt vesz számos ország számítógépes biztonsági incidensekre reagáló csoportjának (Computer Security Incident Response Team – CSIRT) regionális és interkontinentális nemzetközi együttműködésében. Ennek révén naprakészen ismeri a különböző országokban észlelt kiberbiztonsági incidenseket, ami nagy segítséget jelent a hazai kibervédelem megerősítéséhez.

A magasabb szintű kiberbiztonság elérésének természetesen vannak költségvonzatai. Az érintett vállalatoknál három jogcímen merülhetnek fel kiadások a

kiberbiztonsággal kapcsolatban: 1) a rendszeres időközönkénti kötelező audit díja, 2) a felügyeleti díj, és végül 3) legalább a minimumkövetelmények teljesítéséhez, illetve a felügyeleti hatóság által előírt kiberbiztonsági intézkedések megvalósításához szükséges költségek.

A hazai kis- és középvállalkozások kapcsolódó adminisztratív és anyagi terheinek alacsony szinten tartása és ezzel versenyképességük megőrzése érdekében a rendelet az auditor által felszámítható díj maximumát a Magyar Kereskedelmi és Iparkamarával történt egyeztetés alapján úgy határozta meg, hogy a rendelet hatálya alá tartozó cégek kiberbiztonságra fordított költségei lehetőleg mérsékeltek maradjanak.

Az audit legmagasabb, áfa nélkül számított díjának kiszámítási módját a rendelet 3. melléklete tartalmazza. A maximális díj kiszámításához az 1 750 000 forintos alapdíjat kell különféle szorzókkal módosítani az auditálandó cég jellemzői alapján.

Az egy cég auditjáért elkérhető díj maximuma a következőképpen alakul:

A cég előző üzleti évi nettó árbevételétől függően:

árbevétel ≤ 1 milliárd Ft	0,9%
1 milliárd Ft < árbevétel ≤ 5 milliárd Ft	1,1%
5 milliárd Ft < árbevétel ≤ 10 milliárd Ft	1,9%
10 milliárd Ft < árbevétel ≤ 15 milliárd Ft	2,5%
15 milliárd Ft < árbevétel ≤ 25 milliárd Ft	2,75%
25 milliárd Ft < árbevétel ≤ 40 milliárd Ft	3,0%
árbevétel > 40 milliárd Ft	4,0%

Forrás: Magyar Közlöny

A cég elektronikus információs rendszereinek (EIR) száma alapján meghatározott szorzótól függően:

EIR-ek darabszáma	Szorzószám
1–5	1
6–15	2,5
16 vagy annál több	4

Forrás: Magyar Közlöny

A cég elektronikus információs rendszereinek biztonsági osztályától függően: ha mindegyik az alap osztályba tartozik, akkor a szorzó 1; ha van köztük legalább egy jelentős osztályba tartozó (és nincs a magas osztályba tartozó), akkor 3, ha pedig van köztük legalább egy magas osztályba tartozó, akkor 5.

Ha tehát egy cég árbevétele nem éri el az egymilliárd forintot, legfeljebb öt elektronikus információs rendszere van, amelyek mindegyike az alap osztályba tartozik, akkor az audit díja legfeljebb 1 575 000 forint plusz áfa lesz. Ha viszont egy 40 milliárd fölötti árbevétellel rendelkező nagyvállalatnak több mint 16 rendszert kell auditáltatnia, amelyek között magas osztályba tartozó is van, akkor az audit díja akár 140 millió forint plusz áfa is lehet.

A kiberbiztonsági felügyeleti díjat a 2/2025. (I. 31.) SZTFH rendelet határozta meg. A felügyeleti díj a felügyelt cég előző évi nettó árbevételétől függ:

- ha az érintett cég nettó árbevétele nem éri el a 20 milliárd forintot, akkor a felügyeleti díj annak 0,00015 százaléka;
- ha az árbevétele legalább 20 milliárd forint, akkor a felügyeleti díj annak 0,0015 százaléka, de legfeljebb 10 millió forint.

Ha egy cégnek előző évben nem volt árbevétele (ezek többnyire új alapítású cégek), akkor a tárgyév addigi árbevételének az egész évre számított összege alapján kell a díjat meghatározni. Amennyiben a felügyeleti díj nem érné el az ötezer forintot, úgy a felügyeleti hatóság teljesen el is engedheti a díjat.

A különböző jogcímen felmerülő díjakat az érintett vállalatok valószínűleg tovább fogják hárítani a vevőikre. Ennek fejében azonban az ügyfelek nagyobb biztonságban érezhetik magukat, hiszen partnerüknek az ellenállóképessége az auditnak köszönhetően bizonyítottan erősebb, s így alacsonyabb a kockázati kitettségük. Az auditált cégek és az ügyfeleik ezen kívül számíthatnak arra is, hogy könnyebben és feltehetően valamivel kedvezőbb díjjal tudnak kiberbiztosítást kötni, mint korábban.

NIS2 a pénzügyi szektorban

A tőkeáramlást irányító és támogató intézményeket, például bankokat, befektetési cégeket és biztosítótársaságokat magában foglaló pénzügyi szektor az európai gazdaságnak az egyik kritikus eleme, amely az általa kezelt értékes eszközök és érzékeny adatok miatt mindig is a kibertámadások elsődleges célpontja volt. Ezen belül is a fizetési terület a kibertámadásoknak leginkább kitett rész, ahol hatalmas összegek mozognak a felhasználók között és a határokon át. Egyedül a bankkártyás fizetések összege tavaly mintegy 200 trillió eurót tett ki az EU-ban. A fizetési területet az új platformok és az újfajta digitális megoldások növekvő arányú használata jellemzi, ami azonban nemcsak az átutalási költségek csökkenését eredményezi, de fokozza a kibertámadások kockázatát is. Éppen ezért szembetűnő, hogy ennek az ágazatnak a tevékenysége nem szerepel tételesen a NIS2-ben említett különlegesen kockázatos tevékenységek között.

Ennek az a magyarázata, hogy a pénzügyi szektor már a NIS1 irányelv megszületése előtt is fokozott felügyeleti ellenőrzésnek lett alávetve a kibertámadásokkal szembeni ellenállóképessége tekintetében. A pénzügyi szolgáltatási ágazatra ugyanis már régebb óta szigorú kiberbiztonsági követelmények és speciális szabványok vonatkoznak, amelyek azonban teljesen összhangban vannak a NIS2 megközelítésével.

Ezen túlmenően az EU valamennyi tagállamában 2018 májusától hatályba lépett az EU 2016/679 számú általános adatvédelmi rendelete[10] (GDPR), amely alapjaiban változtatta meg az adatvédelem addigi gyakorlatát. Nem véletlen, hogy a legszigorúbb rendeletek között tartják számon: a Nemzeti Adatvédelmi Hivatal (NAIH) akár 20 millió euróig (kb. 8 milliárd Ft-ig) terjedő büntetést is kiszabhat azokra, akik nem tartják be az adatvédelmi szabályokat.

Az adatbiztonság fenntartása és a GDPR előírásait sértő adatkezelés megelőzése különösen nagy feladatot jelent a pénzügyi szektorban tevékenykedő vállalatok számára, hiszen tevékenységükhöz rengeteg személyes adatra és azok tárolására van szükség, melyek megvédését a pénzügyi szolgáltatásokra vonatkozó törvények nevesítetten is előírják (ld. banktitok, biztosítási titok stb.) A GDPR-ból és az egyes pénzügyi ágazatokról szóló törvényben előírt adatvédelmi kötelezettségek maradéktalan teljesítése érdekében az adatkezelő pénzügyi szolgáltatónak, valamint az általa bevont adatfeldolgozó cégnek értékelnie kell az adatkezelés természetéből fakadó valamennyi kockázatot, és kötelesek az e kockázatok csökkentését szolgáló intézkedéseket megtenni. Ezeknek az intézkedéseknek kell szavatolnia a továbbított, a tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közzétételét vagy az azokhoz való jogosulatlan hozzáférést kizáró intézkedéseket –, figyelembe véve a tudomány és technológia állását, valamint a végrehajtási kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeket.

További kihívást jelent a pénzügyi szektor számára a kriptoeszközök használata. A kriptoeszközök gyorsan növekvő piacán a csődök, likviditási válságok és nyílt csalások egyelőre a hagyományos pénzügyek terén megszokottnál gyakrabban fordulnak elő, miközben e piac kapcsolódása a hagyományos pénzügyekhez egyre szorosabbá válik. A Pénzügyi Stabilitási Tanács (FSB) szerint a kriptovaluták léte önmagában véve ugyan még nem teremt rendszerszintű kockázatot, de a legújabb fejlemények azt sugallják, hogy a világ e tekintetben is fordulóponthoz közeledik. A lakossági felhasználók előtt tornyosuló akadályok ugyanis jelentősen csökkentek, különösen a kriptovaluta-tőzsdéken kereskedett alapok (ETF-ek) bevezetésével. A hagyományos pénzügyi rendszerrel való kapcsolatok további erősödését pedig az is elősegítette, , hogy a csekély áringadozású kriptovaluták – a stablecoinok – kibocsátói, éppen az USD-ben jegyzett árfolyamuk stabilizálása érdekében, napjainkra számottevő mennyiségű amerikai kincstári értékpapírállományt halmoztak fel. Mindemellett a kiberbűnözés is fokozott érdeklődést tanúsít a kriptoszektor iránt: egyrészt haszonszerzési lehetőségként tekintenek rá, másrészt pedig a bűnözés útján szerzett pénzek tisztára mosásának helyszíneként használják. A kripto-ökoszisztéma minden bizonnyal tovább fog terebélyesedni, következésképpen a szabályozási kereteknek is tovább kell fejlődniük, ami a kriptográfia eredendően határokon átívelő jellege miatt különösen fontos.

10 Forrás: https://net.jogtar.hu/jogszabaly?docid=a1600679.eup

A kriptográfia térnyerése részben a határokon átnyúló fizetések terén tapasztalható hiányosságokra vezethető vissza, aminek összetett technikai és jogi okai vannak. Ezeknek a problémáknak a kiküszöbölése valós előnyöket hozhat az emberek, a vállalkozások és a gazdaságok számára. Ezen előnyök realizálása a célja a határokon átívelő fizetések javításáról szóló G20 ütemtervnek is, ami olcsóbb, gyorsabb, átláthatóbb és átfogóbb határokon átnyúló fizetési szolgáltatások nyújtását irányozza elő világszerte a polgárok és a vállalkozások javára. Ugyanakkor a G20 országok határozott fellépését szorgalmazza annak érdekében, hogy megakadályozzák a kriptovaluták határokon átívelő pénzmosásra történő felhasználását.

A kiberkockázat mérése a NIS2 által nem érintett vállalati körben

A NIS2 előírásainak következetes alkalmazása esetén a vállalatok széles köre válik ellenállóbbá a kiberbűnözés támadásaival szemben, de az irányelv hatálya alá tartozó vállalatok és szervezetek száma és gazdasági szerepe csak a „jéghegy csúcsát" jelenti. A legtöbb vállalkozás, szervezet (egyesület, alapítvány, mikro- és kisvállalkozás), kiváltképpen a nem kiemelten kockázatos vagy nem kockázatosnak minősített szektorban, haszonélvezője lesz a NIS2 által elért nagyobb kiberbiztonságnak, ám ez korántsem jelent teljes körű és feltétel nélküli biztonságot kiberincidensek bekövetkezése ellen. A védelemre fordítható összegek ugyanis korlátozottak, a megfelelő szintű biztonság pedig technikailag sokszor nem, vagy csak irreálisan magas költségek vállalásával alakítható ki. Ráadásul a kiberincidensek által okozott károkra kötött biztosítás sem tekinthető minden problémán segítő csodaszernek, hiszen nem mindenfajta kockázatra érhető el ilyen védelem, illetve egyes kockázatokra biztosítás csak magas díj fizetése mellett köthető.

A kibervédelem legolcsóbb, egyszersmind leghatékonyabb módja a digitális hálózati eszközök, rendszerek és programok biztonságtudatos használata. A kiberincidensek jelentős része ugyanis azért következik be, mert a digitális eszközök kezelése során az óvatlanság, a hiszékenység, a figyelmetlenség és a gondatlanság teremt lehetőséget a kiberbűnözőknek ahhoz, hogy akár különösebb műszaki felkészültség nélkül is hozzáférjenek a bizalmas személyi adatokhoz és ezáltal jelentősebb összeggel károsítsák meg az embereket.

Ennek a tudatosítása roppant fontos mind a vállalati döntéshozók (tehát a rendszerek védelméért felelős vezetők), mind az üzemeltetők (akik a rendszerek működtetéséről és a szükséges védelmi intézkedésekről gondoskodnak), valamint – nem utolsó sorban – a felhasználók körében is. Különösen az utóbbiak esetében elengedhetetlen, hogy elsajátítsák az internet és az információs technológiák biztonságos használatát, és felelősen, szakszerűen kezeljék a saját adataikat és eszközeiket.

Az ehhez szükséges ismeretek bármikor könnyen elérhetők az interneten, vagy különböző szaktanfolyamok keretében is. A fejezet további része elsősorban a vállalati vezetők és szakemberek számára kíván segítséget nyújtani a biztonságtudatos,

egyszersmind költségkímélő védekezéshez; az egyéni felhasználók számára pedig egy külön fejezet szolgál hasznos tanácsokkal.

A digitalizált világban a vállalkozások jószerint már mindenben a technológiára támaszkodnak. A digitális innovációk, például a mesterséges intelligencia, azonban gyakran meghaladják azokat a védelmi és válaszintézkedéseket, amelyeket a képesek alkalmazni. Nem megfelelő kiválasztás vagy alkalmazás esetén ugyanis egyes innovációk úgy viselkednek, mint egykoron a prágai Gólem: nem engedelmeskednek a gazdáiknak, esetenként pedig akár nagyobb károkat vagy kiadásokat okozhatnak, mint amennyi hasznot hajtanak. Napjainkra – éppen a nagyfokú technikai és technológiai függés miatt – a kibertámadások sok vállalat számára a legvalószínűbb és legköltségesebb fenyegetéssé váltak. A kibertámadások számának szaporodása ugyanis arra kényszeríti a vállalkozásokat, hogy növeljék a kiberbiztonság növelésére fordított kiadásaikat. Mégis, kevés vállalat képes számszerűsíteni, valójában mekkora is a kiberkockázati kitettsége, ez pedig jócskán gyengíti a védekezés hatékonyságát.

Sok vezető különböző „hőtérképek” útmutatására támaszkodik, amelyek a sebezhetőséget „alacsonynak” vagy „magasnak” minősítik olyan meglehetősen homályos becslések alapján, amelyek gyakran egy kalap alá veszik a gyakori kis veszteségeket és a ritkán bekövetkező nagy veszteségeket. Ez a megközelítés azonban nem segíti elő annak megértetését, hogy az adott vállalkozás kockázati kitettsége 10 vagy akár 100 millió euróra tehető-e, nem is szólva arról, hogy szükség van-e, s ha igen, akkor mekkora összegű további befektetésre a rosszindulatú programok elleni védelem vagy éppen a levelezőrendszer védelme érdekében. A vállalatok jelentős hányada azt sem tudja megfelelően megítélni, mely kiberbiztonsági képességeit kellene elsősorban fejleszteni, így gyakran a megfelelő kiberbiztosítási védelem kialakítása is akadályokba ütközik.

Azzal persze tisztában kell lenni, hogy egyetlen vállalatnak, szervezetnek sincs elegendő erőforrása a kiberkockázatok teljes körű kiküszöbölésére. Ebből viszont az következik, hogy döntő fontosságú annak meghatározása, mely fenyegetések elhárítására kell összpontosítani. Ennek során azonban sok vállalkozás és szervezet vezetői hajlamosak az informatikai zavarokat elszigetelt technikai hibának tekinteni, és a kiberbiztonságot sem kezelik alapvető üzleti kockázatként. Ezt csak tetézi, hogy a vállalati felsővezetők, az informatikáért felelős részlegek és a biztonságért felelős vezetők a kiberbiztonsági problémákat különböző szempontok és különböző módszerek alapján értékelik, ennek során egymástól függetlenül dolgoznak, ráadásul különböző szakzsargont használnak, ami lerontja az egymással történő kommunikáció hatékonyságát is.

Az említett párhuzamosságok miatt a kiberbiztonság erősítésére irányuló döntések a különböző sebezhetőségek hatásmechanizmusának kellő megértése nélkül, illetve a megelőzésükhöz szükséges ráfordítások hiányos ismerete alapján születnek meg. A különböző szervezeti egységek összehangolatlanul készülő elemzései nem tudják kellőképpen számításba venni egy-egy incidens összes lehetséges következményét, és nincs átfogó ismeretük arról sem, hogy a védelembe történt beruházások miként csökkentik egy-egy incidens bekövetkezésének valószínűségét. Sokszor még az sem világos,

hogy egy adott intézkedéssel vagy fejlesztéssel egy adott fenyegetés teljesen elhárítható-e, vagy csupán csökkenthető a bekövetkezési valószínűsége, és ha igen, mekkora mértékben.

Egy további jellegzetes probléma, hogy azok az üzleti vezetők, akik egy termék vagy szolgáltatás fejlesztéséhez szükséges informatikai eszközöket megrendelik, gyakran nem viselnek felelősséget a termék vagy szolgáltatás fejlesztésének és karbantartásának tényleges költségeiért. Holott, a tapasztalatok szerint egy-egy termék vagy szolgáltatás fejlesztésével kapcsolatos közvetett költségek (például felhő- és biztonsági szolgáltatások vagy eszközlicencek) néha a termék (vagy szolgáltatás) teljes költségének akár 80 százalékát is elérhetik a termék élettartama során.

Az pedig külön nehezíti a hatékony védekezést, hogy a vállalati érdekeltségi rendszerek általában erőteljesebben jutalmazzák az árbevétel növelését és a nyereség ebből eredő növekedését, mint a vállalkozás értékének alakulását. Pedig a tapasztalatok szerint a kiberincidensek összességében sokkal erőteljesebben hatnak egy vállalat piaci értékére, azaz piaci kapitalizációjára, mint az árbevételére és a nyereségére. Ez egyebek mellett abból adódik, hogy az ügyfelek jelentős része hátat fordít azoknak a cégeknek, amelyek képtelennek bizonyultak a maguk kiberbiztonságát megvédeni, sőt az incidens következtében az ügyfelek adatai is kiszivárogtak.

Az előbb felvázolt problémák miatt a vállalatoknak ki kell fejleszteniük a kiberkockázati kitettségük számszerűsítésének képességét. Csak így tudnak hatékony stratégiákat kialakítani a kockázatok mérséklésére, s annak eldöntésére, hogy mely feladatokat érdemes saját erőből ellátniuk, melyeket pedig célszerű külső szolgáltatóra bízniuk, vagy mely esetekben érdemes biztosítást kötni adott feltételek és díjak mellett. A kérdés tehát az, vajon lehet-e pénzösszeget rendelni a gyorsan változó kiberkockázatokhoz olyan adatokkal, amelyeket nem könnyű megtalálni, és gyakran még nehezebb értelmezni.

A kiberbiztonsági kockázatok számszerűsítésének lehetősége

A kiberbiztonsági kockázatok számszerűsítésétől sokakat eleve eltántorít az a tévhit, miszerint ehhez nem állnak rendelkezésre a szükséges ismeretek vagy adatok. A következőkben igyekszünk eloszlatni az idevágó néhány gyakoribb tévhitet, s segítséget nyújtani a kiberbiztonsági kockázatok számszerűsítéséhez.

Voltaképpen mit is jelent a számszerűsítés? A számszerűsítés valaminek a mennyiségi meghatározását jelenti, azaz valaminek a méretét, mennyiségét vagy kiterjedését numerikus értékkel fejezi ki. Magában foglalhatja a mérést, a statisztikai elemzést vagy bármilyen más módszert, amellyel egy jelenséget vagy adatot számokkal lehet jellemezni. A kiberbiztonsági kockázatelemzésre alkalmazva ez azt jelentheti, hogy a kockázat valószínűségét és hatását numerikus formában fejezzük ki egy skálán vagy valamilyen matematikai képlet segítségével. Ez a folyamat segít a kockázatok rangsorolásában és a hatékony kockázatkezelési stratégiák kidolgozásában.

A kockázat számszerűsítésének lépései:

1. A kockázat azonosítása: meg kell határozni, milyen potenciális kockázatokkal kell számolni.
2. A valószínűség meghatározása: az adott kockázat esetében meg kell becsülni, hogy az milyen valószínűséggel fog bekövetkezni. A valószínűség értéke 0 és 1 között van, de esetenként kifejezhető a bekövetkezés gyakoriságaként is.
3. A hatás mértékének meghatározása: meg kell becsülni, hogy a kockázat bekövetkezése milyen összegű károkozással járhat (pénzügyi, reputációs stb.). A károk között nem csak a közvetlen, hanem a másodlagos – vagyis a közvetett – károkat is számításba kell venni.
4. A kockázati pontszám kiszámítása: a bekövetkezés valószínűségét és hatását összeszorozva kapjuk meg a kockázati pontszámot, ami a kockázat súlyosságát jelzi.
5. Rangsorolás: a kockázati pontszámok alapján a kockázatokat sorba lehet rendezni, és a legmagasabb pontszámú kockázatokkal kell először foglalkozni.

A rangsorolással meghatározott fontossági sorrend (1., 2., 3. stb.), vagy a fontosságot minősítő jelzők (alacsony, közepes, magas) nem a kockázat vagy a kár mennyiségét méri, hanem a különböző kockázatok egymáshoz viszonyított rangsorát jelöli.

A kockázatszámítással kapcsolatos tévhitek

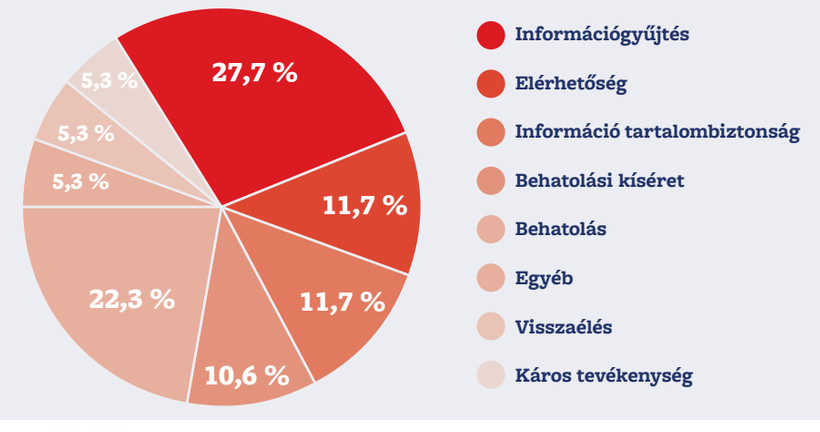
Számos olyan tévhit él a kiberbiztonsági kockázat számszerűsítésével kapcsolatban, amely eltántoríthatja a vállalati szakembereket attól, hogy maguk is megpróbálkozzanak a számszerűsítéssel. Néhány közkeletű tévhit cáfolatát az alábbi táblázatban foglaltuk össze.

22. TÁBLÁZAT: A kockázatszámítással kapcsolatos (tév)hitek – mítosz és valóság

Mítosz	Valóság
„Nem állnak rendelkezésre adatok a számszerűsítéshez.”	Adatok szinte mindig rendelkezésre állnak. Ha azonban kétségek támadnak a rendelkezésre álló adatok megbízhatóságát vagy relevanciáját illetően, akkor éppen a számszerűsítéssel való próbálkozás kínál lehetőséget a kétségek vizsgálatára is. A tapasztalatok szerint azonban általában több adathoz lehet hozzáférni, mint ahogy azt elsőre feltételezik. Megbízható eredmények elérése érdekében célszerű különböző adatforrásokat használni, így például a korábbi incidensek adatait, a naplózott adatokat, vagy szakértők véleményét. A számszerű megközelítés korántsem csak objektív, kvantitatív adatforrások használatát követeli meg. A számszerűsítésnek ugyanis nem az az elsődleges célja, hogy több tizedes pontossággal állapítsa meg egy vizsgált jelenség sajátosságait, hanem az, hogy érzékeltesse egy vizsgált jelenség kiterjedését, arányait, valamint változásának irányait. Ehhez pedig nem csupán a közvetlenül mért adatok adhatnak támpontot, hanem más, analóg jelenségek adatai is.
„A kiberkockázatokat nem lehet ugyanúgy mérni, mint más kockázatokat”	A korábbi incidensek adatainak hiánya, vagy a nehezen meghatározható tényezők (például a hírnévrontás) számszerűsítésének nehézsége korántsem csak a kiberbiztonságot jellemző probléma. Hasonló fenntartások ellenére más tudományágak területén is találtak lehetőséget a számszerűsítésre. Bár egy absztraktabb fogalmat (például a hírnevet) valóban nem biztos, hogy közvetlenül lehet mérni, ám a hírnév károsodásának hatása számszerűsíthető olyan tényezők figyelembevételével, mint pl. az új ügyfelek számának csökkenése vagy a részvényárfolyam esése. A kockázat számszerűsítése során sem szükséges mindig a pénzt használni mérőszámként. Használható például a rendszernek az incidens utáni helyreállításához szükséges idő, vagy az incidens által érintett eszközök száma, ha ezek könnyebben alkalmazható mérőszámok. A lényeg az, hogy valamilyen módon meg lehessen jeleníteni a kockázat számszerű hatását, ami azt érzékelteti, milyen mértékű következménnyel jár az, ha a kockázat bekövetkezik.
„Nem állnak rendelkezésre a számszerűsítéshez szükséges ismeretek vagy eszközök”	A számszerűsítéshez nincs szükség a matematikusok vagy közgazdászok nagy hadára. A kockázat számszerűsítése ugyanis megtörténhet a rendelkezésre álló adatokon alapuló becsléssel is, aminek nem szükséges komplex statisztikai modellen alapulnia. A statisztikai módszerek alkalmazásához sem szükséges statisztikai diploma. Számos elemzési módszer érhető el a rendelkezésre álló táblázatkezelő programok (pl. Excel vagy Calc) segítségével.
„A nulláról kell kezdeni a kockázatkezelési folyamatot”	Nem kell sutba dobni a korábban készült elemzéseket. A számszerűsítés a korábbi elemzések felhasználásával is megtörténhet anélkül, hogy további adatok szerzésére vagy további időre lenne szükség. Nem kell a számszerűsítést a kockázatkezelési folyamat minden területére alkalmazni; lehet úgy is dönteni, hogy a számszerűsítést csak egy adott részkérdés elemzésére használják. Szélesebb körű vagy részletesebb elemzésekhez pedig olyan kvantitatív kockázati módszertanok állnak rendelkezésre, mint például az amerikai FAIR nonprofit intézet által kidolgozott információs kockázati faktoranalízis (Factor Analysis of Information Risk – FAIR), vagy a Nemzetközi Szabványügyi Szervezet és a Nemzetközi Elektrotechnikai Bizottság ISO/IEC 27001[11] és 27005[12] számú szabványai, amelyek keretrendszert biztosítanak az információbiztonsági kockázatok azonosításához, értékeléséhez és kezeléséhez.

Forrás: Szerzők összeállítása

11. ÁBRA Magyarországi incidensek eloszlása típus szerint 2025.09.19. - 2025.09.25.



Forrás: (NKI, 2025)

11 https://hu.wikipedia.org/wiki/ISO_27001
12 https://mersz.hu/dokumentum/m1153fvbm__79/

A kiberincidensek tanulságai

Az olyan incidensek, mint a 2024 júliusában bekövetkezett globális CrowdStrike leállás, amikor világszerte bankok, repterek, légitársaságok, kórházak, biztosítók, vasúti rendszerek, sőt még futballklubok informatikai rendszerein egyszerre állt be a „kék halál” és ezért teljesen hasznavehetetlenné váltak, számos tanulsággal szolgálnak. Hogy mi is történt valójában, arról sokan sokfélét írtak össze a globális informatikai káosz első 12 órájában. Az incidenst kiváltó szoftverhibát kiküszöbölő javítóprogram ugyan már 90 percen belül rendelkezésre állt, csakhogy a hiba kiküszöbölése nem jelentette automatikusan a normál üzletmenet azonnali helyreállítását a lebénult rendszereken. A sikeres helyreállítás ugyanis több tényezőtől függ:

- **A kritikus infrastruktúra érintettsége:** Az incidens által érintett infrastruktúra mérete jelentősen befolyásolja a helyreállítás időtartamát.
- **Az infrastruktúra komplexitása:** Az infrastruktúra jellege – legyen az lokális, hibrid vagy felhős környezet – szintén befolyásolja a helyreállítás időigényét.
- **Kompetens üzemeltetői kapacitás:** A belső és külső szakértők rendelkezésre állása, különösen a szabadságok időszakában, meghatározó tényező. A megfelelő ismeretekkel rendelkező emberi erőforrások szűkössége lassíthatja a folyamatot.
- **Szervezeti felkészültség:** a helyreállítás gyorsaságát a szervezet és munkatársainak felkészültsége, a szükséges teendők sorrendbe szervezett forgatókönyve, valamint a korábban szerzett gyakorlati tapasztalatok együttesen határozzák meg.
- **Az incidens elhárításának szervezettsége:** az ad hoc módon, kapkodva végzett incidenselhárítás még ronthat is a helyzeten, és meghosszabbíthatja a helyreállítást.
- **IT-rendszerek összehangolási problémái:** Az egymáshoz kapcsolódó, de egymástól fizikailag és szervezetileg független IT-rendszerek közötti szinkronizáció elhúzódása további késedelmeket okozhat. (Így pl. a repülőterek és a légitársaságok számítástechnikai rendszereit össze kell hangolni a légiforgalom zavartalansága érdekében.)
- **Külső szolgáltatóktól való függés:** Ha egy szervezet működése erősen függ külső szolgáltatóktól, akkor azok válaszkészsége is meghatározhatja a helyreállítási időt.

A támadás tanulságainak kiértékelése során a résztvevők annak meghatározásával küszködtek, vajon ki is az, aki elsődlegesen felelős a keresztfunkcionális feladatok elvégzéséért, és miként lehet egymással összehangolni a helyreállítási tevékenység különböző szakaszait. Egy feladat keresztfunkcionalitása azt jelenti, hogy az adott

A kiberincidens típusok kiválasztása és meghatározása jelentős részben az AAG IT Services (2025): The Latest 2025 Cyber Crime Statistics, https://aag-it.com/the-latest-cybercrime-statistics/ tanulmány felhasználásával történt.

feladat vagy projekt elvégzéséhez különböző szakterületek szakembereinek csapatként kell együtt dolgozniuk, és a közös cél eléréséhez mindegyikük szakértői csoportjának hozzájárulása szükséges. A feladat tehát nem kötődik egyetlen szervezeti egységhez vagy szakterülethez, hanem több területet fog át. A történtek rávilágítottak az irányítás kritikus hiányosságaira. Világossá vált, hogy a megoldás csakis az üzleti, informatikai és biztonsági csapatok együttműködésének előmozdításával, az ösztönzők összehangolásával, továbbá a kiberbiztonság és a rugalmasságszélesebb üzleti stratégiába történő beágyazásával lehetséges. Ennek sikere pedig legalább annyira emberi, mint technikai kérdés.

A korlátozott megközelítés veszélyei

Sok vállalat és szervezet úgy reagál a digitális zavarokra, hogy jószerint csak a megfelelőségre vagy a fenyegetések csökkentésére összpontosít, anélkül, hogy foglalkozna a zavarok tágabb üzleti hatásaival, következményeivel. A korlátozott megközelítés ráadásul figyelmen kívül hagyja a biztonsági réseket. Például, a számítástechnikáért felelős részleg számára triviálisnak tűnő eszközök fontosak lehetnek a vállalkozás egészének. Emellett ez a megközelítés értékes időt és erőforrásokat is elfecsérel, sőt késleltetheti az üzleti tevékenység élénkítését is.

A felügyeleti hatóságok hamar felismerték, hogy a rossz kiberbiztonsági és adatvédelmi gyakorlat kockázatot jelent az adott vállalkozás gazdasági stabilitására, a befektetők által elvárt átláthatóságára és a fogyasztók elégedettségére is. A mesterséges intelligencia gyors bevezetése, amely minden más technológiánál gyorsabban fejlődik és számos korábbi szabályozás megváltoztatását teszi indokolttá, sőt szükségessé, csak növeli a tétet. Nem véletlen, hogy a felügyeleti szervek nemcsak a szakmai vezetés felelősségét vizsgálják, hanem esetenként a bekövetkezett digitális zavarok és az adatszivárgások miatt a felső vezetők és az igazgatótanácsok felelősségét is.

A vállalatok és szervezetek erre sokszor a meglévő folyamataik újragondolása helyett újabb és újabb fejlesztésekkel reagálnak. Meghúzzák a lazának tűnő csavarokat, ám a megfelelésre való túlzott törekvés, valamint a sűrűsödő ellenőrzések gyakran merev hozzáálláshoz vezetnek. Így fordulhat elő, hogy az ügyfelek a kiberbiztonsági szabályok megtartására való görcsös törekvéseket nem az ő érdekükben hozott intézkedésként, hanem az innováció, a digitális átalakulás és az MI-alapú megoldások bevezetésének lassításaként élik meg.

A silók „csatája”

A számítástechnikáért, a biztonságért és az üzletmenetért felelős részlegek tevékenysége egymással óhatatlanul szoros kapcsolatban áll, ám a szoros együttműködést sokszor mégsem tekintik elemi követelménynek.

A számítástechnikai részlegekre gyakran erős nyomás nehezedik az innovációk mihamarabbi bevezetése érdekében. A szoros határidők betartására irányuló elvárások miatt azonban többnyire csak a funkcionalitást és a funkciókat helyezik előtérbe

a biztonsággal szemben. Sőt, egyes informatikai vezetők túlságosan bürokratikusnak tartják a biztonsági követelményeket, és úgy döntenek, hogy azok kiiktatásával takarítanak meg időt. Emiatt az alapvető folyamatok, például a robusztus eszközkezelés vagy a vállalati architektúra hiánya következik be, ami megnehezíti a digitális infrastruktúra hatékony nyomon követését és védelmét.

A jogszabálykövetésért felelős részleg (compliance) tevékenysége kockázatkerülő és elszigetelt. A mindennemű szabálysértés kivédésére összpontosító kockázatkerülő gondolkodásmódjuk óhatatlanul súrlódásokhoz vezet az informatikai és üzleti csapatokkal. A compliance részleg vezetését általában arra ösztönzik, hogy a cég mindenáron kerülje el a jogsértéseket, akár az innováció rovására is. A compliance részlegek jellegzetes kommunikációs stílusa – teletűzdelve jogi szakzsargonnal és tengernyi mérőszámmal – könnyen elidegenítheti a többi érdekelt felet. Nem meglepő, hogy a compliance részleget gyakran kizárják a digitális kezdeményezések, például a mesterséges intelligencia alkalmazási koncepciója kidolgozásának korai szakaszából, ami viszont korlátozza a hatékony fékek és ellensúlyok integrálásának képességét.

Az üzleti részleg vezetői olyan prioritásokra összpontosítanak, mint az árbevétel növelése, az ügyfelek lojalitásának megőrzése és erősítése, valamint a működés hatékonysága. Bár elismerik a kiberbiztonság fontosságát, sokukból hiányzik a kockázatok felméréséhez vagy a befektetések hatékony rangsorolásához szükséges technikai ismeret. Ez a hiányosság gyakran az informatikai és biztonsági részlegre való túlzott hagyatkozáshoz vezet anélkül, hogy megfelelő felügyeletet vagy összehangolást biztosítana. Ha pedig fennakadások lépnek fel, akkor könnyen előfordulhat, hogy az üzleti vezetők nincsenek felkészülve a hatékony válaszadásra.

Összehangolás a sikerért: egységes megközelítés

A három terület munkájának összehangolása a leghatékonyabb eszköz a legfontosabb üzleti szolgáltatások védelmére, a kockázati forgatókönyvek tesztelésére, valamint a megfelelő képzés, tudatosság és kommunikáció fenntartására. Megfelelő összehangolt intézkedések révén a vállalkozások és a pénzügyi intézmények a kiberbiztonságot és a digitális ellenállóképességet versenypozíciójuk javára fordíthatják. De mit kell ehhez tenni?

1. A célokat és az ösztönzőket össze kell hangolni. A vállalatoknak és szervezeteknek olyan egységes célokat kell maguk elé tűzni, amelyek egyensúlyt teremtenek valamennyi érdekelt fél prioritásai között. Így például az informatikai rendszer gyorsaságát vagy a mesterséges intelligencia fokozott használatát az olyan üzleti célok eléréséhez is köthetik, mint az ügyfelek bizalmának vagy a piaci versenyképességnek növelése. Az együttműködés ösztönzése érdekében az IT-, a biztonsági és az üzleti csapatoknak közös ösztönzőkkel kell rendelkezniük.

2. Közös nyelv kialakítása. A közös szókincs és zsargon hiánya komoly akadályt jelent az erőfeszítések sikeres összehangolásban. Amikor a számítástechnikai, illetve a biztonságért és az üzleti eredményért felelős vezetők elbeszélnek egymás mellett, elkerülhetetlen a zűrzavar és a késedelmek bekövetkezése, majd a kudarcoknak egymásra történő áthárítása. Az esetleges problémák egységes értékelése viszont lehetővé teszi, hogy a biztonsági vonatkozású informatikai incidensekről valamennyi részleg azonnal értesüljön. Emellett a képzések vagy workshopok tovább erősíthetik a közös nyelv kialakítását, elősegítve egymás jobb megértését és az együttműködést. A műszaki embereknek képeseknek kell üzleti fejjel gondolkodniuk és üzleti nyelven „beszélniük”, az üzletembereknek pedig meg kell érteniük az alapvető digitális fogalmakat. Minden alkalmazottnak tisztában kell lennie azzal, hogyan védheti meg az adatokat, függetlenül attól, hogy azokat nagy nyelvi modellüzenetekben használják-e, vagy adatbázisban tárolják.
3. Erősíteni kell a tehetségek sokoldalúságát. Egy jól összehangolt szervezet felépítéséhez olyan vezetőkre van szükség, akik képesek áthidalni a technikai és az üzleti megközelítés között esetenként tátongó rést. A biztonságért felelős vezetőknek meg kell ismerniük a vállalat működését, a gyárak bejárásától az értékesítésért felelős munkatársakkal való kapcsolattartásig. Hasonlóképpen, az informatikai és üzleti vezetőknek jobban meg kell érteniük a kiberbiztonság kritikus szerepét, és a stratégiai megbeszélésekre már a kezdetektől fogva meg kell hívni a biztonságért felelős szakembereket.
4. Kiforrott, összekapcsolt munkafolyamatok kialakítása. A szervezeteknek integrálniuk kell a kiberbiztonságot az alapvető informatikai és üzleti munkafolyamataikba, például a vállalati architektúra, az eszközkezelés és az incidenskezelés terén. Ezeket a folyamatokat úgy kell kialakítani, hogy megkönnyítsék a zökkenőmentes együttműködést, lehetővé téve az egyes részlegek számára, hogy gyorsan és hatékonyan tudjanak reagálni az esetleges fennakadásokra.

A számítástechnikai, a biztonsági és az üzleti részlegek összehangolt együttműködésének kialakítása ugyan rendkívül összetett és kihívásokkal teli feladat, ám elk engedhetetlen az eredményes működéshez. Ehhez létfontosságú a vezetés kitartása, elkötelezettsége, valamint annak képessége, hogy a fennálló állapotokat folyamatosan megkérdőjelezze és fejlessze. A tevékenységet sikeresen összehangoló szervezetek teljes mértékben képesek kiaknázni a digitális kezdeményezéseikben rejlő üzleti lehetőségeket, miközben csökkentik az adatszivárgások és a működési zavarok kedvezőtlen hatását, ha incidensek történnek (és minden bizonnyal történnek is). Emellett vezető szerepet töltenek be a rugalmasság, az innováció és a növekedés terén is.

Kiberbiztosítás

23. TÁBLÁZAT: A kiberbiztosítás fejlődése a ’90-es évektől

1990-es évek	2000-es évek	2010-es évek
Az önálló termékek az 1990-es évek közepén/végén jelentek meg az Egyesült Államokban. A szakmai felelősségi szabályzatból, a szakmai hibákból és mulasztásokból eredő károkra fedezetet nyújtó E&O-ból és a vállalatvezetés hibáival és döntéseivel kapcsolatos felelősségre kiterjedő D&O módozatokból fejlődött ki. Az első irányelveket az online tartalomnak vagy szoftvernek való kitettség kezelésére írták. Ezek az „internetes biztosítási” kötvények: számítógépes biztonsági hibákra korlátozódtak; nem nyújtottak fedezetet az adatvédelmi incidensből eredő belső költségekre; és nem terjedtek ki a nem elektronikus iratokra vagy a véletlen nyilvánosságra hozatalra.	Az online médiairányelvekben megjelentek a „jogosulatlan hozzáférés”, a „hálózati biztonság” és a „vírusok” okozta veszteségek. Voltak azonban jelentős kizárások (pl. szélhámos alkalmazottak intézkedései és hatósági bírságok). A 2000-es évek közepén fedezetet vezettek be a belső alkalmazottak által okozott egyes veszteségekre (pl. számítógépes üzlet megszakítása, kiberzsarolás), és a véletlen adatszivárgásból származó károkra. Az Egyesült Államok adatvédelmi szabályozása katalizálta a termékinnovációt, beleértve az IT kriminalisztika, PR és ügyfélértesítés költségeivel kapcsolatos védelmet.	Az önálló termékekkel rendelkező szolgáltatók számának növekedése, nem csak az Egyesült Államokban. Az informatikára való fokozott támaszkodás és a nagy horderejű hackerbotrányok világszerte felpörgették a kiberbiztosítások iránti keresletet (mind a dedikált fedezetet, mind a hagyományos vagyon- és balesetbiztosítási szerződések támogatását). Az uniós hatóságok megállapodásra jutottak az adatvédelmi reformról: a jogszabályokat 2018-tól kell végrehajtani. Hatályba lépnek más joghatóságok adatvédelmi törvényei, amelyek felhívják a figyelmet a kiberfenyegetésekre és a védelem szükségességére. A biztosítók külső informatikai szakértőkkel működnek együtt, hogy jobban megértsék a kiberkockázatokat.

Forrás: Szerzők összeállítása a Swiss Re és a Munich Re anyagainak a felhasználásával

A biztosításnak helye van a vállalati kockázatcsökkentési stratégiában, így természetesen a kiberkockázat kezelésében is. A kiberbiztosítások fő rendeltetése, hogy egy kibertámadás esetén a biztosító átvállalja a „talpraállás” és a rendszerek helyreállítáá sának költségeit. Sok magyar vállalat számára a kiberbiztosítás egyelőre még rejtély, de a nemzetközi trendekben a kiberbiztosítások már erősen jelen vannak. Bár globálisan sem kellőképpen ismertek, de egyre több külföldi vállalat köt már ilyen biztosítást. A Munich RE piacvezető viszontbiztosító szerint a kiberbiztosítások piaca gyorsan növekszik: a globális kiberbiztosítási piac mérete 2023-ban 16,66 milliárd dollár volt. Az előrejelzések szerint a piac a 2024-es 20,88 milliárd dollárról 2032-re 120,47 milliárd dollárra nő, vagyis az előrejelzési időszak alatt 24,5%-os összetett éves növekedési rátát (CAGR-t) mutat.

Egy 2022-es felmérés adatai szerint kibertámadás esetén mintegy félmilliárd forintjába kerül egy nagyobb vállalatnak a talpraállás, ami már teljes egészében magában foglalja az adatvisszaállítás költségét is. A kiberbiztosításról azt is érdemes tudni, hogy bár a legtöbb vállalat proaktívan törekszik a kiberkockázatok kezelésére, közülük mégis nagyon kevesen gondolják komolyan, hogy biztosítást is kössenek. Magyarországon ez a szolgáltatás még nem terjedt el, de nemzetközi szinten egyre inkább növekszik a kiberbiztosítással rendelkező cégek száma. Ha ugyanis mindenféle megelőzést szolgáló intézkedés ellenére is kibertámadás ér egy vállalatot, a kiberbiztosítás csökkentheti az úgynevezett maradványkockázatokat, illetve fedezheti a helyreállítási költségeket is.

Létező és látens biztosítások

Nagyon fontos tisztázni, hogy a kiberkockázatokkal kapcsolatban kétféle biztosítás létezik. Az egyik a vagyoni kockázat biztosítása, ami fedezetet nyújt a vállalkozásoknak az online térben elszenvedett károk – például adatszivárgás, kibertámadás vagy zsarolóvírus – okozta veszteségekre és javarészt a szoftver-meghibásodások, valamint az infrastruktúra-meghibásodások okozta károkra is. A kiberbiztosításoknak többnyire kulcsfontosságú jellemzője az átfogó biztosítói segítségnyújtás káresemény esetén, mint például 24 órás forródrót a kiberincidensek bejelentésére. Egyes biztosítók közvetlen technikai támogatást is nyújtanak a kötvénytulajdonosoknak az incidensre adott válaszok és a számítástechnikai kriminalisztikai szolgáltatók révén. Káresemény bekövetkezése esetén a gyors reagálás nem csupán jószolgálati tevékenység, ugyanis a biztosítóknak is elemi érdeke a kár minimalizálása. A kiberbiztosítások esetében mindig az adott biztosító kínálata határozza meg, hogy mely piaci szegmensek számára és milyen típusú károk fedezésére kínál biztosítást. Ezért fontos, hogy alaposan tájékozódjunk mind a hazai, mind a külföldi piacon, hogy megtaláljuk az adott igényeknek leginkább megfelelő biztosítási feltételeket és káreseményeket lefedő konstrukciót.

A másik típusú biztosítást a felelősségbiztosítások köre jelenti. A felelősségbiztosítások olyan károkra nyújtanak fedezetet, amelyeket az adott cég ügyfelei szenvednek el egy kiberincidens következtében. Külföldön már létezik GDPR-felelősségbiztosítás és NIS2 felelősségbiztosítás is, de ilyen kötvény egyelőre nem érhető el hazai biztosítóknál. A Magyarországon tapasztalható lemaradást ezen a területen minden szektor megszenvedi, legyen az akár az infrastruktúra, akár a szolgáltatások, a felhőszolgáltatások piaca, vagy bármely egyéb terület. A lemaradás a fő oka az, hogy a hazai biztosítóknak nincs még kellő kibervédelmi ismerete és kárstatisztikai adatbázisa. Nem ismerik még alaposan a hazai kiberkockázatokat és kockázati kitettséget, s ezért nem is képesek még megfelelő terméket kínálni. Nincs továbbá kiforrott tapasztalatuk a felelősségbiztosítás árazására sem, ezért sem léptek még ilyen termékkel a piacra. Ám mivel Nyugat-Európában ilyen termékek már léteznek, előbb-utóbb megjelennek majd Magyarországon is, főleg a NIS2 által előírt kiberbiztonsági auditálást követően.

Az említett lemaradásban az is szerepet játszik, hogy egyelőre nem mutatkozik nagy kereslet a felelősségbiztosítások iránt. Sok cég véli úgy még külföldön is, hogy az

egyre inkább digitalizált és egymással egyre szorosabban összefonódó ellátási láncokon belül saját szervezete kisebb kiberbiztonsági kockázatot jelent partnerei és beszállítói számára, mint fordítva. Ez azonban többnyire olyan önáltatás, amit a tények egyáltalán nem támasztanak alá.

A kötelező kiberaudit bevezetése azonban feltehetően a felelősségbiztosítás téren is hoz majd változást, hiszen a biztosítók kockázata nagymértékben függ attól, mennyire erős és kiforrott a felelősségbiztosítást kötni kívánó cégnél a kiberkockázat kezelése. A biztosítási célú kiberkockázat-értékelések magukban foglalhatják a kiberauditok megismerését, illetve a biztosítók helyszíni látogatásait, amelyek során interjúkat készítenek az informatikai vezetőkkel, hogy megértsék a vállalat kiberkockázati kitettségét, valamint az érvényben lévő ellenőrzési folyamatokat és a megvalósított védelmet.

A kiberkockázat persze nem tekinthető csupán technológiai kérdésnek, mert része az üzleti kockázatnak, s ezért stratégiai vállalati kockázatkezelés keretében kell foglalkozni vele. Ennek megfelelően a technológiai beszerzéseket és a kockázatátháríási intézkedéseket olyan befektetési stratégiába kell illeszteni, amely tükrözi a szervezet egyedi kockázati profilját és kockázatvállalási hajlandóságát.

Alternatív termékek és az insuretech

A befektetők érdeklődése a kiberkockázatok megvásárlása iránt egyelőre csekély, mivel a kockázat mértéke és az időben korlátozott kitettség nem mindig átlátható a befektetők számára, ez pedig korlátozza a biztosítók által vállalható kockázatok körét.

A biztosítási piacon ugyanakkor az elmúlt évtized során megjelentek az insurtech vállalatok. Ezek a vállalkozások olyan fejlett technológiákat alkalmaznak, mint a mesterséges intelligencia, a big data és a blokklánc, amelyek használatával átalakítják a biztosítás különböző aspektusait a terméktervezéstől és a kockázatértékeléstől kezdve a kárigények feldolgozásáig és az ügyfélszolgálatig. Így például algoritmikusan levezetett biztonsági besorolásokat és benchmarkokat, valószínűségi kibermodelleket; technikai és viselkedésalapú veszteségbecslési modelleket, továbbá olyan kiberkockázat-modellező és -előrejelző platformokat is alkalmaznak, amelyek több százezer vállalat kiberrezilienciájára vonatkozó adatainak segítségével számítanak ki biztosítási benchmarkokat, előrejelzéseket és készítenek becslést a várható veszteségekre.

Az insurtech cégek a biztosítóknak nyújtott szolgáltatások mellett különféle kocü kázati szolgáltatásokat is kínálnak közvetlenül a biztosítási kötvények tulajdonosainak. Egyebek között egy olyan szabadalmaztatott személyazonosság-ellenőrző botot is, amely folyamatosan szerez be élő digitális adatokat és gépi tanulás segítségével holisztikus ügyfélazonosító modellt hoz létre.

Mire kell figyelemmel lenni kiberbiztosítás megkötésekor?

A piacon lévő biztosítási termékek gyakran lényeges részletekben különböznek egymástól. Az optimális biztosítás kiválasztása ezért gyakran korántsem egyszerű feladat.

Célszerű megbízható független biztosítási alkuszhoz fordulni, és részletes tanácsot kérni. A biztosítási szerződés megkötése előtt pedig elengedhetetlen a megfelelő kockázatelemzés ahhoz, hogy a vállalat meg tudja határozni tényleges biztosítási igényét, és ezáltal kiválaszthassa a maga számára optimális terméket.

Figyelmet kell arra is fordítani, hogy a biztosítási kötvény tartalmaz-e a biztosítást kötő cég vezetése számára olyan előírásokat (pl. a cégvezetés ellenőrzési kötelezettségét), amelyek be nem tartása esetén a biztosító megtagadhatja a kártérítést.

Ugyancsak figyelemmel kell lenni arra, hogy a kiberbiztosítás jellemzően nem terjed ki a biztosítást kötő társaság pénzügyi vagyonát érő kockázatokra. Ez konkrétan azt jelenti, hogy például a kibercsalás miatt teljesített kifizetésekre nem terjed ki a biztosítás.

Hogyan köthető meg kiberbiztosítás?

A kis- és középvállalkozásoknak többnyire egy rövid (1-2 oldalas) űrlapot kell kitölteniük; a nagyvállalatok számára pedig részletesebb kockázati kérdőívek állnak rendelkezésére. Fontos, hogy a kockázatokkal, de különösen az adatmentéssel kapcsolatos kérdésekre őszinte választ adjon a biztosítást kötni szándékozó cég, mert a pontatlan vagy hamis nyilatkozat a kártérítés megtagadásához vezethet.

Kössön-e a vállalat kiberbiztosítást – igen vagy nem?

A kibertámadások áldozatává válásának kockázata évről évre jelentősen nő. A koronavírus-válság fellendítette a digitalizációt, és ezzel növelte a támadási felületet, jelenleg pedig a geopolitikai bizonytalanságok játszanak a kiberbűnözők kezére. Különösen a kis- és középvállalkozások kiszolgáltatottabbak a kiberbűnözőkkel szemben, mivel gyakran nem rendelkeznek elegendő emberi és pénzügyi erőforrással ahhoz, hogy intenzíven foglalkozzanak a védekezéssel.

Az szinte magától értetődik, hogy a kiberbiztosítás nem általános gyógyír és nem is helyettesíti vagy pótolja a megfelelő vállalati kiberbiztonsági intézkedéseket. Ugyanakkor fontos és hasznos kiegészítője a vállalati biztonsági intézkedéseknek, ezért megkötése minden iparágban és minden méretű vállalat számára megfontolandó. Különösen akkor, ha az információs technológia fontos része a vállalat üzleti folyamatainak. Így például a szállodák vagy szupermarketek informatikai rendszereit ért támadások megbéníthatják a pénztárgépeket, a készletnyilvántartási vagy a szobafoglalási rendszert, és elhúzódó fennakadásokhoz vezethetnek. A feldolgozóipar esetében pedig a számítóó géppel vezérelt gyártás vagy megmunkálás bénulhat le huzamosabb időre egy vírusos támadás esetén.

A kiberbiztonság belső veszélyeztetése

A hagyományos biztonsági eszközöket, mint például a tűzfalak és a végpontfigyelő programok, elsősorban a kívülről érkező támadások észlelésére és elhárítására tervezték, nem szolgálnak a belülről szándékosan indított vagy gondatlanságból eredő – úgynevezett bennfentes – támadások elleni védelemre. Ennek megfelelően a

hagyományos felderítési eszközök általában hatástalannak bizonyulnak az ilyen jellegű támogatások felismerésében. Ugyanakkor különböző okoknál fogva a vállalati informatikai rendszerek biztonsága a való életben belülről is komoly fenyegetésnek van kitéve, akár a vállalat alkalmazottai, akár a beszállítói vagy a vevői részéről. A bennfentes fenyegetettségnek számos indoka lehet: legtöbbször vélt vagy valós személyes sérelem megtorlása, vagy anyagi haszonszerzés. A bennfentes támadások azért különösen veszélyesek, mert – mint említettük – a kibervédelmi rendszerek többnyire a külső, idegen támadások megelőzésére, elhárítására irányulnak, a munkatársak és az üzleti partnerek tekintetében viszont hallgatólagosan feltételezik a lojalitást. Tapasztalatok alapján a biztosítók a bennfentes támadásokat eleve kizárják a biztosítható kockázatok köréből, főleg mert ezek nem modellezhető mintákat követnek. A bennfentes támadások kockázataira ezért minden vállalkozásnak kellő figyelmet kell fordítania. Természetesen ezzel nem azt kívánjuk sugallni, hogy eleve bizalmatlannak kell lenni a munkatársakkal és az üzleti partnerekkel szemben, hanem csupán azt, hogy oda kell figyelni minden szokatlan, indokolatlan adatgyűjtési, adatkezelési magatartásra.

A hagyományos korrelációs szabályok alkalmazása a biztonsági információ- és eseménykezelő (security information and event management – SIEM) rendszerekben csak korlátozottan képes észlelni a bennfentes fenyegetéseket, legalább három okból eredően:

1. A korrelációs szabályok statikusak (csak azt észlelik, ha előre megadott nagyságú eltérés következik be az előre beprogramozott feltételekhez képest), ezért hatástalanok a dinamikus felhasználói tevékenységekkel szemben.
2. A helyi sajátosságoktól függetlenül ugyanazok a szabályok vonatkoznak minden entitásra, ami gyakori téves vészjelzést válthat ki.
3. A korrelációs szabályokat jellemzően rövid időtávra szokták meghatározni, ezért nem képesek figyelembe venni a folyamatosan, ám lassan végbemenő változásokat.

A hálózaton végbemenő felhasználói tevékenységek dinamikus természetűek, és olyan környezetet hoznak létre, amely folyamatosan változó állapotban van. Ebből eredően a helyi kontextus vizsgálata nélkül alkalmazott hagyományos statikus módszerek nem is képesek kiszűrni a valóban veszélyes bennfentes fenyegetéseket.

A bennfentes fenyegetés észlelésének és elhárításának korszerű módszerei

A gépi tanuláson (ML) és más mesterséges intelligencia-fejlesztéseken alapuló SIEM-ek új generációja már megfelelő elemzési lehetőségeket kínál a bennfentes fenyegetések észlelésére. Az ML-alapú módszereket felhasználói és entitási viselkedéselemzésének nevezik (user and entity behavior analytics – UEBA). A sikeres UEBA hálózati és biztonsági naplókat gyűjt, aktív címtárat és más identitásszolgáltatókat, továbbá

adatvesztés-megelőzési eszközöket alkalmaz. Az így gyűjtött adatok elemzése teljes körű képet ad a felhasználók és az eszközök viselkedéséről változásairól. Az egyes felhasználók és eszközök tevékenységének hosszú távú figyelemmel kísérésével, a helyi kontextusok vizsgálatával, valamint a hitelesítő adatok és eszközök közötti kapcsolatok feltárásával egy adattudományon alapuló rendszer minimális tévedéssel képes azonosítani a kiszűrni kívánt anomáliákat.

Bemutatunk néhány, a hétköznapitól a súlyosig terjedő valós példát a bennfentes alapú támadásokra:

- Egy értékesítési menedzser lemásolja az aktuális vevői és folyamat-előrejelzéseket, mielőtt „átigazolna” egy versenytárshoz.
- Egy mérnök egy olyan startup vállalkozást alapít, amely majd versenybe száll a jelenlegi munkaadójával, ezért a cégtől való távozása előtt még lemásolja az új termékek dokumentációját.
- Egy IT-menedzser a közzététel előtt megszerzi a cége negyedéves gyorsjelentésének adatait, és ezek birtokában bennfentes kereskedést folytat a vállalat részvényeivel a tőzsdén.
- Egy tudós több ezer tervezési és műszaki dokumentumot másol le, hogy azokat eladja egy külföldi országnak. (Ez az ipari kémkedés leggyakoribb formája.)
- Egy hírszerző ügynökség hatalmas mennyiségű belső információt szerez meg illegálisan az ellenfél állami szervezeteitől, majd azt kiszivárogtatja a sajtónak.
- Egy adatelemző engedély nélkül visz haza egy személyes adatokat is tartalmazó merevlemezt otthoni munkavégzés céljából, de azt betörök ellopják a lakásából.
- Egy alkalmazottat telefonos adathalászat során megtévesztenek, és ennek következtében a támadó hozzáférést szerez az alkalmazott cégének belső hálózatához.
- Egy ügyfélszolgálati csoport alkalmazottja nagyobb összegért eladja a hitelesítő adatait egy hackercsoportnak.
- Egy mérnökgyakornok nem változtatja meg az alapértelmezett jelszót, így a fejlesztői környezet sebezhetővé válik, és ezzel kitárja az ajtót egy ellátási lánc elleni támadás számára.

A felsorolt esetekben a bennfentesek szokatlan vagy tiltott módon használták vagy fértek hozzá a rendszerekhez. Utólag visszatekintve mindegyik esetet időben lehetett volna észlelni és megakadályozni. Az ipari kémkedést folytató tudós például hosszú időn át tízszer gyakrabban lépett be a biztonságos fájlszerver-rendszerbe, mint egy átlagos alkalmazott hasonló a szerepkörben. Tény viszont, hogy a bennfentes kockázatok korai felismerése nagy kihívást jelent, hiszen a figyelmeztető jelek szétszórtan keletkeznek és nehezen is vonhatók össze.

Bennfentes fenyegetések és adatfolyam-észlelési pontok

Néhány gyakrabban észlelhető bennfentes fenyegetés színtere:

- **Végpontok.** Egy alkalmazott fájlokat másol helyi USB-kulcsra? Tett már ilyet korábban is? Olyan fájlkészletet másol, amelyek bizalmas adatokat, információkat tartalmaznak? A szokásosnál jóval több fájlt másol, mint máskor?
- **Fájlszerverek.** A vállalkozó hozzáfér a bizalmas fájlokhoz, és azokat helyben másolja? Hány fájlt olvas be? Hozzáfért már a vállalkozó ehhez a szerverhez?
- **Identitáskezelő rendszerek.** A rendszerbe bejelentkező személy alkalmazott vagy külsős vállalkozó? Melyik osztályon dolgozik, és milyen fájlokhoz fér hozzá? Hozzáférési jogai megfelelnek a jelenlegi feladatának? Szaporodtak, vagy módosultak a hozzáférési engedélyei az utóbbi időben?
- **Adatbázis szerverek.** Az adott személy jogosult hozzáférni ehhez az adatbázishoz? Milyen adatokat tekintett meg az elmúlt időszakban?
- **Kitűző-leolvasók.** Az adott személy máskor is ugyanabban az idősávban szokott be- és kilépni? Belépett-e valaha is ebbe az épületbe és a szerverszobába? Szükség volt a belépésére?
- **Nyomtatók.** A vizsgált alkalmazott küld-e névtelen fájlokat a nyomtatóra? (Gyakori adatlopási trükk ugyanis az érzékeny adatok másolása, azoknak új Word-dokumentumba történő beillesztése majd kinyomtatása.) A fájlokat munkaidő után nyomtatják ki, amikor mások nincsenek a közelben? A kinyomtatott oldalak száma nagyobb a szokásosnál?
- **Fejlesztési rendszerek.** A fejlesztők szabványos folyamatokat követnek? Létezik kódellenőrzési folyamat? A vizsgált személy követi a tanúsítványkezelés bevált gyakorlatait?
- **A felhőben.** Egy beszállító fájlokat helyez a OneDrive-ba vagy egy nem engedélyezett felhőtárolóba? Érzékenyek ezek a fájlok?

Adatfolyamok vizsgálata a bennfentes fenyegetés észleléséhez:

- **Helyi és távoli hozzáférési naplók.** Az internet, a virtuális magánhálózatok (VPN) és a Wi-Fi csatlakozási pontok naplói fontos jelzéseket adhatnak a kockázatos tevékenységekről.
- **Személyazonossági szolgáltatások.** A címtárszolgáltatások (Active Directory), a címtárhozzáférési protokoll (LDAP), a felhasználóazonosítási rendszerek (pl. Okta, és Ping Identity) és más szolgáltatások hasznos információkat nyújtanak a felhasználók hálózathasználati szokásairól.
- **Az adatvesztést megakadályozó** (Data Loss Prevention – DLP) eszközök, például a Broadcom/Symantec vagy a Netskope DLP termékei, különféle módszereket alkalmaznak a rendszerekben található és a hálózaton keresztül áramló bizalmas adatok észlelésére és azonosítására.

- **A PC/laptop biztonsági megoldások,** például a SentinelOne, a CarbonBlack vagy a Crowdstrike Falcon értékes kontextust biztosítanak a felhasználói fájltevékenységhez, valamint a rendszerkonfigurációhoz.
- **Hálózati hírcsatornák.** Bár a nettó áramlási adatok figyelése gyengébb viselkedési jeleket ad, kiegészítheti a SIEM-ből és a végponti megoldásokból származó adatokat.
- **Adatbázis tevékenység.** Közvetlenül az adatbázis-naplókból vagy adatbázis-tűzfalakon (például az Imperva) keresztül lehívható adatbázis-tevékenység naplózás hasznos rálátást nyújthat az érzékeny tábla-hozzáférésekre.
- **Alkalmazási tevékenység.** Az alkalmazástevékenység magában foglalja a hozzáféréssel kapcsolatos naplókat és a funkcionális tevékenységeket, valamint a kommunikációt is, ahol elérhető.
- **Felhőtevékenység.** A legtöbb nagy szervezet felhőalapú IaaS- vagy PaaS[13]-szolgáltatásokat használ az architektúrája részeként.
- **USB-meghajtó-hozzáférés.** A helyi fájlmásolás, általában egy USB kulcsra, fontos jelzéseket adhat, különösen, ha DLP-fájlvizsgálati ítéletekkel kombinálják.
- **Nyomtatószerverek.** A rosszindulatú bennfentesek táblázatokat nyomtathatnak ki papírra, hogy ezzel kikerüljék a digitális vizsgálati technikák „éberségét”.
- **Fizikai biztonság.** A kitűző-leolvasók adatokkal szolgálnak a megfigyelt védett épületekbe vagy szerverszobákba történő belépésekről, ezek időpontjáról és tartamáról.

A felsorolt adatfolyamatok mindegyike olyan adatokkal tud szolgálni, amelyeket adatlopás gyanúja esetén feltétlenül át kell vizsgálni.

Mindazonáltal az összes adathozzáférési és -felhasználási tevékenység összegyűjtése, az adatvesztés-megelőzés (DLP) eredményeinek integrálása , valamint ezek valós idejű értékelése olyan szintű szakértelmet és energiát igényel, amelyet kevesen képesek maradéktalanul biztosítani, legyen az akár rendszer, akár ember.

A telemetria és az összes adatfolyam által generált hatalmas mennyiségű adatot az emberek segítség nélkül nem képesek kezelni. A bennfentes fenyegetések pontos felméréséhez a gépi tanuláson alapuló technikák szükségesek a rögzített hozzáférési adatok feldolgozásához. Ehhez egy modern SIEM-nek a következő képességekkel kell rendelkeznie:

- **Viselkedési szokás mérése.** Felhasználónként és eszközönként a normál viselkedést leíró karakterisztikát kell meghatározni A kockázatpontozás segítségével ezután megállapítható, hogy egy új adathasználati tevékenység rendellenes-e és potenciálisan kockázatos-e.

13 IaaS (Infrastruktúra mint Szolgáltatás), PaaS (Platform mint Szolgáltatás) és SaaS (Szoftver mint Szolgáltatás), a felhőalapú számítás három legfontosabb szolgáltatási modellje.

- **Referenciacsoport (Peer group) elemzése.** Automatikusan összehasonlítja az egyes felhasználók viselkedését és hozzáférési mintáit az azonos szerepkörrel rendelkező többi felhasználó viselkedésével és hozzáférési mintáival. Kulcsfontosságú, hogy tudjuk, mi a normális. Az elsőre szokatlannak tűnő viselkedés ugyanis kevésbé gyanús akkor, ha a csoport többi tagjára is jellemző a minta.
- **Kiváltságos fiókok elemzése:** Az adminisztrátorok általában magasabb szintű hozzáférési jogokkal rendelkeznek, ami jelentős mennyiségű érzékeny adathoz való hozzáférést tesz lehetővé számukra. A kiemelt jogosultságokat be kell vonni a rendszer kockázatelemzésébe. Ezen kívül szorosan figyelemmel kell kísérni a kiváltságok bármely kiszélesítését.
- **Megosztott fiók elemzése.** A megosztott fiókok gyakran különös gondot jelentenek a szervezetek számára, mivel megnehezítik a kockázatos tevékenységeket végző felhasználók azonosítását. Sok esetben előfordulhat, hogy egy szervezet nem is ismeri a megosztott hitelesítő adatokat. A modern SIEM-nek képesnek kell lennie a megosztott fiókok felismerésére, az ezekhez a fiókokhoz kapcsolódó tevékenységek azonosítására és személyekhez való hozzárendelésére, továbbá testre szabható kockázati értékelést kell alkalmaznia ezen tevékenységekre.
- **Védett fiókok elemzése.** A fiókvédelemnek számos oka van, lehet jó-, de rosszindulatú is. A bennfentes fenyegetések elemzéséhez a SIEM-nek azonosítania kell azokat a felhasználókat, akik először próbálnak bejelentkezni egy védett fiókba, valamint azokat a védett fiókokat, amelyek egy korábbi munkakörükhöz kapcsolódhattak. Ezután azonosítania kell a hozzáférés körüli szokatlan tevékenységet, hogy a biztonsági elemzők különös figyelmet fordíthassanak a fiók egy bennfentes általi esetleges feltörésére.

Ha a rendszer több szokatlan viselkedést tanúsító felhasználót azonosít, akkor a legpasszívabb intézkedéstől kezdve (biztonsági elemző értesítése), az információadáson át (e-mail küldése egy alkalmazottnak a titoktartási kötelezettségére emlékeztetve) egészen a szélsőséges válasz kezdeményezéséig (a hozzáférés blokkolásáig) számos műveletet végrehajthat. A modern SIEM-ek gyakran automatizálják a választ, és csökkenthetik a lehetséges károkat.

Feltört hitelesítési adatok

Feltört hitelesítési adatok akkor fordulnak elő, ha egy jogosult felhasználó hitelesítő adatait a rosszindulatú szereplők szándékosan szerezték meg, mint például a Lapsus$ hackercsoport esetében, amikor azokat egy külső csoportnak adták el, majd vállalati erőforrásokhoz való hozzáférésre használták.

Az alábbiakban bemutatunk néhány olyan támadástípust, amelyet a valódi hitelesítő adatok megtalálására, ellopására vagy más módon történő megszerzésére használtak:

ADATHALÁSZAT

Üzenet küldése a felhasználónak egy olyan rosszindulatú hivatkozással, amely ráveszi a felhasználót arra, hogy adja meg érvényes jelszavát. Az adathalászat különösen nagy értékű fiókokat céloz meg, amelyek gyakran kiváltságos felhasználókhoz tartoznak.

JELSZÓ „PORLASZTÁS”

Hitelesítési próbálkozás ismert felhasználónévvel és gyakran használt, de nem hiteles jelszavakkal.

HITELESÍTÉSI ADATOK ÚJRAFELHASZNÁLÁSA

Más adatbázisokból ellopott felhasználónév és jelszó kombinációk használata abban a reményben, hogy azokat itt is felhasználták.

KEYLOGGERS HASZNÁLATA

Olyan rosszindulatú szoftver telepítése, amely naplózza a billentyűleütéseket, és továbbítja azokat a támadónak, hogy a kapott adatok alapján rekonstruálhassa a felhasználónevet és a jelszót. Az ilyen típusú rosszindulatú programok Bluetooth-alapú módszereket is tartalmaznak a hitelesítő adatok és jelszavak megszerzésére.

BRUTÁLIS ERŐ ALKALMAZÁSA

Hitelesítési kísérlet a lehetséges jelszavak listáján, például a szótárban lévő összes szó iterálásával, abban a reményben, hogy egyezik a valódi jelszóval.

SOCIAL ENGINEERING

A hackerek tisztában vannak azzal, hogy minden védelmi rendszer leggyengébb pontja az ember. A social engineering támadási módszer is erre felismerésre épít. E módszerrel a kiberbűnözők a célba vett felhasználókat oly módon manipulálhatják, hogy az áldozatok ne tartsák be a biztonsági- vagy egyéb üzleti folyamatok eljárásrendjét, és ezzel akaratlanul teret engedjenek a káros tevékenységeknek vagy az érzékeny információk kiszivárogtatásának. A social engineering magában foglalja a megvesztegetést, vagy a hitelesítő adatok megosztására, illetve „kölcsönadására” irányuló mesterséges kényszert is.

Védekezési módszerek

A felhasználói és entitási viselkedéselemzési (UEBA) módszerek SIEM-mel együtt csökkentik a veszélyeztetett eszközök által okozott fenyegetéseket azáltal, hogy létrehozzák az összes felhasználó hálózatban tapasztalt viselkedésének és hitelesítési adatainak mintázatát. Ezután kockázati pontszámokat lehet a szokatlan eseményekhez rendelni, majd vizualizációval jól megjeleníthetők az alapvonaltól való eltérések.

E módszerek alkalmazása jobb lefedettséget biztosít és alacsonyabb riasztási fáradtsággal jár, mint a statikus korrelációs szabályok használata.

Oldalirányú mozgás

Oldalirányú mozgásról akkor beszélünk, amikor a támadó megsérti vagy átveszi az irányítást egy hálózaton belüli eszköz felett, majd a hálózaton belül („keletről nyugatra"), az adott eszközről a többire vándorol. Általában ez a következő lépés, amelyet a támadó megtesz a hitelesítő adatok megsértése után. Míg az oldalirányú mozgás nem mindig szükséges ahhoz, hogy a támadó elérje céljait, általában további eszközök feltörésére van szükség ahhoz, hogy elérje azokat a rendszereket és jogosultságokat, amelyek lehetővé teszik számára, hogy hozzáférjen ahhoz, amit keres.

A támadók oldalirányú mozgásának végrehajtására használt módszerek a következők:

PORT VIZSGÁLAT

A támadók port-ellenőrző eszközöket, vagyis egy operációs rendszer kommunikációs végpontjait ellenőrző eszközöket használnak, például a network mappert, egy olyan eszközt, amely segít felfedezni és feltérképezni egy számítógépes hálózatot. Képes észlelni a hálózaton lévő eszközöket, azonosítani az IP-címeiket, és információkat gyűjteni a konfigurációjukról és szolgáltatásaikról. Lényegében egy hálózati topológiai térképet hoz létre, amely megmutatja, hogyan kapcsolódnak az egyes eszközök egymáshoz. Ez lehetővé teszi a kiberbűnözők számára, hogy olyan sebezhető végpontokat keressenek, amelyek segítségével behatolhatnak a rendszerbe, oldalirányban mozoghatnak, vagy más fiókokat találhatnak, amelyekkel feltörhetik a védett adatbázist.

TÁVOLI MUNKAASZTAL (REMOTE DESKTOP)

A rosszindulatú szereplő érvényes hitelesítő adatokkal, és a jogos felhasználónak a számítógépétől való távollétében, teljes hozzáférést szerezhet a megtámadott számítógéphez. Ezzel a hozzáféréssel a támadó büntetlenül mozoghat.

WINDOWS TÁMADÁSOK

A Windows Server Message Block (SMB) egy olyan protokoll, amely lehetővé teszi a felhasználók számára a hálózat más részeihez való hozzáférést anélkül, hogy folyamatosan meg kellene adni a hitelesítési adataikat. Ez az áteresztő hitelesítés hasznos ahhoz, hogy a jogosult felhasználók hozzáférjenek a hálózat más helyeihez. A támadók e protokoll parancsait használják a hálózaton történő mozgáshoz, például a PsExec hozzáférésmegtagadás megkerüléséhez.

HASH ÁTADÁS

A Pass-the-Hash (PtH) támadások során a támadó egy titkosított jelszókivonatot rögzít (nem pedig a jelszó karaktereit), hogy kihasználja a hitelesítési protokollt egy élő munkamenet során, és ezt használja a Security Accounts Manager (SAM), a Helyi biztonsági alrendszer (LSASS) folyamatmemórián, az Active Directory (AD) vagy a Credential Manager (CredMan) tárolón való áthaladáshoz.

GOLDEN ÉS SILVER TICKET TÁMADÁS

A Kerberos exploit során a támadó hozzáfér az ügyfél felhasználónevéhez és kivonatolt jelszavához. Ez lehetővé teszi a támadó számára, hogy hozzáférjen egy jegyet generáló jegyhez (TGT) egy Golden vagy Silver Ticket támadás során, és a tartományban bejelentkezzen egy tetszőleges fiókba.

A „PASS-THE-TICKET" (PTT) TÁMADÁS

A PtT egy olyan kiberbiztonsági támadás, amely a Kerberos hitelesítési protokollt célozza meg. Az ilyen támadás során az elkövetők ellopnak egy érvényes Kerberos jegyet (Ticket Granting Ticket - TGT vagy Service Ticket - TGS) egy feltört rendszerről, és ezt arra használják, hogy jogosult felhasználóként hitelesítsék magukat más hálózati erőforrásokon, anélkül, hogy az eredeti felhasználó jelszavát ismernék. A Golden és Silver Ticket támadásokhoz hasonlóan a Pass-the-Ticket támadások is kihasználják a Kerberos szinte javíthatatlan gyengeségeit a protokollban.

Lehetséges megoldások

Léteznek előre meghatározott szabályokat tartalmazó programok, amelyek kiszűrik az olyan tevékenységeket, mint a portszkennelés, a távoli asztalhoz való hozzáférés, a lehetséges Windows-támadásokat jelző eseménykódok, a hash és az aranyjegyek átadása.

A szabályok növelik a működési hatékonyságot azáltal, hogy kockázati pontszámokat adnak a rangsoroláshoz. Növelik az elemzők hatékonyságát is az oldalirányú mozgáson alapuló incidensek megoldásában, így órákról percekre csökkentik a szükséges időt. Ugyanakkor erősítik a biztonsági helyzetet is azáltal, hogy csökkentik az oldalirányú mozgás lehetőségét a hálózaton.

Mit kell figyelembe venni a bennfentes fenyegetésekkel szembeni védekezés során?

Ha a vállalat még nem rendelkezik bennfentes fenyegetés elleni programmal vagy védelemmel, akkor azt mielőbb be kell vezetnie. A következő tanácsok segíthetnek abban, hogy a vállalati védekezés átfogó és hatékonyan végrehajtható legyen.

1. A TERVEZÉSI CSAPAT ALAKÍTÁSA

Ahhoz, hogy hatékony védekezési programot lehessen létrehozni, egy olyan csoportot kell felállítani, amely teljeskörű ismeretekkel rendelkezik a vállalat műveleteiről, céljairól és sebezhetőségeiről. Ennek a csoportnak a biztonsági, informatikai, jogi, humánerőforrás és az üzleti részlegek képviselőiből kell állnia, továbbá az adatvédelmi tisztviselőt is be kell vonni (ha szervezet rendelkezik ilyennel). Ez a csapat irányelveket és működőképes eljárásokat dolgozhat ki, amelyek megfelelnek a szabályozási, szakpolitikai és jogi irányelveknek, lefedve a munkatársak belépésétől kezdve egészen a munkaviszony megszűnéséig terjedő valamennyi eseményt.

2. A KRITIKUS ESZKÖZÖK MEGHATÁROZÁSA

Ha a csoport megalakult, el kell készíteni a megfigyelendő eszközök térképét és meg kell határozni a fenyegetések fontossági (veszélyességi) sorrendjét. Ez magában foglalja mind a virtuális, mind a fizikai és a felhőalapú eszközöket, például a belső dokumentációt, kulcskártyákat, termékprototípusokat, SaaS-alkalmazásokat és az alkalmazottak adatait. A programnak elsődlegesen a legérzékenyebb eszközökre kell fókuszálnia, ugyanakkor az alacsony prioritásúakat sem szabad figyelmen kívül hagynia. Annak meghatározásához, hogy mely információk vagy hozzáférések tekintendők lényegesek, a tervezőcsoport útmutatásaira kell építeni. Miután kiválasztották a csoport tagjait, a csapat átfogó képet kap majd arról, hogy mit kívánnak elérni, illetve mire vágynak mások, milyen igényei vannak a többi érintett félnek. Hasznos lehet figyelőlisták létrehozása a legkritikusabb szolgáltatásokról, például kódtárakról, ügyféllistákról és egyéb érzékeny információkról, beleértve a tranzakciós rendszereket és a személyzeti adatokat. A csapatnak képesnek kell lennie arra, hogy azokra a kritikus eszközökre összpontosítson, amelyek kulcsfontosságúak a vállalkozás zavartalan működése és jövedelmezősége szempontjából.

3. FENYEGETÉSI KOCKÁZAT ÉRTÉKELÉSE

A műveletek jelenlegi állapotának és megfelelőségének felmérése segíthet azonosítani a meglévő, figyelmet igénylő biztonsági hiányosságokat. Ez a következőket foglalhatja magában:

- Rendszerkonfigurációk auditálása az ismert benchmarkok alapján,
- Beállítások rögzítése a megállapított házirend szerint,
- Behatolási teszt végrehajtása az alkalmazott eszközök hatékonyságának vizsgálata érdekében,
- Red-Blue teaming[14], azaz a folyamatok és az eszközök tesztelése eltérő csoportprioritás alapján.

Különösen a rendszereket és a védelmet kell felmérni annak érdekében, hogy képesek legyenek észlelni a jogosult felhasználóktól kiinduló fenyegetéseket. Ez azt jelenti, hogy tesztelni kell a gyanús viselkedésminták – mint például nagy mennyiségű adat hirtelen másolása – azonosításának képességét.

4. ALKALMAZOTTAK HÁTTÉRELLENŐRZÉSE

A fenyegetettség kockázatának megértéséhez az is hozzátartozik, hogy a cég tisztában legyen azzal, kik is valójában a csoport tagjai. Az egyik lehetőség a háttérellenőrzés. Ha valakit korábban vállalati visszaélés miatt elbocsátottak, erről tudni kell. Ha valaki jelentős pénzügyi nehézségekkel küzd, akkor ez is kockázatot jelenthet. A háttérellenőrzés azonban nem tévedésmentes, és hamis információkkal is szolgálhat.

14 A vörös csapat és a kék csapat két egymást kiegészítő megközelítés, amelyet a kiberbiztonságban használnak a szervezet biztonsági helyzetének javítására. A vörös csapatok támadásokat szimulálnak, hogy azonosítsák a sebezhetőséget, míg a kék csapatok védekeznek ezekkel a támadásokkal szemben, és reagálnak az incidensekre. Mindkét csapat együtt dolgozik, bár céljuk és módszereik eltérőek.

5. AZ INFORMÁCIÓBIZTONSÁGI ELLENŐRZÉSEK VÉGREHAJTÁSA ÉS KARBANTARTÁSA

Az adatok egyik legerősebb védelmét a hozzáférés korlátozása jelenti, még a bennfentes vezetők számára is. Mindenki számára csak a munkája elvégzéséhez feltétlenül szükséges adatokhoz indokolt hozzáférést adni. Ha valakinek ideiglenesen nagyobb hozzáférésre van szüksége, akkor az a tényleges szükség szerint tartalmi és időbeli korlátozással megadható. Az adatokhoz való hozzáférés korlátozása a hozzáférési szabályzatok és a titkosítás révén csökkenti annak lehetőségét, hogy az alkalmazottak visszaéljenek jogosultságukkal.

6. KI KELL DOLGOZNI A BENNFENTES FENYEGETÉS TIPIKUS ESETEIT

A tipikus esetek iránymutatásul szolgálnak arra vonatkozóan, mikor kell végrehajtani a program eljárásait – például, ha valaki nem a számára jóváhagyott felhőtárhelyet használja. A leggyakrabban előforduló problémák korábbi eseteinek dokumentálása segíthet a biztonsági csapatoknak abban, hogy megbízhatóan felügyeljék a lehetséges fenyegetéseket, és megfelelő lépéseket tegyenek a sérülékenységek megoldására. Ezeknek a felhasználási eseteknek tartalmazniuk kell a védelmi ellenőrzési eljárásokat (például fokozott biztonságot az alkalmazottak felvétele vagy elbocsátása esetén). Különösen elbocsátás (munkáltatói felmondás) esetén a legvalószínűbb a bennfentes fenyegetések előfordulása, ezért ezeket az eseteket különösen óvatosan kell kezelni. Ez a fajta nyomon követés egyébként a megfelelés vagy az iparág legjobb gyakorlatának követelménye.

7. KORSZERŰ MEGFIGYELÉSI ÉS ÉSZLELÉSI ESZKÖZÖKET KELL ALKALMAZNI

Lehet, hogy valaki már rendelkezik az összes szükséges biztonsági eszközzel, vagy azt tapasztalhatja, hogy a jelenlegi eszközei hiányoznak. Utóbbi esetben el kell kezdeni a hiánypótlásra alkalmas eszközök értékelését. Ez általában azt jelenti, hogy átfogóbb felügyeleti eszközöket kell alkalmazni – különösen azokat, amelyek viselkedéselemzési funkciókkal rendelkeznek. Előnyben kell részesíteni azokat az eszközöket, amelyek végponttól végpontig követhetik a felhasználói tevékenységet, és valós idejű láthatóságot biztosítanak. Célszerű olyan eszközöket is keresni, amelyek központosíthatják a műveleteket, beleértve a megfigyelési, naplózási, vizsgálati és riasztási képességeket, ha lehetséges. Ez a központosítás lehetővé teszi a rendszerállapotok alaposabb elemzését, és növeli annak esélyét, hogy korán észlelhetők legyenek a gyanús tevékenységek.

8. BENNFENTES FENYEGETÉSI KEZDEMÉNYEZÉSEK VIZSGÁLATA

A bennfentes fenyegetések kezelésére irányuló folyamatos erőfeszítések részeként alapvető fontosságú, hogy rendszeres időközönként ellenőrizzék az eszközöket, az engedélyeket és az eljárásokat. A rendszerek, a személyzet és a fenyegetések dinamikusak, ezért gondoskodni kell a változások követéséről. Az auditálás során figyelembe kell venni az

elavult vagy sérülékeny területeket, és ennek megfelelően átalakítani a programokat. Ha mégis előfordulnak incidensek, meg kell győződni arról, vajon adott-e visszajelzést az incidens-kezelési munkafolyamat. Egy incidens utáni frissítés elmaradása a fenyegetés ismétlődő előfordulását idézi elő.

Végül, elengedhetetlen az alkalmazottak biztonsági oktatása. Az adathalászat veszélyének tudatosításáról, a fizikai javak védelmének fontosságáról, valamint a „miért ne használjunk soha munkahelyi hitelesítési adatokat a munkával nem kapcsolatos eszközökben, webhelyeken vagy alkalmazásokban” témáról tartott megbeszélések kedvező változást hozhatnak.

Fejlett, bevált gyakorlatok a bennfentes fenyegetési programokhoz

A TERMINOLÓGIA ÖSSZEHANGOLÁSA A KULTÚRÁVAL

A vállalat programjában használt terminológiában az alkalmazottak szövetségesnek tekinthetők, vagy létrehozható egy „mi kontra ők” környezet. Ez utóbbit lehetőleg el kell kerülni. Például „bennfentes fenyegetési program” helyett érdemes inkább a „munkavállalói védelmi program” elnevezést használni. A semleges vagy barátságos terminológia használatával jóindulat mutatható ki a munkatársak irányába, és elkerülhető a sértődöttség keltése. Az együttműködés nyelvezetének használatával könnyebb alkalmazottakat toborozni az eszközök biztonságának fenntartása érdekében. Ha a munkatársak úgy érzik, hogy fontos részei a vállalat céljainak, nagyobb valószínűséggel osztoznak a felelősségen.

A SZÜKSÉGES BIZALOM KIÉPÍTÉSE

A védelmi programok sikerének záloga, ha világosan megfogalmazzák, miért lényeges ezek működtetése, milyen eseményeket követnek nyomon és milyen céllal teszik mindezt. Nem kell részletezni a rendszerek felügyeletét, de nem szabad elrejteni a vezetői szintű információkat sem. Ha az alkalmazottak tisztában vannak azzal, hogy megfigyelés történik, de nem érzik úgy, hogy személyesen ők lennének a célkeresztben, akkor nagyobb valószínűséggel bíznak meg a szervezetben és értékelik annak tevékenységét. Ez csökkentheti a rosszindulatú tevékenységek kockázatát, és növelheti annak esélyét, hogy az alkalmazottak gyanús eseményeket jelentsenek.

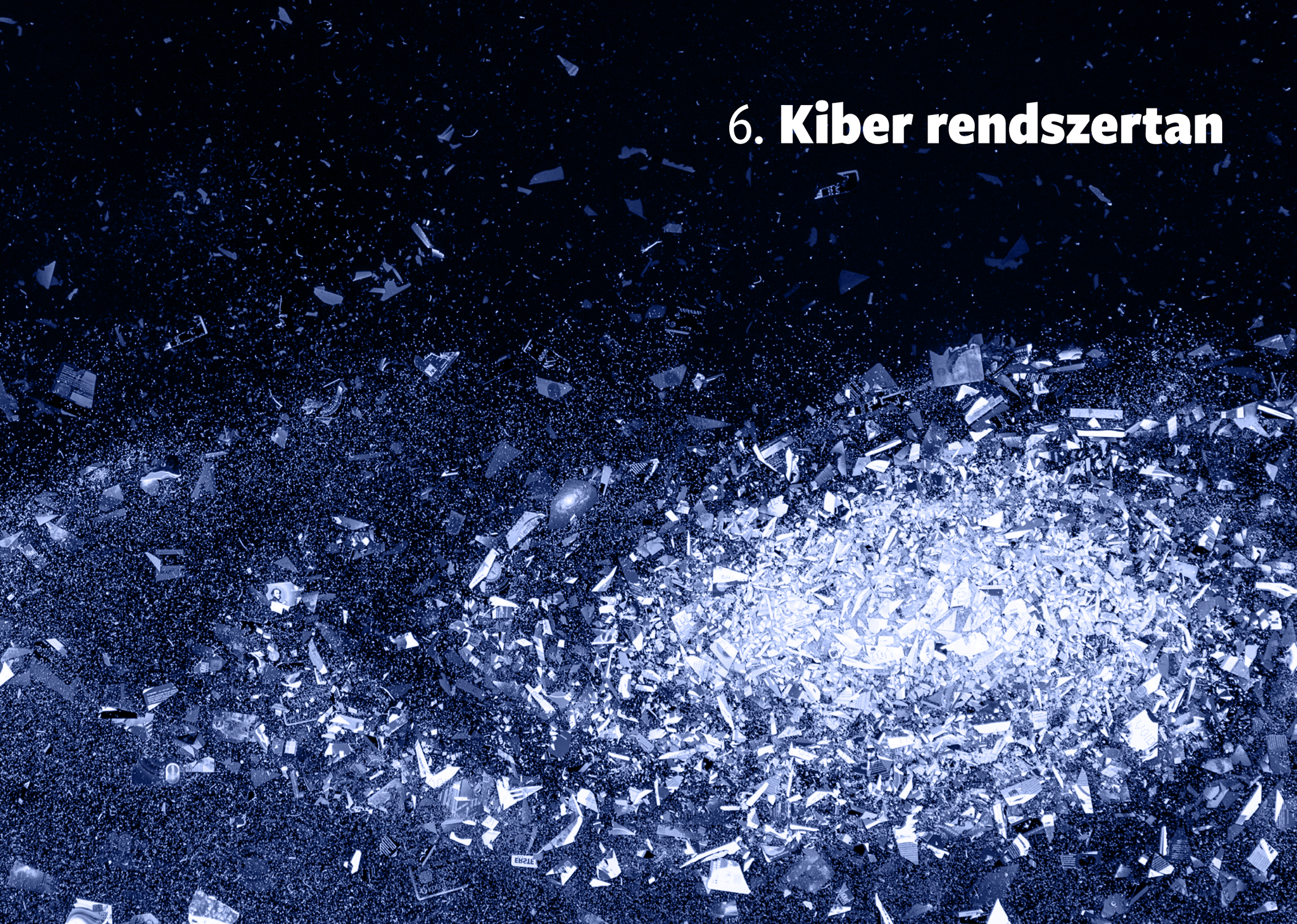
Meg kell könnyíteni az alkalmazottak számára a szokatlan és gyanús jelenségek bejelentését – legyen szó akár kapott e-mailekről, akár megfigyelt viselkedésről.

FÓKUSZBAN AZ AUTOMATIZÁLT FELÜGYELET

A rendszerek kézi vezérlése nem biztosítja az eszközök kellő lefedettségét és mélyzségét ahhoz, hogy a védelem valóban hatékony legyen. Az automatizált megfigyelés segít feldolgozni és elemezni a rendszerekből származó információkat, és lehetővé teszi a biztonsági csapatok számára, hogy a fenyegetések elhárítására és megelőzésére

összpontosítsanak. A vállalkozás védelme a bennfentes fenyegetésekkel szemben ugyanolyan fontos, mint a hagyományos, külső fenyegetésekre összpontosító kiberbiztonsági gyakorlatok. A bennfentes fenyegetéseket azonban gyakran sokkal nehezebb észlelni, mint a külső fenyegetéseket, ráadásul a vírusirtó és a tűzfal sem képes hatékonyan blokkolni ezeket.

6. Kiber rendszertan



A kibertámadások elleni hatékony védekezés egyik kulcseleme egy világosan strukturált osztályozási rendszer, amely elősegíti a támadások azonosítását és megértését. Egy ilyen taxonómia nemcsak a jogalkotók és a szabályozók, hanem az oktatók, a diákok, az érdeklődők és a potenciális áldozatok számára is hasznos. A kiberfenyegetések száma, formái és technikai komplexitása ugyanis folyamatosan növekszik, ami indokolttá teszi a rendszerezett megközelítést.

A kiberbűnözés mértéke

A kiberbűnözés, különösen a pénzügyi visszaélések formájában, egyre nagyobb hatást gyakorol a nemzetgazdaságra és a pénzügyi rendszer iránti bizalomra. E jelenségek vizsgálata kiemelten fontos a bűnüldöző szervek, a felügyeleti hatóságok, a pénzügyi intézmények, az oktatók és a felhasználók számára, hogy hatékony megelőzési és reagálási stratégiákat dolgozhassanak ki.

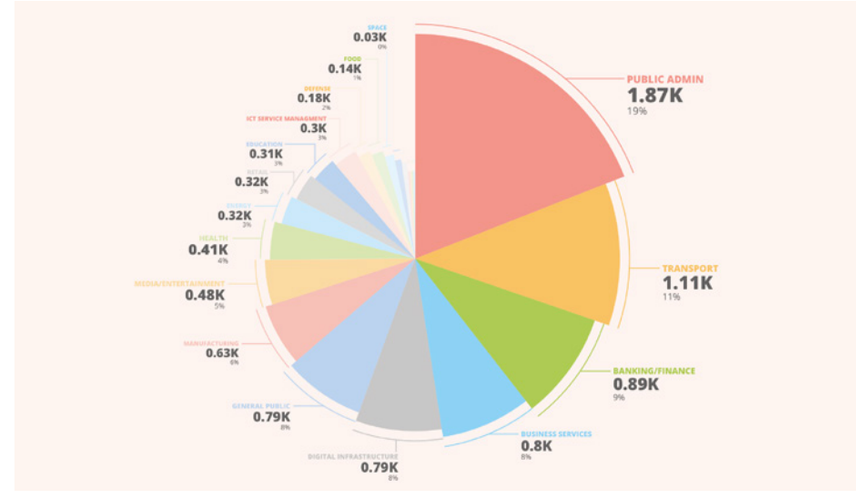
A védekezés nemcsak technológiai eszközöket, hanem tudatosítási és oktatási tevékenységet is igényel, különösen a potenciális áldozatok és a kibervédelemmel foglalkozó szakemberek képzése révén.

Az elmúlt években, különösen az elmúlt évtizedben, jelentős átalakuláson ment keresztül a pénzügyi bűnözés jellege és megjelenési formája. A hagyományosan fizikai térben elkövetett bűncselekmények – mint például a pénzlopás vagy a bankrablás – egyre inkább a digitális környezetbe, a kibertérbe helyeződtek át (Jaishankar, 2007). Ez a folyamat nem csupán technológiai, hanem strukturális és jogi kihívásokat is generál. A Mastercard „A kiberbűnözés kora” című jelentésében hangsúlyozza, hogy „[a] kiberbűnözés olyan, mint bármely más bűncselekmény, ezért ennek megfelelően kell kezelnünk. Ha pénzt hoz, felível” (Mastercard, 2025). Ez a megállapítás rávilágít arra, hogy a digitális vagyon elleni bűncselekmények nemcsak gyakoribbá váltak, hanem nemzetközi jelleget is öltöttek, tovább nehezítve az ellenük való fellépést. Ennek következtében a kiberbűnözés napjainkra a globális biztonságpolitika egyik legégetőbb problémájává vált. Magyarországon például a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) által közzétett adatok szerint 2024-ben mintegy 13 000 személy vált valamilyen formában kiberbűncselekmény áldozatává, amely esetek összesített anyagi kára megközelítette a 30 milliárd forintot (SZTFH, 2024). Ezek az adatok is alátámasztják, hogy a kiberbűnözés a 2020-as évekre rendszerszintű és általános társadalmi-gazdasági problémává vált Magyarországon is. Fontos hangsúlyozni, hogy a kiberbűncselekmények hatása nem egyenletesen oszlik meg az egyes ágazatok között. Az Európai Unió Kiberbiztonsági Ügynöksége (European Union Agency for Cybersecurity – ENISA) szerint a kibertámadások megközelítőleg 19%-a a közszektort érinti, míg 11%-a a közlekedési, 9%-a pedig a pénzügyi szolgáltatókat célozza (ENISA, 2024). A legsúlyosabb fenyegetések közé sorolhatók a zsarolóprogramok (ransomware), a rosszindulatú szoftverek (malware), a pszichológiai manipuláción alapuló támadások (social engineering), az adatsértések, a szolgáltatásmegtagadást célzó akciók (Distributed Denial-of-Service – DDoS),

Ez a fejezet Kiss Milán – Kovács Levente: A pénzügyi kiberbűnözés rendszertana (megjelent: Gazdaság és Pénzügy 2025/3) tanulmánya alapján, annak jelentős részben az átvételével készült.

az információs befolyásolás, valamint az ellátási láncokat célzó kibertámadások. Ezek a fenyegetések nemcsak közvetlen anyagi károkat okoznak, hanem aláássák az intézményekbe vetett bizalmat, gyengítik az infrastruktúrák stabilitását, és közvetve a társadalmi-gazdasági biztonságot is veszélyeztetik. A jelenség kezeléséhez tehát integrált, több szektorra kiterjedő stratégiai megközelítésre van szükség, amely ötvözi a technológiai fejlesztést, a szabályozási szigort, valamint a felhasználói tudatosság és szakmai képzés fejlesztését.

12. ÁBRA: A kibertámadások által megcélzott szektorok az incidensek száma szerint (2023 július – 2024 június)

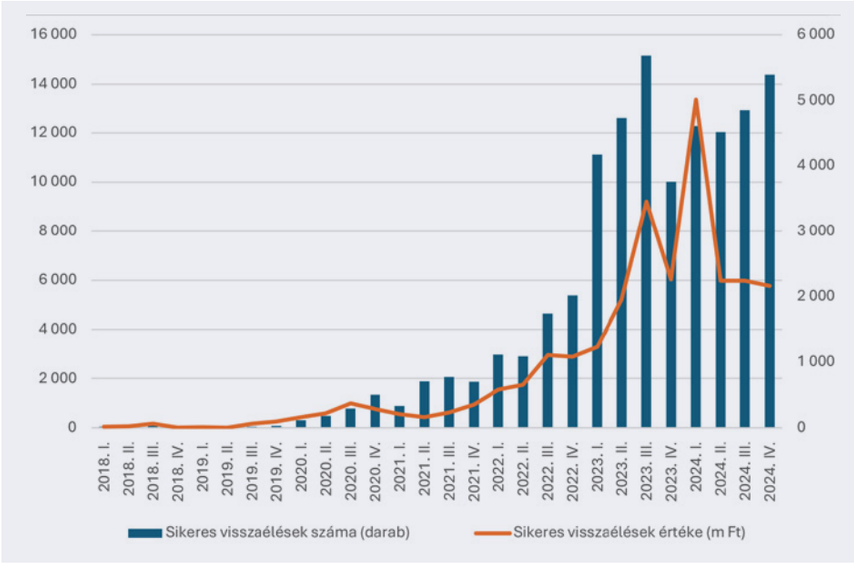


Forrás: (ENISA, 2024)

A pénzügyi szektor esetében megállapítható, hogy a sikeres kibertámadások jellemzően nem a pénzügyi szervezeteket, azaz a szolgáltatókat érintik, hanem a pénzügyi szolgáltatásokat igénybe vevő ügyfeleket. Mindez elsősorban azért lehet, mert Magyarországon az IT biztonságot érintő jogi keretrendszer magasan fejlett[15], valamint ezen jogi elvárásoknak a pénzügyi szektor nagymértékben meg is felel (MNB, 2022). Azaz az „általános” kiberveszélyek a pénzügyi szektorban speciálisan érvényesülnek. Vagyis kijelenthető, hogy például egy bankot vagy egy fizetési rendszert működtető szervezetet nagyon nehéz lehet „meghekkelni”. Ebből kifolyólag a kibertámadásokat elkövetők elsősorban a pénzügyi szolgáltatásokat igénybe vevő ügyfeleket támadják. Ezen visszaéléseket elsősorban az (elektronikus) pénzforgalmon keresztül lehet megfigyelni, mivel az elkövetők a visszaélések során eltulajdonított összegeket a pénzforgalmi rendszerek útján tudják megszerezni.

15 Az európai jogalkotó a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló 2022. december 14 (EU) 2022/2554 európai parlamenti és tanácsi rendelet (Digital Operational Resilience Act – DORA) megalkotásával jutott el olyan szintre, amelyen a magyar szabályozás a megelőző 5 évben volt.

13. ÁBRA: A pénzforgalmon keresztül megfigyelhető visszaélések száma és értéke



Forrás: (MNB, 2025b)

Az ábra adatai is alátámasztják, hogy az elmúlt években a pénzforgalmon keresztül észlelhető visszaélések mind számosságukban, mind értékükben folyamatosan emelkedtek. A Magyar Nemzeti Bank (MNB) statisztikái szerint a sikeresen végrehajtott visszaélések száma folyamatosan növekedik, miközben a visszaélésekből származó pénzügyi kár értéke – az elmúlt negyedévek átmeneti korrekciói ellenére – továbbra is magas szinten maradt.

Kiberfenyegetések csoportosítási szempontjai

A szakirodalomban számos olyan tanulmány található, amely különféle ismérvek mentén rendszerezi a kiberbűncselekményeket (pl. Gordon - Ford, 2006; Onwubiko, 2020). Ezek a munkák jellemzően átfogó, elméleti megközelítést alkalmaznak, és a kiberbűnözést tág értelemben értelmezik – beleértve az információs rendszerek elleni támadásokat éppúgy, mint például az illegális online tartalmak terjesztését is. Bár ezek az osztályozások hasznos támpontot jelentenek a bűnüldöző és szabályozó szervek számára, gyakorlati alkalmazhatóságuk korlátozott lehet a pénzügyi szektor szereplői számára.

Ezért indokolt olyan célzott, gyakorlatorientált kategóriák kialakítása, amelyek kifejezetten a pénzügyi szervezetek, az őket felügyelő hatóságok, a kibervédelmi oktatási anyagokat és kommunikációkat készítők, valamint a vonatkozó pénzügyi jogszabályokat megalkotók számára nyújtanak közvetlen segítséget a releváns kockázatok azonosításában és kezelésében.

1. A támadás módszere szerinti csoportosítás

A kiberbűncselekmények rendszerezésének egyik alapvető szempontja a támadás módszere, vagyis annak vizsgálata, milyen jellegű fenyegetés vagy támadási forma éri a célzott alanyt vagy rendszert. A kategóriák alapja jellemzően a támadáshoz használt eszköz vagy technika.

A fenyegetés típusától függően három fő csoport különíthető el:

A. MALWARE-ALAPÚ TÁMADÁSOK

E típusba olyan támadások tartoznak, amelyek során rosszindulatú kódot (malware) juttatnak el az áldozat informatikai eszközére. A cél lehet adatlopás, rendszerleállás, zsarolás vagy akár fizikai károkozás. A leggyakoribb malware-típusok:

- **Ransomware** – Zsarolóprogram, amely a felhasználó adatait titkosítja, majd váltságdíjat követel.
- **Adware** – Kéretlen reklámokkal bombázza a felhasználót, gyakran megfigyeléssel kombinálva.
- **Keylogger** – A billentyűleütések naplózásával érzékeny adatok (pl. jelszavak) megszerzésére szolgál.
- **Killware** – Fizikai károkozásra is képes kártékony szoftver, például egészségügyi rendszerek elleni támadások során.

B. SZOCIÁLIS MANIPULÁCIÓS (SOCIAL ENGINEERING) TÁMADÁSOK

E támadások célpontja nem maga az informatikai rendszer, hanem annak felhasználója, akit pszichológiai eszközökkel próbálnak megtéveszteni, manipulálni.

- **Phishing (adathalászat)** – Hamis e-mailek vagy weboldalak révén bizalmas adatok kicsalása.
- **Baiting (csalizás)** – Ígéretes ajánlatokkal (pl. ingyenes letöltések) csalogatják az áldozatot.
- **Whaling (bálnavadászat)** – Magas rangú vezetőket célzó célzott adathalászat.

Ezek a támadások gyakran az emberi kíváncsiságra vagy mohóságra (pl. nyeremények, irreális hozamígéretek) építenek.

C. TECHNIKAI VAGY RENDSZERSZINTŰ TÁMADÁSOK

Ebben az esetben a támadás célja az informatikai rendszer sérülékenységeinek kihasználása. Ezek gyakran automatizált, kódszintű támadások, amelyek célja a működés ellehetetlenítése, vagy az adatokhoz való illetéktelen hozzáférés.

- **DoS/DDoS** – Szolgáltatásmegtagadásos támadás, amely túlterheli a célzott rendszert.
- **Nulladik napi támadás** – Még nem ismert vagy nem javított sérülékenység kihasználása.
- **Exploit** – Kifejezetten egy ismert biztonsági rés kiaknázására készült kód.

A támadás eszközei lehet tehát valaki által megírt rosszindulatú kód, a már meglévő informatikai hiányosság kihasználása, vagy a felhasználó közvetlen támadása.

2. Támadó profilja szerinti csoportosítás

A kiberfenyegetések rendszerezésének egyik emberközpontú megközelítése a támadó profilja szerinti osztályozás, amely a fenyegetést jelentő szereplők szándékai, képességei, szervezettségi szintje és rendelkezésre álló erőforrásai alapján kategorizálja az elkövetőket. Ez a tipológia különösen hasznos a kockázatelemzés, a célzott védelmi stratégiák kialakítása, valamint a fenyegetésmodellezés (threat modeling) szempontjából.

A támadók jelentősen különbözhetnek egymástól motivációik, technikai tudásuk, hozzáférhető eszközeik és szervezeti hátterük tekintetében.

E jellemzők alapján az alábbi fő támadói típusok különíthetők el:

ÁLLAMILAG TÁMOGATOTT SZEREPLŐK / FEJLETT FENYEGETÉSI CSOPORTOK (APT – ADVANCED PERSISTENT THREAT)

Jellemzően magas technikai színvonalat képviselő, jól szervezett csoportok, amelyek mögött gyakran állami vagy katonai háttér áll. Képesek saját fejlesztésű eszközök (pl. zero-day exploitok) alkalmazására, és rendszerint hosszú távú, célzott és rejtett műveleteket hajtanak végre. Célpontjaik többnyire stratégiai jelentőségű szereplők: kormányzati intézmények, kritikus infrastruktúrák (pl. pénzügyi rendszerek, energiaellátás), nagyvállalatok vagy hadiipari szervezetek.

SZERVEZETT BŰNÖZŐI CSOPORTOK

E csoportok elsősorban gazdasági haszonszerzésre törekednek, gyakran pénzügyi visszaélések vagy zsarolás útján. Komplex eszköztárral rendelkeznek: jellemzően adathalász technikákat alkalmaznak (phishing, business email compromise), de malware-t, botneteket és más automatizált eszközöket is. Egyes esetekben kiberbűnözést nyújtanak „szolgáltatásként" (pl. *malware-as-a-service*), lehetővé téve ezzel, hogy alacsonyabb technikai tudású szereplők is komoly károkat okozhassanak.

HACKTIVISTÁK

Ezek a támadók politikai, társadalmi vagy ideológiai indíttatásból hajtanak végre kibertámadásokat, gyakran a nyilvánosság figyelmének felkeltése céljából. Jellemző módszereik közé tartozik a weboldalak feltörése, adatlopás és kiszivárogtatás, illetve szolgáltatásmegtagadással járó támadások (pl. DDoS). Anyagi haszonszerzés általában nem céljuk.

KEZDŐ VAGY ALACSONY TUDÁSÚ TÁMADÓK (SCRIPT KIDDIES)

Ebbe a kategóriába olyan egyének tartoznak, akik korlátozott technikai ismeretekkel rendelkeznek, és elsősorban mások által készített kódokat, szoftvereket alkalmaznak. Motivációjuk lehet hírnév szerzése, szórakozás vagy személyes bosszú. Támadásaik gyakran alacsony szofisztikáltságúak, de bizonyos környezetekben mégis jelentős károkat okozhatnak. Egy hazai példa erre a Budapesti Közlekedési Központ (BKK) elektronikus jegyrendszerét ért támadás, amelyet egy 18 éves fiatal követett el.

A felsorolt támadói típusok mellett meg kell említeni az etikus hackereket és a kiberbiztonsági szakembereket, akik jogszerű keretek között vizsgálják az informatikai rendszerek sebezhetőségét. Ilyen tevékenység például a penetrációs tesztelés, illetve a jogszabály vagy uniós rendelet által előírt vizsgálat, például a DORA 26. cikkében említett fenyegetés alapú behatolási tesztelés (TLPT – threat-led penetration testing).

3. A célpont típusa szerint csoportosítás

A kiberfenyegetések célpontjai különböző típusú szereplők lehetnek: természetes személyek, vállalkozások (mikrovállalkozások, KKV-k, de nagyvállalatok is), vagy akár nemzetbiztonsági szempontból kiemelt infrastruktúrák.

TERMÉSZETES SZEMÉLYEK ELLENI KIBERTÁMADÁSOK:

Ezen támadások esetében a cél jellemzően a pénzügyi visszaélés mellett a személyes adatok megszerzése vagy privát információk ellopása. Jellemző támadások: keylogger, phishing, doxing (személyes információk nyilvánosságra hozása, lejáratás céljából), nigériai típusú csalás (romantikus vagy segélykérő történettel pénzt csalnak ki), cyberbullying (online zaklatás közösségi platformokon vagy egyéb üzenetküldő alkalmazások útján). Az emberi kapzsiságra építő támadások (váratlan nyeremények vagy magas hozamot ígérő befeketések ígérete) szintén jellemzőek.

VÁLLALKOZÁSOK:

A vállalkozások vagy egyéb szervezetek, például alapítványok vagy non profit szervezetek[16] elleni támadások célja elsősorban pénzszerzés üzleti adatok ellopásával, rendszerek megbénítása váltságdíjért (ransomware), beszállítói lánc kompromittálása, versenyelőny szerzése vagy bizalmas adatok kiszivárogtatása. Jellemző támadások lehetnek a Business Email Compromise (BEC) – céges levelezések manipulálása, hamis számlaadatokkal történő csalás, spear phishing / whaling – amely nem más, mint célzott adathalászat döntéshozók ellen, illetve rosszindulatú kódokkal történő támadások (pl. ransomware támadás, amely fájlok titkosítása után a feloldásért váltságdíj követelésével jár.

KRITIKUS INFRASTRUKTÚRÁK:

Ezek az ágazatok a társadalom működéséhez alapvető fontosságúak: egészségügy, közlekedés, energia, vízellátás, kormányzati rendszerek stb. A pénzügyi szervezetek esetében példák lehetnek erre a fizetési és értékpapírelszámolási rendszerek[17], de akár jelentős lakossági ügyfélállománnyal rendelkező hitelintézetek is.

16 Egyes kutatás-fejlesztési területen tevékenykedő magas hozzáadott értéket termelő szervezetek az Európai Unióban non profit vagy alapítványi formában működnek.

17 Az MNB által működtetett Valós Idejű Bruttó Elszámolási Rendszer (VIBER), a GIRO Elszámolásforgalmi Zrt. által üzemeltetett klíring rendszerek, továbbá a KELER Központi Értéktár Zrt. és a KELER KSZF Központi Szerződő Fél Zrt. értékpapírelszámolásokhoz és nyilvántartásokhoz kapcsolódó infrastruktúrái.

A támadások célja rendszerint: fizikai vagy gazdasági károkozás, politikai destabilizálás, illetve a lakosság ellátásának megzavarása. A támadásokat jellemzően killware, APT támadások és DoS/DDoS támadások útján hajtják végre.

A célpont típusa szerinti megkülönböztetés különösen fontos a védelmi mechanizmusok meghatározásánál, mivel a támadhatóság és az alkalmazható védekezési eszközök jelentősen eltérnek egyéni, vállalati vagy állami szinten.

4. A védekezés eszköze szerinti csoportosítás

A védekezési megoldások célja az, hogy megelőzzék, észleljék, elhárítsák vagy csökkentsék a kiberfenyegetések hatását. Ezek az eszközök lehetnek szoftverek, hardverek, eljárások vagy hírszerzési (intelligence) módszerek.

ALAPSZINTŰ VÉDELMI ESZKÖZÖK:

Ezen eszközök célja a hálózati és végponti rendszerek automatikus védelme, valamint kártékony programok és anomáliák észlelése, blokkolása. Ilyen eszközök lehetnek az antivírus programok, tűzfalak, IPS (Intrusion Prevention System, behatolás-megelőző rendszer) és az IDS (Intrusion Detection System, behatolás-észlelő rendszer.

TITKOSÍTÁSI ÉS ADATBIZTONSÁGI TECHNOLÓGIÁK:

Céljuk az adatok védelme átvitel közben (pl. e-mail, böngészés) vagy tárolás alatt, továbbá az adatokhoz történő hozzáférés védelme, azaz csak az arra jogosult férhessen hozzá az adott tartalomhoz. Ezen technológiákra lehetnek példák a virtuális magánhálózatok (Virtual Privtave Network, VPN), SSL (Secure Sockets Layer) és TLS (Transport Layer Security) technológiák, amelyek titkosított adatátvitelt tesznek lehetővé a szerver és a kliens között, például böngészés közben.

HALADÓ HÍRSZERZÉS:

A hírszerzés célja az esetleges támadások előrejelzése és azonosítása, megtörtént támadások digitális nyomok (indikátorok) alapján történő visszafejtése, illetve proaktív védelem és reagálás. Ezen módszerek esetében jellemzően nem egy-egy technológiát használnak a szakértők, hanem komplex megoldásokat, például Cyber Threat Intelligence (CTI) keretében elemzik a veszélyeket.

Ezek a kategóriák gyakran egymásra épülnek: egy hatékony védelem több rétegű, kombinálja az automatikus védelmet, a titkosítást és az intelligens, adatalapú reagálást.

5. A támadáshoz használt eszköz jellege szerint

A kibertámadások egyik alapvető jellemzője a végrehajtás módja, különösen az, hogy milyen mértékben támaszkodnak automatizált folyamatokra, illetve emberi beavatkozásra.

E szempont alapján két fő típust különböztethetünk meg: automatizált és manuális (interaktív) támadásokat. Az előbbiek előre programozott kódokra épülnek, míg az utóbbiak valós idejű emberi döntéshozatalt, beavatkozást igényelnek.

AUTOMATIZÁLT TÁMADÁSOK:

Ezek a támadások nagy mennyiségben, gyakran tömegesen zajlanak, minimális vagy teljesen hiányzó emberi beavatkozással. Előnyük a gyorsaság, a skálázhatóság és az ismételhetőség. Jellemzően gyengén védett, nem célzott rendszerek ellen hatékonyak. Tipikus példák a botnet alapú támadások, melyek során fertőzött eszközök hálózatát használják például DDoS, spamküldés, vagy brute force jelszótörés végrehajtására.

MANUÁLIS TÁMADÁSOK:

Ezek célzott műveletek, amelyek emberi megfigyelést, döntéshozatalt és taktikai tervezést igényelnek. Jellemzőjük a részletes előkészület, az intelligens kivitelezés, valamint a komplex támadási láncba való illeszkedés. Tipikus formája a spear phishing, amikor egy adott személy vagy szervezet ellen irányul az adathalászat, gyakran vezető beosztású személyekre fókuszálva (whaling). A támadó előzetes információgyűjtéssel és bizalomépítéssel próbál hozzáférni érzékeny adatokhoz.

A két támadástípus eltérő jellemzői miatt eltérő védekezési stratégiák kialakítását igényli.

6. Egyéb csoportosítási szempontok

A fent bemutatott főbb kategóriákon túl a kiberfenyegetések rendszerezését további dimenziók is segíthetik, amelyek mélyebb elemzést és célzottabb védelmi intézkedések kidolgozását teszik lehetővé.

A. TÁMADÁS CÉLPONTJA AZ INFORMATIKAI ARCHITEKTÚRÁBAN

Az egyik további szempont az, hogy a támadás melyik informatikai komponensre irányul:

Kliensoldali támadások:

A felhasználó eszközeit vagy alkalmazásait célozzák. Jellemző fenyegetések: adware (kéretlen reklámmegjelenítés), keylogger (billentyűleütések rögzítése), spyware, valamint olyan social engineering típusú támadások, mint a phishing vagy baiting.

Szerveroldali támadások:

A szolgáltatást nyújtó rendszereket (pl. web-, alkalmazás- vagy adatbázis-szervereket) célozzák. Jellemző módszerek: szolgáltatásmegtagadással járó támadások (DoS/DDoS), zsarolóprogramok (ransomware), hátsó kapuk (backdoor), kihasználó kódok (exploit), brute force támadások.

Hálózati szintű támadások:
A célpont az adatátvitel vagy hálózati kommunikáció. Jellemző módszerek: DNS tunneling (rosszindulatú adatátvitel DNS-protokollon keresztül), evil twin (hamis Wi-Fi hálózat létrehozása megtévesztés céljából), illetve közbeékelődéses támadások (man-in-the-middle).

Ez a csoportosítás elsősorban IT biztonsági szakértők számára lehet releváns, mivel a védendő eszközök képezik a csoportosítás alapját.

B. JOGSZABÁLYI MEGKÖZELÍTÉS

Szempont lehet az is, hogy az adott cselekedet jogilag megengedett, tiltott vagy bizonytalan megítélés alá esik:

Kifejezetten büntetendő cselekmények:
Ide tartoznak azok a tevékenységek, amelyek kifejezetten a büntetőjog hatálya alá esnek. Például: fizetési kártyák klónozása (készpénz-helyettesítő eszköz elleni visszaélés), vagy a phishing és egyéb adatlopási módszerek.

Jogszerű tevékenység speciális keretek között:
Jogszabály vagy szerződés alapján végzett biztonsági tesztek, mint etikus hackelés, penetrációs teszt Threat-Led Penetration Testing (TLPT), bug bounty program. Ilyen lehet például a DORA rendelet szerinti TLPT.

Szürkezóna:
Az OSINT (Open Source Intelligence) alkalmazása, azaz nyilvánosan elérhető adatok gyűjtése hírszerzési céllal, egyes esetekben kockázatos zónába eshet, mivel jogilag például adatvédelmi vagy büntetőjogi jogszabályok alapján, nem mindig egyértelmű a megengedettsége vagy a felhasználhatósága.

A jogalkotók és a jogalkalmazó pénzügyi szervezetek és hatóságok számára lehet releváns ez a csoportosítás, mivel alapját képezheti a joghézagok azonosításának.

C. A FOGALOM JELLEGE SZERINT

A kiberbiztonsági fogalmak jellegük szerint is csoportosíthatóak.

Technikai fogalmak:
Például exploit, malware, amelyek informatikai szakmai terminusok.

Köznyelvi vagy szleng kifejezések:
Nem szakmai, inkább felhasználói környezetben használt kifejezések, gyakran a támadások hétköznapi leírására.

Jogi terminológia:
Például információs rendszer, elektronikus pénz, készpénz-helyettesítő fizetési eszköz, amelyeket jogszabályok vagy Európai Uniós jogalkotási aktusok határoznak meg.

Ezek a további szempontok lehetővé teszik a fogalmak többdimenziós vizsgálatát, ami segíthet a kiberbiztonsági fenyegetések komplexebb elemzésében, valamint a szabályozási, oktatási és védelmi mechanizmusok hatékonyabb kialakításában.

D. A TÁMADÁS FÁZISA SZERINT

A támadás fázisai szerinti csoportosítás az egyik legelterjedtebb módszer a célzott, összetett kibertámadások megértésére és modellezésére. E szemlélet alapját a Cyber Kill Chain modell adja (Abawajy et al., 2015), amely lépésről lépésre mutatja be egy támadás kibontakozását.

A modell szerint a támadás a következő fázisokból áll:

Felderítés:
A támadó információt gyűjt a célpontról, annak rendszereiről, alkalmazottjairól, e-mailcímeiről, technológiai környezetéről. Ennek célja, hogy a támadó megértse a célpont működését, és a támadás testreszabható legyen.

Belépés / Inicializálás:
A támadó kiválasztja és eljuttatja az eszközt, amely lehetővé teszi a hozzáférést, például socal engineering segítségével. Célja a kártékony kód bejuttatása vagy a felhasználó rávétele, hogy „megnyissa az ajtót”.

Installálás:
A támadó stabil hozzáférést alakít ki és megpróbál magasabb jogosultságot szerezni. Innen „mozogni kezd” a hálózaton belül. Cél: az infrastruktúra mélyebb rétegeihez való hozzáférés biztosítása és a jelenlét elrejtése.

Cél elérése és kivonulás:
A támadó végrehajtja a valódi célját (pl. adatlopás, zsarolás), majd elhagyja a rendszert – lehetőleg nyom nélkül. Ezen fázis célja az adatok megszerzése, zsarolás vagy más támadási cél teljesítése, a felfedezés minimalizálása mellett.

Természetesen a fent felsorolt csoportosítási szempontokon túlmenően számos egyéb csoportosítás is elképzelhető.

A pénzforgalmon keresztül megfigyelhető visszaélések

Az MNB több alkalommal hangsúlyozta, hogy a magyar pénzügyi rendszer európai viszonylatban is biztonságosnak tekinthető (MNB, 2023). Ennek megfelelően az 5/2023. (VI.23.) MNB ajánlás – az ún. Anti-fraud ajánlás – címében is a *pénzforgalmi szolgáltatásokon keresztül megfigyelhető* visszaélések szerepelnek, nem pedig a szolgáltatásokat közvetlenül érintő támadások. Ennek ellenére a pénzforgalmi szolgáltatások ügyfelei – különösen lakossági felhasználók és vállalkozások – kitettséget mutathatnak különféle kiberbűncselekményeknek. E támadások a korábban ismertetett kategóriák szerint rendszerezhetők.

24. TÁBLÁZAT: A leggyakoribb pénzforgalmon keresztül megfigyelhető visszaélések

Típus	Fő célpont	Eszköz	Célja
Business Email Compromise	Vállalkozások	E-mail, számla	Átutalás manipulálása
CEO-fraud / Social engineering	Vállalkozások pénzügyei	E-mail, pszichológiai manipuláció	Belülről utalás kezdeményeztetése
Phishing / Smishing / Vishing	Magánszemélyek	E-mail, SMS, telefon	Hozzáférés adatlopással
Kártyacsalás	Pénzforgalmi szolgáltatók ügyfelei	Kártyaadatok	Jogosulatlan vásárlás
Ál-webáruházak	Vásárlók	Hamis oldal	Pénz vagy adat megszerzése
Ransomware	Vállalkozások, intézmények	Káros kód és kriptofizetés	Váltságdíj
Előrefizetéses csalás	Bárki	E-mail	Pénz kicsalása ígéretért

Forrás: (OECD, 2022; CISA, 2023; FBI, 2023; Kovács - Terták, 2024)

Megjegyzendő továbbá, hogy az 24. táblázatban bemutatott támadási módok csupán jelenleg, 2025 nyarán a leggyakoribbak. Természetesen, ahogy általában a kibertámadások esetében, a pénzforgalmi úton megfigyelhető visszaélések esetében is folyamatos a változás. Míg 2020-ban a hagyományos módszerek domináltak, pl. fizikálisan eltulajdonították az ügyfelek fizetési kártyáit, addig 2025-re lényegesen kifinomultabb csalások váltak gyakoribbá. Például a rendőrség az ún. mátrix projekt keretében számolt fel egy banki ügyfélközpontokhoz hasonló rendszert működtető csoportot (ORFK, 2024).

A fentiek alapján kijelenthető, hogy a leggyakrabban előforduló, a pénzügyi szervezeteket is érintő, a kibertérben elkövetett visszaélések számos, az előzőekben ismertetett csoportosítás szerint klasszifikálhatóak. Megállapítható továbbá az is, hogy ezen csoportosításokra szükség van, mivel jelentősen elősegíthetik a visszaélések elleni védekezést azáltal, hogy hatékonyabb kommunikációt, illetve egyértelműbb jogalkotást tesznek lehetővé.

A visszaélések elleni védekezés korántsem egyszerű. A napi pénzügyi tapasztalat a pénzügyi tudatosság növelését hangsúlyozza, ahogy (Hergár et al., 2024) teszik tanulmányukban. Míg más szerzők a technológia és jogszabályok nyújtotta lehetőségeket emelik ki (Doeland, 2019). A hazai szabályozó, az MNB a második pénzforgalmi irányelv (PSD2 – Payment Services Directive 2) hazai jogba történő átültetése és az azonnali átutalások bevezetése óta egy négy elemből álló komplex keretrendszer mentén igyekszik fellépni a visszaélések megelőzésének érdekében (Kiss, 2023).

Az egyes pénzszolgáltatók a saját ügyfélkörük tapasztalatai alapján tudják kialakítani azokat a csalási mintázatokat, amelyekkel az új megbízásokat – mesterséges intelligencia bevonásával – kibercsalás ellen szűrni tudják. Ezt a megoldást szektor szinten egységesítette és továbbfejlesztette a GIRO Zrt.

A magyar hitelintézeti elszámolóház, a GIRO Zrt. 2025. július 1-én indította el a Központi Visszaélésszűrő Rendszerét (KVR), amely a fizetési rendszerben részt vevő pénzforgalmi szolgáltatóktól (bankoktól) feldolgozásra átvett adatok szabályalapú, csalási mintázatot kutató, mesterséges intelligencián alapuló öntanuló mechanizmusok segítségével kiberbiztonsági szempontból elemezni tudja a fizetési műveleteket. A rendszer a csalási trendek fejlődésével párhuzamosan a folyamatos tanulási képességének megfelelően képes párhuzamosan fejlődni és az új típusú visszaélésekre megfelelően reagálni. A KVR a beküldött pénzforgalmi adatokon visszaélési kockázati értékelést végez és megállapítja a visszaéléskockázati információt, azt megküldi a pénzforgalmi szolgáltatónak, ami ezt beépíti a visszaélés szűrő rendszerébe. A pénzforgalmi szolgáltató a kockázati besorolás alapján dönthet úgy, hogy a fizetési műveletet nem teljesíti.

7. A szociális manipuláció és kezelése

A kibercsalások egyik jelentős alcsoportját azok az esetek alkotják, amelyekben a csaló személyes jellegű pszichológiai manipulációval él annak érdekében, hogy megtévessze áldozatát. Ilyen esetekben a megtévesztés célja rendszerint a jogtalan haszonszerzés, melynek során az elkövető tudatosan félrevezeti, vagy szándékosan tévedésben tartja az érintettet, ezáltal számára anyagi vagy más természetű kárt okoz.

A megelőzés és tudatosságnövelés szerepe a kibercsalások elleni védekezésben

A szociális manipulációra épülő kibercsalások elleni küzdelem egyik leghatékonyabb eszköze a felkészítés, amely magában foglalja az oktatást, a figyelemfelkeltést és az önálló döntéshozatal képességének fejlesztését. A tudatos felhasználók könnyebben felismerik a manipulatív technikákat, és hatékonyabban képesek ellenállni a megtévesztési kísérleteknek.

A megelőzés tehát nem pusztán technikai biztonsági intézkedésekre szorítkozik, hanem kiemelt figyelmet fordít a pszichológiai védekezőképesség növelésére is. Ennek része a kritikus gondolkodás fejlesztése, az érzelmi manipuláció jeleinek felismerése, valamint a digitális írástudás mélyítése. A cél nem a félelemkeltés, hanem a tudatosság megerősítése: az emberek képesek legyenek felismerni a veszélyt, és felelős döntéseket hozni az online térben.

Különösen fontos, hogy ez a tudás már fiatal korban elérhető legyen az iskolai oktatás keretében, ugyanakkor a felnőttek számára is hozzáférhetőek legyenek a célzott ismeretterjesztő programok, workshopok és tanácsadások. A közösségi médiafelületeken, munkahelyi érzékenyítő rendezvényeken, illetve ügyféltájékoztatók útján zajló edukáció szintén hozzájárulhat az általános kockázatérzékelés erősítéséhez.

A bankszektor példája jól mutatja, hogy a technikai védelem önmagában nem elegendő: a jogszabályi keretek szigorú betartása mellett a folyamatos, egyértelmű és közérthető kommunikáció az egyik legfontosabb eszköz a csalások megelőzésében. Amennyiben a pénzintézet gyanús eseményt észlel, haladéktalanul intézkedik — például zárolja a bankkártyát vagy visszatartja az utalást —, még azelőtt, hogy az ügyfelet tájékoztatná. Ezzel biztosítja a potenciális károk megelőzését.

Nem lehet elégszer hangsúlyozni: a felhasználók védelme érdekében elengedhetetlen, hogy tisztában legyenek azokkal az adatokkal, amelyeket egyetlen szolgáltató – különösen egy bank – soha nem kérne telefonon, e-mailben vagy más nem biztonságos csatornán keresztül. Ilyen például:

- internetbanki vagy mobilbanki belépési adatok (jelszó, PIN kód),
- bankkártyaadatok (szám, lejárati dátum, CVC),
- e-mail fiókhoz tartozó azonosítók,
- online belépési linkek megnyitása és adatok megadása,
- alkalmazások vagy programok telepítése kérésre,
- keresőprogramon keresztül történő bejelentkezés a banki felületre.

Ennek a fejezetnek az elkészítéséhez az „Ajánlás az online pénzügyi visszaélések áldozataival történő kommunikáció elősegítésére” nem publikus anyag (Készítette: Magyar Bankszövetség a Kiberpajzs keretében 2024-ben) felhasználásra került.

A tudatos viselkedés és a gyanús megkeresések elutasítása kulcsfontosságú lépés a kibertérben való biztonságos jelenléthez.

A szociális manipulációs csalások elsődleges célja, hogy az elkövetők a megtévesztett személy bankszámlájához, bankkártyájához kapcsolódó alapvető adatokhoz, illetve belépési jelszavaihoz hozzáférjenek. Ezek birtokában a csalók képesek saját céljaikra átutalni az áldozat — vagy vállalkozása — pénzeszközeit, jellemzően magyarországi, majd később külföldi, vagy azonnal külföldi és anonimitást biztosító – például kriptovaluta-alapú – számlákra.

A szociális manipulációs csalásokat a következő alkategóriákba lehet besorolni:

Megrémisztésen alapuló csalások

Ezek a módszerek gyakran az érzelmi reakciók gyors kiváltására építenek. A félelem, a sürgetés, illetve a hivatalos hangnemmel társított fenyegetettségérzet gyakran blokkolja a kritikai gondolkodást. Különösen veszélyeztetettek azok, akik kevésbé jártasak a digitális világban, illetve időskorúak, akik hajlamosak megbízni az autoritással fellépő személyekben.

A félelemkeltésre épülő csalások pszichológiája a klasszikus ‚fight or flight’ (harcolj vagy menekülj) reakciót aktiválja, ami sokszor blokkolja a racionális gondolkodást. Az emberek ilyenkor hajlamosak impulzívan reagálni, különösen akkor, ha úgy érzik, hogy sürgős döntést kell hozniuk egy fenyegető helyzetben. Ez a módszer kifejezetten hatásos az idősebb korosztály, valamint a technikailag kevésbé képzett felhasználók körében. A stresszhelyzet fokozásával a csalók elérik, hogy az áldozat ne kérdőjelezze meg a történteket, hanem azonnal cselekedjen. Fontos lenne ezen manipulációs taktikák szélesebb körű oktatása a lakosság körében, különösen célzott programokkal az idősek és egyedül élők számára.

a. Az első forgatókönyv szerint az áldozat telefonhívást kap, amelyben a hívó azt állítja, hogy a számlavezető bank visszaélést észlelt a számláján — például egy nagy összegű utalási kísérletet. A hívó azzal a szándékkal keresi meg az ügyfelet, hogy megerősítést kérjen: ő kezdeményezte-e a tranzakciót. A csaló ezt követően azt állítja, hogy a folyamatban lévő utalást csak az áldozat közreműködésével tudják leállítani — holott a valóságban a pénzintézetek képesek ügyfélbeavatkozás nélkül is azonnal zárolni bármilyen tranzakciót. A megtévesztés következő lépése, hogy az elkövetők elkérik az internet- vagy mobilbanki belépési adatokat, esetenként a bankkártya információkat is, vagy utasítják az áldozatot, hogy telepítsen olyan szoftvert, amely távoli hozzáférést biztosít a készülékéhez. A tapasztalatok szerint ezek a hívások gyakran valamelyik nagyobb lakossági bank nevében történnek, mivel így statisztikai alapon nagyobb az esély arra, hogy az érintett valóban ügyfele az adott intézménynek. A beszélgetés során, amikor az ügyfél elárulja, hol vezeti számláját, a csaló „átkapcsolást” imitál a megfelelő bankhoz vagy akár a „rendőrséghez”,

hogy még hitelesebbnek tűnjön. Fontos tudni: a hívó fél telefonszámát technikailag könnyen felül lehet írni, így a megjelenő szám lehet akár egy ismert banki call centeré is — ez azonban nem garancia a hívás hitelességére.

b. Egy másik gyakori forgatókönyv szerint a csaló a hatóság képviselőjének adja ki magát — például pénzmosás, terrorizmus finanszírozása, adótartozás, vagy adó-visszatérítés ügyében. Előfordulhat, hogy az elkövető azt állítja: az érintett az elmúlt időszakban több banknál nyitott számlát, amely alapján bűncselekmény gyanúja merült fel. A telefonáló hivatalos hangnemet használ, és gyakran jogi következményekkel fenyeget. A cél minden esetben az, hogy az áldozat félelmében együttműködjön, és önként átadja a személyes és banki adatait.

c. A harmadik típusú támadás a vállalati szférát célozza. Itt a csaló a cég felső- vagy pénzügyi vezetőjét keresi meg úgy, mintha egy még magasabb pozíciójú vezetőtől — például a cég tulajdonosától vagy vezérigazgatójától — jönne az utasítás. A cél egy sürgős, magas összegű átutalás elrendelése egy látszólag jogos vállalati cél érdekében. A megkeresés történhet e-mailben, telefonon vagy videóhívás formájában. A modern technológiák, különösen a mesterséges intelligencia, lehetővé teszik, hogy a csalók valósághű hang- és arcmintákat használjanak az átverés hitelességének növelésére. A történelem legnagyobb összegű online csalásai közül több is e módszerrel valósult meg.

A csalók jellemzően nem rendelkeznek pontos információval arról, hogy az adott személy mely pénzintézetnél vezeti bankszámláját. Általában véletlenszerűen generált vagy kiszivárgott telefonszámokat hívnak, gyakran anélkül, hogy tudnák, ki van a vonal túlsó végén. Az esetek többségében a hívott fél nevét sem ismerik, hacsak az nem mutatkozik be önként a beszélgetés elején — amivel sajnos megkönnyíti a csaló dolgát. Bár az ilyen támadások első pillantásra „vakon” történő próbálkozásnak tűnhetnek, a közösségi médiában elérhető információk jelentős részét — például név, lakhely, munkahely, iskolai végzettség, családi kapcsolatok — ma már strukturált formában adatbázisokba lehet gyűjteni. Ezt a csalók rendszeresen ki is használják, és így célzottabb, személyesebb kommunikációt tudnak alkalmazni, ami növeli a megtévesztés esélyét.

A kibercsalások során alkalmazott telefonhívások egyik közös és egyértelmű jellemzője, hogy a csalók kizárólag információt kérnek, de semmiféle ellenőrizhető adatot nem adnak meg önmagukról. Minden kérdésre gyors, határozott és meggyőző válaszuk van, gyakran még azt is előre „tudják”, mit fog kérdezni az áldozat — vagy legalábbis olyan stílusban kommunikálnak, mintha így lenne. A beszélgetést folyamatos sürgetés jellemzi: azt az érzetet keltik, hogy sürgős döntést kell hozni, különben a pénz veszélybe kerül. A nyomásgyakorlás célja, hogy az áldozat ne tudjon átgondolt, higgadt döntést hozni. A csaló sietséget színlel, és biztonságot ígér: például arra sürgeti az áldozatot, hogy a pénzét egy „védett” számlára utalja át — természetesen a csalók által megadott

címre. A valóságban ilyen biztonsági intézkedés nem létezik, és minden ilyen kérés valójában a megtévesztés részét képezi.

A figyelmeztető jelek — ismeretlen hívó, túlzott sürgetés, személyes és banki adatok kérése, hamis biztonsági megoldások felajánlása — mind együttesen utalnak arra, hogy az adott megkeresés nem megbízható, és azonnal meg kell szakítani a kapcsolatot, valamint jelenteni kell az esetet a banknak vagy a rendőrségnek.

Nyereményen vagy mohóságon alapuló csalások

Az ebbe a csoportba tartozó kibercsalások a szerencsébe vetett hitet, az anyagi gyarapodás iránti vágyat, valamint az elismerés iránti emberi szükségletet használják ki. A csalók ezekre az érzelmi és pszichológiai motivációkra építve manipulálják az áldozatokat. Noha az ilyen típusú átverések leggyakrabban e-mail formájában jelennek meg, egyre gyakrabban fordulnak elő telefonos megkeresések is, amelyek még közvetlenebb hatást gyakorolhatnak.

A nyeremény ígérete még akkor is megtévesztő lehet, ha az illető valóban részt vett valamilyen játékban, de ha nem is jelentkezett nyereményjátékra, úgy az ilyen megkeresések megbízhatósága gyakorlatilag nulla. Fontos tudatosítani, hogy sem vállalatok, sem alapítványok nem szoktak véletlenszerűen jelentős értékű ajándékokat osztani előzetes regisztráció, részvétel vagy valamilyen feltétel teljesítése nélkül.

Hasonlóképpen, a befektetési csalások esetében a hozamok mindig arányosak a vállalt kockázattal. A véletlen szerencsére épülő nyeremények (mint például a lottó) valószínűsége rendkívül alacsony – például az ötös lottó esélye 1 a 43 949 268-hoz. A klaszszikus pénzügyi alaptétel szerint a biztonságos befektetések (pl. állampapír, bankbetét) alacsonyabb, de stabil hozamot kínálnak. Ennek megfelelően, ha valaki kockázatmentesnek mondott, de kiugró hozamot ígér, szinte biztosra vehető, hogy csalás áll a háttérben.

A LEGGYAKORIBB TRÜKKÖK ÉS TECHNIKÁK:

a. Ál-nyeremények: Az áldozat üzenetet vagy telefonhívást kap, amelyben arról tájékoztatják, hogy értékes nyereményt nyert. A „nyeremény” átvételéhez azonban regisztrációra van szükség, vagy egy kisebb összegű „ügyintézési díjat” kell előre befizetni. A cél valójában az áldozat bizalmas adatainak megszerzése, illetve közvetlen anyagi kár okozása.

b. „Kihagyhatatlan” vásárlási ajánlatok: Alacsony árú, exkluzív termékeket kínálnak, gyakran „csak most, csak Önnek” jellegű reklámszövegekkel. A megrendeléshez kapcsolódó hosszú és bonyolult szerződés apró betűs részében szerepel, hogy a vásárlással az ügyfél rendszeres, havi szintű levonásokhoz járul hozzá — gyakran a tudtán kívül.

c. Álörökségek: Az áldozat egy állítólagos, ismeretlen távoli rokontól vagy nagyvonalú adományozótól származó örökségről kap hírt. Az összeg megszerzéséhez azonban előzetesen ügyvédi, közjegyzői vagy banki költségeket kell kifizetnie — természetesen a csalók részére.

d. Álbefektetési lehetőségek: A csaló azt ígéri, hogy egy kisebb összeg befizetésével az áldozat hozzáférhet egy nagyobb értékű befektetési lehetőséghez vagy bekerülhet egy exkluzív befektetői körbe. Ezeket gyakran „induló projekt", „új pénzügyi termék" vagy „gyors hozamú befektetés" ürügyén tálalják.

e. Rejtett, „banktitokként" kezelt szuperbefektetések: A csalók azt állítják, hogy egy rendkívül jövedelmező, titkos befektetési lehetőségről van szó, amelyet a pénzügyi elit elzár a hétköznapi emberek elől. Az első befizetések után rendszerint hamis hozamigazolásokat küldenek, amelyek meggyőzően igazolják a „sikeres befektetést", ezzel újabb összegek átutalására ösztönözve az áldozatot.

A FIGYELMEZTETŐ JELEK

Az ilyen típusú csalások ellen a szolgáltatók védelmi lehetőségei korlátozottak, különösen akkor, ha az áldozat maga ragaszkodik a hithez, hogy valóban szerencse érte. Gyakori, hogy az érintettek még többszöri figyelmeztetés ellenére továbbra is együttműködnek a csalókkal, abban bízva, hogy a „nagy lehetőség" valós. Ez a fajta viselkedés az emberi pszichés természetes vonzódását tükrözi a gyors sikerhez és az anyagi függetlenség illúziójához.

Romantikus történeteken alapuló csalások

A romantikus csalások pszichológiai alapja a kötődési szükségletek kihasználása. Az érzelmi manipuláció hatására az áldozat gyakran figyelmen kívül hagy minden racionális érvet, és a kapcsolatba vetett érzelmi befektetés dominálja a döntéseit. A csalók ezzel képesek hónapokon keresztül fenntartani a kapcsolatot, és folyamatosan pénzt kérni különböző ürügyekkel.

A romantikus csalások egyik legfontosabb pszichológiai mozgatórugója az emberi kapcsolatok iránti vágy és a társas támogatottság hiányának kihasználása. Ezek a csalók gyakran hosszú hónapokon keresztül építik fel a bizalmat, amely során az áldozat érzelmileg egyre jobban bevonódik. A folyamat során a csalók fokozatosan izolálják az áldozatot másoktól, és egyre jobban megerősítik magukat a legmegbízhatóbb személy szerepében. Ezek az esetek gyakran nemcsak anyagi, hanem súlyos pszichológiai káh rokat is okoznak, többek között depressziót, szégyenérzetet, bizalomvesztést és társas elzárkózást. Az ilyen típusú csalások megelőzése érdekében szükséges lenne az online ismerkedési platformok részéről egyfajta előszűrés, vagy kockázatbecslő algoritmus alkalmazása, illetve figyelemfelkeltő kampányok indítása.

Az áldozat a világháló valamely kapcsolatkereső alkalmazásán, vagy random módon ilyen kezdeményező levelet kapott és megismert valakit, akivel a kibertérben, de akár telefonon szoros kapcsolata alakult ki, aki a közeli személyes találkozás vagy segítségkérés ürügyén kér „kölcsön" az áldozattól. Altípusként értékes csomagot küld az áldozatnak és a nem létező csomag utáni vámot fizettetik meg az áldozattal a csalók. Ebbe a típusba sorolhatók az unokázós csalók is, akik az unoka számára, adósságaira hivatkozva stb. kérnek pénzösszeget idős emberektől.

A TÖRTÉNETEK FŐ TÍPUSAI:

- színlelt szerelem, házasság legendájával,
- menekültek vagyonának vagy jogtalanul elvett örökség visszaszerzéséhez,
- valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez,
- háborús övezetből, ENSZ misszióból történő kilépés,
- diplomáciai, rendőrségi eljárásból szabadulás okán,
- egyéb: a sor a következő időszakban nyilvánvalóan folytatódni fog.

A csalók lehetséges motivációi

A bűnelkövetők egy része strukturált bűnszervezetek tagja, mások egyéni vállalkozásként működnek. A motivációk hátterében gyakran anyagi nehézségek, munkanélküliség, vagy egyszerűen a gyors meggazdagodás iránti vágy húzódik meg. A digitalizáció fejlődésével ezek a módszerek egyre kifinomultabbá váltak, a támadások célzottabbak és technológiailag összetettebbek.

A csalók motivációs háttere sokrétű lehet, a puszta pénzszerzéstől kezdve a hatalmi érzés megtapasztalásáig. Egyes esetekben a csalók saját torz igazságérzetük mentén indokolják meg cselekedeteiket, például azt hangoztatva, hogy ők csak a rendszer hibáit használják ki, vagy hogy az áldozatok is ‚megérdemelték'. A bűnelkövetők egy másik típusa teljesen érzéketlen mások kárára, és a pszichopátiás vonások is megfigyelhetők – például az empátia hiánya, gátlástalanság, manipulativitás. Fontos megértenünk, hogy nem minden csaló egyformán tudatos vagy profi; vannak köztük impulzív elkövetők is, akiket a könnyű haszonszerzés csábít, de nem ismerik fel tetteik súlyát vagy következményeit.

A kibertéri csalók nemzetközi „best-practice" módszerekkel dolgoznak. Az ötletek tárháza folyamatosan bővül. Kommunikációjuk állandóan fejlődik, a gyors és kizárólagos bizalomba férkőzésre törekszenek. Kiszemelt áldozataikat időnyomás alá helyezik. Gátlástalanok, mivel jól tudják, hogy az idősebbek, magányosak és elesettebbek könnyebb célpontok, amit könyörtelenül ki is használnak. A következő ösztönzők hajthatják őket:

- így akar pénzt keresni, és fontos számára a kevés munkával történő biztos megélhetés,
- nem tud másként pénzt szerezni, mert nem képes a beilleszkedésre, ezért nem képes a társadalom által elfogadott értékekhez igazodó munkával pénzkeresésre,
- úgy érzi, hogy neki mindent szabad, nem fogad el korlátokat, szabályokat,
- öntörvényűség,
- elismerésre vágyik (ha lebukik, benne lesz a TV-ben, és ettől sikeresnek érzi magát),
- torz értékrendszer,
- súlyos szociális zavar,
- a másik ember helyzetébe és érzéseibe történő beleérzési képesség teljes hiánya,
- bűnbandába való bekerülés.

Személyesen találkozni sohasem szabadna velük. Veszélyes bűnözők, akiket a rendőrség üldöz.

Hogyan éri el a csaló, hogy higgyen nekik az áldozat?

A kibercsalók gyakorlott és sokszor professzionálisan működő bűnözők, akik kifinomult módszerekkel dolgoznak. Előre megtervezett forgatókönyv alapján tevékenykednek, kiválóan manipulálnak, és rendkívül meggyőzően kommunikálnak. Előfordul, hogy minimálisan módosított hanggal (pl. hangtorzító eszközzel) hívják fel áldozataikat.

A leggyakoribb megtévesztési módszereik:

- Hivatalos személy szerepében lépnek fel – például rendőrként vagy banki szakemberként mutatkoznak be, és azt állítják, hogy az áldozatot védeni szeretnék egy online csalással szemben. Elmondják, mit kell tennie, hogy elkerülje a veszteséget vagy a jogi következményeket.
- Vészhelyzetet szimulálnak – azt állítják, gyanús tranzakciót észleltek az áldozat bankszámláján, és azt javasolják, hogy a pénzt egy „biztonságos” számlára helyezze át.
- Kihagyhatatlan lehetőséget kínálnak – például rendkívül jövedelmező, de egyszeri befektetési lehetőséget, amely sürgős döntést igényel.
- Hamisítják a hitelességet – például a bankok kommunikációs stílusát, e-mail-címeket, hívószámokat utánoznak. A levelezés tárgyilagos, a hívás során akár rögzítést is említenek, hogy még meggyőzőbbek legyenek.
- Stresszhelyzetet teremtenek – az áldozatot nyomás alá helyezik, siettetik a döntéshozatalt, így csökkentve az esélyét annak, hogy végiggondolja, amit hall.
- Valótlan, de csábító ajánlatokkal keresik meg – például világhírű márkák termékeit kínálják akár 80%-os kedvezménnyel egy online vásárlási akció keretében.
- Fenyegetéssel vagy zsarolással próbálkoznak – például azt állítják, hogy a számítógép vírussal fertőzött, vagy hogy sértő tartalmú képeket fognak nyilvánosságra hozni, ha az áldozat nem fizet.
- Érzelmi kötődést alakítanak ki – romantikus kapcsolatot kezdeményeznek, kihasználva a magányt és a szeretet utáni vágyat. Előadják magukat szimpatikus, gondoskodó, vagy éppen elesett emberként.
- Barátként közelednek – figyelmes hallgatóságnak mutatják magukat, akik megértik és támogatják az áldozatot, ezzel fokozatosan leépítve annak bizalmatlanságát.

A lehetséges áldozatok, reakciójuk és kezelésük

Életkortól, nemtől, iskolai végzettségtől, anyagi helyzettől, neveltetéstől, ideológiai hovatartozástól, a társadalomban elfoglalt státusztól függetlenül bárki lehet online csalás áldozata.

A tapasztalatok azt mutatják, hogy bár vannak, akik esetében nagyobb a kitettség, hogy online csalás áldozatává válnak, de semmiképpen nem lehet meghatározni és körülírni olyan pszichológiai gyengeségeket, amelyek az áldozati célcsoport jellemzőjeként lehetne meghatározni.

Az online csalás áldozatául esett személyek a legkülönbözőbb módon reagálhatnak és fordulhatnak rendőrségi és/vagy szolgáltatói ügyintézőhöz segítségért. A csalás és a csalás általi kiszolgáltatottság (elvesztette a pénzének egy részét vagy akár a teljes megtakarítását) minden embernél más reakciót vált ki. A reakciók nem mindig vannak összefüggésben az elvesztett pénz nagyságával, hiszen egy adott összeg minden ember számára más jelentőséggel bír.

Az online csalás áldozatai az alábbi érzelmi állapotokban lehetnek, amikor felkeresik a rendőrséget vagy a szolgáltató cég ügyintézőjét:

- Szégyenérzet a társas környezet (család, barátok, ismerősök) vélt vagy valós megítélése miatt.
- Önvád és bűntudat, az áldozat önmagát okolja a történtekért.
- Önértékelési zavar, amely a saját ítélőképességbe vetett bizalom megrendüléséhez vezet.
- Kognitív feldolgozási kísérletek, az események logikai-oksági láncolatának rekonstruálása és értelmezése.
- Bizalomvesztés a digitális technológiák, a pénzügyi szolgáltatók vagy általánosan a társadalmi rendszerek iránt.
- Tartós szorongás és veszélyérzet, különösen az online tér és a saját otthoni környezet biztonságosságának megkérdőjeleződése esetén.
- Félelem a jövőbeli ismételt áldozattá válástól, amely tartós pszichés feszültséget generálhat.
- Ingerlékenység, az alvásminőség romlása, csökkent koncentrációs képesség.
- Feszültség, ami akár állandósulhat is,
- Védtelenség és kontrollvesztés élménye, amely a személy autonómiájának sérüléseként élhető meg.
- Disszociatív tünetek – például emlékezetkihagyás, a realitásérzék csökkenése – különösen a súlyosabb pszichotraumatikus élményeket követően.
- Egzisztenciális szorongás, amely a pénzügyi stabilitás megrendülése miatt alakul ki, különösen akkor, ha a csalás a megélhetést közvetlenül veszélyezteti.

A bejelentések, feljelentések során az ügyintézőknek figyelemmel kell lennie az ügyfél lelkiállapotára, és különös figyelmet kell fordítania arra, hogy szakmailag adekvát módon, az ügyfél számára a leghatékonyabb kommunikációs stílus alkalmazásával reagáljon.

Panaszkezelési javaslatok

- Az ügyfél feltétel nélküli elfogadása: Az ügyintéző nem alkot véleményt az ügyfél személyéről, vagy az általa elmondottakról, és semmilyen negatív értékítéletet nem fogalmaz meg. A cél az empatikus, megértő hozzáállás, amely során az ügyintéző törekszik a kliens perspektívájának átvételére – „az ő szemével látni, fülével hallani, szívével érezni". Ugyanakkor az empátia mértékének olyannak kell lennie, hogy az ne veszélyeztesse a professzionális szerep megtartását.
- Értő, ítélkezésmentes figyelem: Az ügyfél mondandójának figyelmes meghallgatása ítélkezés, hibáztatás vagy tanácsadás nélkül. A kommunikációnak végig tárgyilagosnak, nyitottnak és elfogadónak kell maradnia. Kerülni kell az olyan megjegyzéseket, amelyek utólagos „okos tanácsokat" vagy címkézést tartalmaznak (pl. „Ezt el kellett volna kerülni..."). Fontos az aktív visszacsatolás – jelezni, ha az ügyintéző megértette az elhangzottakat, és kérdezni, ha nem világos valami.
- Kongruens viselkedés: Az ügyintéző kommunikációja (szóban, arckifejezésben és testbeszédben egyaránt) legyen hiteles és legyen összhangban a belső meggyőződésével. A verbális és nonverbális jelek közötti összhang növeli a hitelességet és támogatja a bizalmi kapcsolat kialakítását.
- Biztonságos, bizalmi légkör megteremtése: A cél egy olyan környezet biztosítása, amelyben az áldozat érzelmileg is biztonságban érzi magát, és meg meri osztani a történteket. Ez különösen fontos a traumatizált ügyfelek esetében.

Az online csalás másként hat a különböző életkorokban. Egy idősebb személy számára teljesen érthetetlen és valószínűtlen az, ami vele történt. Különleges bánásmódot igényelnek az időskorú áldozatok: esetükben figyelemmel kell lenni az idősödés ún. patológiás folyamataira, amikor az idős ember nem képes a beleélésre és a fantáziája is jelentősen megkopott.

Teendők kibercsalás bejelentése során

A kibercsalás gyanújának bejelentése során az egyik legfontosabb cél a további károk azonnali megelőzése, valamint az ügyfél által tapasztalt események pontos és hiteles dokumentálása. Az alábbi lépések követése különösen fontos az ügyintézők számára a hatékony kezelés érdekében:

1. Azonnali blokkolási intézkedések megtétele
2. A legkritikusabb lépés a bejelentés pillanatában annak gyors ellenőrzése, hogy a csalók hozzáférnek-e még aktív pénzügyi csatornákhoz — például folyamatban lévő átutaláshoz, személyi kölcsön igényléséhez, bankkártyás tranzakciókhoz, társkártyákhoz vagy meghatalmazással kezelt számlákhoz. Amennyiben bármilyen kockázat fennáll, a zárolást, tiltást vagy visszahívást azonnal, lehetőség szerint még a beszélgetés során meg kell kezdeni.
3. Kapcsolódó pénzintézetek vizsgálata
4. Az ügyintézőnek kell rákérdeznie, illetve meggyőződnie kell arról is, hogy a csalók nem férhettek-e hozzá más pénzintézeteknél — például egy másik banknál vagy a Magyar Államkincstárnál — vezetett számlákhoz, esetleg más magánszemély (pl. családtag) számláihoz, amelyekhez az ügyfél jogosultsággal rendelkezik. Ha ilyen hozzáférés lehetséges, a zárolásokat ezekre az esetekre is haladéktalanul ki kell terjeszteni.
5. Az események rögzítése az ügyfél elmondása alapján
6. Az eset körülményeinek pontos feltérképezése érdekében célszerű, hogy az ügyfél saját szavaival ismertesse a történteket. Ezt a beszámolót jegyzőkönyvben vagy rögzített vonalon dokumentálni kell. Ha a közlés nem egyértelmű vagy hiányos, az ügyintézőnek érzékenyen, irányítás nélkül kell rákérdeznie a részletekre — kerülve, hogy saját értelmezést vagy szavakat sugalljon az ügyfélnek.
7. Visszajelzés a megtett intézkedésekről
8. Az azonnali intézkedések végrehajtását követően az ügyfelet részletesen tájékoztatni kell a megtett lépésekről, illetve arról is, hogy van-e további teendője. Fontos annak ellenőrzése is, hogy az ügyfél megértette-e az elhangzottakat. Amennyiben bizonytalan vagy zavart, az információkat érthető módon meg kell ismételni, szükség esetén jegyzetelési lehetőséget is biztosítani (pl. lediktálás).
9. Az érzelmi reakciók kezelése empatikus módon
10. Előfordulhat, hogy az ügyfél nem csupán a csalókat, hanem saját pénzügyi szolgáltatóját is hibáztatja a történtekért. Az ügyintézőknek erre tudatosan fel kell készülniük, és az ügyfél feszültségét megértéssel, empátiával, de szakmai keretek között kell kezelniük. Az együttérző kommunikáció és a bizalom újraépítése kulcsfontosságú a további kapcsolat fenntartása szempontjából.

Javaslatok az online csalások ismétlődésének megelőzésére

Fontos alapelv, hogy bármilyen döntést hozott is az áldozat, semmiképpen sem szabad hibáztatni érte. A csalások mögött álló megtévesztési technikák gyakran professzionálisan felépítettek, és még a tájékozott, jó szándékú embereket is képesek félrevezetni. A cél nem az áldozat felelősségre vonása, hanem a jövőbeni kockázatok csökkentése és a tudatosság növelése.

Éppen ezért kulcsfontosságú, hogy minden ilyen esetet követően megfelelő tájékoztatásban részesüljön az érintett személy, amely során megismerheti azokat az alapvető szabályokat és jelzéseket, amelyek a jövőben segíthetnek elkerülni a hasonló megtévesztéseket. A megelőzés szempontjából hasznos lehet a személyes vagy online tanácsadás, edukációs anyagok biztosítása, illetve hiteles források ajánlása.

Az alábbi, megbízható weboldalakon bővebb információk, gyakorlati tanácsok és segédanyagok találhatók az online csalások felismeréséhez és megelőzéséhez:

- **KiberPajzs:** https://kiberpajzs.hu — Átfogó tájékoztatás a kibertér veszélyeiről, esettanulmányokkal és megelőzési tanácsokkal.
- **Magyar Nemzeti Bank – Fogyasztóvédelem és Pénzügyi Navigátor:** https://www.mnb.hu/fogyasztovedelem — A pénzügyi tudatosság és biztonságos bankolás elősegítésére létrehozott tartalmak.
- **Áldozatsegítő Központ:** https://vansegitseg.im.gov.hu — Jogilag és pszichológiailag támogatást nyújtó központ, amely segíti a csalás áldozatait a helyzet feldolgozásában és továbblépésben.

Ezek az oldalak nemcsak aktuális információkat nyújtanak, hanem eszközöket is adnak a felhasználók kezébe ahhoz, hogy magabiztosabban és tudatosabban mozogjanak az online térben.

8. Védekezési javaslatok

A jelszavak általános védelméről

A digitális környezetben a személyes adatok és információk védelme napjaink egyik legfontosabb biztonsági kihívása. Az olyan informatikai eszközök és rendszerek esetében, amelyeket több felhasználó is elérhet, illetve amelyekhez érzékeny adatokhoz való hozzáférés kapcsolódik, az azonosítás elsődleges védelmi vonalát a felhasználónév (user name) és a hozzá tartozó titkos kód, azaz jelszó (password) megadása biztosítja. Ez az autentikációs forma széles körben elterjedt a legkülönfélébb területeken, így például vásárlói kluboknál, munkahelyi rendszerekben, oktatási platformokon vagy online ügyfélszolgálatokon.

Az Európai Unióban az online banki és kereskedelmi szolgáltatások biztonságát jelentősen növelte a 2018-ban életbe lépett második pénzforgalmi irányelv, ismertebb nevén a PSD2 (Payment Services Directive 2). E jogszabály előírásait Magyarország 2021. január 1-től alkalmazza. A PSD2 egyik legjelentősebb újítása az erős ügyfél-hitelesítés (Strong Customer Authentication – SCA) bevezetésének kötelezettsége, amely a gyakorlatban a kétfaktoros azonosítás (2FA – Two Factor Authentication) alkalmazását jelenti.

Az erős ügyfél-hitelesítés lényege, hogy a felhasználónak nem csupán a megszokott felhasználónevét és jelszavát kell megadnia, hanem ezen túlmenően egy második, független hitelesítési tényezőt is. Ez a második tényező lehet például:

- egy időalapú, vagy egyszer használatos jelszót (OTP – One Time Password) generáló fizikai vagy szoftveres token által előállított kód,
- egy SMS-ben kapott egyedi azonosító szám,
- vagy valamilyen biometrikus azonosító (pl. ujjlenyomat, arcfelismerés, retina- vagy hangazonosítás).

Az Európai Unióban működő pénzintézetek számára kötelezővé vált az erős ügyfél-hitelesítés alkalmazása minden olyan esetben, amikor az ügyfél mobilalkalmazáson vagy internetbanki felületen keresztül kíván belépni fiókjába. Emellett a webáruházak esetében is kötelező a kétfaktoros azonosítás minden internetes bankkártyás fizetés alkalmával.

A kétfaktoros azonosítás előnyei különösen a webshopok működése során lényegesek: jelentősen csökkenthetők az online fizetési visszaélések, illetve megakadályozható, hogy egy ellopott vagy elveszített bankkártyát illetéktelenek felhasználjanak internetes vásárlásokhoz. (https://biztosdontes.hu/cikkek/ketfaktoros-hitelesites)

A legelterjedtebb és legismertebb egyéni védekezési forma a megfelelően megválasztott és biztonságosan kezelt jelszó. E jelszavak hatékonyságának megértéséhez érdemes betekinteni az informatikai háttérfolyamatokba, különösen a jelszavak tárolásának és ellenőrzésének módjába.

Minden jelszóhoz a szolgáltatók egy ún. kriptográfiai algoritmus segítségével egyedi azonosítót, azaz Hash kódot rendelnek hozzá. A Hash függvények olyan matematikai műveletek, amelyek a bemeneti szövegből (pl. a jelszóból) egy egyedi karaktersorozatot (Hash értéket) generálnak. A mai informatikai gyakorlatban nem ismert olyan hatékony algoritmus, amely visszafejtené a Hash kódból az eredeti jelszót – ez

garantálja a titkosságot. A szolgáltatók tehát nem magát a jelszót tárolják, hanem csak a belőle képzett Hash értéket. Amikor a felhasználó bejelentkezik és megadja jelszavát, a rendszer ugyanazzal a Hash algoritmussal generál egy új Hash értéket, és ezt veti össze az adatbázisban tárolt Hash kóddal. Amennyiben a két Hash érték megegyezik, az elsődleges azonosítás sikeresnek minősül, és a rendszer kéri a másodlagos, kétfaktoros azonosító megadását.

Korábban a szolgáltatók gyakran előre definiált jelszavakat biztosítottak a felhasználók számára, azonban napjainkban elterjedt gyakorlat, hogy az első bejelentkezés során a felhasználónak kötelező új, saját jelszót megadnia. Emellett a legtöbb rendszer előírja a jelszavak rendszeres időközönkénti (általában 3–12 havonta történő) megváltoztatását a biztonsági kockázatok minimalizálása érdekében.

A jelszavak minősége kulcsfontosságú. Egy erős jelszó általában legalább 12 karakterből áll, és tartalmaz kis- és nagybetűket, számokat, valamint speciális karaktereket. Kerülendők a szótári szavak, a személyes információk (pl. születési dátum, név), valamint az ismétlődő vagy sorozatszerű karakterek. A jelszavak létrehozásához használhatóak jelszógenerátor eszközök, amelyek véletlenszerű, nehezen kitalálható karakterláncokat hoznak létre. A hosszú és összetett jelszavak kezelhetőségét jelentősen megkönnyítheti egy megbízható jelszókezelő alkalmazás (pl. Bitwarden, LastPass, KeePass), amely titkosított formában tárolja a jelszavakat és automatikusan kitölti azokat a bejelentkezés során.

Tekintettel arra, hogy egy adott felhasználó több online szolgáltatást is használhat (pl. email, közösségi média, internetbank, webshop), kiemelten fontos, hogy minden felülethez egyedi jelszót használjon. Ennek hiányában egy kevésbé védett rendszer feltörése esetén a támadó hozzáférést nyerhet más, komolyabb biztonsági szintet igénylő platformokhoz is. Az ún. „jelszó-újrafelhasználás” az egyik leggyakoribb biztonsági rés a felhasználói szokásokban, így ennek tudatos elkerülése alapvető jelentőségű.

A jelszavak biztonságos kezelése nem csupán a technikai megválasztásukban, hanem azok tárolásának módjában is kulcsfontosságú. A gyakorlatban elkövetett leggyakoribb hibák egyike, ha a felhasználó a jelszavait – különösen a mobilkészülékhez kapcsolódókat – magában a telefonkészülékben rögzíti. Ez kockázatos gyakorlat, különösen abban az esetben, ha ugyanarra az eszközre érkezik meg a kétfaktoros azonosító (például SMS formájában). A mobiltelefon elvesztése ilyen esetben közvetlen veszélyt jelenthet a netbank vagy más érzékeny rendszerbe való illetéktelen belépés szempontjából. Hasonló megfontolásból szintén kerülendő a bankkártyák PIN kódjának mobiltelefonon történő tárolása vagy bárminemű, azonosítható formában való rögzítése.

A jelszavak kiszivárgásának kockázata is valós fenyegetés. Számos olyan eset ismert, amikor tömeges adatlopás során jelszavak kerültek nyilvánosságra, és ezek adathalász támadások vagy más visszaélések alapjául szolgáltak. A felhasználók számára elérhetők olyan nyilvános ellenőrző szolgáltatások, ahol egyszerűen ellenőrizhető, hogy e-mail címük vagy jelszavuk szerepelt-e valaha adatszivárgásban. Az ilyen események után azonnali jelszócsere, valamint a kétfaktoros azonosítás bekapcsolása ajánlott.

A jelszavak jövője is változóban van. Egyre több szolgáltatás tér át az úgynevezett jelszómentes hitelesítésre (passwordless authentication), amely olyan technológiákat alkalmaz, mint a biometrikus azonosítás, hardveres biztonsági kulcsok vagy a FIDO2/WebAuthn protokoll. Ezek célja a biztonság növelése mellett a felhasználói élmény egyszerűsítése – hiszen egyre kevesebbet kell ténylegesen jelszavakat megjegyezni.

Nem szabad figyelmen kívül hagyni a felhasználói viselkedést sem, hiszen a legmodernebb technológiák is hatástalanok lehetnek, ha a felhasználó nincs tisztában az alapvető biztonsági szabályokkal. Az emberi tényező – a szokások, a kényelem, a biztonsági tudatosság hiánya – gyakran a leggyengébb láncszem a védelemben. Ezért különösen fontos az oktatás és a tájékoztatás mind a magánszemélyek, mind a munkavállalók körében. A vállalatoknál egyre gyakrabban kötelező IT-biztonsági tréningeket és jelszóbiztonsági auditokat tartanak.

A jelszavak tehát továbbra is alapvető szerepet töltenek be a digitális világ védelmében, azonban a technológiai fejlődés és a fenyegetések változása új megközelítéseket és szemléletmódot követel. A jelszavak mellett – és helyett – egyre nagyobb szerepet kapnak a komplex hitelesítési rendszerek, a felhasználói edukáció, valamint a személyre szabott védekezési módszerek.

Az INTERPOL konkrét csalástípusonkénti figyelmeztetései

Habár az eddigiekben részletesen bemutattuk a kibercsalási típusokat, tekintettel arra, hogy „ismétlés a tudás anyja” most az Interpol tapasztalatai alapján készült csalástípusokat osztjuk meg a hozzájuk tartozó figyelmeztetésekkel.

Hallgasson mindig a józan ész szabályaira és ezzel csökkentse annak esélyét, hogy pénzügyi bűncselekmény áldozatává váljon!

A bűnözők igyekeznek gyorsan kihasználni áldozataik tájékozatlanságát és/vagy kiszolgáltatottságát. Az okostelefonoktól és táblagépektől az internetre csatlakoztatott készülékekig terjedő eszközök széles körű elterjedtsége még nagyobb kockázatoknak tett ki mindenkit.

A józan észre alapuló néhány szabály betartásával azonban erőteljesen csökkenthető a kitettségünk és annak kockázata, hogy csalók áldozatává váljunk.

Repülőjegy-csalás

Feltétlenül óvatosan kell eljárni az olyan előnyösnek tűnő vásárlási, pl. a repülőjegy-ajánlatokkal, amelyek „túl szépek ahhoz, hogy igazak is legyenek.”

Ha bárki úgy véli, hogy megtalálta élete nagy ajánlatát, amikor azt látja, hogy a Last minute repülőjegy, vagy bármilyen termék a szokásos ár töredékéért kapható, akkor legyen nagyon óvatos a vásárlás előtt. A hiszékeny vevő ugyanis többnyire jegy, szolgáltatás és termék nélkül marad, miközben a pénzét a bűnözők bezsebelték.

Hogyan működik a repülőjegy-csalás?

a. A bűnözők lopott, feltört vagy feltört hitelkártyák adatait használják repülőjegyek vásárlásához.

b. A bűnözők ezeket a jegyeket akciós áron kínálják eladásra olyan professzionális megjelenésű weboldalakon vagy közösségi hálózati fiókokon keresztül, amelyek mintha törvényes utazási irodáké vagy ügynöké lennének.

c. A bűnözők „utazási irodái” azonnali fizetést kérnek, jellemzően készpénzzel, banki átutalással vagy virtuális valutával.

d. A fizetés megtörténte után a bűnöző elküldi a repülőjegy-foglalási visszaigazolást az eredeti vásárlási adatok törlésével.

Hol ebben a probléma?

Ha ön ilyen módon vásárol repülőjegyet, akkor a pénzét közvetlenül a bűnözők kezébe adja, akik azt más súlyos bűncselekmények finanszírozására használják fel.

Ha a bűnöző által a jegyvásárláshoz használt lopott hitelkártya tulajdonosa a menetrend szerinti járat indulása előtt jelenti be a lopást, akkor a légitársaság törli a jegyet, és ön nem tud elutazni.

Ha az ellopott hitelkártya tulajdonosa a csalárd vásárlást az utazás során jelenti be, akkor ön kint rekedhet, mert a retúrjegyét érvénytelenítik. Persze ekkor jöhet a kalandos vakáció a Mézga családdal!

INTŐ JELEK, HOGY A JEGYELADÁS CSALÁRD LEHET:

Van néhány olyan intő jel, amire figyelni kell, ha rendkívül alacsony áron hirdetik meg álmai úticéljára tartó járat jegyét:

Lényegesen olcsóbb a jegy ára, mint bárhol máshol? – Mivel 100 százalékos nyereséget termelnek, a bűnözők akciós árakat kínálnak, hogy rávegyék a vásárlót az „ajáne latuk” elfogadására.

Az indulás időpontja a következő napokban van? – A bűnözők csak egy vagy két nappal a járat indulása előtt (vagy akár ugyanazon a napon) kínálják a csalárd módon vásárolt jegyeket, mielőtt a valódi hitelkártya-tulajdonos észrevenné a csalást és töröltetné a jegyet.

Készpénzben vagy banki átutalással kell fizetnie? – Ezekkel a módszerekkel a pénze azonnal eltűnik, és csalás esetén kevés lehetősége lesz azt visszaszereznie.

Az utazási iroda weboldala/közösségi média-fiókja tartalmazza-e az elérhetőségeinek teljes körét, beleértve az iroda fizikai címét és vezetékes telefonszámát? – Ha nem, akkor a vásárlás előtt végezzen némi kutatást, hogy megbizonyosodjon arról, valóban létező, törvényes utazási irodáról van-e szó.

TIPPEK A BIZTONSÁGOS VÁSÁRLÁSHOZ

a. Foglaljon repülőjegyet közvetlenül a légitársaságtól, vagy egy olyan jó nevű utazási irodától, amelyet az Ön országának illetékes hatóságai regisztráltak.

b. Csak biztonságos fizetési rendszerrel rendelkező weboldalakról vásároljon jegyet online (pl. https a webcím elején).
c. Tájékozódjon arról az utazási irodáról, amelytől vásárolni szeretne. Van-e hivatalos weboldala? Vannak-e róla pozitív vagy negatív online vélemények? Van-e mód arra, hogy probléma esetén kapcsolatba lépjen velük?
d. Vásárlás előtt ellenőrizze az utazási iroda Általános Szerződési Feltételeit, különösen a visszatérítési szabályzatot és eljárásokat.
e. Keresse a Nemzetközi Légi Szállítási Szövetség (IATA) logóját az utazási iroda honlapján.

Üzleti e-mail kompromittáló csalás

Legyen óvatos – ne hagyja, hogy a csalók becsapják, és az ő számlájukra utaljon pénzt. A bűnözők feltörik az e-mail rendszereket, vagy social engineering taktikákat alkalmaznak, hogy információkat szerezzenek a vállalati fizetési rendszerekről. Ezután a csalók megtévesztik a vállalat alkalmazottait, hogy pénzt utaltassanak át a saját bankszámlájukra.

Védje meg vállalati rendszereit a hackelési kísérletektől:

a. Használjon víruskeresőt, tűzfalat és egyéb eszközöket, és rendszeresen vizsgálja át az Ön által használt számítógépeket, tableteket és mobileszközöket a rosszindulatú programok fertőzésének megelőzése érdekében.
b. Tartsa naprakészen személyi és üzleti számítógépeit: figyeljen a biztonsági riasztásokra, frissítse a biztonsági javításokat, és rendszeresen végezzen rendszerellenőrzéseket.
c. Győződjön meg arról, hogy e-mail fiókjai jól védettek, és ne ossza meg azok jelszavát senkivel.
d. NE kattintson olyan mellékletekre vagy linkekre, amelyekre nem számított, még akkor sem, ha ártalmatlannak hangzó nevük van (például számla). Azok ugyanis gyakran tartalmazhatnak rosszindulatú programokat, amelyek hozzáférést biztosítanak az e-mailek/számítógépes tevékenységek figyeléséhez.
e. Engedélyezze a spamszűrőket, és blokkolja a gyanús vagy feketelistán szereplő webhelyekhez való hozzáférést.

Legyen éber a gyanús vagy váratlan „sürgős” fizetési kérésekkel, vagy módosításokkal szemben.

a. Figyelmesen nézze meg a feladó e-mail-címét. A bűnözők gyakran hoznak létre fiókokat az üzleti partnereihez nagyon hasonló e-mail-címekkel, ezért tartsa nyitva a szemét!
b. Terjessze a hírt, hogy a bankszámlákkal foglalkozó kollégái értesüljenek az átverési kísérletről.

c. Ha e-mailt kap a fizetési mód vagy a bankszámla megváltozásával kapcsolatban, vegye fel a kapcsolatot a fizetés kedvezményezettjével egy másik csatornán (pl. telefonon), hogy ellenőrizze ezt az igényt. NE válaszoljon közvetlenül az e-mailre!
d. Ellenőrizze a webhelyek hitelességét, mielőtt bármilyen személyes vagy érzékeny adatot megadna.

Kerülje el, hogy támadás célpontjává váljon:

a. NE tegyen közzé érzékeny vagy személyes adatokat a közösségi médiában. Ezt ugyanis a csalók felhasználhatják arra, hogy Önt vegyék célba.
b. Iratmegsemmisítővel aprítson fel minden bizalmas nyomtatott dokumentumot.
c. Használjon különböző jelszavakat minden fiókhoz, azokat rendszeresen változtassa meg, és engedélyezze a kétfaktoros hitelesítést minden fiókjában, amikor csak lehetséges.
d. Használjon olyan, legalább nyolc karakteres erős jelszavakat, amelyek számokat, szimbólumokat, valamint nagy- és kisbetűket egyaránt tartalmaznak.

Tennivalók, ha már kifizette/elutalta a pénzt:

a. Gyűjtse össze a tranzakcióval kapcsolatos összes dokumentumot és a kapott e-maileket/számlákat, és a lehető leghamarabb jelentse az esetet a helyi rendőrségen.
b. Azonnal értesítse bankját a csalárd tranzakcióról. A másodperceknek is jelentősége van! A bankok azonnal megpróbálják visszahívni a pénzeszközöket.

Telefonos csalások

A telefonos csalások tipikus formái és gyakorlata:

a. Ismeretlen hívások, még valódinak tűnő telefonszámról is, „banki, jegybanki, bankfelügyeleti, közüzemi szolgáltatói, kórházi, rendőri, adóhivatali, kormányzati” stb. tisztviselőktől.
b. E-mailek nemzeti vagy globális rendőrségi, közüzemi szolgáltatói, egészségügyi, adóhivatali, vámhivatali, bankfelügyeleti, kormányzati stb. hatóságoktól.
c. Személyes adatok kérdezése, sürgetés, sokkhatást jelentő történet/helyzet. A kérdezett adatok olyanok, amelyeket a szolgáltatók vagy tudnak, vagy nincs rájuk szükségük.
d. Rosszindulatú pénzkimentési, biztonságos megoldási javaslat, programok, hivatkozások, appok letöltetése.

Összefoglalva, a csalók törvényes cégeknek adják ki magukat, hasonló neveket, webhelyeket és e-mailcímeket használnak, hogy becsapják a gyanútlan személyt/

nyilvánosságot. Gyakran proaktívan megkeresik a kiszemelt áldozatot telefonhívással, e-mailekben vagy üzenetekben a személyes csatornákon vagy a közösségi média platformokon.

a. NE adjon meg semmilyen személyes vagy bizalmas információt telefonon.
b. NE bízzon meg valakiben, aki azt állítja, hogy kormányzati, ügyészségi vagy rendőrségi tisztviselő; ezek ugyanis soha nem követelnek fizetést vagy bizalmas információkat.
c. Vegye fel a kapcsolatot a helyi rendőrséggel, a bankjával vagy az adott szolgáltatóval/hivatallal, hogy ellenőrizze a hívó féltől kapott információkat.

A pénzügyi és szolgáltatói szektor csalásgyanú esetén azonnal letiltja a számlát, majd értesíti az ügyfelet a tiltásról. Azaz, akit hívnak, annak legfeljebb annyi lehet a teene dője, hogy ő veszi fel személyesen a kapcsolatot a szolgáltatóval és állíttatja helyre a szolgáltatást.

Figyelmeztető jelek online vásárlásnál

Ha online szeretne árut vásárolni, vagy szolgáltatást kínáló e-maileket vagy linkeket szeretne kapni, figyeljen a lehetséges átverés jeleire, hogy megvédje magát és pénzét.

a. Vásárlás előtt önállóan – az ajánlattevő bevonása nélkül – ellenőrizze a termékeket kínáló céget vagy magánszemélyt;
b. Legyen tisztában a hamis weboldalakkal – a bűnözők gyakran olyan webcímet használnak, amely szinte teljesen megegyezik a valóságossal, pl. „abc.org” az „abc.com”, vagy „bank.nu” a „bank.hu” helyett;
c. Vásárlás előtt ellenőrizze a vállalatról közzétett online véleményeket – például panaszkodtak-e más vásárlóktól az ígért termékek nem kézhezvétele miatt;
d. Legyen óvatos, ha a vállalat székhelyétől eltérő országban található bankszámlára kellene utalnia;
e. Ha úgy véli, hogy csalás áldozata lett, azonnal értesítse bankját, hogy a fizetést még leállíthassák. Majd tegyen a rendőrségen feljelentést.
f. Ne kattintson olyan hivatkozásokra és ne nyisson meg olyan mellékleteket, amelyekre nem számított, vagy amelyek ismeretlen feladótól származnak;
g. Legyen óvatos a kéretlen e-mailekkel, amelyek orvosi felszerelést kínálnak, vagy személyes adatait kérik orvosi vizsgálatokhoz. A törvényes egészségügyi hatóságok általában nem lépnek kapcsolatba a nagyközönséggel ilyen módon.

Kézbesítés elmulasztásával kapcsolatos csalás

A kézbesítés elmulasztásával kapcsolatos csalások során a bűnözők nagyon keresett árukat ígérnek az áldozatoknak, elfogadják a fizetést, de soha nem szállítják le az árut, vagy utánvéttel olyan értéktelen árut küldenek, amire az áldozat nem tartott igényt. Bár az elv egyszerű, a csalási rendszer gyakran kifinomult. A bűnözők egy jól bevált működési módot alkalmazhatnak, amely bármilyen termékhez illeszkedik, legyen szó orvosi felszerelésekről, kölyökkutyákról, irodaszerekről vagy elektronikai cikkekről.

Romantikus csalások

A bűnözők a közösségi médián keresztül „érzelmi kapcsolatot” alakítanak ki az áldozatokkal azzal a végső szándékkal, hogy tőle pénzt szerezzenek.

a. Széles körben ossza meg ismerősei körében életének nagy szerelmét és a vele való kapcsolatot.
b. Legyen éber, ha olyan személy fordul Önhöz, akit nem ismer közelebbről, különösen akkor, ha az illető valamilyen ürüggyel pénzkérést hoz szóba.
c. Gondolja át kétszer is, mielőtt pénzt utalna, bármennyire hihetőnek is tűnik a kérés.
d. NE tegyen közzé személyes/bizalmas információkat a közösségi médiában.

Befektetési/”kazánházi”-csalás

Ennél a csalási módnál arra próbálják rábírni az áldozatokat, hogy csalárd vagy értéktelen részvényekbe fektessenek be, mesés hozamígéretek mellett.

a. Legyen gyanakvó, ha ismeretlen helyről vagy nem várt hívást kap vonzó befektetési lehetőségekről.
b. Ellenőrizze a felajánlott befektetési termékek hitelességét, és konzultáljon legalább egy független pénzügyi tanácsadóval.
c. NE utaljon pénzt senkinek pusztán hívás, mail, prospektus alapján.

Szexzsarolás

Egy szimpatikusnak tűnő idegen rábírja az áldozatokat (gyakran férfiakat, fiatalokat), hogy meztelenül folytatott videócsevegésekben vegyenek részt, amelyeket titokban rögzítenek, majd zsarolásra használnak.

a. Ne feledje, hogy az interneten semmi sem privát, és az oda került adatok általában nem törölhetők teljesen/véglegesen.
b. Tegyen fel releváns kérdéseket, és próbálja meg ellenőrizni a személyazonosságát annak, aki megkeresi.
c. Ha zsarolási fenyegetést kap, NE fizessen, hanem jelentse a rendőrségen.

Bankkártyák

Habár ezt a témát már alaposan tárgyalta a könyv, érdemes a következő pontokat megjegyezni.

a. Tartsa biztonságban bankkártyáit. Rendszeresen ellenőrizze bank-/hitelkártyaszámláit.

b. Alaposan nézze meg az ATM-eket és a fizetési (POS) terminálokat, hogy megbizonyosodjon arról, hogy nincsenek gyanús (előtét) tárgyak a kártyanyílás körül.

c. Fizetési terminálok használatakor tartson, és tartasson elegendő távolságot másoktól.

d. NE adja meg PIN-kódját/jelszavát. A bankok soha nem kérik ezt telefonon vagy e-mailben.

e. NE adja meg banki adatait, hacsak nem Ön kezdeményezte a fizetési folyamatot.

f. Ha bankjától olyan e-mailt vagy SMS-t kap, hogy frissítse az adatait vagy vegye igénybe a különleges ajánlatát, akkor NE kattintson az e-mailben található linkre. Ehelyett keresse fel meg a bank hivatalos weboldalát (ne keresővel, hanem minden esetben végig gépelve a teljes honlapcímet!), vagy lépjen kapcsolatba a bankkal.

g. NE fizessen online, és NE vegyen igénybe online banki szolgáltatást, ha nyilvános (pl. éttermi vagy repülőtéri) W-Fi-hálózathoz csatlakozik, mert azon adatait könnyen ellophatják.

A tényleges kártyalopás mellett a bűnözők különféle módszereket alkalmaznak az adatok megszerzésére, beleértve az ATM-eknél vagy jegykiadó automatáknál történő „kártyalefölözést” és az adathalászatot. Az emberek gyakran csak akkor szereznek tudomást arról, hogy kártyaadataikat ellopták, amikor már túl késő. Az ellopott adatokat hamis kártyák létrehozására használhatják fel, vagy később felhasználhatják a kártya nélküli csaláshoz (CNP).

A csalók a megszerzett bankkártya adatokat arra használják, hogy árukat vásároljanak az áldozatok nevében, vagy jogosulatlanul szerezzenek pénzeszközöket az áldozatok számláiról. A feltört kártyaadatokat az internet fekete piacán, a darknet-en is értékesíthetik. Sok esetben az egyik országban ellopott adatokat máshol használják fel, ami megnehezíti a nyomon követést.

Pénzmosás

Legyen gyanakvó, ha bármilyen indokkal arra kérik, engedje meg valaki másnak, hogy pénz fogadására és továbbítására használja az Ön bankszámláját. Mivel minden körözés vagy eltiltás alatt nem álló személy tud saját magának bankszámlát nyitni, ilyen segítségre nincs szüksége senkinek, hacsak nincs valamilyen hátsó szándéka.

Legyen óvatos a nagy pénzösszegű készpénzes tranzakciókkal. Nagy összegek átutalására sokkal több biztonságos, elektronikus fizetési mód áll rendelkezésre.

Ne hagyja, hogy befolyásolhassák. A bűnszövetkezetek gyakran úgy működnek, hogy először valamelyik közösségi média felületen személyes kapcsolatot alakítanak ki áldozataikkal, mielőtt rávennék őket arra, hogy valaki más helyett végezzenek pénzügyi műveleteket (átutalásokat).

Kiber fogalomtár

Adathalászat: lásd phishing

APT (Advanced Persistent Threat): Az APT csoportok olyan kiberbűnözői szervezetek, amelyek hosszú távú, célzott támadásokat hajtanak végre az áldozataik ellen, akik jellemzően nagyobb gazdasági szervezetek, elvétve államok. Az APT csoportok célja általában olyan adatok megszerzése, amelyek titkosítottak, érzékenyek, személyes jellegűek vagy szellemi tulajdon részét képzik. Továbbá, bármely olyan adat célponttá válhat, amely zsarolásra vagy a célszemély megkárosítására használható és komoly anyagi vagy politikai haszonnal járhat. Az egyes szereplők motivációi eltérhetnek egymástól, és jelentős különbségek adódhatnak képességeik, kifinomultságuk, képzési szintjük és a tevékenységükhöz nyújtott támogatások tekintetében. Ezek közül a nemzetállami szereplők számítanak a legkifinomultabb kártékony aktoroknak, akik elkötelezettek, valamint korszerű erőforrásokkal és eszközökkel rendelkeznek. Többnyire a lehető legnagyobb gondossággal végzik műveleteiket azért, hogy elkerüljék a lebukást. Ennek érdekében alapos felderítést végeznek, hogy információkat gyűjtsenek a célpont szervezeti és informatikai infrastruktúrájáról, a vállalati kultúráról, az alkalmazottakról, a biztonsági irányelvekről és eljárásokról. Képesek alkalmazkodni a célpontnál bevezetett biztonsági ellenőrzések változásaihoz. Különleges jellemzőik mellett az APT-k általában időt szánnak a nulladik napi sebezhetőségek felfedezésére és olyan exploitok vagy rosszindulatú programok kifejlesztésére, amelyeket a célpontok nem tudnak időben észlelni. Az ilyen fenyegetéseket elkövető szereplők motivációi jellemzően politikai vagy gazdasági jellegűek.
https://nki.gov.hu/wp-content/uploads/2023/07/APT-csoportok.pdf
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Adware: Reklámot megjelenítő speciális futtatható alkalmazás, elsődleges célja olyan reklámanyag kézbesítése, amely a felhasználó számára váratlanul, illetve kéretlenül érkezik. Sok adware alkalmazás hajt végre nyomkövető funkciókat, éppen ezért sorolják ezeket a fürkésző technológiák közé. Számos felhasználó el szeretné távolítani a gépéről ezeket a kéretlen reklámprogramokat, ha azok kémkednek a szokásaik után, nem kívánják látni az adware által megjelenített reklámokat, illetve zavarja őket a reklámprogramnak a rendszer teljesítményét korlátozó hatása. Másrészt vannak olyan felhasználók is, akik részben meg szeretnék tartani ezeket a reklámprogramokat, mert azok jelenléte költségcsökkentő egy adott program vagy szolgáltatás használata esetében, vagyis szándékos, illetve hasznos. Jó példa erre az olyan típusú reklám, amely egyenesen segíti vagy kiegészíti azt, amit a felhasználó alkalmaz, illetve amit éppen keres.
https://www.eset.com/hu/termektamogatas/veszelyek/
https://hu.wikipedia.org/wiki/Rekl%C3%A1mprogram

Ez a fejezet a szerzők egy korábbi közös tanulmányából (Kovács – Terták, 2025) utánközlés.

Angler phishing (hamis szolgáltatói ügyintézés a közösségi médiában): A „horgász adathalászat” az adathalász támadások egy sajátos típusa, amely a közösségi médiában terjedt el. A kiberbűnözők tisztában vannak azzal, hogy a különböző szolgáltatók egyre gyakrabban használják a közösségi médiát az ügyfeleikkel való kapcsolattartásra: nemcsak marketingre és promóciós célra, hanem akár panaszkezelés vagy problémamegoldás céljából is. Az elkövetők figyelik a szolgáltatók közösségi csatornáira érkező ügyfélpanaszokat, majd a szolgáltató képviselőjének kiadva magukat – annak közösségimédia-profilját lemásolva, vagy ahhoz nagyon hasonló, de hamis fiókról – felveszik a kapcsolatot a panasz bejelentőjével. Látszólag a panasz kezelése, a bejelentett probléma érdekében érzékeny információkat (személyes, banki, valamint különböző fiókbejelentkezési adatokat, jelszavakat) kérnek el az ügyféltől, amelyekkel aztán hozzáférhetnek annak bankszámláihoz és különböző online fiókjaihoz.
https://kiberpajzs.hu/csalastipusok/szamitogepes/angler-phishing/
https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/angler-phishing-hamis-szolgaltatoi-ugyintezes-a-kozossegi-mediaban

Anti-Phishing: Az anti-phishing olyan védekezési gyakorlat, amelynek célja az adathalász támadások megelőzése vagy mérséklése. Ezek során a támadók megbízhatónak tűnő forrásokat utánozva próbálnak érzékeny adatokat kicsalni. Az anti-phishing technikák kombinálják az emberi éberséget és a fejlett szoftveres megoldásokat, például e-mail szűrőket, linkelemzést és rosszindulatú tartalmak kiszűrésére szolgáló integrált anti-malware rendszereket. A cél egy többrétegű, megelőző és helyreállító biztonsági védelem kialakítása.
https://perception-point.io/guides/phishing/how-to-prevent-phishing-attacks/

Antivírus: Az „antivírus” egy szoftver, amely véd a számítógépes vírusok és más károsító programok ellen. A vírusirtó programok célja, hogy azonosítsák, kiszűrjék és megszüntessék a veszélyes szoftvereket a számítógépről, így megvédve a felhasználó adatvédelmét és a rendszer stabilitását. Webshopok esetében a vírusirtók kiemelkedően fontosak, mivel védelmet nyújtanak mind a vásárlók, mind a kereskedők adatainak biztonsága érdekében, lehetővé téve ezzel a biztonságos online tranzakciókat. Az antivírus programok folyamatosan figyelik a rendszeres szoftver-, fájl- és weboldalaktivitásokat, hogy észleljék a potenciális fenyegetéseket. A legújabb vírusminták és támadási formák elleni védelem érdekében az antivírus szoftverek folyamatosan frissítéseket kapnak. Az észlelt kártevőket azonnal eltávolítják vagy karanténba helyezik a további károk elkerülése érdekében.
https://webshopautomatizalas.hu/e-comm-lexikon/antivirus

Attack Vector: A kiberbiztonsági támadási vektor egy olyan útvonal, amelyet egy hacker vagy rosszindulatú szereplő használ, hogy jogosulatlan hozzáférést szerezzen egy hálózathoz, szerverhez, alkalmazáshoz, adatbázishoz vagy eszközhöz a rendszer sebezhetőségeinek kihasználásával. Ezeken keresztül különféle támadások indíthatók, például adatlopás, kártékony programok terjesztése vagy zsarolóvírusos támadások. A támadási vektorok gyakori formái közé tartoznak a rosszindulatú e-mail-mellékletek, fertőzött linkek, felugró ablakok és social engineering technikák. Az ilyen támadások mögött gyakran pénzügyi indíték, adatlopás vagy politikai cél húzódik meg.
https://www.fortinet.com/resources/cyberglossary/attack-vector

Cyber Attribution: A kiberattribúció célja annak megállapítása, hogy ki követte el a kibertámadást, vagyis a támadó, illetve annak esetleges közvetítője személyazonosságának vagy tartózkodási helyének azonosítása. Az azonosítás eredményeként kiderülhet egy személy neve, felhasználói fiókja, álneve, vagy más olyan információ, amely egy adott személyhez köthető. A helymeghatározás vonatkozhat fizikai (földrajzi) helyre vagy virtuális helyre is, például IP-címre vagy Ethernet-címre.
https://en.wikipedia.org/wiki/Cyber_attribution

Backdoor: A backdoor (magyarul: hátsó ajtó) egy rejtett, jellemzően kártékony program vagy kódrészlet, amely lehetővé teszi, hogy a támadók megkerüljék a számítógép, hálózati eszköz (pl. router), vagy más beágyazott rendszer hitelesítési és titkosítási mechanizmusait. Célja, hogy engedély nélküli hozzáférést biztosítson a fertőzött eszközhöz, gyakran teljes irányítást adva a támadónak. A backdoorok általában a háttérben, észrevétlenül működnek, így nehéz őket felismerni. Működésük hasonlít más típusú kártevőkhöz, de az egyik legveszélyesebb fajtának számítanak, mivel lehetővé teszik a felhasználó megfigyelését, fájlok módosítását, új (gyakran szintén kártékony) programok telepítését, vagy akár további eszközök megtámadását. Ezek a programok gyakran további funkciókkal is rendelkeznek: képesek billentyűleütések rögzítésére, képernyőképek készítésére, adatállományok titkosítására, és egyéb adatvédelmet veszélyeztető tevékenységek végrehajtására. A backdoorok súlyos biztonsági kockázatot jelentenek, különösen azért, mert működésükhöz nincs szükség folyamatos külső irányításra. Fontos megjegyezni, hogy ezek a kártevők jellemzően nem képesek önállóan bejutni a rendszerbe a felhasználó tudta nélkül – gyakran valamilyen más szoftverrel együtt, szándékosan vagy megtévesztéssel kerülnek telepítésre.
https://avirus.hu/backdoors/
https://en.wikipedia.org/wiki/Backdoor_(computing)

Baiting: A baiting, azaz csalizás egy speciális társadalmi manipuláció, amely arra csábítja az áldozatokat, hogy ingyenes termékeket, információkat, kedvezményeket

vagy jutalmakat fogadjanak el bizalmas információk közléséért vagy biztonsági kockázatot jelentő lépésekért cserébe. Például egy hirdetés felkérheti a webhely látogatóit, hogy kattintsanak egy ingyenes film letöltésére vonatkozó ajánlatra, de az ajánlatra való válaszadáshoz az áldozatnak meg kell adnia az e-mail címét, ami előkészíti a terepet a további személyazonosság-lopási támadásokhoz. A csalitámadások jellemzően arra törekszenek, hogy az áldozatokat bizalmas információk megadására, rosszindulatú programok telepítésére vagy pénz fizetésére bírják rá. A bűnözők a csali segítségével mind a fogyasztókat, mind a vállalkozásokat megcélozhatják. A rosszindulatú szereplők digitális ajánlatokat és fizikai tárgyakat is használhatnak a csalitámadások indításához. A csalizás bizonyos szempontból hasonlít az adathalászatra, de a két taktika kulcsfontosságú szempontból különbözik; mind a csalizás, mind az adathalászat a társadalmi manipulációra, az áldozatok megtévesztésére támaszkodik. A csalizás azonban látszólagos értéket kínál, hogy az áldozatokat rávegye a válaszadásra. Az adathalászat általában nem kínál semmi értékeset, de legitim forrásnak adja ki magát, és a bizalomra, a sürgősségre vagy a félelemre játszva bírja rá az áldozatokat válaszadásra. Míg az adathalászat a személyes adatokkal való visszaélésre épül, a csalizás csalási taktikákra alapul.
https://www.cobalt.io/blog/cybersecurity-baiting-definition-introuduction

Bálnavadászat: Bálnavadászatnak nevezik azt az adathalászatot, amikor a támadók „nagy halnak” számító szereplőre, például egy üzleti vezetőre vagy híresség re vetik ki a hálójukat. Ezek a csalók gyakran mélyreható kutatást végeznek a célpontjaikkal kapcsolatban, hogy megtalálják az alkalmas pillanatot a bejelentkezési hitelesítő adatok vagy más bizalmas adatok eltulajdonítására. Ha valakinek sok a vesztenivalója, akkor nála a bálnavadászok sokat nyerhetnek.
https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

Beaconing: A kártevőprogramok világában a beaconing (jelzőfény), azt a gyakorlatot jelenti, amikor egy fertőzött számítógép rövid, rendszeres üzeneteket küld egy támadó által irányított szervernek annak jelzésére, hogy a fertőzött gépen futó kártevő aktív, működőképes, és készen áll az utasítások fogadására. Ezek a jeladások gyakran a vállalati hálózat belső, fertőzött gépeiről (például botokról vagy „zombikról”) indulnak, és külső, úgynevezett parancs- és vezérlőszerverekre irányulnak. Ez a „hazatelefonálásként” is ismert kommunikációs stratégia lehetővé teszi a botnetek üzemeltetői számára, hogy automatikusan nyomon kövessék, irányítsák és vezéreljék a több száz- vagy akár több százezer fertőzött gépet.
https://en.wikipedia.org/wiki/Web_beacon

Beugratások: lásd hoax

Billentyűzetfigyelő: lásd keylogger

Binder: A binder kifejezés gyakran használatos a kiberbiztonságban és a vírusvédelmi programozás területén, olyan szoftvereszközökre utalva, amelyek két különálló fájlt képesek egyetlen futtatható fájlba egyesíteni. Bár hasonló technológiát legitim célokra is használnak szoftverfejlesztésben és rendszergazdai feladatokban, a binderek legfontosabb jellemzője a kiberbiztonsági kontextusban az, hogy jellemzően rosszindulatú szándékkal alkalmazzák őket. Gyakran hackerek használják, hogy egy látszólag ártalmatlan fájlban lévő káros kódrészletet álcázzanak vagy maszkoljanak, ezáltal megtévesztve az átlagfelhasználót, aki akaratlanul is káros rosszindulatú programokat vagy vírusokat futtat az eszközén. A kiberbiztonságban a binder egy legitim fájlt (ami lehet kép, dokumentum vagy futtatható program) választ, és egy további rosszindulatú szoftvert vagy kódrészletet ágyaz be bele. Ezáltal egy olyan új fájl jön létre, amely a gyanútlan felhasználó számára úgy jelenik meg és úgy viselkedik, mint az eredeti fájl. Amikor ezt a fájlt megnyitják, akkor nemcsak a várt funkcióját látja el, hanem diszkréten futtatja a beágyazott káros kódot is. Ez a technika különösen népszerű a kiberbűnözők körében, mivel elfedi a valódi szándékot, így téve nehezebbé a felderítést. A binderek kulcsszerepet játszanak számos rosszindulatú program, többek között trójaiak, férgek és más vírusok terjesztésében. Veszélyük elsősorban mindennapos jellegükből fakad, hiszen egy jogos fájlt rejtett rosszindulatú programmal kombinálva a legtöbb víruskereső szoftver az eredeti fájl jogossága alapján figyelmen kívül hagyhat. A víruskereső szoftverek számára nehezebb az ilyen fenyegetések észlelése, mert a normál viselkedés, például egy fénykép vagy dokumentum megnyitása általában nem aktivál semmilyen biztonsági protokollt. A kiberbűnözők kifinomult technikákat alkalmaznak, hogy ezeket a kötött fájlokat rendkívül rejtetté tegyék, például fejlett titkosítást használnak a rosszindulatú rész olvashatatlanná tételére, vagy áldozati kódrészleteket, amelyek összezavarják a víruskereső programokat anélkül, hogy befolyásolnák a binder működését.
https://cyberpedia.reasonlabs.com/EN/binder.html

Biometrikus alapú azonosítás: A biometrikus azonosítás az emberi szervezet bizonyos jellemzőinek felismerésén alapszik. Ezek közül ismert az arc-, hang-, írisz-, retina-, véna-, DNS-, tenyér- és ujjlenyomat-azonosítás, de még az is az egyénre jellemző pontos megkülönböztető jel lehet, ahogyan járunk vagy aláírunk, mi több, a gépelési stílusunk is. A biometrikus azonosítás célja olyan rendszerek kialakítása, amelyek nem kódokkal, jelszavakkal vagy okmányokkal — melyek bárkinek a birtokába kerülhetnek — azonosítják az egyént, hanem annak saját személyes tulajdonságai alapján. Az azonosítási eljárások lehetnek aktívak vagy passzívak. Az aktív eljárások a személy tevékeny közreműködését igénylik, míg a passzív eljárások esetén a személy részvétele csak a mintaadásra korlátozódik (például ujjlenyomat-szkenner használata vagy DNS-minta szolgáltatása).
https://www.ludovika.hu/blogok/cyberblog/2023/03/07/biometrikus-alapu-szemelyazonositas/

Bizonytalanságon alapuló biztonság: A „bizonytalanságon alapuló biztonság” (security through obscurity) szemlélet szerint ajánlott minden olyan technikai információt (pl.: szoftvertípusok és verziószámok, belső hálózati IP-k stb.) eltávolítani a potenciális támadók számára elérhető felületekről (pl.: HTTP-fejlécek, kiszolgálói szoftverek bannerei stb.), ami elősegítheti egy támadás sikerességét.
https://makay.net/kiberbiztonsagi-fogalomtar
https://en.wikipedia.org/wiki/Security_through_obscurity

Black Hat Hacker: A black hat, magyarul „feketekalapos” kifejezés olyan hackerekre utal, akik rosszindulatú célból hatolnak be számítógépes rendszerekbe és hálózatokba. Ezek az egyének vagy csoportok szándékosan megsértik a kiberbiztonsági szabályokat és törvényeket, hogy személyes vagy pénzügyi előnyre tegyenek szert, kárt okozzanak, adatokat lopjanak, rendszereket tegyenek működésképtelenné vagy zsarolóprogramokat helyezzenek el. A black hat hackerek általában kihasználják a biztonsági réseket, jelszavakat törnek fel, rosszindulatú szoftvereket használnak, vagy adathalász támadásokat indítanak. Tevékenységük gyakran bűncselekménynek minősül, és jelentős fenyegetést jelentenek a vállalatok, kormányzati szervek, valamint magánszemélyek adatbiztonságára nézve. Ők azok, akik a legtöbb kibertámadás mögött állnak, és szemben állnak a white hat (fehérkalapos) hackerekkel, akik épp a biztonsági gyengeségek azonosításával segítik a védekezést. A black hat kifejezés az 1950-es és 1960-as évek westernfilmjeiből származik, ahol a gonosz szereplők rendszerint fekete kalapot viseltek – innen ered a modern kiberbiztonsági szóhasználatban is a negatív jelentéstartalom.
https://www.fortinet.com/resources/cyberglossary/black-hat-security
https://en.wikipedia.org/wiki/Black_hat_(computer_security)

Bloatware: A bloatware-ek olyan, jellemzően kéretlen alkalmazások, amiket a gyártók telepítenek elő az általuk gyártott/forgalmazott készülékekre (számítógépekre, tabletekre és okostelefonokra). Eredendően nem tekinthetőek kártékony kódoknak, ugyanis csupán kényelmi szolgáltatásokat nyújtanak, viszont nem egy esetben derült ki, hogy egyes előtelepített alkalmazások valamilyen kártevőt rejtettek, vagy lehallgatták a felhasználók tevékenységét – a gyártók tudtával, vagy tudta nélkül.
https://makay.net/kiberbiztonsagi-fogalomtar

Blocklist/Blacklist: A tiltólista, más néven feketelista, egy hozzáférés-szabályozó rendszer, amely megakadályozza, hogy a rajta szereplő felhasználók, programok vagy hálózatok hozzáférjenek bizonyos rendszerekhez vagy szolgáltatásokhoz. A tiltólista célja a nem kívánt vagy káros forgalom — például spam, illetéktelen hozzáférés vagy rosszindulatú tevékenységek — kiszűrése. A felhasználók vagy entitások automatikusan vagy manuálisan kerülhetnek fel a listára, és a rendszer ennek alapján blokkolja őket.
https://www.infobip.com/glossary/blocklist

BOT: A robot szó rövidített alakja, a bot egy feladatokat automatikusan végrehajtó program. Kezdetben a botokat a UNIX világban alkalmazták a rendszergazdák a rendszeresen elvégzendő, sablonos feladatoknál. Némely bot automatikusan cseveg is a felhasználóval, vagy válaszol a feltett kérdésekre, mintegy utánozva egy valódi, hús-vér embert. A bot rossz célokra is felhasználható: segítségével egy távoli támadó átveheti az irányítást az áldozat megfertőzött számítógépén. A cél pontosan ez: egyetlen gépről fertőzött számítógépek százezrei válnak távirányíthatóvá. A károkozók (botherder, azaz botnet pásztor) az eltérített számítógépek erőforrásait kéretlen levélszemét (spam) küldésére, illegális szoftverek letöltésére és tárolására használják. Nem ritkán pornográf anyagok tárolására, illetve különféle számítógépes támadásokban (DoS, DDos) való részvételre is használják, sőt meghatározott tarifa fejében akár bérbe is adják ezt a kapacitást. A bot ezenfelül képes végigpásztázni az áldozat merevlemezét, és arról bizalmas adatokat továbbít egy távoli weboldalra, és ezekkel a lopott személyes, banki-, lakcím-, társadalombiztosítási stb. információk segítségével további bűncselekményeket követnek el (identity theft, azaz személyiség lopás). Az ilyen fertőzött gépeket gyakran zombi gépeknek is nevezik.
https://www.eset.com/hu/termektamogatas/veszelyek/

Botnet: A botnet, vagy más néven zombihálózat tagjai olyan felhasználói készülékek, amelyek egy vírusfertőzés következtében távolról irányítható kártevőt futtatnak. A zombihálózat „parancsnokai" képesek tömegesen (esetenként több százezres nagyságrendben) irányítani az áldozatok készülékeit, hogy azok túlterheléses támadást indítsanak egy-egy megadott célpont ellen. Így a támadók nem kerülnek közvetlen kapcsolatba a fő célponttal, helyettük az áldozatok fertőzött eszközei végzik el a munkát.
https://makay.net/kiberbiztonsagi-fogalomtar

Bug bounty: A bug bounty, magyarul hibajavító program egy olyan program, amelyben szervezetek jutalmat – általában pénzt – ajánlanak fel azoknak az etikus hackereknek vagy biztonsági kutatóknak, akik biztonsági hibákat, sebezhetőségeket tárnak fel a vállalat rendszereiben, szoftvereiben vagy szolgáltatásaiban. A cél a hibák felelősségteljes bejelentése és kijavítása még azelőtt, hogy azok rosszindulatú kezekbe kerülnének.
https://www.techtarget.com/whatis/definition/bug-bounty-program

Business Email Compromise: Az üzleti e-mail-feltörés (BEC) során a támadók hozzáférnek egyes cégek levelezéséhez, megfigyelik az esetleges pénzügyi tranzakciókérelmeket (számla, díjbekérő, előlegbekérő stb.) és a szervezet nevében hamis, átírt bankszámlaszámmal ellátott dokumentumokat küldenek az érintett partnereknek, akik így a támadók által kezelt bankszámlákra utalják az összegeket.
https://makay.net/kiberbiztonsagi-fogalomtar

Büntető rutin: lásd Payload

Célzott adathalászat: A célzott adathalászat módszerét használják, amikor a támadó kifejezetten egy személyt, vagy a cégét akarja támadni, bizalmas információkhoz igyekszik hozzáférni, mint például a cég üzleti titkai, az érzékeny technológiai tervek, vagy bizalmas kormányzati kommunikáció. Az is előfordulhat, hogy a bizonyos személy csak első lépésként szolgál ahhoz, hogy egy másik egyént/céget érjenek el. A támadók igen sokat nyerhetnek, ezért hajlandóak időt és pénzt nem sajnálva feltérképezni a célpontjaikat. Például egy külföldi kormányzat úgy gondolja, hogy a kiválasztott cég olyan terméket vagy technológiát fejleszt, ami kulcsfontosságú a gazdaságukhoz és támadni kezdi a céget. Megvizsgálják a cég weboldalát, és beazonosítanak pár kulcsszereplőt, akikről komplett dossziét készítenek. A kiválasztott egyének elemzését követően, a támadók egy célzott adathalász levelet készítenek, pl. a cég egy beszállítója nevében. A levél egy csatolmányt tartalmaz, amely számlának tűnhet, miközben az a valóságban egy káros kódot tartalmazó fájl. Az emberek kb. 50-60%-át sikerül megtéveszteni, megnyitják a csatolmányt, és ezáltal hozzáférést adnak a támadónak a számítógépükhöz. A célzott adathalászat sokkal veszélyesebb fenyegetés az egyszerű adathalász támadásoknál, mivel a támadók személyre szabott támadást intéznek néhány kiválasztott ember ellen. Ez nem egyszerűen a támadók sikerének esélyét növeli, de ezen támadások felfedezése is sokkal nehezebb.
https://www.biztonsagosinternet.hu/tippek/szemelyes-biztonsag-az-interneten/celzott-adathalaszat

CIRT (A Computer Incident Response Team): A CIRT, azaz Számítógépes Incidens Válaszadó Csapat egy speciális, jól képzett információbiztonsági szakemberekből álló csapat, amelynek fő feladata a szervezetek kiberbiztonsági eseményeinek és incidenseinek gyors és hatékony kezelése. A CIRT elsődleges szerepe az informatikai rendszerek és hálózatok védelme az esetleges kibertámadásokkal szemben, valamint a támadások következményeinek minimalizálása. A CIRT tevékenységi körébe tartozik az incidensek észlelése, elemzése, a támadások forrásának azonosítása, a helyreállítási folyamatok végrehajtása, valamint a támadások megismétlődésének megakadályozása érdekében kidolgozott védekezési stratégiák és javaslatok készítése. Emellett a CIRT együttműködik más biztonsági egységekkel, például a CERT-ekkel (Computer Emergency Response Team), és aktívan részt vesz az információbiztonsági tudatosság növelésében is. A csoport munkája kulcsfontosságú ahhoz, hogy a szervezetek gyorsan reagáljanak a kibertámadásokra, minimalizálják a károkat, megőrizzék az adatbiztonságot, és fenntartsák az üzletmenet folytonosságát.
https://www.group-ib.com/resources/knowledge-hub/cirt/

Cookie: A cookie, magyarul „süti”, egy kis adatcsomag, amelyet a böngésző tárol el egy weboldal kérésére, és minden későbbi oldalletöltés során visszaküld ugyanannak a weboldalnak. A süti tetszőleges információt tartalmazhat, amit a weboldal határoz meg. Fontos, hogy egy weboldal kizárólag a saját sütijeit tudja beállítani, és más oldalak sütijeihez nem férhet hozzá. A weboldalak gyakran használnak sütiket például a felhasználók bejelentkeztetéséhez. Ilyenkor a sikeres azonosítás után a weboldal egy egyedi azonosítót küld a böngészőnek, amelyet az elment. A böngésző ezt az azonosítót minden újabb kéréskor visszaküldi, így a rendszer tudja, melyik felhasználó melyik tartalmat láthatja. Enélkül például egy felhasználó nem tudná elérni saját e-mailjeit. Az európai szabályozások értelmében a weboldalaknak kötelező tájékoztatniuk a felhasználókat a sütik használatáról. Bizonyos típusú sütik – például marketing vagy statisztikai célúak – használatához pedig a felhasználó előzetes, kifejezett hozzájárulása szükséges.
https://lexiq.hu/cookie
https://en.wikipedia.org/wiki/HTTP_cookie

Cross-site scripting: Ez egy olyan támadás, amelyben egy támadó egy rosszindulatú szkriptet ad hozzá egy legitim weboldal tartalmához. A cross-site scripting (XSS) támadások lehetővé teszik a támadó számára, hogy különféle nyelveken írt szkripteket futtassanak (például JavaScript) gyanútlan weboldal felhasználóinak böngészőiben. A támadók XSS-t használhatnak munkamenet sütilopásra, amely lehetővé teszi számukra, hogy áldozatul esett felhasználóknak tűnjenek. De eloszthatnak rosszindulatú szoftvert, megcímkézhetik a weboldalakat, felhasználói hitelesítő adatokat keresnek, és más káros tevékenységeket végeznek az XSS segítségével. Sok esetben a társadalmi manipulációs technikákkal, például a phishinggel kombinálják. Az XSS mind a közös támadási vektorok között állandóan jelen van, és 2023-ban a CWE legveszélyesebb 25 listáján a második helyen állt.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/
https://en.wikipedia.org/wiki/Cross-site_scripting

Cryptojacking: A cryptojacking egy olyan támadási metódus, amely során a támadók az áldozat készülékére valamilyen formában kriptovaluta-bányászó kódot juttatnak – tehát az áldozat készüléke a támadók számára termeli a digitális pénzt, általában Bitcoin, Ethereum vagy Monero pénznemben.
https://makay.net/kiberbiztonsagi-fogalomtar
https://en.wikipedia.org/wiki/Cryptojacking

Cryptotrojan: A cryptotrojan (kriptotrójai) egy olyan digitális kártevő, amit felhasználói szoftverekbe rejtenek, hogy azok használata közben a kártevő a háttérben digitális pénzt (kriptovalutákat) bányásszon a felhasználók eszközeinek erőforrásaival, a felhasználók tudta nélkül, a kártevő készítői számára.
https://makay.net/kiberbiztonsagi-fogalomtar

Cyber Threat Intelligence: A kifejezésnek jelenleg nincs közismert magyar megfelelője, de leginkább olyan hírszerzési műveleteknek feleltethető meg, amelyek során a legkülönfélébb forrásokból (Open Source Intelligence, Social Media Intelligence, Deep Web stb.) összegyűjtött, hatalmas mennyiségű információban egy erre a feladatra szakosodott csapat azonosítja azokat a potenciális kiberfenyegetéseket, amik veszélyeztethetik az adatok és a rendszerek biztonságát.
https://makay.net/kiberbiztonsagi-fogalomtar

Cyber warfare: A cyber warfare-t, azaz kiberháború kifejezést gyakran használják mindenféle online fenyegetés leírására, függetlenül attól, hogy ki a támadó vagy a célpont. Azonban a biztonsági szakemberek körében van egy szűkebb értelmezése is: egy ország által végrehajtott támadás egy másik ország infrastruktúrája ellen. A kiberháború jogi definíciója szerint olyan cselekmények tartoznak ide, amelyek hadüzenettel, háborús cselekményekkel, halálesetekkel vagy pusztítással járnak. Az ilyen események meghatározása és minősítése azonban gyakran vitatott és összetett kérdés.
https://nki.gov.hu/figyelmeztetesek/archivum/tisztazni-kell-a-kiberfegyver-es-kiberhaboru-fogalmat/?utm_source;
https://nki.gov.hu/figyelmeztetesek/archivum/kiberhaboru/?utm_source;
https://en.wikipedia.org/wiki/Cyberwarfare

Cyber weapon: A cyber weapon, azaz kiberfegyver olyan digitális eszköz, rosszindulatú program vagy kód, amelyet kifejezetten érzékeny információk ellopására, rendszerek megbénítására vagy jelentős károkozásra terveztek. Célja lehet a kritikus infrastruktúrák – például energiahálózatok, kommunikációs rendszerek vagy egészségügyi szolgáltatások – megzavarása, illetve katonai vagy politikai célok elérése. Használatuk lehet támadó, védekező vagy kettős rendeltetésű, és működésük során alkalmazhatnak adatmegsemmisítést, kémkedést vagy fizikai szabotázst. A kiberfegyverek gyakran állami szereplők kezében jelennek meg, mivel lehetőséget nyújtanak a valószínűsíthető tagadhatóságra, azaz az érintett ország megtagadhatja a közvetlen felelősséget a támadásért.
https://www.ebsco.com/research-starters/science/cyberweapon
https://en.wikipedia.org/wiki/Cyberweapon

Cyber: A cyber angol nyelvű szó, aminek a magyar jelentése számítógépes, számítógépekkel kapcsolatos, virtuális. Más szavakkal összekapcsolva szokták használni. Magyar nyelven kiber formában terjedt el. A kifejezés a scifikből került át a hétköznapi szóhasználatba. Akkor használják egy szóhoz kapcsolva, ha azt szeretnék jelezni, hogy az adott dolog számítógépes változatáról beszélnek. Az angol cyberbullying szó például internetes zaklatást, a kiberbűnözés pedig számítógépes bűnözést jelent.
https://lexiq.hu/cyber
https://en.wikipedia.org/wiki/Cyber

Cyberbullying: A cyberbullying, azaz internetes zaklatás, digitális technológiák használatával történő zaklatás. Történhet közösségi médiában, üzenetküldő platformokon, játékplatformokon és mobiltelefonokon. Ismétlődő viselkedés, amelynek célja a célpontok megijesztése, feldühítése vagy megszégyenítése. Példák többek között: hazugságok terjesztése, vagy kínos fotók vagy videók közzététele valakiről a közösségi médiában; bántó, bántalmazó vagy fenyegető üzenetek, képek vagy videók küldése üzenetküldő platformokon keresztül; valakinek a nevében vagy hamis fiókokon keresztül visszaélve, gonosz üzeneteket küldve másoknak; szexuális zaklatás vagy zaklatás elkövetése generatív mesterséges intelligencia eszközök használatával. A személyes és az internetes zaklatás gyakran párhuzamosan történhet. Az internetes zaklatás azonban digitális lábnyomot hagy – egy olyan feljegyzést, amely hasznosnak bizonyulhat, és bizonyítékként szolgálhat a bántalmazás megállításához.
https://www.unicef.org/stories/how-to-stop-cyberbullying
https://hu.wikipedia.org/wiki/Cyberbullying

Cybercrime: A kiberbűnözés olyan bűncselekmény, amely számítógépet, számítógépes hálózatot vagy hálózati eszközt céloz meg, illetve használ fel. A legtöbb kiberbűncselekményt pénzszerzésre törekvő kiberbűnözők vagy hackerek követik el. Előfordul azonban, hogy a kiberbűnözés célja a számítógépek vagy hálózatok megkárosítása nem anyagi indíttatásból, hanem politikai vagy személyes okokból. A kiberbűnözést magánszemélyek vagy szervezetek követhetik el. Egyes elkövetők szervezettek, fejlett technikákat alkalmaznak, és magasan képzett technikai szakemberek. A számítógépeket célzó kiberbűnözők kártevőkkel fertőzhetik meg az eszközöket, hogy adatokat töröljenek vagy lopjanak. Előfordulhat, hogy a támadók megakadályozzák a felhasználókat egy webhely vagy hálózat elérésében, vagy gátolják egy vállalkozás szoftverszolgáltatásának működését – ezt szolgáltatásmegtagadási (DoS) támadásnak nevezik. A számítógépek más bűncselekményekhez való felhasználása során kiberbűnözők rosszindulatú programokat, illegális információkat vagy tiltott tartalmakat terjeszthetnek. Gyakori, hogy a támadók többféle módszert is kombinálnak: például először vírussal fertőzik meg a számítógépeket, majd ezeket a gépeket felhasználják további rosszindulatú szoftverek terjesztésére más eszközökre vagy hálózatokon keresztül. Egyes joghatóságok a kiberbűnözés egy harmadik típusát is elismerik, amikor a számítógépet bűnsegédként használják fel – például lopott adatok tárolására.
https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Cybersecurity: A cybersecurity, azaz kiberbiztonság olyan folyamatok, ajánlott eljárások és technológiai megoldások összessége, amelyek segítenek a felhasználónak megvédeni kritikus rendszereit, adatait és hálózatát a digitális támadásoktól. Mivel szinte mindenütt használunk adatokat, és egyre többen dolgoznak és csatlakoznak bárhonnan, az elkövetők széles körű szakértelemre és készségekre tettek szert. A kibertámadások száma évről évre nő, ahogy a támadók folyamatosan fejlesztik taktikájukat, technikáikat és eljárásaikat és skálázzák működésüket. Ez a folyamatosan változó fenyegetési környezet megköveteli, hogy a szervezetek dinamikus, folyamatos kiberbiztonsági programot hozzanak létre, hogy ellenállóak maradjanak, és alkalmazkodjanak a felmerülő kockázatokhoz. Egy hatékony kiberbiztonsági program olyan személyeket, folyamatokat és technológiai megoldásokat ötvöz, amelyek mérséklik a támadásból eredő üzletmenet-kiesések, adatlopások, pénzügyi veszteségek és hírnévcsorbulás kockázatát. A kiberbiztonság elengedhetetlen a jogosulatlan hozzáférés, az adatszivárgás és más kiberveszélyforrások elleni védelemhez.
https://www.microsoft.com/hu-hu/security/business/security-101/what-is-cybersecurity

Cyberspace: A kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.
https://makay.net/kiberbiztonsagi-fogalomtar

Csalizás: lásd baiting

Dark web: A dark web (vagy magyarul sötét web) a deep webnek (azaz a hagyományos keresők által nem látott oldalaknak) az a része, ami csak valamilyen speciális szoftver, beállítás vagy elérési jog segítségével tekinthető meg. Egyes dark webes szolgáltatások lehetőséget biztosítanak az állami cenzúra megkerülésére, anonim böngészésre vagy például újságírókkal való biztonságos kommunikációra. Ezen kívül a dark webet gyakran használják illegális tevékenységekre is, például fegyverek, drogok, hamisított termékek adásvételére.
https://lexiq.hu/dark-web

DDoS-támadás: A DDoS-támadás (Distributed Denial-of-Service, azaz elosztott szolgáltatásmegtagadásos támadás) egy informatikai szolgáltatás szándékos túlterhelését jelenti, melynek célja a szolgáltatás részleges vagy teljes megbénítása, illetve rendeltetésszerű működésének megzavarása. A támadás során több – gyakran több ezer – fertőzött eszköz (ún. zombihálózat tagjai) egyszerre küld túl sok kérést a célrendszer felé, amit az nem tud kezelni, és így elérhetetlenné válik a felhasználók számára. A támadók ezeket az eszközöket központilag irányítják, és a tömeges forgalommal kényszerítik szolgáltatásmegtagadásra a célpontot.
https://makay.net/kiberbiztonsagi-fogalomtar

Deepfake: A deepfake olyan képek, videók vagy hanganyagok gyűjtőfogalma, amelyeket mesterségesintelligencia-alapú eszközökkel vagy szerkesztőszoftverek segítségével módosítottak vagy hoztak létre. Ábrázolhatnak valós vagy kitalált személyeket, és a szintetikus média egyik formájának tekintik őket, azaz olyan médiának, amelyet általában mesterségesintelligencia-rendszerek hoznak létre különböző médiaelemek kombinálásával, egy új médiatermékké. Bár a hamis tartalmak létrehozása nem új keletű dolog, a deepfake-ek egyedülálló módon kihasználják a gépi tanulás és a mesterséges intelligencia technikáit, beleértve az arcfelismerő algoritmusokat és a mesterséges neurális hálózatokat, mint például a variációs autoenkódereket és a generatív adverzális hálózatokat. A képelemzés területe viszont olyan technikákat fejleszt, amelyekkel manipulált képeket lehet észlelni. A deepfake-ek széles körű figyelmet kaptak a gyermekek szexuális zaklatásával kapcsolatos anyagok, híresség pornográf videók, bosszúpornó, álhírek, átverések, zaklatás és pénzügyi csalások létrehozásában való potenciális felhasználásuk miatt.
https://en.wikipedia.org/wiki/Deepfake

Deep web: A deep web (vagy magyarul mély/láthatatlan web) a webnek az a része, amit nem látnak a hagyományos keresők, mint például a Google. A deep web részei például a webes email vagy banki oldalak jelszóval védett részei, a fizetett tartalmak, a csak regisztráció után megtekinthető oldalak, zárt orvosi adatbázisok, vagy olyan oldalak, amelyek csak valamilyen speciális szoftver (pl. Tor böngésző[18]) letöltése után érhetőek el, a keresők által nem ismert formátumban vannak vagy sehova nincsenek linkelve, ezért nem találnak rájuk a keresők. A kifejezést gyakran tévesen a dark web szinonimájaként használják, az utóbbi azonban valójában csak egy kisebb része a deep webnek.
https://lexiq.hu/deep-web

Demilitarizált zóna (DMZ): A demilitarizált zóna, más néven demarkációs zóna vagy határhálózat egy olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek. A DMZ célja, hogy egy plusz biztonsági réteget biztosítson a szervezet helyi hálózatának (LAN). Így egy külső támadónak csak a DMZ-ben található berendezésekhez lehet hozzáférése, nem az egész hálózathoz.
https://hu.wikipedia.org/wiki/Demilitariz%C3%A1lt_z%C3%B3na_(informatika)

Digitális lábnyom: Digitális lábnyom minden olyan információ, amit valaki az online jelenlétével hagy maga után az Interneten vagy tágabban értelmezve minden

18 A Tor (a The Onion Router – magyarul a hagyma útválasztó – rövidítése) lényegében egy olyan hálózat, amely elrejti az online forgalmat. A Tor böngésző egy önkéntesek által kezelt nyílt forráskódú platform, és az onion routing-nak köszönhetően anonimitást biztosít azoknak a felhasználóknak, akik ezen a hálózaton keresztül érik el a weboldalakat és a szervereket.

olyan adat, amit valamilyen digitális technológia rögzített, és összefüggésbe hozható a személyével. Például szándékos digitális lábnyom egy közösségi oldalon közzétett fotó vagy hozzászólás, egy regisztráció valamilyen weboldalon, vagy egy poszt lájkolása. Léteznek akaratlan lábnyomok is, amiket egyes cégek vagy államok gyűjtenek rólunk, például az általunk meglátogatott oldalakról, vagy hogy mennyit görgettünk le egy oldalon és hova kattintottunk. Tágabb értelemben digitális lábnyomnak számítanak például mobiltelefon használata során keletkezett hívásadatok, SMSek vagy a térfigyelő kamerák felvételei is. Az így keletkezett adatokat jellemzően arra használják, hogy segítségükkel a felhasználókat érdeklő hirdetéseket tudjanak megjeleníteni számukra; a digitális lábnyomoknak azonban vannak veszélyei is, például felhasználhatják adathalász vagy social engineering támadások során, esetleg manipulatív célokra. Problémát okozhat az is, ha például egy új munkahelyen a korábbi internetes tevékenysége alapján döntenek a jelentkező felvételéről vagy elutasításáról. A széles körű adatgyűjtés miatt a digitális lábnyomok eltüntetése a legtöbb esetben nem megoldható, azonban a csökkentésükre van lehetőség, például törölhetők a korábbi regisztrációk, a GDPR alapján az egyes cégektől kérhető a tárolt adatok törlése, és ellenőrizhető a használt szolgáltatásoknál a beállításokban bizonyos adatok gyűjtésének letiltása is.
https://lexiq.hu/digitalis-labnyom

DKOM (Direct Kernel Object Manipulation): A DKOM olyan technika, amely közvetlenül módosítja az operációs rendszer kernelében található adatstruktúrákat és objektumokat. Legfőbb célja rendszerint a rosszindulatú tevékenységek elrejtése és a biztonsági intézkedések kijátszása. A kiberbiztonság területén a DKOM-ot gyakran használják arra, hogy folyamatokat, fájlokat vagy rendszerkulcsokat elrejtsenek a hagyományos biztonsági eszközök elől, ezáltal lehetővé téve a kártékony vagy jogosulatlan műveletek észrevétlen végrehajtását. Az ilyen támadások felismerése rendkívül nehéz, mivel a változtatások mélyen, a kernel szintjén történnek, és láthatatlanok maradhatnak a standard védelmi megoldások számára. Éppen ezért az észlelésükhöz speciális elemző eszközök és fejlett technikák alkalmazása szükséges.
https://dotcommagazine.com/2023/09/dkom-a-fascinating-comprehensive-guide/

DNS spoofing: A DNS, Domain Name Server lehetővé teszi a felhasználók számára, hogy weboldalakhoz férjenek hozzá oly módon, hogy a domain neveket és URL-eket IP-címekhez rendeli, amelyeket a számítógépek használnak a weboldalak megtalálásához. A hackerek kihasználhatják a DNS-eket, hogy átírásokat eszközölve az áldozatokat az eredetileg várt helyett egy a támadó által ellenőrzött weboldalra irányítsák. Ezek a hamis weboldalak pontosan olyanok, mint a felhasználók által várt weboldalak. Ennek eredményeként a DNS spoofing támadások áldozatai nem gyanakodnak, amikor arra kérik őket, hogy adja meg a fiókjuk bejelentkezési hitelesítő adatait egy olyan weboldalon, amelyet valósnak gondolnak.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

DNS tunneling: DNS-protokoll manipulálását jelenti, amelynek célja a rosszindulatú forgalom átirányítása a szervezet védelmi rendszerén. Rosszindulatú domainek és DNS-kiszolgálók használatával a támadó a DNS segítségével megkerülheti a hálózati biztonságot, és adatokat szerezhet ki.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

DoS-támadás: A DoS-támadás (Denial-of-Service) során egyetlen támadó egyetlen forrásból próbál túlterhelni és szolgáltatásmegtagadásra kényszeríteni egy célpontot. A különböző célpontoldali sebezhetőségek esetenként eredményre is vezethetnek és akár egyetlen okostelefonnal elvégezhető a támadás.
https://makay.net/kiberbiztonsagi-fogalomtar

Doxing: Egy személy, vagy szervezet magán-, vagy azonosításra alkalmas adatainak (különösen személyazonosításra alkalmas információinak) közzétételi. Ezen információk megszerzésére alkalmazott módszerek tartalmazzák a nyilvánosan hozzáférhető adatbázisok és a közösségi média (Social Network) oldalak (mint pl. a Facebook) kereséseit, a hekkelést, és a pszichológiai befolyásolást is. A doxing szorosan kapcsolódik az internetes bosszúálláshoz és hacktivizmushoz. A „doxing”-ot különböző okok miatt alkalmazzák, beleértve (a társadalmilag pozitív értelmű) a bűnüldözés támogatását, az üzleti elemzést, de a rosszindulatú (adott esetben törvényellenes) cselekvést is, vagyis pl. a zsarolást, a kényszerítést, a zaklatást, az online megszégyenítést és a bosszúállást egyaránt.
https://sealog.hu/tudastar/fogalomtar/doxing-v-doxxing

Easter Egg: A „húsvéti tojás” egy rejtett kód a számítógépes szoftverekben, amely a normál működésén kívül eső funkciót lát el, néha a gyártó által beépített vagy jogellenesen elhelyezett kód, hogy back door-t biztosítson. Ezek a rejtett funkciók vagy üzenetek különféle digitális platformokon, például videojátékokban, weboldalakon és szoftveralkalmazásokban találhatók és népszerűek a felhasználók körében, a felhasználói élmény javítására és a fejlesztők kreativitásának bemutatására törekednek.
https://www.twingate.com/blog/glossary/easter-egg

Etikus hackelés: Az etikus hackelés magában foglalja a számítógépes rendszerek vagy hálózatok gyenge pontjainak megkeresését – de ahelyett, hogy illegális tevékenységekre használnák, segítik a biztonsági ellenintézkedések kidolgozását. Az általuk feltört számítógépes rendszer vagy hálózat a tulajdonos engedélyével, a jogszabályok betartásával történik. Minden általuk azonosított biztonsági kockázatról beszámolnak a tulajdonosnak, amennyiben szükséges, tájékoztatják a hardver- és szoftvergyártókat a talált sebezhetőségekről. Az etikus hackelést végző szakértőket „etikus hackereknek” nevezik, akik biztonsági értékeléseket végeznek a szervezet biztonsági intézkedéseinek javítása érdekében.
https://www.unite.ai/hu/what-is-ethical-hacking-how-does-it-work/

Evil twin phishing: Ennél az elkövetési módnál a támadók egy ismert, legitim vezeték nélküli (wifi) hozzáférési ponttal azonos nevű hamis hozzáférési pontot hoznak létre. A támadók ezután ráveszik az áldozatokat, hogy csatlakozzanak rá az eszközükkel, majd megfigyelik, lehallgatják az óvatlanul a hálózatra csatlakozó felhasználók online forgalmát. Így érzékeny adatokhoz, például felhasználónevekhez és jelszavakhoz férhetnek hozzá. A felhasználók gyakran észre sem veszik, hogy támadás áldozatául estek.
https://kiberpajzs.hu/csalastipusok/szamitogepes/evil-twin-phishing/

Exploit: A kizsákmányolás olyan program vagy kódrészlet, amelynek célja egy alkalmazás vagy számítógépes rendszer biztonsági hibájának vagy sebezhetőségének észlelése és kihasználása, általában aljas okokból, mint pl. malware telepítés. A kizsákmányolás egy olyan módszer, amelyet a számítógépes bűnözők használnak rosszindulatú programok szállítására, nem pedig magát a rosszindulatú programot. A kihasználások olyan adatokat vagy végrehajtható kódot tartalmaznak, amelyek egy vagy több szoftverhibát képesek kihasználni egy helyi vagy távoli számítógépen. Tegyük fel például, hogy van egy olyan sebezhetőségű böngészőn, amely lehetővé teszi „tetszőleges kód” futtatását, vagyis egy rosszindulatú alkalmazás telepítését és futtatását a rendszeren, vagy váratlan rendszerviselkedés előidézését a felhasználó tudta nélkül. A támadók kezdeti lépése általában a jogosultság eszkalációja, amely lehetővé teszi számukra, hogy bármit megtegyenek a támadott rendszeren. A böngészők, a Flash, a Java és a Microsoft Office mellett a leginkább célzott szoftverkategóriák közé tartoznak. Elterjedtségük miatt mind a biztonsági szakemberek, mind a hackerek aktívan vizsgálják őket, a böngészőfejlesztők pedig arra kényszerülnek, hogy rendszeresen készítsenek javításokat a sebezhetőségek kiküszöbölésére. Célszerű ezeket a javításokat a lehető leghamarabb telepíteni, de ez nem mindig lehetséges – elvégre minden lapot el kell vetni. Természetesen a bűnözők által felfedezett és feltáratlan sebezhetőségek, az úgynevezett nulladik napi sebezhetőségek kihasználása egyedülálló kihívást jelent. Sok időbe telhet, amíg a gyártók felismerik és kijavítják a problémát.
https://mpost.io/hu/glossary/exploit/

Féreg: lásd worm

Firewall: A tűzfalak olyan szoftverprogramok vagy hardvereszközök, amelyek szűrik és megvizsgálják az interneten keresztül érkező információkat. Az első védelmi vonalat képviselik, mivel megakadályozhatják a rosszindulatú programokat vagy a támadókat abban, hogy hozzáférjenek a hálózathoz és az információkhoz, mielőtt bármilyen potenciális kár keletkezhetne. Hardveres tűzfalakat egyes útválasztók tartalmaznak, és csak alig vagy egyáltalán nem igényelnek konfigurációt, mivel be vannak építve magába a hardverbe. Ezek a tűzfalak az útválasztó hálózatához csatlakozó számítógépek és készülékek forgalmát figyelik, azaz egyetlen berendezéssel szűrhetik

az összes készülékhez való hozzáférést. A hardveres tűzfalak alapvető biztonságot nyújtanak az IoT-eszközök, például az intelligens termosztátok és az intelligens izzók számára. Ezeknek az új eszközöknek gyakran gyenge biztonsági jellemzői vannak, amelyek a hálózatot sebezhetővé teszik, ám a hardveres tűzfal segít megakadályozni az ilyen biztonsági problémákat.
https://www.mcafee.com/hu-hu/antivirus/firewall.html

Gray Hat Hacker: A gray hat hacker, magyarul szürke kalapos hacker olyan személy, aki ugyan engedély nélkül fér hozzá számítógépes rendszerekhez biztonsági rések feltárása céljából, de nem károkozási vagy anyagi haszonszerzési szándékkal cselekszik. Tevékenysége a fehér kalapos (etikus) és a fekete kalapos (rosszindulatú) hackereké között helyezkedik el. Bár előfordulhat, hogy törvénysértő módszereket alkalmaz – például egy rendszer sebezhetőségét a rendszergazda előzetes értesítése nélkül hozza nyilvánosságra –, szándéka gyakran a biztonság növelése. Mivel azonban ezeket az akciókat nem minden esetben végzi az érintett fél tudtával vagy beleegyezésével, a gray hat hackerek tevékenysége jogi és etikai szempontból is megosztó. Egyesek hasznosnak, mások kockázatosnak tartják őket a kiberbiztonság szempontjából.
https://www.twingate.com/blog/glossary/gray-hat-hacker

Hacker: A hacker olyan informatikában, programozásban jártas személy, akinek célja egy számítógépes rendszer gyenge pontjainak megtalálása. A hacker (vagy olykor cracker) leggyakrabban olyan kiberbűnözőt takar, aki „feltöri" informatikai eszközöket az ott lévő információk, adatok ellopása érdekében. A köznyelvben a kiberbűnözőket is ezzel a névvel illetik, az esetek többségében tévesen. – Nem minden hacker kiberbűnöző és nem minden kiberbűnöző hacker.
https://makay.net/kiberbiztonsagi-fogalomtar

Hacktivist: hacktivisták olyan csoportok, amelyek valamilyen politikai ügy támogatása érdekében kibertámadásokat hajtanak végre a számukra kedvező döntés kikényszerítésére. A hacktivisták jellemzően egész iparágakat céloznak meg, de néha olyan szervezeteket is támadnak, amelyek tevékenységéről úgy vélik, hogy az ellentétes a politikai nézeteikkel vagy gyakorlatukkal. Bizonyos esetekben a hacktivisták nem a kiszemelt áldozat támadásával, hanem annak ügyfelei és üzleti partnerei révén próbálják kikényszeríteni a számukra kedvező döntést.

Hálózatvadászat: lásd wardriving

Hamis banki SMS: lásd smishing

Hamis banki telefonhívás: lásd vishing

Hamis szolgáltatói ügyintézés a közösségi médiában: lásd Angler phishing

Hamis wifi-hálózat létrehozása: lásd Evil twin phishing

Hátsó kapu: lásd backdoor

Hitelesítés: A hitelesítés az a folyamat, amellyel a vállalatok gondoskodnak arról, hogy csak a megfelelő engedélyekkel rendelkező személyek, szolgáltatások és alkalmazások használhassák a szervezeti erőforrásokat. Ez fontos része a kiberbiztonságnak, mert a rosszindulatú szereplők első számú prioritása, hogy jogosulatlan hozzáférést szerezzenek a rendszerekhez. Teszik ezt úgy, hogy ellopják a hozzáféréssel rendelkező felhasználók felhasználónevét és jelszavát. A hitelesítési folyamat a következő három elsődleges lépésből áll: azonosítás (a felhasználó kilétének megadása, pl. felhasználónévvel), hitelesítés (a megadott kilét igazolása, pl. jelszóval, eszközzel vagy biometrikus adatokkal), valamint engedélyezés (annak ellenőrzése, hogy az adott felhasználó hozzáférhet-e a kért erőforráshoz).
https://www.microsoft.com/hu-hu/security/business/security-101/what-is-authentication

Hívószám-hamisítás: lásd spoofing

Hoax: A hoaxok általában ostoba csínyek, amik lánclevelek vagy úgynevezett városi legendák (Urban Legends) formájában terjednek. A computer vírusokról szóló beugratások megpróbálnak félelmet kelteni, bizonytalanságot és kétséget ébreszteni a címzettekben, hogy egy észrevehetetlen vírussal állnak szemben. Néhány ilyen levélben valóban volt olyan rosszindulatú kód, amely képes volt fájlokat törölni a felhasználók gépeiről. Az ilyesfajta üzeneteket hagyjuk figyelmen kívül, és egyszerűen töröljük ki őket. Jó szerencsénk az életben semmilyen módon nem függ attól, hogy egy figyelmeztető levelet elküldünk-e húsz legjobb barátunknak, és ez a módszer semmiképp nem szolgálja gépünk biztonságát, ráadásul felesleges levélforgalmat is okoz.
https://www.eset.com/hu/termektamogatas/veszelyek/

Időzített bomba: lásd Time Bomb

Indicator of Compromise: Az IOC, azaz jogosulatlan adathozzáférésre vagy biztonsági incidensre utaló jel olyan digitális nyom, amely arra enged következtetni, hogy egy végpontot vagy hálózatot esetlegesen feltörtek. Ahogyan a fizikai bizonyítékok is segítenek a nyomozásban, ezek a digitális nyomok lehetővé teszik

az információbiztonsági szakemberek számára, hogy azonosítsák a rosszindulatú tevékenységeket vagy biztonsági fenyegetéseket, például az adatlopásokat, belső visszaéléseket vagy kártékony szoftveres támadásokat. A nyomozók manuálisan is összegyűjthetik ezeket a jeleket, ha gyanús tevékenységet észlelnek, de az információk automatikusan is gyűlhetnek a szervezet kiberbiztonsági megfigyelőrendszereinek részeként. Ezeket az adatokat felhasználhatják egy épp zajló támadás mérséklésére vagy egy már megtörtént biztonsági incidens orvoslására, valamint arra is, hogy fejlettebb eszközöket hozzanak létre, amelyek a jövőben képesek azonosítani és karanténba helyezni a gyanús fájlokat. Sajnos az IOC-figyelés reaktív jellegű, ami azt jelenti, hogy ha egy szervezet ilyen jelet talál, szinte biztos, hogy már megtörtént egy jogosulatlan adathozzáférés vagy biztonsági incidens. Ugyanakkor, ha az esemény még folyamatban van, az IOC gyors felismerése segíthet a támadás korai szakaszban való megfékezésében, így csökkentve annak üzleti hatását. Ahogy a kiberbűnözők egyre kifinomultabb módszereket alkalmaznak, úgy válik egyre nehezebbé az IOC-k észlelése is.
https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/indicators-of-compromise-ioc/

Internetes csalások: lásd scams

Internetes zaklatás: lásd cyberbullying

Internet of Things (IoT): Az IoT, vagyis a dolgok internete, olyan összekapcsolt objektumok és eszközök hálózatát jelenti, amelyek érzékelőkkel, szoftverekkel és más technológiákkal vannak felszerelve, így képesek adatokat küldeni és fogadni más rendszerektől vagy eszközöktől. A legáltalánosabb értelemben minden olyan „dolog” az IoT részét képezheti, amely vezeték nélkül kapcsolódhat az internethez. Napjainkban az IoT különösen azokra az eszközökre utal, amelyek célja, hogy adatokat gyűjtsenek és továbbítsanak a felhasználók tájékoztatása vagy különféle műveletek automatizálása érdekében. Míg korábban a kapcsolódás főként wifi-n keresztül történt, ma már az 5G és más fejlett hálózati technológiák teszik lehetővé a nagy mennyiségű adat gyors és megbízható kezelését, szinte bárhol a világon.
https://www.sap.com/hungary/products/technology-platform/what-is-iot.html

Intrusion Prevention System (IPS): Az IPS, azaz behatolásmegelőző rendszer egy hálózatbiztonsági technológia, amely figyeli a hálózati forgalmat, azonosítja a rosszindulatú tevékenységeket, és automatikusan megakadályozza azok végrehajtását. Az IPS rendszerek képesek észlelni és blokkolni a különféle fenyegetéseket, például a rosszindulatú szoftvereket, a sebezhetőségek kihasználását és a parancs- és vezérlési kommunikációkat, még mielőtt azok elérnék a célrendszert. Az IPS rendszerek kulcsfontosságú szerepet játszanak a modern hálózatbiztonságban,

mivel képesek valós időben észlelni és megakadályozni a különféle fenyegetéseket, hozzájárulva ezzel a szervezetek informatikai infrastruktúrájának védelméhez.
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Kártevőalapú adathalászat: Elterjedt adathalászati módszer. Az ilyen típusú támadások közé tartoznak például az e-mailekben megbízható mellékletnek (például önéletrajznak vagy bankszámlakivonatnak) álcázott kártevők. Bizonyos esetekben a kártevőt tartalmazó mellékletek megnyitása akár a teljes informatikai rendszert megbéníthatja.
https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing

Kémprogram: lásd spyware

Kéretlen reklám program: lásd adware

Kernel mode: A kernel mód a számítógépes rendszer központi feldolgozóegységének (CPU) privilegizált működési módja. Az operációs rendszer architektúrájának kritikus elemeként lehetővé teszi az összes gépi utasítás végrehajtását, valamint korlátlan hozzáférést biztosít a hardver- és rendszererőforrásokhoz. Ebben a módban a CPU a legmagasabb szintű vezérléssel rendelkezik, így képes a memória, a hardvereszközök és a folyamatok kezelésére.
https://www.ituonline.com/tech-definitions/what-is-kernel-mode/

Keylogger: A keylogger, vagyis billentyűzetfigyelő egy olyan program vagy hardvereszköz, amely nyomon követi és rögzíti a felhasználó billentyűleütéseit gépelés közben. Az így begyűjtött információkat elküldi egy hackernek egy úgynevezett parancs- és vezérlőszerveren (C&C – Command and Control) keresztül. A hacker ezután elemzi a billentyűleütéseket, hogy megtalálja a felhasználóneveket és jelszavakat, amelyeket felhasználva bejuthat egyébként védett rendszerekbe. A keyloggereknek két típusa van: a szoftveres keylogger kártékony programként települ a számítógépre, és akár más eszközökre is képes átterjedni, míg a hardveres keylogger egy fizikai eszköz, amely ugyan nem terjed tovább, de szintén képes érzékeny információk kiszivárogtatására. Mindkét típus komoly veszélyt jelent a digitális biztonságra, mivel képesek hozzáférést biztosítani a támadók számára különféle fiókokhoz és rendszerekhez.
https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

Kiberbiztonság: lásd cybersecurity

Kiberbűnözés: lásd cybercrime

Kiberfegyver: lásd cyber weapon

Kiberháború: lásd cyber warfare

Kibertér: lásd cyberspace

Kiberterrorizmus: lásd cyberterrorism

Killware: A killware olyan digitális kártevők (malware-ek) gyűjtőneve, amelynek célja, hogy fizikai sérülést vagy veszélyt okozzon a kritikus infrastruktúrákban, mint például az olajvezetékek, vízellátó rendszerek vagy kórházak. Ide sorolhatók például az olyan zsarolóvírusok, amelyek kifejezetten kórházakat és létfenntartó rendszereket támadnak meg.
https://makay.net/kiberbiztonsagi-fogalomtar

Lándzsás adathalászat: lásd spear phishing

Levélszemét: lásd spam

Live Response: A Live Response (vagy Live Triage) a kiberbiztonságban egy olyan valós idejű incidenskezelési módszer, amely során a biztonsági szakemberek aktív, működő rendszerekről gyűjtenek adatokat egy kibertámadás vagy gyanús tevékenység idején. A cél az, hogy gyorsan azonosítsák a fenyegetéseket és megtegyék a szükséges lépéseket a károk minimalizálása érdekében. A folyamat során például futó folyamatokat, hálózati kapcsolatokat, naplóállományokat és memóriaadatokat vizsgálnak, gyakran távoli parancssori hozzáféréssel.
https://www.upguard.com/blog/cybersecurity-triage

Logic Bomb: A logikai bomba egy szoftverbe ágyazott rosszindulatú kód, amely addig marad alvó állapotban, amíg bizonyos feltételek nem teljesülnek. Bekapcsoláskor a logikai bomba vírus romboló műveletet hajt végre, például fájlok törlését vagy kritikus rendszerek megzavarását. A hagyományos rosszindulatú programokkal ellentétben a logikai bomba nem terjed aktívan, hanem az előre meghatározott aktiválási eseményre vár.
https://www.beyondtrust.com/resources/glossary/logic-bomb

Logikai bomba: lásd Logic Bomb

Malvertising: A malvertising az online hirdetési hálózatokat használja arra, hogy kártevőkkel fertőzze meg az áldozatok számítógépét vagy mobil eszközét. A támadók hamis hirdetéseket vagy rosszindulatú kódot helyeznek el a legitim hirdetési hálózatokon, amelyeket a megjelenő weboldalak egy része megjeleníthet, és amelyek megfertőzhetik az áldozatok számítógépét, ha rákattintanak a hirdetésre.

Előfordult, hogy a támadók rosszindulatú hirdetéseket helyeztek el az eBay online aukciós weboldalán is.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

Malware: A malware kifejezés magába foglal mindenféle rosszindulatú szoftvert vagy kódot, beleértve ezek legismertebb fajtáit, mint a trójaiak, zsarolóvírusok, vírusok, férgek és banki kártevők. A közös tulajdonságuk a szerzőik és alkotóik rosszindulatú szándéka. Egy általános felhasználó nehezen tudja megállapítani, melyik fájl malware, és melyik nem. Ezért vannak a biztonsági megoldások, amelyek hatalmas adatbázisokat tartanak fent a korábban felismert rosszindulatú mintákból, és többféle védelmi technológiát alkalmaznak az újak ellen, ezzel segítve a hatékony felismerést. A malware-írók az utóbbi időben sajnos nagyon kreatívak. „Termékeik" elavult rendszerek sebezhetőségein keresztül terjednek, korábbi biztonsági szabályokat játszanak ki, a memóriában rejtőznek vagy ismert alkalmazásokat utánozva maradnak észrevétlenek. Azonban még ma is a leggyengébb láncszem a leghatékonyabb fertőzésekhez maga a felhasználó. A jól kialakított, rosszindulatú melléklettel ellátott e-mailek bizonyítottan hatékony, mégis olcsó módjai annak, hogy kellemetlen helyzetbe hozzanak egy rendszert.
https://www.eset.com/hu/malware/

Man in the middle támadás: Az MitM támadás során a két fél közötti kommunikációt egy támadó jogosulatlan hozzáféréssel és manipulációval befolyásolja úgy, hogy a kommunikációs csatornát (tipikusan valamilyen számítógépes hálózatot) eltérítve mindkét fél számára a másik félnek adja ki magát. Így a két fél azt hiszi, hogy egymással beszélget, miközben valójában mindketten a támadóval vannak csak kapcsolatban, aki így kijátszhatja az ilyen támadásra fel nem készített kihívás/válasz protokollokat, egyszerűen továbbítva a kihívást a másik félnek, majd visszaküldve annak válaszát. Egy sikeres MitM támadás lehetővé teszi a támadóknak, hogy elfogják vagy manipulálják az érzékeny személyes információkat, például a bejelentkezési hitelesítő adatokat, tranzakciós részleteket, számlaadatokat és hitelkártya számokat. Ezek a támadások gyakran az online banki alkalmazások és az e-kereskedelmi weboldalak felhasználóit célozzák meg, és sok esetben a phishing e-maileket használják fel a felhasználók megfertőzésére, hogy olyan kártevőket telepítsenek, amelyek lehetővé teszik a támadást.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

Man in the Disk: Az MitD sérülékenység a sebezhető szoftveren és annak felhasználóján kívül egy harmadik fél (személy vagy kártékony kód) számára is hozzáférést és/vagy módosítási lehetőséget biztosít a szoftver lokálisan tárolt adataihoz, komponenseihez.
https://makay.net/kiberbiztonsagi-fogalomtar

Multifactor Authentication (MFA): A multifactor authentication, magyarul többtényezős hitelesítés egy olyan biztonsági eljárás, amely során a felhasználónak a bejelentkezéshez nemcsak egy, hanem legalább két különböző hitelesítési tényezőt kell megadnia. Ezek a tényezők három kategóriába sorolhatók: valami, amit a felhasználó tud (például jelszó vagy PIN-kód), valami, ami a birtokában van (például mobiltelefon vagy biztonsági kulcs), valamint valami, ami ő maga (például ujjlenyomat vagy arcfelismerés). A többtényezős hitelesítés célja, hogy jelentősen csökkentse az illetéktelen hozzáférések esélyét, és növelje az online fiókok és adatok biztonságát.
https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Nigériai típusú csalások: A „nigériai típusú" csalás a megtévesztés egyik legrégebbi, 19. század végén elterjedt formája, amit nigériai levelekként vagy 419-es átveréseként is említenek. Kezdetben hagyományos, postai úton vagy faxon terjedt, de a telekommunikációs eszközök fejlődésével, valamint az internet és az e-mail terjedésével ennek a csalástípusnak is az online tér vált a fő platformjává. A nigériai csalások során az elkövetők valamilyen megtévesztő kommunikációval – jellemzően e-mailben – pénz utalására veszik rá az áldozatukat, vagyis ezekben az esetekben az ügyfelek maguk utalnak! A hamis levelekben, megkeresésekben, általában – jelentős részesedés ígérete mellett – segítséget kérnek az elkövetők: menekültek vagyonának vagy jogtalanul elvett örökség visszaszerzéséhez, valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez stb. Közösségimédia-oldalakon, online társkereső portálokon terjed a nigériai csalás azon változata, amelynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen megható történettel pénzt kér tőle. A megtévesztő történetet valódinak látszó, de hamis közösségimédia-profillal és eredetinek tűnő, de szintén fiktív iratokkal igyekeznek alátámasztani. Hogy a történet hihetőbb legyen, előfordulhat, hogy a csalók nemzetközi átutalást kezdeményeznek, amit aztán visszavonnak, így mutatva, hogy az összeg valójában rendelkezésre áll, csak a levélben jelzett adminisztratív nehézség áll a kifizetés útjában. A levélben kért segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti. Mindezért későbbi busás jutalmat ígérnek, amit azonban a károsultak végül nem kapnak meg, de a befizetett összeget elvesztik. Az is egy bevett forma, hogy a vagyon kimenekítéséhez a címzettnek meg kell adnia a bankszámlaadatait, aminek az eredménye természetesen nem az, hogy pénzösszeg érkezik rá, ellenkezőleg: az elkövetők immár hozzáférnek a bankszámlához, így akár le is nullázhatják azt.
https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/nigeriai-csalas

Nulladik napi támadás: A nulladik napi támadás egy olyan biztonsági kockázat egy szoftverben, amelyről nyilvánosan nem tudunk, és amelyről a szállító sem tud. A nulladik napi támadást azért nevezik így, mert azelőtt történik, hogy a célpont tudomást

szerezne sebezhetősége létezéséről. A „nulladik napi" támadás az első vagy „nulladik" napon történik, amikor a fejlesztő már tud a hibáról, így még nem volt lehetősége arra, hogy a biztonsági javítást eljuttassa a szoftver felhasználóihoz. A támadó rosszindulatú programot bocsát ki, még mielőtt a fejlesztőnek vagy a szállítónak lehetősége lett volna javítócsomagot készíteni a sebezhetőség javítására. A nulladik napi támadás azzal kezdődik, hogy egy szoftverfejlesztő sebezhető kódot tesz közzé, amelyet egy rosszindulatú szereplő észrevesz és kihasznál. A támadás ezután vagy sikeres, ami valószínűleg azt eredményezi, hogy a támadó személyazonosság- vagy információlopást követ el, vagy a fejlesztő létrehoz egy javítást a terjedések korlátozására. Amint a javítást megírták és alkalmazzák, a kihasználást már nem nevezik „nulladik napi" kihasználásnak.
https://www.fortinet.com/resources/cyberglossary/zero-day-attack
https://hu.wikipedia.org/wiki/Nulladik_napi_t%C3%A1mad%C3%A1s

Online Fraud (Online csalás): Az online csalás – más néven kibercsalás vagy internetes csalás – olyan jogellenes tevékenységeket foglal magában, amelyek célja magánszemélyek vagy szervezetek megtévesztése annak érdekében, hogy pénzbeli vagy más jellegű előnyhöz jussanak. Ezek a csalások különböző módszereken alapulnak, és az internet anonimitását, valamint széles körű hozzáférhetőségét használják ki. Következményei lehetnek adatvesztés, anyagi kár vagy a jó hírnév sérülése is.
https://www.fraudsmart.ie/personal/fraud-scams/online-fraud/

OSINT: Az OSINT (Open Source Intelligence vagyis nyílt forrású hírszerzés) olyan hírszerzési módszer, amely nyilvánosan elérhető információkat gyűjt és analizál, hogy információkat szerezzen, például az interneten. Az OSINT célja a hírszerzési szempontokból fontos információk gyűjtése, szelektálása, elemzése, értékelése és felhasználása, például biztonsági célokból, de más szervezetek és egyének számára is használható.
https://makay.net/kiberbiztonsagi-fogalomtar

Payload: Káros rutin, vagy gyakran payload néven emlegetett funkció az, amit egy rosszindulatú program (például vírus, féreg vagy trójai) valóban végrehajt, miután bejutott egy rendszerbe. Ez a kiegészítő funkció a támadó eredeti célját szolgálja. A káros rutin sokféle lehet: adatlopás (érzékeny információk, például jelszavak, bankkártya adatok vagy személyes fájlok ellopása), fájlok módosítása vagy törlése (fontos dokumentumok, rendszerelemek megsemmisítése vagy átírása), rendszerösszeomlás (a számítógép működésképtelenné tétele), lemezterület felülírása (a merevlemez adatainak helyreállíthatatlan tönkretétele), BIOS felülírása (a számítógép alapvető indítási programjának megrongálása, ami megakadályozza a gép elindulását). Fontos szem előtt tartani, hogy nem minden kártékony program okoz azonnal észrevehető károkat. Vannak például olyan régebbi vírusok, amelyek csak kisebb, zavaró hatásokat idéztek elő – például hangot adtak ki billentyűlenyomásra –, és bár nem rongálták meg a rendszert, kellemetlenséget okoztak a felhasználónak. A trójai programok esetében

a kártékony működés egy rejtett funkció, amelyet a készítő szándékosan elrejtett. Ez a funkció jelenti a program valódi célját – például egy hasznosnak tűnő alkalmazás mögé elrejtett adatlopó modul formájában jelenhet meg.
https://www.eset.com/hu/termektamogatas/veszelyek/

PDoS-támadás: A PDoS-támadás (Permanent Denial-of-Service) során a támadó arra törekszik, hogy egy adott szolgáltatást vagy rendszer-alkalmazást tartósan elérhetetlenné tegye fizikai vagy hardveres károsítással. Ez ellentétben áll a hagyományos DoS (Denial of Service) támadásokkal, amelyek a szolgáltatást túlterhelésen keresztül elérhetetlenné teszik. A PDoS támadások veszélyesek lehetnek, mivel a szolgáltatást hosszabb ideig elérhetetlenné teszik, sőt, akár fizikai károkat is okozhatnak.
https://makay.net/kiberbiztonsagi-fogalomtar

Penetrációs teszt: A penetrációs teszt egy informatikai rendszer (kiszolgáló, weboldal stb.) értékelése biztonsági (szoftveres, konfigurációs) sebezhetőségek szempontjából. A sérülékenységvizsgálattal ellentétben a penetrációs (behatolás) tesztelés a vizsgálat tárgya által küldött válaszokból és viselkedési mintákból nemcsak feltételezi egy-egy sérülékenység meglétét, de azok kihasználhatóságát is teszteli offenzív módszerekkel.
https://makay.net/kiberbiztonsagi-fogalomtar

Phishing: adathalász csalási forma ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák. Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha valaki nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra. A kiberbűnözők arra építenek, hogy az emberek elfoglaltak: felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.
https://kiberpajzs.hu/csalastipusok/emailes/phishing/

Phreaking: A phreaking olyan tevékenységet jelent, amely telekommunikációs rendszereket, például nyilvános telefonhálózatokhoz csatlakoztatott berendezéseket és rendszereket tanulmányoz, kísérletezik vagy felfedez. A phreaking során az illetéktelen személyek technikai eszközökkel manipulálják vagy megkerülik a telefonrendszerek működését, hogy ingyenes hívásokat kezdeményezzenek vagy hozzáférnek a hálózat bizalmas részeihez. Eredetileg az analóg telefonhálózatokkal kapcsolatos csalásokra vonatkozott, de a digitális technológia fejlődésével a fogalom kiterjedt a modern kommunikációs rendszerek feltörésére is.
https://www.ninjaone.com/it-hub/endpoint-security/what-is-phreaking/

Polimorf vírus: A polimorf vírusok olyan összetett kódok, amelyek képesek minden fertőzés során módosított verziókat létrehozni magukból, miközben megőrzik az alapvető működési rutinokat. A forráskód felismerés elkerülése érdekében a vírus kódját titkosítják, és minden alkalommal más titkosítási kulcsokat alkalmaznak. Működésük alapja a mutációs motor, amely minden új fertőzésnél megváltoztatja a visszafejtési rutint. Ezáltal a polimorf vírus nem statikus kódot használ, így a hagyományos víruskereső szoftverek számára nehezebben észlelhető. A fejlettebb mutációs motorok akár több milliárd különböző dekódoló rutint is képesek előállítani, még tovább növelve a vírus rejtőzködő képességét.
https://www.trendmicro.com/vinfo/us/security/definition/polymorphic-virus

Pretty Good Privacy (PGP): A PGP egy titkosító szoftver, amelyet az online kommunikációs rendszerek adatvédelmének, biztonságának és hitelesítésének biztosítására terveztek. Bár kezdetben csak e-mail üzenetek és mellékletek védelmére használták, a PGP-t ma már széles körben alkalmazzák, beleértve a digitális aláírásokat, a teljes lemeztitkosítást és a hálózati védelmet. A PGP egyik leggyakoribb felhasználási módja az e-mailek védelme. A PGP-vel védett e-mail olvashatatlan karakterláncá (titkosított szöveggé) alakul, amelyet csak a megfelelő visszafejtési kulccsal lehet megfejteni. A működési mechanizmusok gyakorlatilag megegyeznek a szöveges üzenetek védelme esetében alkalmazottakkal, és vannak olyan szoftveralkalmazások is, amelyek lehetővé teszik a PGP más alkalmazásokra való telepítését, így gyakorlatilag titkosítási rendszert adnak hozzá a nem biztonságos üzenetküldő szolgáltatásokhoz. Bár a PGP-t elsősorban az internetes kommunikáció biztonságossá tételére használják, egyes eszközök titkosítására is alkalmazható. Ebben az összefüggésben a PGP alkalmazható számítógép vagy mobileszköz lemezpartícióira. A merevlemez titkosításával a felhasználónak minden rendszerindításkor meg kell adnia a jelszavát.
https://academy.binance.com/en/articles/what-is-pgp

Pszichológiai manipuláció: A pszichológiai manipuláció olyan stratégia, amelyet egyének vagy csoportok alkalmaznak, hogy manipuláció és megtévesztés révén rávegyék az embereket arra, hogy érzékeny információkat fedjenek fel vagy a biztonságukat veszélybe sodró dolgokat tegyenek. E módszer inkább a pszichológián és az emberi viselkedésen, mintsem a technikai szaktudáson alapul. A pszichológiai manipulációs támadások során gyakran előfordul, hogy a támadó megbízható személynek vagy forrásnak adja ki magát, hogy az áldozat bizalmába férkőzzön. A támadók által használt taktikák közé tartozik többek között a hamis személyiség felvétele, a meggyőzés, illetve a megtévesztés az olyan értékes információk megszerzése céljából, mint például: jelszavak, pénzügyi adatok, rendszerek és hálózatok hozzáférési adatai. A pszichológiai manipulációs támadások többféle formát ölthetnek. E stratégia lényege az emberi sebezhetőségek kihasználása: a támadók így akarják elérni céljaikat, legyen az akár jogosulatlan hozzáférés, akár adat- vagy pénzlopás.
https://www.consilium.europa.eu/hu/policies/cybersecurity-social-engineering/

QR-kódos csalás: Az ilyen típusú csalások esetében az elkövetők azt használják ki, hogy a QR-kód beolvasása előtt a felhasználók nem tudhatják biztosan, mi fog történni, így kénytelenek megbízni annak készítőjében. A csalás célja adathalászat: az elkövetők személyes adatokhoz, illetve bankszámla-adatokhoz próbálnak hozzáférni. Hamis weboldalakon vagy matricákon helyeznek el QR-kódokat, és különféle trükkökkel ösztönzik az embereket azok beolvasására. A QR-kódok adatokat tartalmaznak, és linkként, hivatkozásként működnek, amelyek mögött lehet egy hamis weboldal, káros alkalmazás letöltési linkje, vagy akár egy automatikus fizetési művelet is. Gyakran előfordul, hogy a támadók legitim szervezetek arculatát kihasználva hivatalos plakátokon, posztereken vagy szórólapokon cserélik ki az eredeti QR-kódokat a sajátjaikra.
https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai/qr-kodos-csalas

Ransomware: A zsarolóprogramok olyan típusú rosszindulatú szoftverek vagy kártevők, amelyeket a kiberbűnözők arra használnak, hogy megakadályozzák az áldozat kritikus adataihoz való hozzáférést, megsemmisítsék vagy közzétegyék azokat, hacsak nem fizetnek jelentős összegű váltságdíjat. A hagyományos zsarolóprogramok mind magánszemélyeket, mind szervezeteket veszélyeztetnek, de két közelmúltbeli fejlesztés, az ember által irányított zsarolóprogramok és a szolgáltatásként nyújtott zsarolóprogramok egyre nagyobb fenyegetést jelentenek a vállalatokra és más nagy szervezetekre nézve. Az ember által irányított zsarolóprogramok esetében a támadók egy csoportja a kollektív intelligenciát használja arra, hogy hozzáférjen a vállalati hálózatokhoz. A zsarolóprogram telepítése előtt kutatást végeznek a vállalattal kapcsolatban, hogy megismerjék a biztonsági réseket, és egyes esetekben pénzügyi dokumentumokat tárnak fel, amelyek segítségével meghatározhatják a váltságdíj összegét. A szolgáltatásként nyújtott zsarolóvírus-modell lényege, hogy egy csapat bűnszervezeti fejlesztő létrehozza a zsarolóprogramot, majd felbérel más kiberbűnöző társvállalatokat, hogy feltörjék a szervezet hálózatát és telepítsék a zsarolóprogramot. A két csoport megállapodás szerinti arányban osztozik a nyereségen. Minden zsarolóprogram jelentős veszteséget okoz a megtámadott egyéneknek és szervezeteknek. Napokba, hetekbe vagy akár hónapokba is telhet, amíg az érintett rendszerek ismét online állapotba kerülnek, ami a termelékenység és az értékesítés csökkenését eredményezi. A szervezetek jó hírneve is sérülhet az ügyfelek és a közösség körében.
https://www.microsoft.com/hu-hu/security/business/security-101/what-is-ransomware

Reklámprogram: lásd adware

Romance Scam: A romance scam, magyarul romantikus csalás a csalások olyan formája, amelyben romantikus szándékot színlelnek a csalók, hogy elnyerjék az áldozatok szimpátiáját, majd a jóindulatukat kihasználva rávegyék őket, hogy különböző

hamis ürügyekkel pénzt küldjenek nekik. A célcsoport kiválasztásának pszichológiai okai vannak, ugyanis megfigyelhető, hogy egy idősebb, egyedülálló hölgy esetén van a legnagyobb esély a magány érzésére, amely magában hordozza annak a veszélyét, hogy egy párkapcsolat reményében az átlagosnál óvatlanabb legyen. A csalók ilyenkor kihasználják azt az emberi tulajdonságot is, hogy a racionalitás és a józan döntések meghozatala háttérbe szorul, vagyis azt az állapotot, amikor a szív dominál. A csalás létjogosultságát és a növekvő tendenciáját sajnálatos módon az adja, hogy az emberek nem kellően tudatosak. Amennyiben képesek lennének felismerni a csalókat és azok trükkjeit, rövid időn belül eltűnnének a közéletből, mert nem érné meg számukra a befektetett energia. A használt technikákban, történetekben és kisebb részletekben előfordulnak eltérések az egyes esetek között, de általánosan elmondható, hogy az említett főbb pontok az ilyen jellegű csalások mindegyikében megtalálhatók.
https://nki.gov.hu/wp-content/uploads/2024/02/A-romantikus-csalas.pdf

Rootkit: A rootkit egy olyan rosszindulatú program, amely lehetővé teszi a kiberbűnözők számára, hogy észrevétlenül hozzáférjenek a számítástechnikai eszközökhöz és átvegyék egy számítógép vezérlését. Kezdetben a rootkitek a UNIX operációs rendszerre jelentek meg (beleértve a Linux platformokat is), és ezek olyan eszközök gyűjteményét jelentették, amely alkalmas arra, hogy egy támadó rendszergazdai jogokat szerezhessen az adott rendszeren belül (ezt hívják a UNIX alatt „root” jognak). A rootkit kifejezést Windows alapú rendszereken általában az olyan programok meghatározására szokták használni, amelyek futó folyamatokat, állományokat vagy rendszerleíró adatbáziskulcsokat (Registry) rejtenek el az operációs rendszer, illetve a felhasználó elől. Az ilyen Windowsra telepített rootkit olyan funkciókat használ, amelyekkel nem csak saját magát képes elrejteni, hanem további kártékony kódokat – például billentyűleütés-naplózót (keylogger) – is észrevehetetlenné tud így tenni. A rootkitek nem szükségképpen csak rosszindulatú kódok elkészítéséhez használhatók, de az utóbbi időben jelentősen növekvő mértékben használták fel ezt a rejtőzködő technikát a rosszindulatú kódok készítői.
https://www.eset.com/hu/termektamogatas/veszelyek/

Rosszindulatú program: lásd malware

Sandbox: A sandboxing egy olyan kiberbiztonsági gyakorlat, amely egy elszigetelt detonációs környezetet, vagy „homokozót” használ, ahol a biztonsági csapatok a biztonsági műveleti központban (SOC) az incidensreakciós ciklus részeként detonálják, megfigyelik, elemzik, észlelik és blokkolják a gyanús leleteket. Ez a módszer további védelmi réteget biztosít az ismeretlen támadási vektorokkal szemben. A sandbox használatával a biztonsági csapatok fejlett rosszindulatú programok elemzését végezhetik el a gyanús fájlok elkülönített környezetben történő futtatásával, amely a végfelhasználó operációs rendszerét emulálja. A sandboxing legfontosabb előnye, hogy megfigyelheti a futtatható fájlok, szkriptek vagy rosszindulatú dokumentumok

viselkedését, és ezáltal lehetővé teszi teljesen új és ismeretlen rosszindulatú programok – vagy akár olyan rosszindulatú programok – felderítését, amelyeket egy adott környezetben történő futtatásra terveztek. Ez a következő evolúciós lépés a vírusirtó (AV) motorok által megvalósított aláírás-alapú felismerés után.
https://hungarian.opswat.com/blog/what-is-sandboxing

Scams: A csalások nagyon hasonlatosak az adathalászathoz, de ilyenkor nem a személyes adatok kifürkészése a támadók célja, hanem az emberi érzések manipulálására (social engineering) építenek: szánalmat ébresztenek, vagy az emberi kapzsiságra alapoznak. Például, majdnem minden természeti katasztrófa (földrengés, vihar, áradás, háború, éhínség) után megjelenik a csalási szándék állítólagos jótékony gyűjtések formájában. Van aztán a csalásoknak egy illetékekkel kapcsolatos csoportja (ezeket gyakran nigériai típusnak vagy 419-esnek is nevezik), amikor a csalók azzal kecsegtetik a célszemélyt, hogy nagy összegű pénzhez juthat, ha segít egy vagyont kimenekíteni valamelyik afrikai országból. Ezek a trükkök mindig arra épülnek, hogy megkérik az áldozatot, küldjön előlegbe az adminisztrációhoz egy kisebb összeget (ez lehet akár több ezer dollár is). Előfordulhat az is, hogy az adott országba utazó megtévesztett áldozatot egyszerűen elrabolják vagy megölik. A kevésbé szélsőséges csalási esetekben igen sok ember vesztett már el így sok ezer dollárt. Íme néhány jó tanács, hogyan kerülhetők el az ilyen csalárd trükkök: A jótékonysági intézmények csak olyan érdeklődőkkel veszik fel a kapcsolatot e-mailjeikben, akik ezt kifejezetten kérik (előzetesen külön kérték, illetve hozzájárultak ahhoz, hogy ilyen levelet kaphassanak a szervezettől, ezt szakkifejezéssel Opted In-nek nevezik). A kéretlen, spam jellegű levelek szinte minden esetben csalások – és különösen katasztrófák, rendkívüli események után egészen hamar megjelennek. Éljen bennünk egy egészséges gyanakvás! Az e-mail üzenetek lemásolják egy adott szervezet levélformátumát, grafikai elemeit, ezáltal szinte teljesen hitelesnek látszanak. Sok levél tartalmazza a katasztrófák áldozatainak tragikus történetét.
https://www.eset.com/hu/termektamogatas/veszelyek/

Script Kiddie: A „script kiddie” egy lekicsinylő kifejezés, amelyet a számítógépes hackerek alkottak meg az internetes biztonsági réseket kihasználó éretlen, de gyakran ugyanolyan veszélyes személyekre. A script kiddie-k már meglévő, jól ismert technikákat, programokat és szkripteket használnak az internetre csatlakoztatott számítógépek gyengeségeinek felkutatására és kihasználására. Támadásaik véletlenszerűek, és kevés ismerettel rendelkeznek az általuk használt eszközökről, azok működéséről és az általuk okozott károkról. A forgatókönyvíró gyerekeket jellemzően egyszerű, személyes okok motiválják – szórakozás, káoszkeltés, figyelemfelkeltés vagy bosszú.
https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

Sérülékenységvizsgálat: A sérülékenységvizsgálat egy informatikai rendszer (kiszolgáló, weboldal stb.) értékelése biztonsági (szoftveres, konfigurációs) sebezhetőségek szempontjából. A penetrációs (behatolás) teszteléssel ellentétben a sérülékenységvizsgálat a vizsgálat tárgya által küldött válaszokból és viselkedési mintákból feltételezi egy-egy sérülékenység meglétét, annak kihasználhatóságát viszont nem teszteli offenzív módszerekkel.
https://makay.net/kiberbiztonsagi-fogalomtar

Smishing: A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadók SMS segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat. Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot például a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát. A csalás célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az óvatlan ügyfél pénzét.
https://kiberpajzs.hu/csalastipusok/sms/smishing/

Social engineering: A social engineering, magyarul társadalmi manipuláció egy olyan biztonsági támadási technika, amely során a támadó pszichológiai manipulációt alkalmaz, hogy megtévessze vagy rávegye az embereket bizalmas információk kiadására, hozzáférések megadására, vagy olyan cselekedetek végrehajtására, amelyek általában nem lennének megengedettek vagy biztonságosak. Ez a módszer nem technikai eszközökre, például szoftveres vagy hardveres feltörésekre épít, hanem az emberi bizalomra, figyelmetlenségre vagy jóhiszeműségre alapoz. A társadalmi manipuláció különféle formákban jelenhet meg, például telefonos átverésként, e-mailes adathalászatként, vagy személyes meggyőzésként, és célja, hogy az áldozat akaratlanul segítsen a támadónak megszerezni érzékeny adatokat vagy hozzáférést rendszerekhez.
https://en.wikipedia.org/wiki/Social_engineering_(security)

Spam: A spam bármilyen kéretlen digitális kommunikáció, amelyet tömegesen küldenek szét. A spam gyakran e-mailben érkezik, de terjedhet szöveges üzenetekben, telefonhívásokban vagy közösségi médiában is. A spammerek számos kommunikációs formát használnak a kéretlen üzenetek tömeges elküldésére. Ezek némelyike kéretlen árukat kínáló marketingüzenet. Más típusú spamüzenetek rosszindulatú programokat terjeszthetnek, rávehetik a címzettet személyes adatok megadására,

vagy elriaszthatják azzal a gondolattal, hogy fizetnie kell a baj elkerülése érdekében. Az e-mail spamszűrők sok ilyen típusú üzenetet kiszűrnek, és a telefonszolgáltatók gyakran figyelmeztetnek az ismeretlen hívóktól származó „spamveszélyre". Akár e-mailben, SMS-ben, telefonon vagy közösségi médiában érkezik, egyes spamüzenetek átjutnak, és érdemes felismerni őket, és elkerülni ezeket a fenyegetéseket.
https://www.malwarebytes.com/spam

Spear phishing: A spear phishing, magyarul lándzsás adathalászat vagy szigonyozás olyan csalási technika, amely során a támadók személyre szabott üzenetekkel próbálják tőrbe csalni a potenciális áldozatot. A támadók folyamatosan finomítják módszereiket, és egyre több személyes információhoz férnek hozzá a közösségi média és egyéb online platformok révén. A hitelesség látszatát a kiberbűnözők az úgynevezett social profiling módszert alkalmazva építik fel: a leendő áldozatról nyilvánosan elérhető adatokból, részletes elemzést követően összeállítják annak profilját és elkészítik a személyre szabott félrevezető üzenetet. Ezek az üzenetek általában olyan információkat tartalmaznak, mint a személy neve vagy munkahelyének neve stb. A támadás jellemző elemei közé tartoznak a gyanús hivatkozások és mellékletek, amelyek gyakran rosszindulatú weboldalakra vezetnek, vagy kártékony szoftvereket tartalmaznak.
https://kiberpajzs.hu/csalastipusok/szamitogepes/landzsas-adathalaszat/

Spoofing: Spoofingnak (svindlizésnek) általában azt a folyamatot nevezzük, amikor az információt küldő azonosságát módosítják vagy megváltoztatják, ezáltal elrejtve azt. A hívószámspoofing, azaz hívószám-hamisítás, a vishing (hamis banki hívások) adathalász tevékenységek egyik speciális elkövetési technikája. Lényege, hogy az elkövetők módosítják a hívószámot, amely a hívott fél telefonjának kijelzőjén megjelenik, ezzel elrejtve a valódi hívó fél azonosságát. Vagyis híváskor nem a hívást kezdeményező igazi telefonszáma jelenik meg a készüléken, hanem egy másik, jellemzően olyan szám, ami ismerős: például egy banké, ezáltal még inkább hitelesnek tűnik a hívás. Az ilyen hívások célja elsősorban a bizalom kiépítése, illetve az adathalász támadások első számú védvonalának, az óvatosságnak a kiiktatása. Az ismerős telefonszám megnöveli annak esélyét, hogy az áldozat együttműködik, és érzékeny információkat ad át, alkalmazást telepít, vagy pénzügyi műveletet hajt végre a támadó utasítására.
https://kiberpajzs.hu/csalastipusok/telefonos/spoofing/

Spyware: A spyware, magyarul kémprogram egy olyan nyomkövető szoftver, amelyet a felhasználó tudta és beleegyezése nélkül telepítenek egy számítógépre. Célja a felhasználói szokások, érzékeny adatok – például böngészési előzmények, jelszavak, banki azonosítók – megfigyelése és azok illetéktelen harmadik félhez való továbbítása. Egyes spyware-ek más programok beépített részeként, trójai alkalmazásokhoz

hasonlóan, vagy számítógépes férgek részeként kerülnek a rendszerbe. Előfordul, hogy sebezhető weboldalakon keresztül, rejtett módon települnek az eszközre. Léteznek továbbá olyan hamis kémirtó programok is, amelyek valójában maguk is spyware-ek. Tágabb értelemben – az Anti-Spyware Coalition szerint – a kémprogramok közé sorolhatók a kéretlen megfigyelő és adatgyűjtő szoftverek, például egyes sütik (cookie-k), kereskedelmi keylogger-ek és más nyomkövető technológiák is.
https://www.eset.com/hu/termektamogatas/veszelyek/

SQL[19] Injection: Az SQL Injection során a támadó vagy a feljogosított etikus hacker olyan kódot, karakterláncot ad meg az online beviteli felületen (keresés, regisztrációs/bejelentkezési űrlap stb.), ami a szerveroldali feldolgozás során lehetőséget (akár módosítását) biztosít az adatbázis manipulálására, amelyhez nem lenne hozzáférése.
https://makay.net/kiberbiztonsagi-fogalomtar

Szintetikus identitáslopás: Ez a módszer nem csupán a személyes adatok ellopását foglalja magában, hanem egy fiktív digitális személyiség felépítését is. Az adatokat különböző forrásokból gyűjtik össze, mint például nemzeti azonosítók, születési dátumok, email címek, telefonszámok és lakcímek. Az így létrehozott szintetikus identitás első ránézésre valódinak tűnhet, mivel valós adatokból épül fel. A csalók ezt követően életre keltik a személyiséget a digitális térben, ahol valós emberekkel megegyező viselkedést mutatnak, aktívak a közösségi médiában, e-kereskedelmi felületeken, fórumokon és online közösségekben. Ezáltal hiteles, valósnak tűnő személy látszatát keltik.
https://www.fintechradar.hu/fintech/0603/novekvo-fenyegetest-jelent-a-szintetikus-szemelyiseglopas/

Time Bomb: Az időzített bomba egy olyan rosszindulatú kódrészlet, amelyet szoftverbe ágyaznak, és kizárólag egy előre meghatározott időpontban aktiválódik. Ezzel szemben más típusú kártevők működésbe lépéséhez valamilyen felhasználói tevékenység vagy feltétel teljesülése szükséges. Az időzített bomba azonban az idő múlására épít: addig észrevétlenül rejtve marad, míg el nem érkezik az aktiválás ideje. Ez a tulajdonsága különösen alattomossá teszi. Gyakran szándékosan időzítik fontos eseményekhez vagy dátumokhoz, hogy a lehető legnagyobb zavart vagy kárt okozzák – például adatvesztést, rendszerek leállását vagy más jogosulatlan tevékenységeket idézve elő.
https://www.twingate.com/blog/glossary/time-bomb

Titkosítás: A titkosítás olyan technikai módszerekre utal, amelyek biztosítják az adatokat és a rendszereket, megnehezítve az információkhoz való hozzáférést, illetve a hálózatok és tranzakciók megzavarását. A modern kriptográfiában a titkosításhoz

19 Structured Query Language (strukturált lekérdezőnyelv)

egy titkosítási algoritmus vagy rejtjelező használata szükséges, hogy az olvasható egyszerű szöveget rejtjelezett szöveggé (olvashatatlan titkosított adat) lehessen átalakítani. A rejtjelezett szöveget csak azok tudják visszafejteni egyszerű szöveggé, akiknek hozzáférést biztosítottak az adatokhoz.
https://bitmarkets.academy/hu/crypto-for-advanced/what-are-encryption-and-decryption

Trojan Horse: A „trójai" – melynek történetét a görög regékből ismerhetjük – egy olyan program, amely valami mást csinál, mint amit magáról eredetileg állít. Ez a más nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. A klasszikus trójai általában tartalmaz egy billentyűleütés naplózót (keylogger) is, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az ilyen trójaiakat sokféle céllal alkalmazhatják: rejtett távoli elérést (backdoor) szeretnének biztosítani egy adott számítógéphez, ellenőrizni kívánják a billentyűleütéseket, valamint jelszavak lopására specializálódnak (a legtöbb kémprogram ez utóbbi kategóriába tartozik).
https://www.eset.com/hu/termektamogatas/veszelyek/

Tűzfal: lásd firewall

Vírus: A vírus egy olyan rosszindulatú program, amely képes reprodukálni saját magát – akár megegyező, akár módosított formában – egy másik végrehajtható kódba. A vírusok többféle gazdaprogramot (host) használhatnak, a legismertebbek: végrehajtható állományok (számítógépes programok), betöltő (boot) szektorok (amelyek megadják a számítógépnek, hol találja a rendszerindítási folyamathoz szükséges adatokat), szkript kódok (olyan szkript nyelvek, mint például a Windows Scripting, vagy a Visual Basic), dokumentumokba ágyazott makró utasítások (ezek veszítettek a jelentőségükből, amióta a Microsoft Windows nem hajtja végre őket alapértelmezésben). Amikor egy vírus beágyazza saját másolatát egy másik végrehajtható kódba, ezzel biztosítja azt, hogy a vírus kódja is lefuthasson amikor az eredeti program fut, és úgy terjed, hogy futás közben mindig újabb, tiszta és megfertőzhető programok után kutat. Néhány vírus felülírja az eredeti programkódot – tönkre téve ezzel az eredeti programot –, de a legtöbb esetben úgy fűzik hozzá magukat, hogy mind a gazdaprogram, mind a víruskód életképes maradjon. A kódolástól függően a vírusok sokféle fájltípuson keresztül képesek terjedni a rendszerben, hálózati megosztásokon keresztül is, dokumentum állományokban, de akár lemezek rendszerbetöltő (boot) szektoraiban is. Bár néhány vírus e-mail üzenet útján is terjed, az elektronikus levelezésben szereplő kártevők legnagyobb része féreg. A vírusnak elegendő, ha a sokszorosításáról megfelelően gondoskodik, nem szükséges, hogy büntető rutint is tartalmazzon vagy, hogy széles körben elterjedjen.
https://www.eset.com/hu/termektamogatas/veszelyek/

Vishing: A vishing (az angol „voice" és „phishing", vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. A vishing tipikus formája, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.
https://kiberpajzs.hu/csalastipusok/telefonos/vishing/

Visszahívásos telefonos csalás: lásd wangiri

Wallet recovery: A wallet recovery phrase (helyreállító kulcsmondat) egy biztonsági mechanizmus, amelyet a kriptovalutás pénztárcák (wallet) használatakor hoznak létre. Ez egy előre meghatározott, többnyire 12-24 szóból álló sorozat, amely lehetővé teszi a felhasználó számára a pénztárca helyreállítását abban az esetben, ha elveszíti a hozzáférést vagy elfelejti a jelszót. A helyreállító kulcsmondat birtokában bárki képes újra hozzáférni a pénztárcához, tehát kiemelten fontos a kód biztonságos tárolása. A kulcsmondat elvesztése vagy nyilvánosságra kerülése a kriptovalutákhoz való hozzáférés teljes elvesztését eredményezheti.
https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-wallet-recovery-phrase/

Wangiri: A Japánból származó wangiri a mobiltelefonoknak köszönhetően vált az egyik legelterjedtebb csalástípussá. Lényege, hogy a csalók tömegesen generált számítógépes hívások részeként ismeretlen, általában külföldi – jellemzően 2-essel kezdődő országhívószámmal rendelkező afrikai, vagy 5-össel kezdődő országhívószámmal rendelkező közép-amerikai – számról hívják fel áldozataikat, ám a hívást egy-két csöngés után bontják a visszahívás reményében. A visszahívás azonban a belföldinél jóval magasabb tarifán zajlik, és a csalás akkor is eredményes, ha a hívás látszólag sikertelen: például folyamatosan kicsöng, vagy épp nem csöng ki, hanem vonalszakadást vagy folyamatosan foglaltat jelez.
https://kiberpajzs.hu/csalastipusok/telefonos/wangiri/

Wardriving: A wardriving olyan tevékenység, amikor valaki mozgó járműből – például autóból, bicikliről vagy akár gyalogosan – Wi-Fi hálózatokat keres okoseszközök és ingyenesen elérhető szoftverek segítségével. Célja jellemzően a sebezhető vagy nyitott hálózatok azonosítása, amelyeket később illetéktelenül felhasználhatnak, de etikus hackerek is alkalmazhatják biztonsági hibák feltárására. A kifejezés a WarGames (1983) című filmből ered, a jelenlegi értelmében Pete Shipley biztonsági kutató vezette be 2000-ben. A wardriving során gyűjtött adatokat gyakran térképeken is megjelenítik (ún. access point mapping). Az elmúlt években a modern titkosítási technológiák elterjedése miatt csökkent a jelentősége.
https://www.kaspersky.com/resource-center/definitions/what-is-wardriving

Watering hole támadás: A watering hole (itatóhely) támadás során a támadó egy biztonsági sebezhetőséget használ fel ahhoz, hogy rosszindulatú kódot adjon hozzá egy legitim weboldalhoz, hogy amikor a felhasználók ellátogatnak a weboldalra, a kód automatikusan megfertőzze a számítógépet vagy mobil eszközt. A watering hole támadás egyik formája, amelyben a támadók azonosítják és kihasználják azokat a biztonsági réseket, amelyeket rendszeresen látogatott weboldalak nyitva hagynak. A támadók a watering hole támadásokat rendszerint olyan oldalakon hajtják végre, amelyek sok látogatót vonzanak, és akiknek hozzáférésük van olyan információkhoz, amelyeket a támadók meg akarnak szerezni. Például egy biztonsági szakember felfedezte, hogy a támadók egy portugál nyelvű stratégiai tanácsadó weboldalt használtak arra, hogy az európai és dél-amerikai látogatókat fertőzzék meg kémkedő kártevőkkel. A watering hole támadások általában csendesek és láthatatlanok, és gyakran csak akkor észlelhetők, amikor már kárt okoztak.
https://www.zts.hu/blog/hanyfelekeppen-tamadhatjak-meg-a-cegunk-szervereit-2-resz/

White Hat Hacker: A white hat hacker (fehér kalapos hacker), más néven etikus hacker, olyan informatikai szakember, aki engedéllyel és jogszerűen vizsgálja a rendszerek, szoftverek vagy hálózatok biztonsági hibáit annak érdekében, hogy megelőzze a rosszindulatú támadásokat. Csak olyan rendszereken végez teszteket, amelyek vizsgálatára felhatalmazást kapott, gyakran hibavadász programok keretében, amelyek jutalmazzák a sebezhetőségek felelősségteljes felfedését.
https://www.techtarget.com/searchsecurity/definition/white-hat

Wildcard tanúsítvány: A wildcard (helyettesítő karakter) tanúsítvány tipikusan olyan szerveroldali biztonsági tanúsítvány, amelynek „Subject Alternative Name” mezőjében nemcsak az elsődleges domain www aldomaines változata szerepel, hanem a * karakterhelyettesítő segítségével számos egyéb domainvariáció is (pl.: *.makay.net). Ez a tanúsítványkibocsátási és -igénylési politika biztonsági kockázat miatt kerülendő, ugyanis egyetlen (szintén az adott tanúsítványt használó) kiszolgáló biztonsági incidense maga után vonhatja a többi kiszolgáló kommunikációjának jogosulatlan hozzáférését és sérülését is.
https://makay.net/kiberbiztonsagi-fogalomtar

Worm (féreg): A számítógépes terminológia szerint a férgek a vírusok egy részhalmaza, és bár megvan a képességük önmaguk sokszorosítására, a fertőzéshez hordozó gazdaprogramot (host file) nem igényelnek. Ahogy a vírusok programokat fertőznek meg, úgy a férgek rendszereket árasztanak el. Az ilyen férgek rendkívül gyorsan képesek sebezhetőséget tartalmazó hálózatokon terjedni, és ehhez még a felhasználó beavatkozása sem szükséges. A féreg általában fertőzött e-mail üzenetekkel terjed, amelyekben valamilyen számítógépes sebezhetőséget kihasználó kód található, és maga a levél valamilyen csábító, érdekes üzenetet közvetít. A férgeket általában sokkal könnyebb eltávolítani, mint a vírusokat, mert nem fertőznek fájlokat, egyszerűen törölhetőek. A féreg rendszerint gondoskodik arról, hogy minden rendszerindításkor lefuthasson, ezt az Indító Pult (Startup Folder) vagy a rendszerleíró adatbázis (Registry) bejegyzések manipulálásával éri el.
https://www.eset.com/hu/termektamogatas/veszelyek/

Zero Trust: A „Zéró bizalom elv” azt a biztonsági szemléletmódot jelenti, mely szerint feltételezzük, hogy rendszereink jogosulatlan hozzáférése vagy biztonsági incidense elkerülhetetlen — mi több, valószínűleg már meg is történt —, ennélfogva egyetlen rendszerelem vagy hozzáférési kísérlet sem tekinthető megbízhatónak. A modell középpontjában az adatok, rendszerelemek, alkalmazások és szolgáltatások (DAAS) hozzáférés védelme áll, amelyet szigorú ellenőrzéssel, rendszeres újraértékeléssel, valamint a hálózati fenyegetések folyamatos monitorozásával kell biztosítani. Fontos tisztában lennünk azzal, hogy ennek bevezetése egy rendkívül idő- és erőforrás-igényes folyamat, különösen, ha egy már meglévő IT struktúrát szeretnénk átalakítani.
https://nki.gov.hu/it-biztonsag/hirek/nsa-utmutato-a-zero-bizalmi-biztonsagi-modell-megvalositasahoz/

Zombihálózat: lásd botnet

Zsarolóprogram: lásd ransomware

A kibervédelmi fogalomtár az elkészítésekor 144 olyan kibertéri megnevezést, illetve alapfogalmat tartalmaz, mely szükséges ahhoz, hogy a kibervédelem, kiberbiztonság iránt érdeklődők ebben az új térben el tudjanak igazodni.

Ez a fogalomtár akkor lesz időtálló, ha ezen nyomtatott változat melletti „e” változat a www.bankszovetseg.hu oldalon folyamatosan bővül és aktualizálódik. Ebben számítunk a kiberkérdésekkel foglalkozó szakemberek támogatására.

Irodalomjegyzék

AAG IT Services (2025): The Latest 2025 Cyber Crime Statistics, **https://aag-it.com/the-latest-cyber-crime-statistics/**, Barlborough

Abawajy, J.H. – Mukherjea, S. – Thampi, S.M. – Ruiz-Martínez, A. (ed.) (2015): Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. *Proceedings*. 536. Cham: *Springer International Publishing.* **https://doi.org/10.1007/978-3-319-22915-7**.

Adelmann, F. – Elliott, J. – Ergen, I. – Gaidosch, T. – Jenkinson, N. - Khiaonarong, T. – Morozova, A. – Schwarz, N. – Wilson, C. (2020): Cyber Risk and Financial Stability: It's a Small World After All, IMF Staff Discussion Note

Akey, P. - Lewellen, S. - Liskovich, I. - Schiller, C. M. (2021): Hacking Corporate Reputations, ECGI, **https://www.ecgi.global/sites/default/files/working_papers/documents/hackingcorporatereputations_0.pdf**

Aldasoro, I. - Gambacorta, L. - Giudici, P. - Leach T. (2020): Operational and cyber risks in the financial sector, BIS Working Papers No 840, **https://www.bis.org/publ/work840.pdf**

Amir, E. - Levi, S. - Livne, T. (2018): Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets, Review of Accounting Studies, **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3136193**

Arctic Wolf (2024): A Brief History of Cybercrime **https://arcticwolf.com/resources/blog/decade-of-cybercrime**, Eden Prairie,

Biener, C. – Eling, M. – Wirfs, J. H. ((2015): Insurability of Cyber Risk: An Empirical Analysis, University of St Gallen, Working Papers an Risk Management and Insurance No. 151. **https://www.alexandria.unisg.ch/server/api/core/bitstreams/1a69e767-adb7-45b6-a089-8f2bd7c11c30/content**

Bischoff, P. (2023): Cybercrime victims lose an estimated $714 billion annually, Comparitech, **https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost**

Burgard, M. (2021): Cyber Incident Response: The Real Cost of Not Having a Plan or Cyber Insurance., **https://www.marconet.com/blog/cyber-incident-response**

Campbell, K. - Gordon, L. A. - Loeb M. P. - Zhou, L. (2003): The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security 11/3.

Christos A. Makridis (2021): Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018, Journal of Cybersecurity, Vol. 7, Issue 1,2021, **https://doi.org/10.1093/cybsec/tyab021**

CISA (2020): Cost of a Cyber Incident: Systematic Review and Cross-Validation, **https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf**

CISA (2023): #StopRansomware Guide. **https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf.**

Cobos, E. V. – Cakir, S. (2024): A Review of the Economic Costs of Cyber Incidents, World Bank, Washington

Cybercrime Convention Committee (T-CY) (2020): *The Budapest Convention on Cybercrime: benefits and impact in practice*, Strasbourg, 13.07.2020. **https://rm.coe int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac**

Cybercrime Programme Office of the Council of Europe (C-PROC. 2023): The global state of cybercrime legislation 2013 – 2023: *A cursory overview* (2022), **https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137**

De Carbonnel, A. (2013): Ex-Soviet hackers play outsized role in cyber crime world, Reuters, **https://www.reuters.com/article/technology/ex-soviet-hackers-play-outsized-role-in-cyber-crime-world-idUSDEE97L0GZ/**

Doeland, M. (2019): How to keep payments safe and secure in a changing world. *Journal of Payments Strategy & Systems* 13(2): **https:/doi.org/10.69554/FSLK7337**.

ENISA (2024): ENISA threat landscape 2024: July 2023 to June 2024. *LU: Publications Office.* **https://data.europa.eu/doi/10.2824/0710888**.

Facchinetti, S. - Giudici, P. - Osmetti, S. A. (2020): Cyber risk measurement with ordinal data, Statistical Methods & Applications, Springer; Societa Italiana di Statistica, vol. 29(1), p. 173-185, **https://doi.org/10.1007/s10260-019-00470-0**

FBI (2023): Internet Crime Report, **https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf.**

FBI (2024): Internet Crime Report, **https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf**, Washington

Florackis, C. – Louca, C. – Michaely, R. – Weber, M. (2023): Cybersecurity Risk, The Review of Financial Studies, Vol. 36, Issue 1, Jan. 2023, p. 351-407, **https://doi.org/10.1093/rfs/hhac024**

Frész, F. (2025): Az online csalások mögött álló bűnözői csoportok és kötődéseik, CyberThreat Report, **https://www.cyberthreat.report/p/az-online-csalasok-mogott-allo-bunozoi**

Garg, A. – Curtis, J. – Halper, H. (2003): Quantifying the financial impact of IT security breaches, Information Management & Computer Security 11(2): p. 74-83, **https://doi:10.1108/09685220310468646**

Global Cybersecurity Index (2024), International Telecommunication Union (ITU), **https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx**

Gordon, S. – Ford, R. (2006): On the definition and classification of cybercrime. *Journal in Computer Virology* 2(1) 13–20. **https://doi.org/10.1007/s11416-006-0015-z**.

Hergár, E. – Kovács, L. – Németh, E. (2024): A pénzügyi kultúra helyzete és fejlődése Magyarországon. Hitelintézeti szemle 23(1):5–28. **https://doi.org/10.25201/HSZ.23.1.5.**

Ho, H. T. N. – Luong, H. T. (2022): Research trends in cybercrime victimization during 2010-2020: a bibliometric analysis, **https://doi.org/10.1007/s43545-021-00305-4**

Howell, C.J. - Burruss, G.W. (2020): Datasets for Analysis of Cybercrime. In: Holt, T. - Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. **https://doi.org/10.1007/978-3-319-78440-3_15**

IBM Security (2021): Data Breach Report 2021, **https://liangroup.net/blog/wp-content/uploads/2021/07/Cost-of-a-Data-Breach-Report-2021.pdf**, Armonk

Jaishankar, K. (2007): Establishing a theory of cyber crimes. International journal of cyber criminology 1(2): 7–9.

Kamiya, S. - Kang, J. K. - Kim, J. - Milidonis, A. - Stulz, R. M. (2021): Risk management, firm reputation, and the impact of successful cyberattacks on target firms, Journal of Financial Economics, 2021, Vol. 139, Issue 3, p. 719-749, **https://doi.org/10.1016/j.jfineco.2019.05.019**

Kiss, M. (2023): Az MNB szerepe a pénzforgalmon keresztül megfigyelhető visszaélések kezelésében. *HANTOS PERIODIKA* 4(2): 279–290.

Kiss, M. – Kovács, L. (2025): A pénzügyi kiberbűnözés rendszertana, Gazdaság és Pénzügy 2025/3, **https://bankszovetseg.hu/Public/gep/2025/2025_3%20magyar/385-402%20-%20KissM_KovacsL_kiber%20rendszertan.pdf**

Kotidis, A. – Schreft, S. L. (2022). "Cyberattacks and Financial Stability: Evidence from a Natural Experiment," Finance and Economics Discussion Series 2022-025. Washington: Board of Governors of the Federal Reserve System, **https://doi.org/10.17016/FEDS.2022.025**.

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. Gazdaság és Pénzügy 11(1): 6–29. **https://doi.org/10.33926/GP.2024.1.2**.

Kovács, L. – Terták, E. (2025): Kibervédelmi fogalmak és értelmezésük, Gazdaság és Pénzügy 2025/3, **https://bankszovetseg.hu/Public/gep/2025/2025_3%20magyar/403-446%20-%20KovacsL_Tertak%20Kibervedelmi%20fogalmak.pdf**

Lawrence A. Gordon – Martin P. Loeb – Lei Zhou, (2020): Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model, Journal of Cybersecurity, 6(1), **https://doi.org/10.1093/cybsec/tyaa005**

Lending, C. - Minnick, K. - Schorno, P. J. (2018) : Corporate governance, social responsibility, and data breaches', Financial Review, 53(2)

Louis R. Piccotti – Heng (Emily) Wang (2022): Informed Trading in Options Markets Surrounding Data Breaches, **https://ssrn.com/abstract=3478263**

Lusthaus, J. (2018): Industry of Anonymity: Inside the Business of Cybercrime, Harvard University Press, **https://doi.org/10.2307/j.ctv24trdtf**

Mastercard (2025): A kiberbűnözés kora 2025. **https://www.mastercard.hu/content/dam/public/mastercardcom/eu/hu/pdfs/A%2520kiberb%25C5%25B1n%25C3%25B6z%25C3%25A9s%2520kora%25202025.pdf&ved=2ahUKEwjvkaPFo9ONAxUt9rsIHeGvCQ0QFnoECBgQAQ&usg=AOvVaw196oKT7grbPA6T5Bb30sXw**.

MNB (2022): A magyar pénzügyi szektor kiberfenyegettségi térképe 2022. Magyar Nemzeti Bank. **https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf**.

MNB (2023.): Fizetési Rendszer Jelentés 2023. Magyar Nemzeti Bank. **https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2023-hun-0626.pdf**.

MNB (2025a): Fizetési Rendszer Jelentés 2025. **https://www.mnb.hu/letoltes/mnb-fizetesi-rendszer-jelentes-2025-hun-digitalis-vegleges.pdf**
MNB (2025b): Pénzforgalmi táblakészlet. **https://statisztika.mnb.hu/publikacios-temak/penzforgalmi-adatok/penzforgalmi-adatkozlesek/tajekoztato---penzforgalom**.
NKI: Magyarországi incidensek eloszlása típus szerint 2025.09.19. - 2025.09.25. (2025), Nemzeti Kibervédelmi Intézet, **https://nki.gov.hu/szolgaltatasok/tartalom/incidenskezeles,** Budapest
OECD (2022): Online Consumer Fraud in the Digital Age. **https://one.oecd.org/document/DSTI/CP(2021)7/FINAL/en/pdf**.
Onwubiko, C. (2020): Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security,* 96, 101900. **https://doi.org/10.1016/j.cose.2020.101900**.
ORFK: Borult az első Call Center (2024), MÁTRIX Projekt, **https://www.police.hu/hu/hirek-esinformaciok/legfrissebb-hireink/bunugyek/matrix-projekt-borult-az-elso-call-center.**
Paganini, P. (2012): What Is the Deep Web? A First Trip into the Abyss. Security Affairs, 24 May 2012. **https://securityaffairs.co/wordpress/5650/cyber-crime/what-is-the-deep-web-a-first-trip-into-the-abyss.html**
Salgado, K. (2024): Global Cybercrime Report 2025, Poxyrack, **https://www.proxyrack.com/blog/global-cybercrime-report-2025/**
SZTFH (2024): Mintegy 30 milliárd forintnyi kárt okoztak a kibercsalások hazánkban. **https://sztfh.hu/mintegy-30-milliard-forintnyi-kart-okoztak-a-kibercsalasok-hazankban/**.
The Digital Trends Reports (2021), International Telecommunication Union (ITU), **https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC21/Pages/RPM/Digital-Trends-Reports-2021.aspx**
Tosun, O. K. (2021): Cyber Attacks and Stock Market Activity, International Review of Financial Analysis, Vol. 76, **http://dx.doi.org/10.2139/ssrn.3190454**
UNODC, International Classification of Crime for Statistical Purposes (ICCS): Implementation Manual, Vienna, 2024
World Economic Forum (WEF) (2022): The Global Risks Report 2022, 17th Edition Insight Report, Davos
Zettl-Schabath, K. - Bund, J. - Müller, M. (2024): EuRepoC Cyber Conflict Briefing – June 2024, **https://eurepoc.eu/publication/eurepoc-cyber-conflict-briefing-june-2024/**

Felhasznált weboldalak

Avirus. **https://avirus.hu/.**
BeyondTrust. **https://www.beyondtrust.com/.**
Binance Academy. **https://academy.binance.com/en/.**
BitMarkets Academy. **https://bitmarkets.academy/.**
Biztonságosinternet.**hu. https://www.biztonsagosinternet.hu/.**
Biztos döntés. **https://biztosdontes.hu/cikkek/ketfaktoros-hitelesites.**
Cobalt.io. **https://www.cobalt.io/.**
Computer Crime Research Center. **https://www.crime-research.org/news/24.01.2024/4132/.**
CrowdStrike. **https://www.crowdstrike.com/en-us/.**
Cyberpedia – ReasonLabs. **https://cyberpedia.reasonlabs.com/.**
DotCom Magazine. **https://dotcommagazine.com/.**
EBSCO. **https://www.ebsco.com/.**
Európai Unió Tanácsa. **https://www.consilium.europa.eu/.**
FintechRadar. **https://www.fintechradar.hu/.**
Fortinet. **https://www.fortinet.com/.**
FraudSmart. **https://www.fraudsmart.ie/.**
Group-IB. **https://www.group-ib.com/.**
Infobip. **https://www.infobip.com/.**
ISO 27011 (Wikipedia). **https://hu.wikipedia.org/wiki/ISO_27001**
ITU Online. **https://www.ituonline.com/.**
Kaspersky Magyarország. **https://hu.kaspersky.com/.**
Kiberpajzs. **https://kiberpajzs.hu/.**
Lexiq. **https://lexiq.hu/.**
Ludovika Egyetem. **https://www.ludovika.hu/.**
Magyar Nemzeti Bank. **https://www.mnb.hu/web/fooldal.**
Makay.net. **https://makay.net/.**
Malwarebytes. **https://www.malwarebytes.com/.**
Mcafee. **https://www.mcafee.com/.**
Microsoft Magyarország. **https://www.microsoft.com/hu-hu/.**
Mpost.io. **https://mpost.io/.**
Nemzeti Kibervédelmi Intézet. **https://nki.gov.hu/.**
NinjaOne. **https://www.ninjaone.com/.**
OPSWAT Magyarország. **https://hungarian.opswat.com/.**
Palo Alto Networks. **https://www.paloaltonetworks.com/.**
Perception Point. **https://perception-point.io/.**
SAP Magyarország. **https://www.sap.com/hungary/index.html.**
Sealog. **https://sealog.hu/.**
Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH). **https://sztfh.hu/.**
TechTarget. **https://www.techtarget.com/.**
TrendMicro. **https://www.trendmicro.com/en_gb/business.html.**
Twingate. **https://www.twingate.com/.**
UNICEF. **https://www.unicef.org/.**
Unite.AI. **https://www.unite.ai/.**
UpGuard. **https://www.upguard.com/.**
Webshop Automatizálás. **https://webshopautomatizalas.hu/.**
Wikipédia. **https://www.wikipedia.org/.**
Wolters Kluwer Hungary Kft. **https://net.jogtar.hu/jogszabaly**
ZTS Hungary. **https://www.zts.hu/.**

Felelős kiadó:
Kovács Levente

Lektorálta:
Kerényi Ádám

Nyomdai előkészítés, tördelés:
Németh L. Dániel

Borító:
Mátrai Erik, *Bankkártya galaxis,* 2015

ISBN: 978-963-89653-4-9

Kiadó:
Magyar Bankszövetség

Nyomdai munkák: EPC Nyomda, Budaörs
Felelős vezető: Mészáros László


ERSTE