

A kiberbűnözés kora

2025



Előszó

Abban a digitális korban, amelyben élünk, a kiberbiztonság többé már nem csak az IT szektort érintő probléma, a vállalkozások és egyének számára egyaránt kritikus jelentőséggel bír. Jelentésünk mélyrehatóan vizsgálja a kiberfenyegetések folyamatosan változó helyzetét és az ellenük való fellépés egyre nagyobb szükségét. A tét soha nem volt még magasabb, mivel előrejelzések szerint 2028 végére a kibertámadások által okozott károk eléri a 14000 milliárd dollárt. Kutatásunk rámutat a Magyarországon és közép-kelet-európai régióban egyre növekvő kibertámadásokra és hangsúlyozza a fokozott tudatosság és edukáció fontosságát.

Megvizsgáljuk, hogy az automatizáció és az AI hogyan alakította át a globális fenyegetettségi klímát azáltal, hogy lehetővé tette a támadók számára a nagy mennyiségű kifinomult támadások indítását. Elemzésünk feltárja a kiberbűnözés sokszínű természetét, valamint rávilágít a bűnözők közötti kollaboráció térnyerésére és a legújabb technológiák szerepére.

A kutatás hangsúlyozza, hogy az információmegosztás és az iparágak közötti összefogás elengedhetetlen a védekező oldal ellenállóképességének megerősítéséhez. A jelentés emellett gyakorlati ajánlásokat is tartalmaz a kiberbiztonsági ismeretek és az ehhez kapcsolódó tudatosság fejlesztésére, kiemelve, hogy a digitális ökoszisztémánk védelme érdekében közös erőfeszítésekre van szükség.

Ez a dokumentum kulcsfontosságú forrás a jelenlegi kiberbiztonsági környezet megértéséhez és a piaci szereplők számára számos olyan hasznos információval szolgál, amelyekkel megerősíthetik saját kiberbiztonsági stratégiáikat és ellenállóképességüket.



Michele Centemero,
Ügyvezető Alelnök
Regionális Szolgáltatások Vezetője,
Európa

Tartalomjegyzék

01. Frontvonalak a kibertérben

01.A Trendek a támadói oldalon

01.B Trendek a felhasználói oldalon

01.C A kiberbűnözés változó természete

01.D Kihívások a védekezésben

01.D.1 Egyéneket érintő kihívások

01.D.1.1 Információmegosztás

01.D.1.2 Technológia

01.D.1.3 Oktatás

01.D.2 Vállalatokat érintő kihívások

01.D.1.1 Információmegosztás

01.D.1.2 Technológia

01.D.1.3 Oktatás

02. Digitális ellenállás útjai

02.A TTP Keretrendszer

02.B Felhasználó szintű megoldások

02.B.1 Információmegosztás

02.B.2 Technológia

02.B.3 Oktatás

02.C Vállalat szintű megoldások

02.B.1 Információmegosztás

02.B.2 Technológia

02.B.3 Oktatás



01

Frontvonalak a kibertérben

A kiberbiztonság
meghatározó tényezői

01.A

Trendek a támadói oldalon

A kiberbűnözés olyan, mint bármely más bűncselekmény, ezért ennek megfelelően kell kezelnünk. Ha pénzt hoz, felível.

2025-ben már nem az a kérdés, hogy foglalkoznunk kell-e a kibervédelemmel, hanem az, hogy hogyan tudunk lépést tartani a folyamatosan növekvő támadói oldallal. A kiberbűnözés nem új keletű jelenség. Az elmúlt években tanúi lehettünk a térnyerésének, viszont ahogy a digitális szolgáltatások, termékek és online jelenlétünk egyre összetettebb, úgy találunk a bűnözők is egyre kifinomultabb módszereket a felhasználók elérésére.

14000
mrd. USD

A kiberbűnözés megközelítőleg 14000 milliárd dollárnyi kárt fog okozni 2028-ban.¹

41,9
mrd. HUF

2024-ben a kiberbűnözés 220 ezer tranzakció során 41,9 milliárd forintnyi kárt okozott.³

29%

Az európai cégek mindössze 29%-a érzi magát elég felkészültnek jövőbeli kibervédelmi incidensek ellen.²

FORRÁSOK:
¹STATISTA: GLOBAL CYBERCRIME ESTIMATED COST 2029 [HTTPS://WWW.STATISTA.COM/FORECASTS/1280009/COST-CYBERCRIME-WORLDWIDE](https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide)
²STATIONX: DATA BREACH STATISTICS, [HTTPS://WWW.STATIONX.NET/DATA-BREACH-STATISTICS/](https://www.stationx.net/data-breach-statistics/);MAGYAR NEMZETI BANK (2025): PÉNZFORGALMI VISSZAÉLÉSEK [HTTPS://STATISZTIKA.MNB.HU/PUBLIKACIOS-TEMAK/PENZFORGALMI-ADATOK/PENZFORGALMI-ADATKOZLESEK/TAJEKOZTATO---PENZFORGALOM](https://statistika.mnb.hu/publikacios-temak/penzforgalmi-adatok/penzforgalmi-adatkozlesek/tajekoztato---penzforgalom)
³CYBERSECURITY VENTURES X ESENTIRE(2023): 2023 OFFICIAL CYBERCRIME REPORT [HTTPS://WWW.ESENTIRE.COM/RESOURCES/LIBRARY/2023-OFFICIAL-CYBERCRIME-REPORT](https://www.esentire.com/resources/library/2023-official-cybercrime-report)
MEGJEGYZÉS: *2023-BAN



A kiberbűnözés okozta károk az egekbe szöktek, az előrejelzések szerint **2024 végére pedig elérhették a 9500 milliárd dollárt, amely ha egy ország GDP-je lenne, a világ harmadik legnagyobb gazdaságát képviselné.**¹²

A szakértők egyetértenek abban, hogy a kiberbiztonsági incidensek száma és az általuk okozott károk a következő években folyamatosan növekedni fognak, ami tovább növeli a tudatosság és a hatékony oktatás fontosságát.

”Összeségében arra számítunk, hogy a kiberbiztonsági nyomás fokozódni fog, nem csak a mi iparágunkban, hanem általánosságban, mivel bűnözői oldalon rengeteg erőforrás áll rendelkezésre.

Müller Péter,
IT- Fejlesztési és biztonsági vezető, *Ecofamily*

„A kiberbűnözők végcélja a pénzünk megszerzése. Az adataink, amikeút ellopnak tőlünk, eszközök ebben a folyamatban, hiszen előbb, vagy utóbb ezeket is monetizálni fogják.”

Marsi Tamás,
Igazgatóhelyettes, *NBSZ NKI*

“A támadóknak olyan kifinomult módszerei vannak, hogy akár egy rossz kattintás és lenullázzák a sértett számláját.”

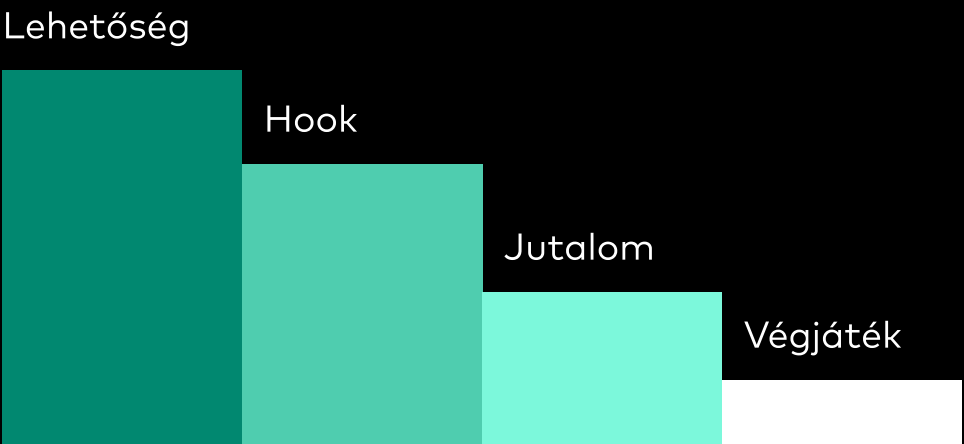
Anonim szakértő



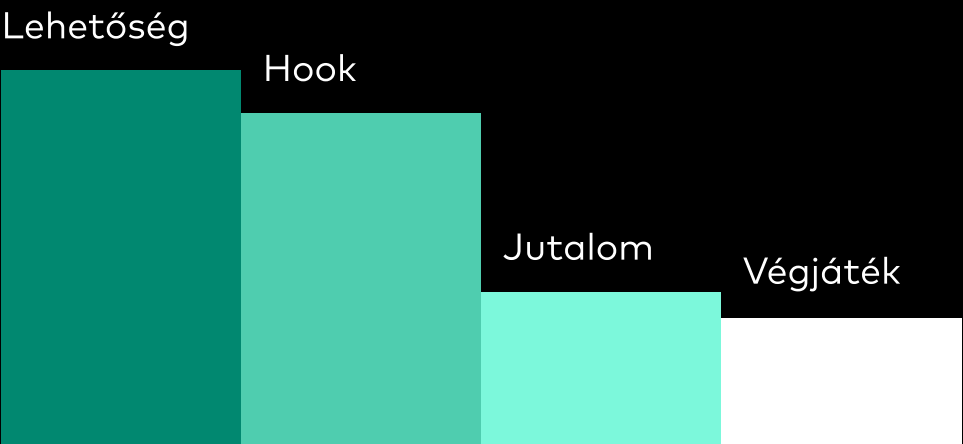
Az AI-alapú automatizálás lehetővé tette a támadók számára a nagy mennyiségű, kifinomult támadások indítását, melyek túlterhelik a védelmi rendszereket, és nagyobb eséllyel tévesztik meg a felhasználókat.

Az automatizálás megnyitotta az utat a támadások új korszaka előtt. A mesterséges intelligencia sokrétű használata lehetővé teszi a támadók számára, hogy olyan nagy léptékű támadásokat indítsanak, melyek még alacsony sikerességi arány mellett is eredményesek. Ha a csalást és az adathalászatot mint folyamatokat nézzük, láthatjuk, hogy az automatizálás jelentősen megnövelte felhasználók elérését. Bár a védelmi rendszerek egyre sikerebben észlelik ezeket a fenyegetéseket, az átjutó támadások már annyira kifinomultak, hogy nagyobb valószínűséggel vezetnek félre a végfelhasználót.

Automatizáció előtt



Automatizáció után



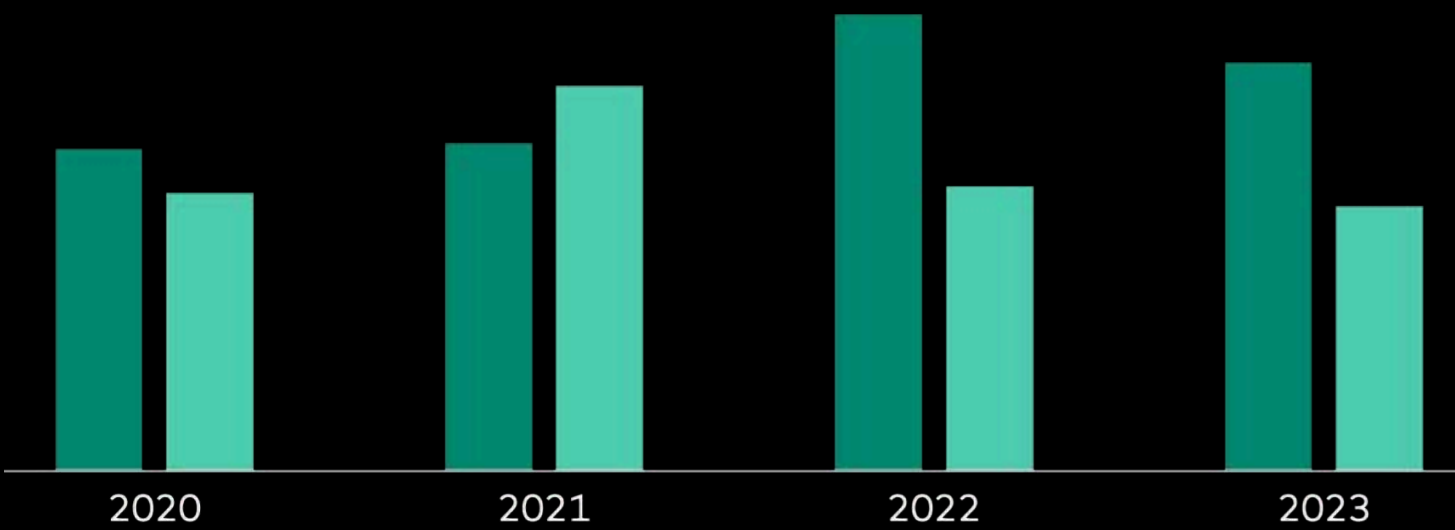
MEGJEGYZÉS:
A grafikon becült hatást ábrázol.

A lehetőség a támadási célpontokat jelzi, a hook az indított támadásokat, a jutalom a sikeresen összegyűjtött adatokat, a végjáték pedig a sikeresen végrehajtott támadásokat.

- Az automatizáció szignifikánsan megemelte a támadások számát.
- Bár a jutalom szakasz aránya alacsonyabb, mint korábban, a támadások ma már annyira kifinomultak, hogy a sikeres végjátékok száma összességében növekedett.

Magyarországon a kiberincidensek száma jellemzően alacsonyabb volt a közép- és kelet-európai referenciaértékhez képest, míg más országok, különösen Lengyelország, gyakrabban voltak célpontok. A lengyel kiugró értékek megnövelték a regionális átlagot, ezzel pedig tovább növelték a különbséget a magyar és a referenciaérték között.

A kiberincidensek alakulása Magyarországon és Közép-Kelet-Európában⁴
Kiberincidensek 1000 főre vetítve



■ Közép-Kelet Európai referencia*
■ Magyarország

FORRÁS: ⁴MASTERCARD CYBER INSIGHTS
MEGJEGYZÉS: MEGKÖZELÍTŐLEGES ADATOK, CSAK TÁJÉKOZTATÓ JELLEGŰEK
*AUSZTRIA, HORVÁTORSZÁG, CSEHORSZÁG, MAGYARORSZÁG, LENGYELORSZÁG, ROMÁNIA, SZLOVÁKIA, SZLOVÉNIA ** 2023-BAN

“Az AI-t a támadók egyre kifinomultabb módon használják, és még nem egyértelmű, hogy a védekező oldal megtette-e a megfelelő előkészítő intézkedéseket. Szükség van mind a szabályozó hatóságok fellépésére a keretek biztosítása érdekében, mind pedig az állam és a különböző piaci szereplők összehangolt közös munkájára.”

Nagy Ádám,
Információbiztonsági igazgató,
K&H



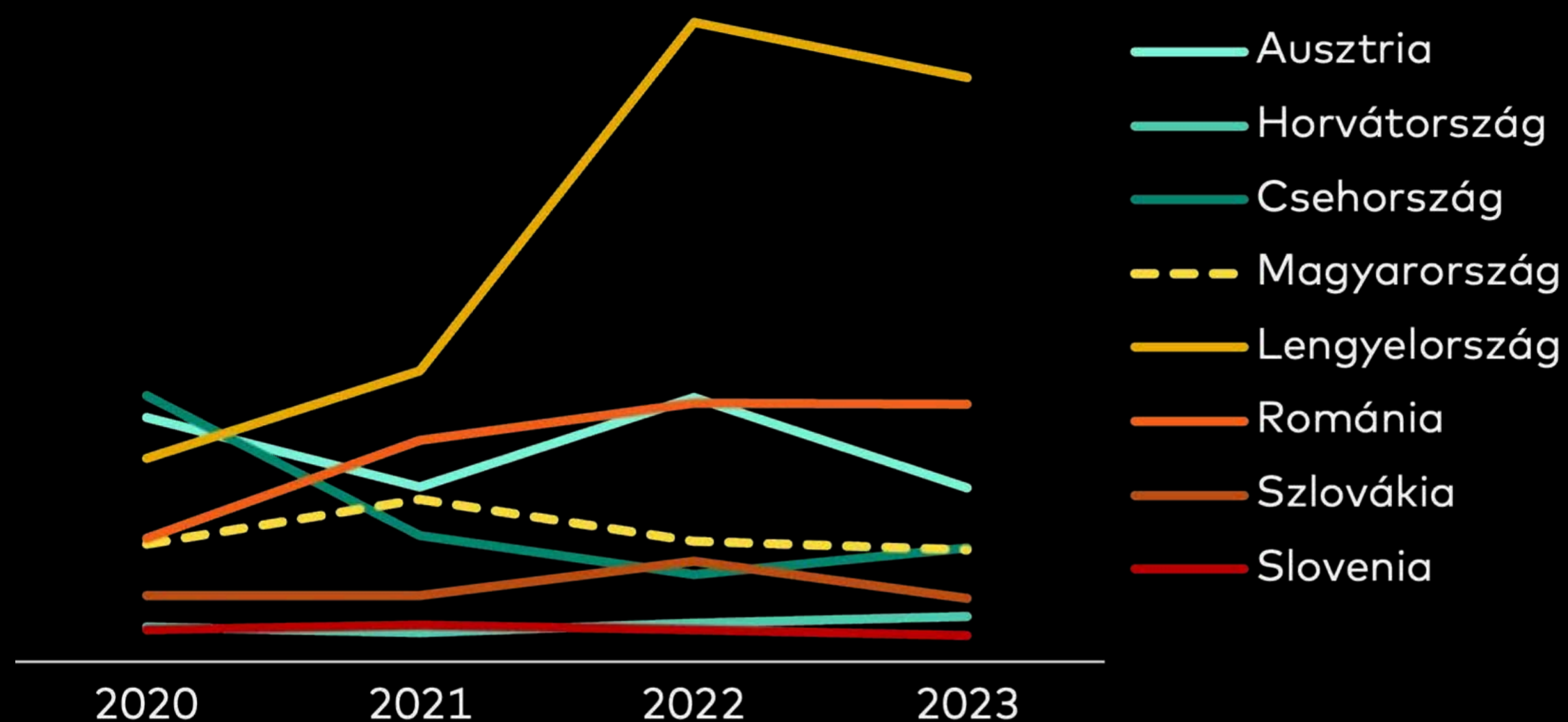
Minél nagyobb és gazdaságilag fejlettebb egy ország, annál vonzóbb célpont a kiberbűnözők számára. Magyarországon az incidensek 2021-ben tetőztek.

Mastercard Cyber Insights

A Mastercard Cyber Insights olyan **stratégiai fenyegetésekkel kapcsolatos információkat** nyújt, amelyek lehetővé teszik a szervezetek számára, hogy átfogó adatelemzés és betekintés révén **proaktívan csökkentsék a kockázatokat, növeljék a kiberbiztonságot és megelőzzék a fenyegetéseket.**

Hogyan működik a Cyber Insights: A fenyegetésinformáció összegyűjtött, feldolgozott és elemzett adatokból áll, amelyek célja a fenyegetések indítékainak, célpontjainak és a támadási magatartásnak a megértése. A Cyber Insights automatikusan összegyűjti a fenyegetésekkel kapcsolatos adatokat, és az adatforrás, a megbízhatóság és a relevancia értékelésével fenyegetettségi intelligenciává alakítja azokat. Ez lehetővé teszi a felhasználók számára, hogy gyorsabb, megalapozottabb döntéseket hozzanak, és a biztonsági fenyegetések elleni küzdelemben a viselkedést reaktívról proaktívra változtassák.

Kiberincidensek alakulása Magyarországon és Közép- Kelet- Európában⁴ Kiberincidensek 1000 főre vetítve



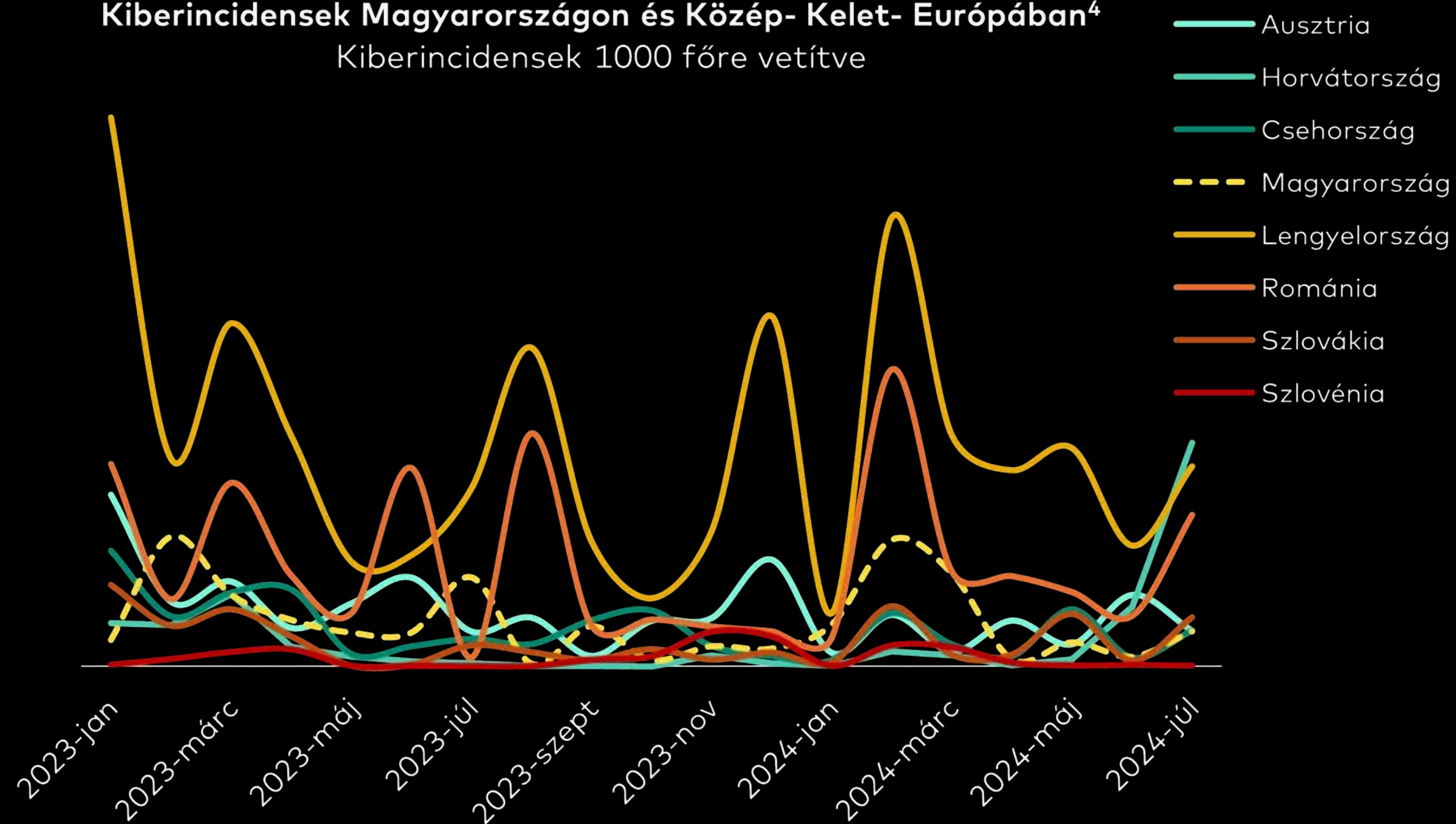
Based on data collected by Mastercard Cyber Insights

- A magyarországi kiberincidensek a **regionális átlaggal összhangban alakultak**, míg a lengyel piac az elmúlt két évben jelentős növekedést mutatott.
- **Ausztria majdnem kétszer annyi** 1000 lakosra jutó **kiberincidenst tapasztalt**, ami potenciálisan a **fejlettebb gazdasági helyzetéből** adódik

Az incidensek gyakorisága és egyes kiugró esetek hasonló tendenciát mutatnak a régióban, ami arra utal, hogy a kiberbűnözés nem az országhatárok között zajlik.

1. A fenyegetésekben történő emelkedés az ION Csoportot érintő Lockbit Zsarolóvírus támadásnak tudható be.
2. A fenyegetések számának növekedése a MOVEit támadásaihoz köthető, amely számos állami, önkormányzati és magánszférában működő szervezetet érintett.
3. Az emelkedés az APT29 Microsoft Teams-en keresztül indított kifinomult adathalász kampányának tudható be.
4. A fenyegetések számának növekedése több jelentős eseményt érintett, köztük egy nagy európai autógyártó ellen elkövetett zsarolóvírus-támadást és egy valószínűleg orosz szervezetekhez köthető kémkedési kampányt.

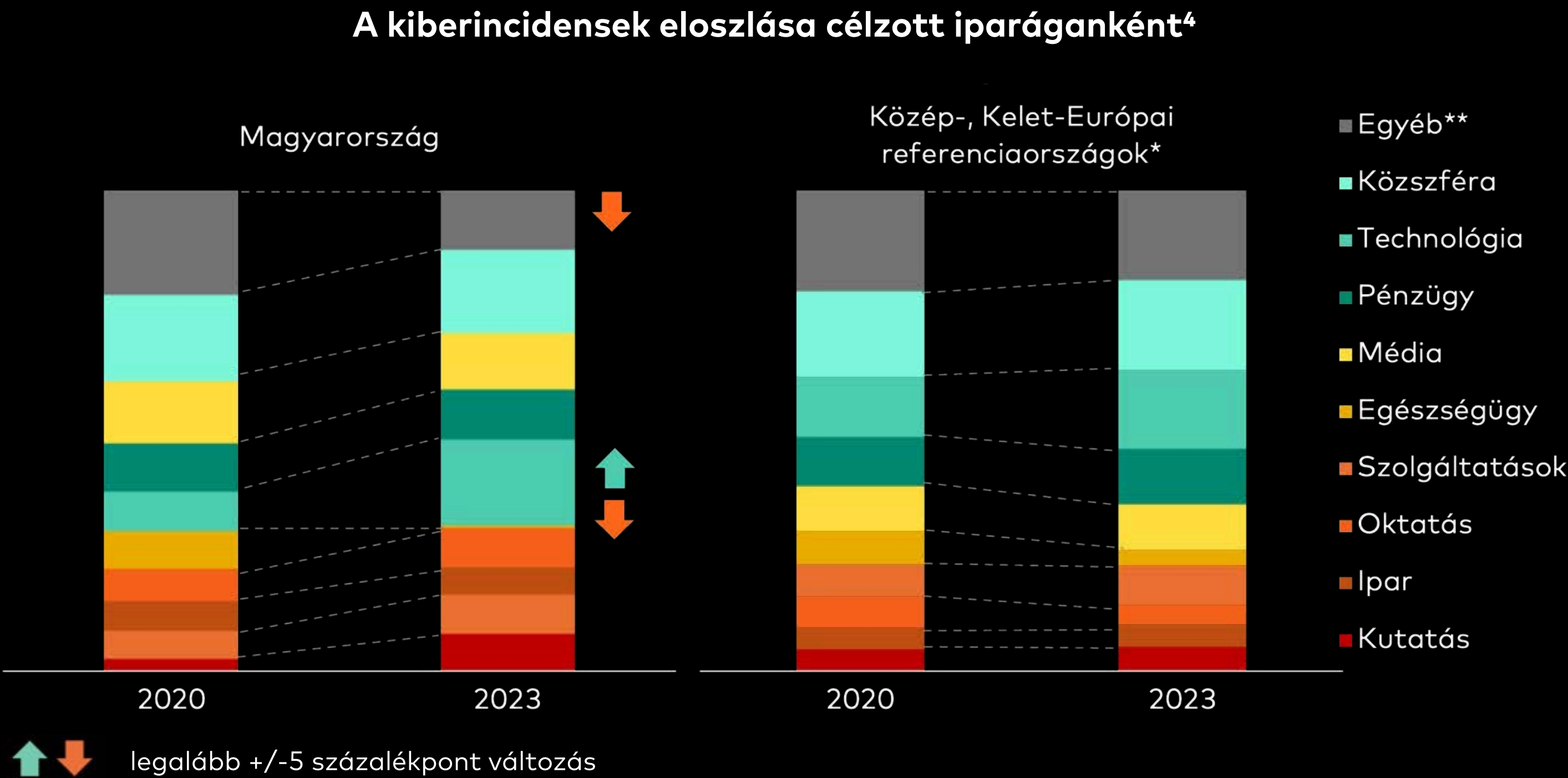
Kiberincidensek Magyarországon és Közép- Kelet- Európában⁴
Kiberincidensek 1000 főre vetítve



Mastercard Cyber Insights által gyűjtött adatok alapján

A Magyarországon támadott iparágak nagyrészt megfelelnek a közép- és kelet-európai referenciaértéknek. Ezek közül a technológia a legcélzottabb ágazat.

- A **közsféra** továbbra is a leggyakrabban célzott terület a régióban.
- Magyarországon a világjárvány óta eltelt idő előrehaladtával az **egészségügyi ágazatot** lényegesen kevesebb támadás érte, míg a technológiai szektort kétszer annyi támadás célozta meg.
- Ahogy a kiberbűnözés természete változik, úgy változnak a célzott szektorok is.



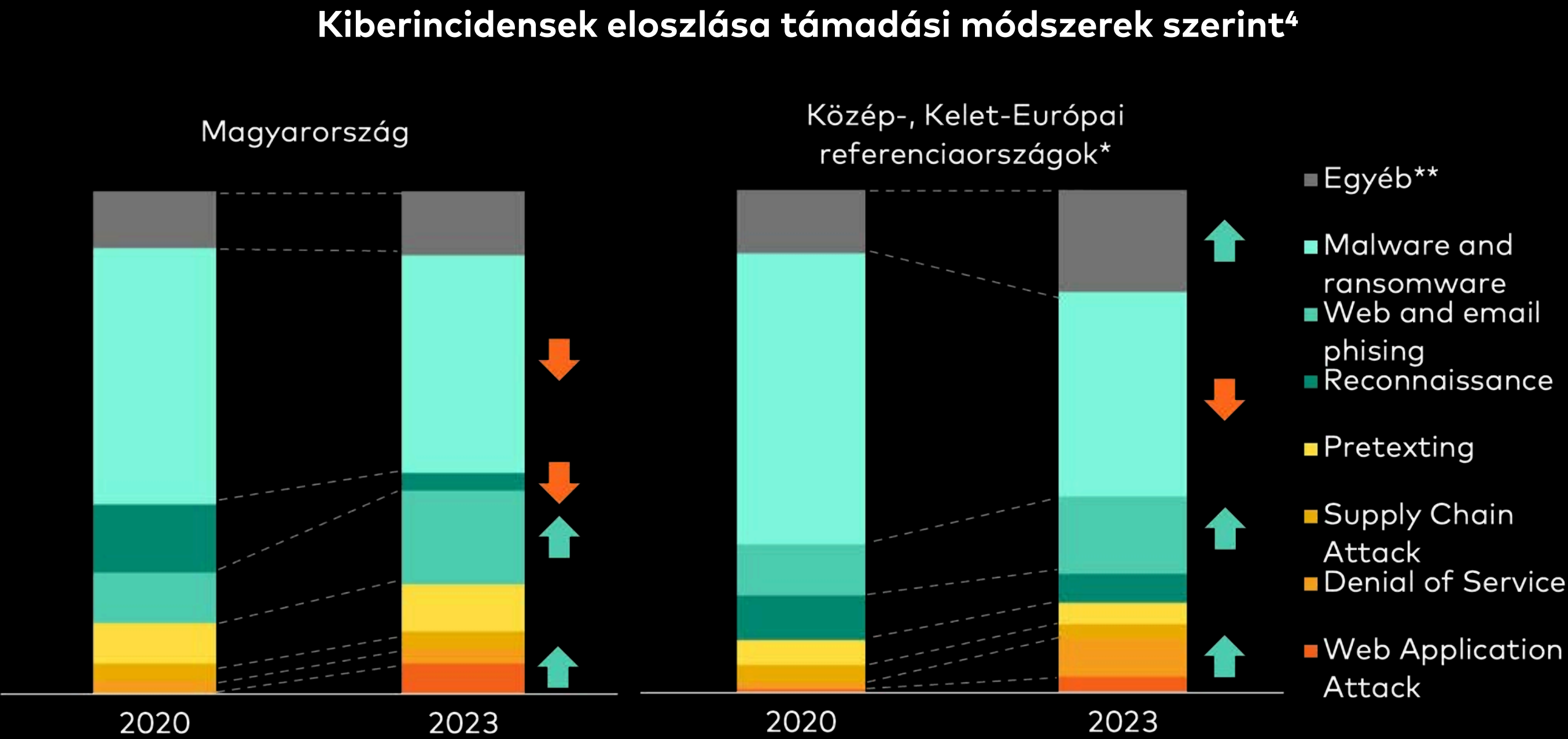
Mastercard Cyber Insights által gyűjtött adatok alapján

FORRÁS: *MASTERCARD CYBER INSIGHTS, MEGJEGYZÉS: MEGKÖZELÍTŐLEGES ADATOK, CSAK TÁJÉKOZTATÓ JELLEGŰEK
*AUSZTRIA, HORVÁTORSZÁG, CSEHORSZÁG, MAGYARORSZÁG, LENGYELORSZÁG, ROMÁNIA, SZLOVÁKIA, SZLOVÉNIA
** EGYÉB: KOMMUNIKÁCIÓ, FOGYASZTÓ, ENERGIA, SZÓRAKOZTATÁS, VENDÉGLÁTÁS, SZERVEZETI MÉRET, GYÓGYSZERIPAR, KISKERESKEDELEM, KÖZLEKEDÉS



A támadók folyamatosan fejlesztik eszköztárukat, ami idővel jelentős változásokat eredményez. Magyarországon a legelterjedtebb támadási módszerek a malware és az adathalászat.

- Magyarországon a **felderítési tevékenységek kevésbé gyakoriak**, míg az **adathalász esetek száma emelkedett a leginkább.**
- Magyarországon és a többi benchmark-országban még mindig a **malware és a zsarolóprogramok a leggyakrabban használt eszközök**, bár arányuk az elmúlt 3 évben csökkent és **változatosabb támadástípusokat** figyelhetünk meg.



Mastercard Cyber Insights által gyűjtött adatok alapján

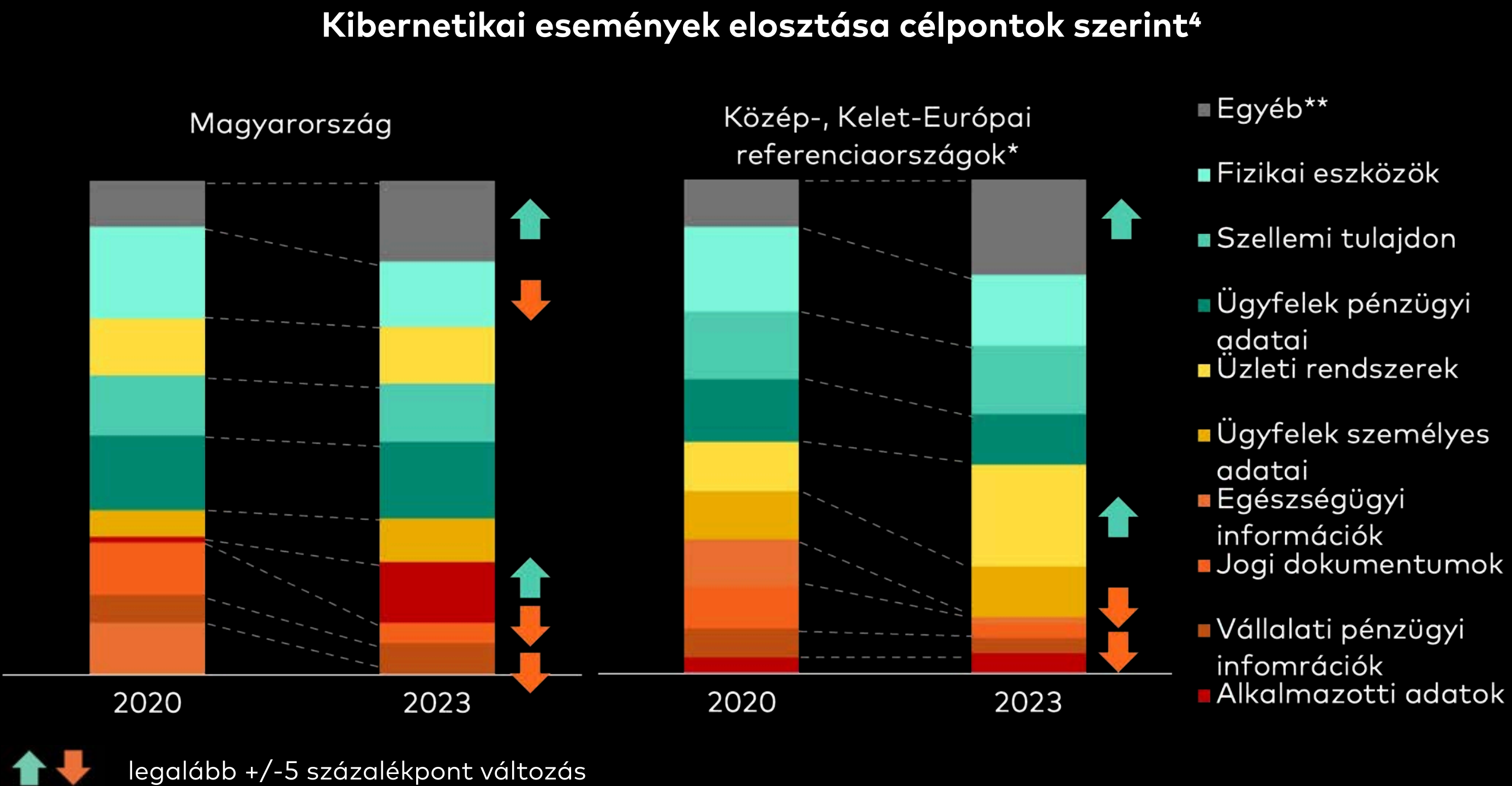
FORRÁS: ⁴MASTERCARD CYBER INSIGHTS, MEGJEGYZÉS: MEGKÖZELÍTŐLEGES ADATOK, CSAK TÁJÉKOZTATÓ JELLEGŰEK

*AUSZTRIA, HORVÁTORSZÁG, CSEHORSZÁG, MAGYARORSZÁG, LENGYELORSZÁG, ROMÁNIA, SZLOVÁKIA, SZLOVÉNIA

**EGYÉB: ADVERSARY IN THE MIDDLE, COMMAND & CONTROL, CONTROL SYSTEM ATTACK, CREDENTIAL ACCESS, INJECTION, LEGITIMATE TOOL, MOBILE DEVICE ATTACK, NETWORK ATTACK, PERSISTENCE, PHYSICAL ATTACK, PRIVILEGE ESCALATION, RESOURCE MANIPULATION, TRANSACTION TERMINAL ATTACK, UNAUTHORIZED DEVICE



A kiberesemények célpontjainak jellege folyamatosan változik, ami jelentős változásokat eredményez a célpontok között mind Magyarországon, mind a régióban.



Mastercard Cyber Insights által gyűjtött adatok alapján

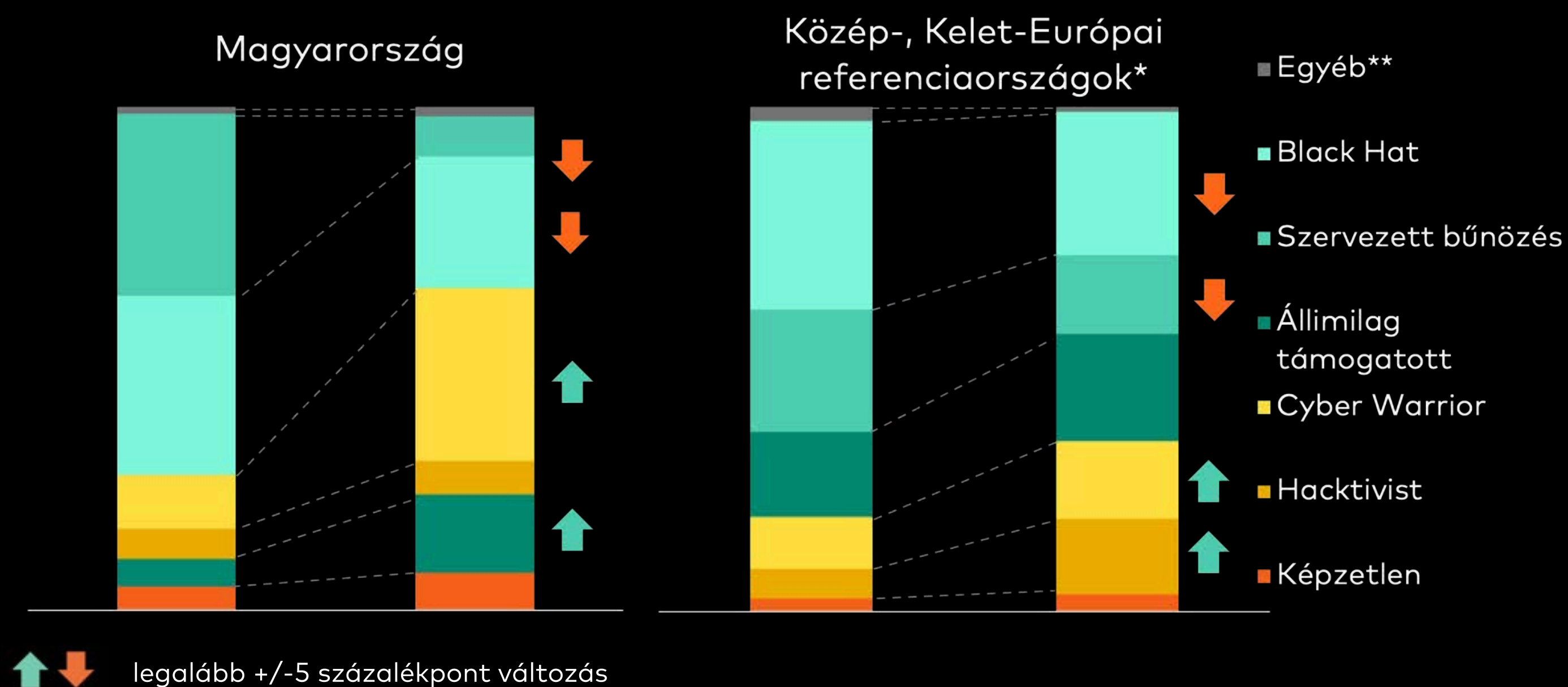
- Magyarországon a munkavállalói adatok vannak a legnagyobb mértékben veszélyeztetve, míg a fizikai eszközök, az egészségügyi információk és a jogi dokumentumok a legritkábban érintettek.
- A régióban az **üzleti rendszerek esetében** volt a legjelentősebb növekedés, ezek váltak az elsődleges célponttá.
- A Mastercard nem figyelt meg globális tendenciát a célpontok típusaiban, **ez régiónként és időszakonként változik.**

FORRÁS: *MASTERCARD CYBER INSIGHTS, MEGJEGYZÉS: * AUSZTRIA, HORVÁTORSZÁG, CSEHORSZÁG, MAGYARORSZÁG, LENGYELORSZÁG, ROMÁNIA, SZLOVÁKIA, SZLOVÉNIA
**EGYÉB: MÁRKA HÍRNEVE, ÜZLETI INFORMÁCIÓK, ÜGYFÉLSZOLGÁLAT, NYILVÁNOSAN HOZZÁFÉRHETŐ ADATOK, BESZÁLLÍTÓI ADATOK



A magyarországi kiberesemények több mint fele a Cyber Warriors és a Black Hat elkövetőihez köthető, míg a szervezett bűnözés részvétele jelentősen csökkent.

Kiberincidensek elosztása elkövetők szerint⁴



Mastercard Cyber Insights által gyűjtött adatok alapján

- Az elkövetők különböző kategóriákba sorolhatók be motiváció szerint. Az egyes csoportok leírása a függelékben található.
- Kiberbűnözők **ciklikus és targetált támadásokat** indítanak, amik országonként **különböző támadói eloszlásokat** eredményeznek.
- **Black Hat** elkövetőihez – kicsi, független támadói csoport, amit csak a pénzügyi haszon motivál– kapcsolható a kiberincidensek jelentős része mind Magyarországon, mind a benchmark régióban.
- Magyarországon a benchmark országokhoz képest nagyobb mértékben nőtt a „**Script Kiddie**”-k (kevésbé képzett elkövetők) aránya, amelynek egyik **oka régiós szinten éppen a technológiai fejlődés**. A mesterséges intelligencia térnyerése alacsonyabbra helyezte a belépési küszöböt a digitális csalások elkövetéséhez, hiszen könnyen automatizálhatóvá, gyorsan adaptálhatóvá és olcsóvá tette a támadásokat.

A rosszindulatú szoftverek és a zsarolóprogramok a bűnözők legelterjedtebb módszerei, de ezek erőforrás-igényesebbek, míg az adathalászat kevésbé képzett szereplők számára is könnyebben hozzáférhető.

Támadók és a módszereik eloszlása⁴



- A „Script Kiddie”-ket leszámítva a támadók főleg rosszindulatú- és zsarolószoftvereket alkalmaznak.
- A technológiailag kevésbé fejlett elkövetők továbbra is az adathalászatot preferálják.
- Mivel a hacktivisták célja nem feltétlenül az anyagi haszonszerzés, hanem a nagy nyilvánosságot adó támadások végrehajtása, gyakran használnak Denial of Service-t.

elenyésző

az események 25%-a a módszerek tulajdonítva

Magyarország

Benchmark országok

FORRÁS: *MASTERCARD CYBER INSIGHTS DATA MEGJEGYZÉS: MEGKÖZELÍTŐLEGES ADATOK, CSAK TÁJÉKOZTATÓ JELLEGŰEK AZ ÖSSZES TÁMADÁS SZÁZALÉKÁZ ÁBRÁZOLJA, IDŐSZAK: 2020-2023
1) KÖZÉP- KELET-EURÓPAI BENCHMARK: AUSZTRIA, HORVÁTORSZÁG, CSEHORSZÁG, MAGYARORSZÁG, LENGYELORSZÁG, ROMÁNIA, SZLOVÁKIA, SZLOVÉNIA





01.B

Trendek a felhasználói oldalon

A kommunikáció segít, önmagában azonban kevés.

A kutatás legfontosabb megállapításai:



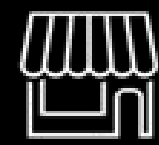
A **márkák kiberbiztonsági kommunikációjának mérhető hatása van** a fogyasztók digitális biztonsággal kapcsolatos ismereteire.



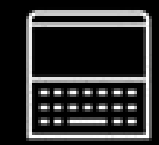
A kiberbiztonság egyszerűsödése a kommunikációban és a **hamis bizalom kiszolgáltatottabbá teszi az embereket**, hiszen emiatt túlbecsülik saját tudásukat.



A **kiberbiztonsági ismeretek és a digitális magatartás között szándék és cselekvés** (intention-action) **szakadék húzódik**.



A fogyasztók feltételezik, hogy **szolgáltatóiknak nagy felelőssége van abban, hogy védőintézkedéseket tegyenek** védelmük érdekében, és ezt egyre inkább el is várják.



A **fogyasztói élmény (CX) kompromittálása veszélyezteti a biztonságot**, a nem megfelelő UX pedig bizalmatlanságot kelt.



Bár Magyarországon a lakosság ismeri a leggyakoribb csalási módokat, a gyakorlatban sokszor rosszul teljesítenek ezeknek a detektálásában.

70%

Egy Mastercard által végzett lakossági kutatás alapján a kitöltők **70%-a szerint nem fordulhat elő, hogy a bank telefonon vagy e-mailben a kártyaadatokat, vagy az online belépési adatokat kéri.** A MÁTRIX projektben összegzett rendőrségi bejelentések mégis több olyan esetet említenek, ahol a sértettektől **10 millió forint feletti összeget csaltak ki ilyen módszerrel.**

60%

A kutatást kitöltők 60%-a ismeri a leggyakoribbnak számító SMS-es adathalászatot, a phishing célú telefonhívásokkal és e-mailekkel pedig szintén több, mint 55%-a találkozott.

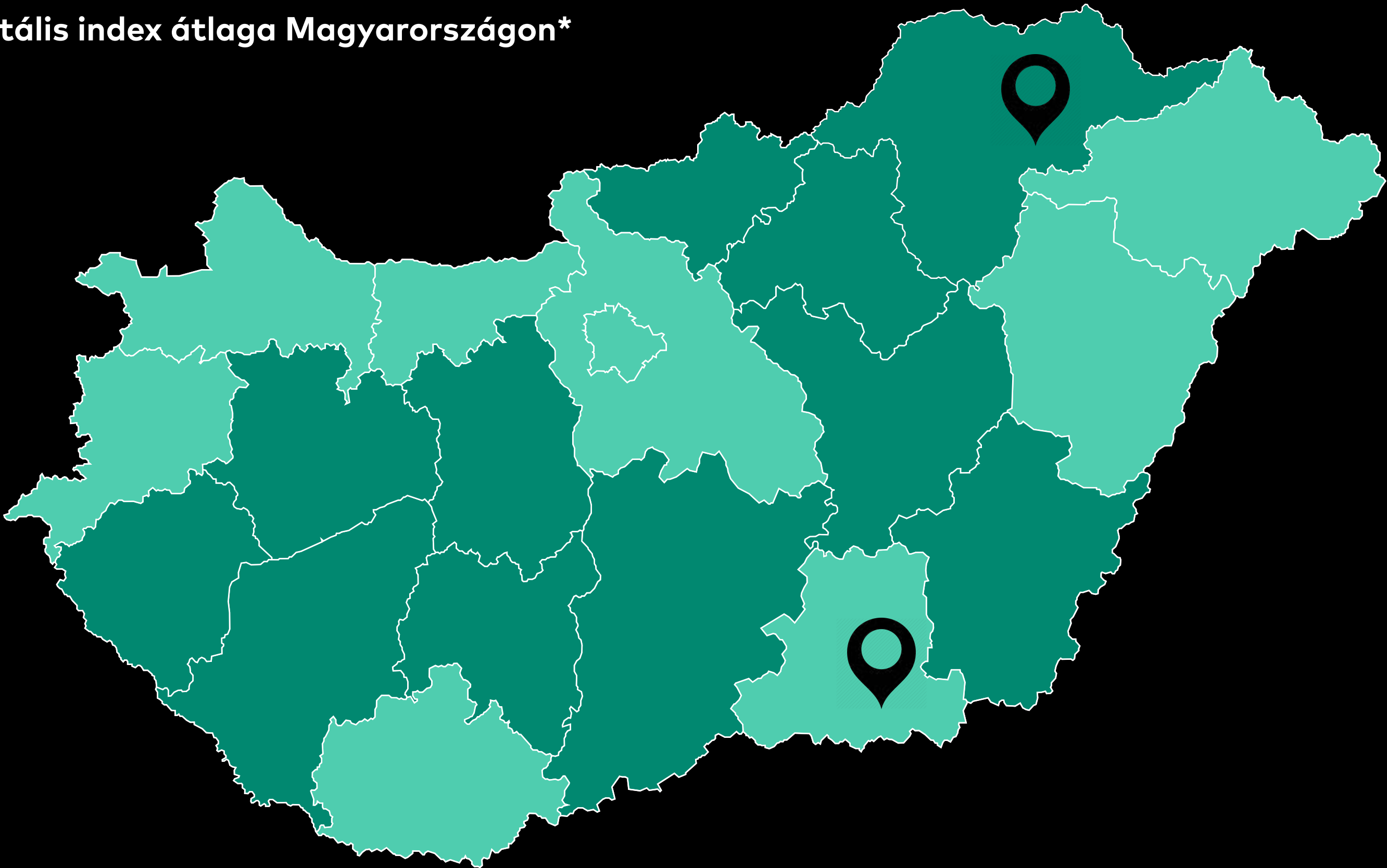
46%

A gyakorlati feladatokban a kitöltők 46%-a azonban **nem tudta eldönteni** a megmutatott üzenetekről, hogy valódiak, vagy csaló szándékúak.



Az emberek tudják, hogyan kellene viselkedniük, de nem feltétlenül értik ennek az okát, vagy tudnak ennek eleget tenni.

Digitális index átlaga Magyarországon*



Magyarországon a biztonságos digitális magatartáshoz szükséges elméleti ismeretekkel aránylag kevés vármegye rendelkezik.

Az országos átlag mindössze 1,86 volt (0-4-ig terjedő skálán), a legmagasabb értéket Csongrád vármegye érte el mindösszesen 2,10 ponttal, míg a legkevesebbet Borsod-Abaúj-Zemplén 1,47 ponttal.

Az emberek, ha ismerik is a leggyakoribb csalási módokat, elméletben tudják, hogyan védekezzenek ellenük, nem feltétlenül értik a támadások alapvető működési mechanizmusait, a támadók motivációt és saját pszichológiai sérülékenységüket.

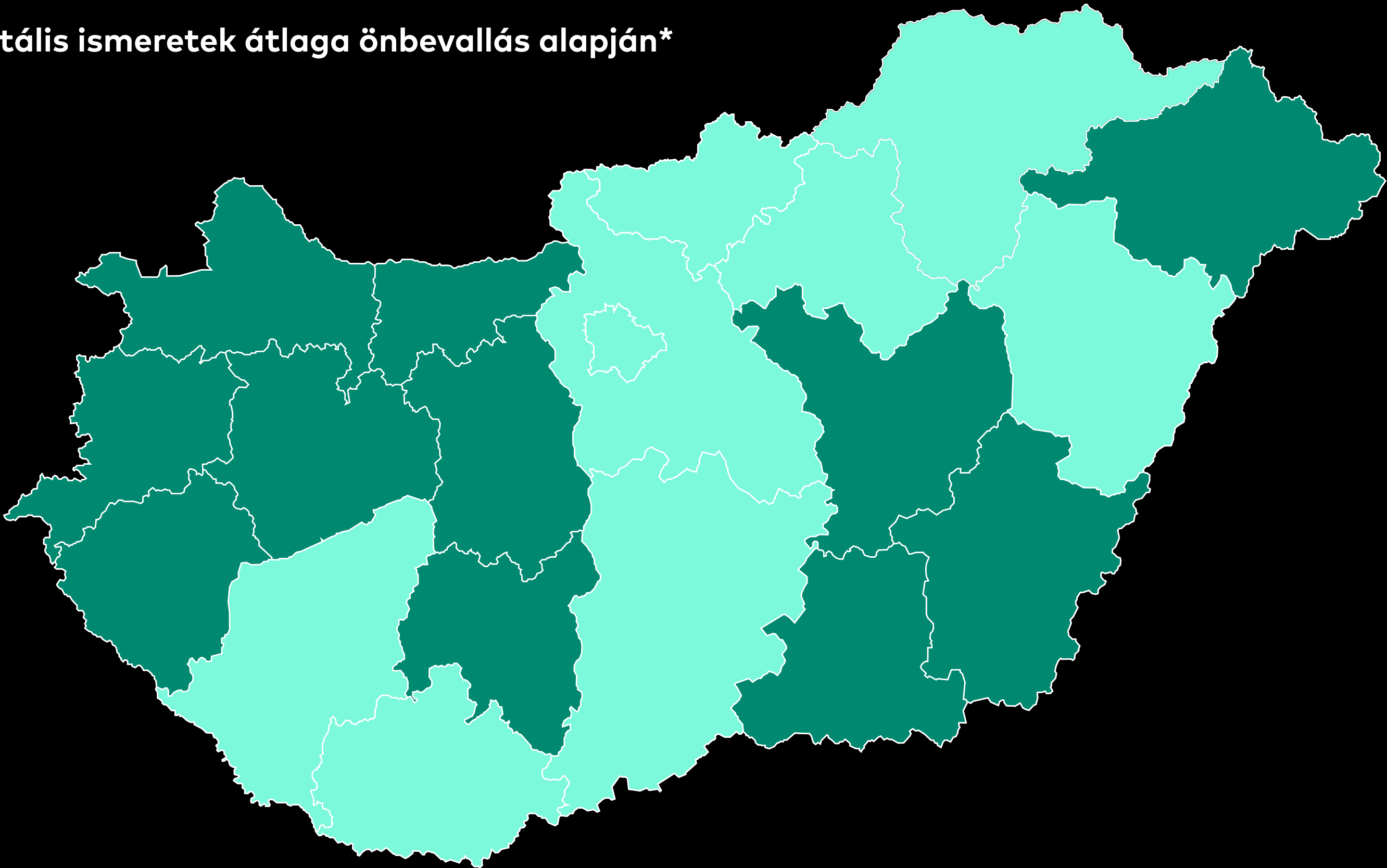
- Országos átlag felett teljesítő vármegye
- Országos átlag alatt teljesítő vármegye

*Egy tíz kérdésből álló elméleti tudást mérő kérdőívből alkotott 4-fokú skála átlag pontszáma Magyarországon 1,86 volt.



A túlzott magabiztosság kiszolgáltatottá tesz bennünket a támadásokkal szemben.

Digitális ismeretek átlaga önbevallás alapján*



Már az országos átlag is tükrözi, hogy egészen nagy eltérések mutatkoznak a lakosság vélt és valós ismeretei között. A kitöltők átlagosan 3,02-re értékelték saját felkészültségüket, míg az elméleti kérdések eredményeinek átlaga csupán 1,86 volt.

Magyarországon bizonyos szegmensek túlbecsülik saját kiberbiztonsági ismereteiket, amelyek hozzájárulhatnak ahhoz, hogy kevésbé körültekintően cselekedjenek.

A kutatás azt mutatta, hogy a **budapesti lakosok** (önbevallás alapján 3,19, digitális index alapján 1,90), **a 18-29 év közöttiek** (önbevallás alapján 3,27, index alapján 1,51) és **az általános iskolai bizonyítvánnyal rendelkezők körében** mutatkoztak a legnagyobb eltérések.

- Országos átlag feletti vélt tudás a vármegyében
- Országos átlag alatti vélt tudás a vármegyében

*A kitöltők egy 4-fokú skálán önbevallásos alapon értékelték a digitális biztonsággal kapcsolatos ismereteiket, melynek az átlag pontszáma 3,02 volt.



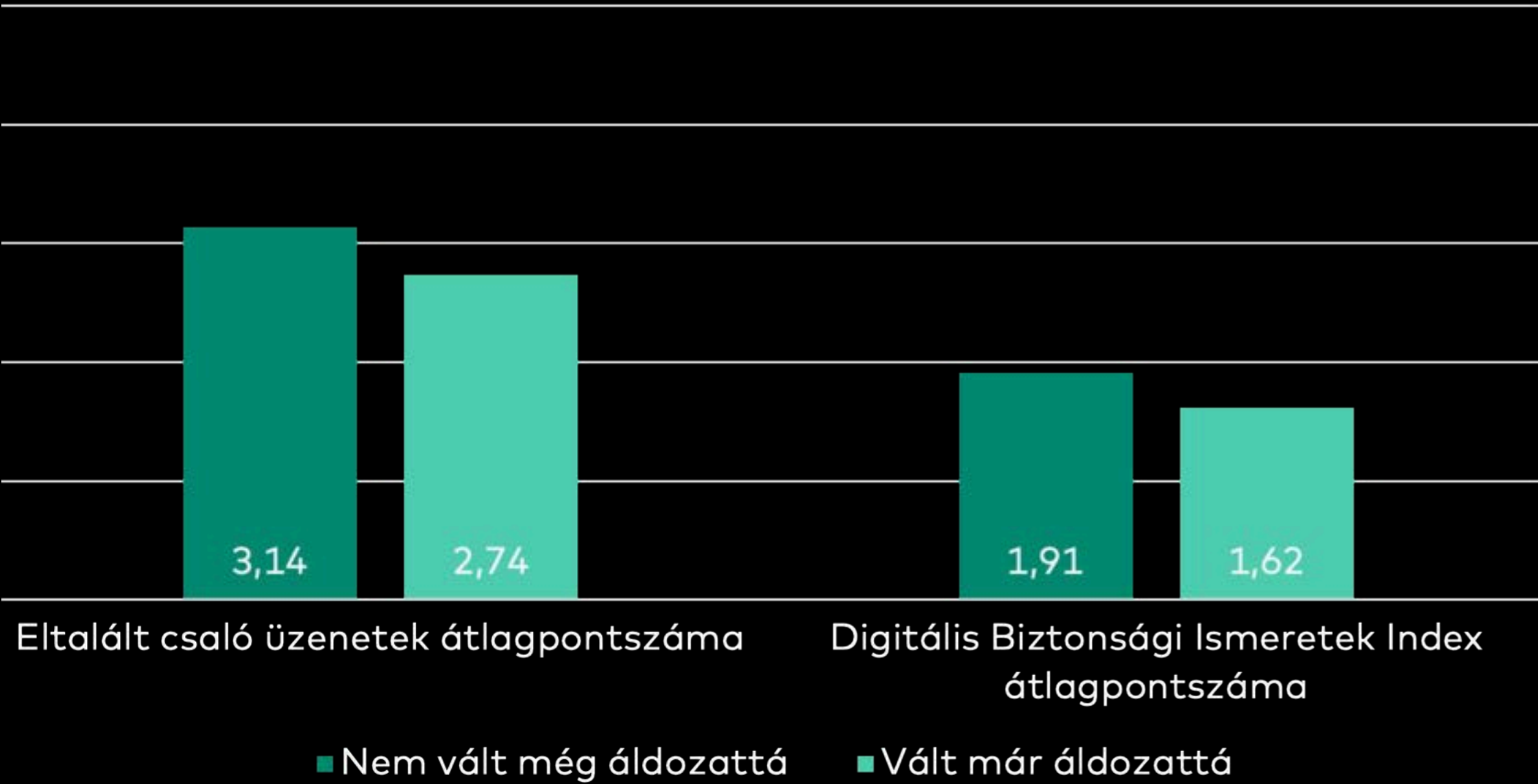
Ismerjük a leggyakoribb módszereket, mégis áldozattá válunk. Jelenleg nem tudunk különbséget tenni csalás és valóság között.

Nemzetközi adatok:



Akik a gyakorlati feladatban jobban teljesítettek, kisebb eséllyel váltak áldozattá a való életben.

Különbség a magasabb tudatosság és az áldozattá válás között



A támadások hatékony kivédéséhez rutinra és reflex szintű biztonságos viselkedésmódokra van szükség.

A gyakorlati feladatokban való jó teljesítmény negatívan korrelál az áldozattá válással, vagyis **minél könnyebben el tudta dönteni valaki az üzenetekről, hogy valódiak, vagy sem, annál biztonságosabban viselkedett éles helyzetben is.** Ez megmutatja nekünk az elméleti oktatás mellett olyan készségeket fejlesztő edukáció jelentőségét is, ami képes lehet felülírni a csalás pillanatában az áldozatra helyezett pszichológiai nyomást. Ehhez könnyen implementálható tanácsokra és gyakorlásra van szükség.

Sokan azt gondolják, hogy vannak kitettebb és kevésbé kitett korcsoportok a kibertámadásokkal szemben. Ezzel szemben az a tapasztalatom, hogy ez nem az életkorhoz, hanem az aktív internethasználathoz kapcsolódik. Mindannyiunknak oda kell figyelnünk a biztonságos online viselkedésünkre.

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI

A szolgáltatói oldal egyre komolyabb nyomással szembesül mind a szabályozók, mind a felhasználók irányából. Egyértelmű, hogy szükség van arra, hogy a vállalatok komolyabban és hatékonyabban foglalkozzanak a témával.



2x

A kitöltők több, mint kétszer olyan nagy valószínűséggel **számítanak saját pénzügyi szolgáltatójukra** digitális tanácsokkal kapcsolatban, mint az állami szervekre, vagy a fogyasztóvédelemre.

“A NIS2 és a hazai implementációja nagyon jó irány a kiberbiztonság erősítésére, azonban a kisebb vállaltoknak és a lakosságnak is ki kell alakítana ezzel kapcsolatban a maga védekezési stratégiáját, mert végső soron az adataik, reputációjuk és pénzük a tét.”

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI

17%

A 18-29 év közöttiek 17%-a várna digitális biztonsággal kapcsolatos információt **saját munkáltatójától**.

„A folyamatos monitorozás és helyzeti tudatosság lassan elvárássá válik a szolgáltatói oldal számára, hiszen amilyen mértékben nő az incidensek száma, annál talán gyorsabban is jelennek meg a szabályozói követelmények és szabályozások, hogy ellensúlyozhassák ezeket.”

Mádi Gábor,
CIO,
Shiwaforce

A felületek kinézete, illetve az általuk nyújtott felhasználói élmény befolyásolja a fogyasztók biztonságérzetét.

A felhasználóbarát design-nak és a biztonságos működésnek nem kizárniuk kellene egymást, hanem egymást kiegészítve támogatni a felhasználókat.

46%

A kutatásban résztvevők közel fele **nem vásárolna** olyan honlapról, aminek a kinézete gyanús.

33%

A kitöltők 33%-a használ **biometrikus azonosítást** banki applikációba belépéskor.

80%

A felhasználók 80%-a szerint a kétfaktoros **azonosítás nem túl bonyolult**, vagy időt rabló, ami **13% pontos javulás 2023-hoz képest**.



“Van összefüggés a vállalatok gyors digitalizációja és az online csalások számának emelkedése között. Láthatóan a digitalizáció üteme gyorsabban növekedett, mint ahogy az embereket felkészíthették volna ezeknek a technológiáknak a helyes használatára.”

Nagy Ádám,
Információbiztonsági igazgató,
K&H

Szükség van arra, hogy a védekezéshez elengedhetetlen információ gyorsan és hatékonyan eljusson mind a felhasználókhoz, mind az üzleti szereplőkhöz. Ehhez pedig valakinek facilitálnia kell a tudásmegosztást és az összefogást.

“Az online térbe áttért csalások egyre kevésbé az infrastruktúrát, sokkal inkább a fogyasztót, az embert támadják. Ezen folyamat tudatosítására, visszaszorítására és kárenyhítésére koncentrál a KiberPajzs az idén.”

Kovács Levente,
Főtitkár,
Magyar Bankszövetség

“A kiberbiztonság közös érdek és közös felelősség. Az alapja pedig a naprakész információk folyamatos megosztása a partnerekkel.”

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI



01.C

A kiberbűnözés változó természete

A magyar lakosság csaknem fele volt már személyesen érintett kiberbiztonsági incidensben, azonban csupán körülbelül ötödük tartja magát felkészültnek az ilyen fenyegetésekkel szemben, ami egyértelműen rávilágít sebezhetőségünkre.

A Mastercard fogyasztói felmérése szerint a kiberbűnözők rendszeresen célba veszik a felhasználókat, mivel arra számítanak, hogy ők a legsebezhetőbbek a támadásokkal szemben. A kiberbiztonság egyre inkább a figyelem középpontjába kerül, de a tudatosság önmagában még kevés.

“Azt tapasztaljuk, hogy a csalások okozta átlagveszteség 100 € körül van. Ez szintén az a lélektani határ, ami alatt az elszenvedők általában nem tesznek rendőrségi feljelentést. A csalások jelentős része feltáratlan marad pont a kisebb összegű bűncselekmények és az ezeket ötvöző szegény miatt.”

Anonim szakértő

FORRÁS: MASTERCARD DIGITAL PAYMENTS INDEX 2023,
*LAKOSSÁGI KUTATÁS A MAGYAR LAKOSSÁG KÖRÉBEN (MASTERCARD, ATLAS, RISE!, SCALE) 2024

48% A magyarok 48%-a tapasztalt valamilyen digitálisan elkövetett bűncselekményt a környezetében.⁵

- A magyarok 30%-nak családtagját, vagy közeli barátját érte már támadás
- 18%-a volt saját maga is érintett
- Az adathalászat e-mailes és SMS-es formája a legelterjedtebb, de az adathalász hívások is kiemelten gyakoriak

miközben

22% A magyarok mindössze 22%-a érzi magát felkészültnek a kiberbűnözéssel szemben.

- Ez az eredmény már önmagában jelzi az egységes kibervédelmi oktatás szükségét
- Jelentős potenciál van a **lakosság tudatosítására**
- **Mindezek mellett pedig központosított csalás elleni fellépésre is szükség van**



A kiberbűnözők már felismerték, hogy az üzleti szereplők is csak emberek; az alkalmazottak vagy a munkáltatók ugyanolyan sebezhetőek, így őket támadva gyakran nagyobb károkat is okozhatnak.

„Általánosságban elmondható, hogy a biztonságtudatosság nem megfelelő, ám az utóbbi időben néhány vezető elkezdte megérezni ennek fontosságát. Ez kulturális szempontból fontos, mert a vezetők példamutatása nélkül nem lesz rendszerszintű változás.”

„A védekezői oldalon nagy probléma az emberi erőforrás és a szakértelem hiánya.”

Anonim szakértő

dr. Policz Tamás,
Stratégiai igazgatóhelyettes,
Semmelweis Egyetem

A kiberbűnözés mindenkit érint, a felhasználókat és a szolgáltatókat egyaránt, mivel a termékek és szolgáltatások egyre bonyolultabbá válnak. Ha valahol sebezhetőség van, az mindenkit veszélybe sodorhat.

A támadók a szolgáltatókat és más vállalkozásokat is célba veszik, kihasználva a dolgozók sebezhetőségét. A szakértői interjúk alapján a nagyvállalatok rendelkeznek a technológiával, de annak alkalmazása fejlesztésre szorul, míg a legtöbb kkv gyenge védelmi rendszerrel rendelkezik.

A szakértők által kiemelt problémák, amik megnehezítik a védelmet:

- A kiberbiztonságra fordítandó források hiánya
- A kulcsfontosságú üzleti szereplők alacsony biztonságtudatossága
- Az emberi erőforrások és a szakértelem hiánya

A kiberbűnözők gyakran együttműködnek, és egymás eszközeire támaszkodva még nagyobb kárt okoznak a támadásaik során.

Amint a Mastercard Cyber Insights elemzése is mutatja, a támadások elkövetőinek motivációja és céljai nagyon eltérőek lehetnek. Mindemellett egyre inkább megfigyelhető az a tendencia, hogy a támadásokat nem egyéni bűnözők hajtják végre, mivel mind a megtámadott rendszerek, mind pedig az adatok, amelyekhez hozzá kell férniük, egyre összetettebbé válnak.

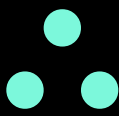
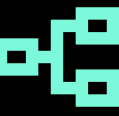
"A legritkább eset, hogy egy személy áll a kibertámadások mögött, hiszen ezt jellemzően specializált csoportok és szakértők hozzák létre."

Fehér Sándor,
CEO,
White Hat IT Security

"A kollaboratív támadások gyakoribbak, mivel sok adatról és összetett rendszerekről van szó."

dr. Palicz Tamás,
Stratégiai igazgatóhelyettes,
Semmelweis Egyetem

Példák a kiberbűnözők közötti együttműködésekre:

-  **Strukturált csapatok:** A bűnözői csoportok működés módja gyakran tükrözi a vállalatok struktúráját specializált szerepkörökkel (pl. rosszindulatú szoftverek vagy adathalászat).
-  **Dark web piacterek:** A dark web olyan kereskedelmi központként működik, ahol a kiberbűnözők eszközöket, adatokat és szolgáltatásokat vásárolhatnak vagy adhatnak el.
-  **Szolgáltatás kiszervezés:** A bűnözői csoportok az erőforrások és a szakértelem maximalizálása érdekében a speciális feladatokat más képzett elkövetőknek adják ki.
-  **Információmegosztás:** Online fórumok segítségével a kiberbűnözők taktikákat cserélhetnek, megbeszélhetik sebezhetőségeiket, és új tagokat képezhetnek.

Az egyéni bűnözők erőforrásai nem elegendőek ahhoz, hogy olyan nagyszabású csalásokat hajtsanak végre, mint amikor csoportosan és összehangoltan működnek együtt.

A bűnözők együttműködése egy organikus folyamat eredménye, amelynek egyik oldalán a **növekvő jutalom reménye**, a másikon pedig a szükségszerűség áll, mivel **egyre összetettebb rendszerekkel és infrastruktúrákkal** szembesülnek.



Mindannyian ugyanannak az ökoszisztémának a részei vagyunk: a probléma és a felelősség is megoszlik közöttünk

A kiberbiztonság mindenkit érint, mivel mindannyian a termékek és szolgáltatások felhasználói, szolgáltatói, vagy termelői vagyunk, egy olyan rendszer tagjai, amelyet kollektív és egyéni döntéseink alakítanak. Ha ebben az ökoszisztémában felelősséget tudunk vállalni, a megoldások is könnyebben elérhetővé válnak.

Mindannyiunk feladata az ökoszisztéma legjobb tudásunk szerinti védelme és az információk megosztása másokkal. Együtt kell megbirkóznunk a különböző kihívásokkal, mind egyéni, mind üzleti szinten. Ezek elsősorban az információmegosztáshoz, a technológiai hozzáálláshoz és felkészültséghez, valamint az oktatás megfelelő szerepének újraértelmezéséhez kapcsolódnak.

„Nehéz eldönteni, hogy a felhasználó, a szolgáltató vagy az államigazgatás felelőssége a legnagyobb az online csalásokkal szembeni védekezésben, hiszen a probléma maga is bonyolult.”

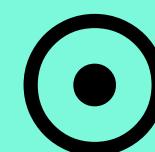
Anonim szakértő



A kiberbűnözés mindenkit különbözőképpen érint, térnyerése pedig komoly aggodalomra ad okot.



Nemcsak a kiberincidensek száma, hanem természete is folyamatosan változik, mivel a támadó oldal egyre szervezettebbé válik.



A technológiai és a közszféra a támadók által leginkább célzott területek, amelyeket a média- és pénzügyi iparágak követnek.



Ahhoz, hogy érdemi hatást érjünk el, az egész ökoszisztémát be kell vonnunk, mert csak így érhetünk el széles körű változást.



01.D

Kihívások a védekezésben

A védekező oldalnak be kell hoznia a lemaradást, amihez elengedhetetlen, hogy az érintett szereplők pontosan tudják hol húzódnak a problémák.



INFORMÁCIÓMEGOSZTÁS

A különböző piaci szereplők közötti információmegosztás elengedhetetlen ahhoz, hogy sikeresen megbirkózzanak a kihívásokkal. Noha már **léteznek erre irányuló kezdeményezések, ezek erősítésére és fejlesztésére továbbra is szükség van.**



Egyéni
kihívások



Vállalkozói
kihívások



TECHNOLÓGIA

A technológiai fejlesztések elengedhetetlenek, de **figyelembe kell vennünk az emberi tényezőt is.** A felhasználók és alkalmazottaik egyszerű, felhasználóbarát megoldásokat keresnek. **Ha túlbonyolítjuk a biztonságos megoldásokat, azzal kevésbé biztonságos utakra terelhetjük őket.**



Egyéni
kihívások



Vállalkozói
kihívások



OKTATÁS

A fogyasztók edukációja fontos, de nem mindegy, hogyan. **Jelenleg sok oktatási kampány a fogyasztók vélt gyengeségeire épül, de nem mindig nyújt kézzelfogható, hosszú távú lépéseket.** Meg kell értenünk, hogyan és mire használjuk az oktatást.



Egyéni
kihívások



Vállalkozói
kihívások





01.D.1.

Felhasználókat érintő kihívások

01.D.1.1

Információ- megosztás

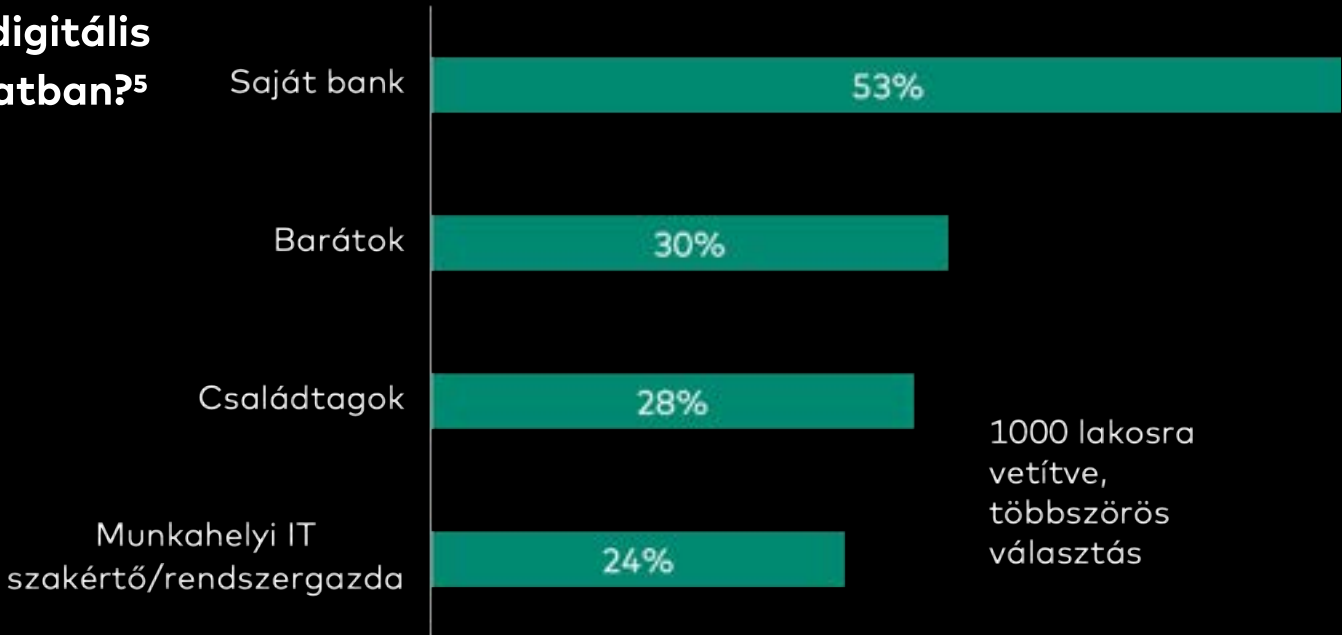


Az emberek közel egyharmada fordulna a szociális hálójához digitális biztonsággal kapcsolatos kérdésekben, de ez csak akkor hatékony, ha a megfelelő tudás is rendelkezésre áll.

Bár a legtöbben a pénzügyi szolgáltatójuktól várják a digitális biztonsághoz kapcsolódó információkat, a szociális háló szerepe is számottevő. **A magyarok gyakran támaszkodnak barátaikra és családtagjaikra** a digitális biztonsággal kapcsolatos kérdésekben, ez viszont hiábavaló, ha a kapcsolati hálójuk nem rendelkezik a szükséges ismeretekkel.

Magyarországon a kiberbiztonságra fókuszáló közösségek még nem terjedtek el. **A kiberbiztonsággal foglalkozó közösségek támogatása alapvető fontosságú**, mivel az informális véleményformálók és gondolatvezérek csomópontként szolgálnak e hálózatokon belül, biztosítva a pontos és értékes információk terjesztését.

Kitől kérne tanácsot digitális biztonsággal kapcsolatban?⁵



FORRÁS: ⁵LAKOSSÁGI KUTATÁS A MAGYAR LAKOSSÁG KÖRÉBEN (MASTERCARD, ATLAS, RISEI, SCALE) 2024

A közösségépítés számos formában megvalósulhat, mind online, mind offline térben. Magyarországon több offline kezdeményezés működik, miközben az olyan online platformok, mint a Reddit, kulcsszerepet töltenek be a közösségek formálásában és támogatásában.



A megkérdezett szakértők **a magyar piacon belüli és a különböző ágazatok közötti együttműködés komoly hiányát állapították meg.**

Megemlítették azonban a külföldi jó gyakorlatokat is, például a **belgiumi Kiberbiztonsági Központot (CCB)**⁷, amely az állami, kormányzati és magánszektorok közötti együttműködés és információmegosztás révén erősíti a kibervédelmi ellenállóképességet. Növelik a tudatosságot, szakértői közösséget építenek, részt vesznek a képzésben és kutatásban egyaránt. A CCB fontos szerepet játszik a végfelhasználók oktatásában és a kiberbiztonsággal kapcsolatos ismeretek terjesztésében.

55%

A safeonweb.be éves kampányával - egy specifikus kibervédelmi témában – a belga lakosság legalább 55%-a találkozott.⁸

5 mil.

A safeonweb kampányhoz csatolt email évente 5 millió üzenetet kap.⁸

FORRÁS: ⁷⁻⁸CENTRE FOR CYBERSECURITY BELGIUM



01.D.1.2

Technológia



A felhasználók a kényelmet és a könnyű kezelhetőséget részesítik előnyben. Ha ezek a tulajdonságok hiányoznak gyakran keresnek egyszerűbb és olcsóbb alternatívákat, még akkor is, ha ez a biztonság rovására megy.

30%

A válaszadók 30%-a az internetbankot a böngészőben elmentett könyvjelzőn keresztül éri el.⁵

20%

A válaszadók 20%-a úgy gondolja, hogy a két-faktoros hitelesítés bonyolult és időigényes.⁵

10%

A válaszadók 10%-a használ jelszókezelőt. A megfelelő erősségű és az eszközönként és fiókonként eltérő jelszavak, valamint a jelszókezelő használata még mindig nem elterjedt az átlag felhasználók körében.⁵

„Sem az otthonokban, sem a munkahelyeken nincs biztonságtudatosság, pedig ha az egyik területen megszokja a felhasználó, hogy biztonságos döntéseket hoz, akkor valószínűleg a többin is az lesz.”

dr. Palicz Tamás,
Stratégiai igazgatóhelyettes,
Semmelweis Egyetem

FORRÁS: MASTERCARD DIGITAL PAYMENTS INDEX 2023,
⁵ LAKOSSÁGI KUTATÁS A MAGYAR LAKOSSÁG KÖRÉBEN (MASTERCARD, ATLAS, RISEI, SCALE) 2024

A JELSZÓ PROBLÉMA

A felhasználók többsége még mindig egyszerű, könnyen megjegyezhető jelszavakat választ, vagy ugyanazt használja különböző fiókokhoz, még akkor is, ha az összetett, egyedi jelszavak biztonságosabbak lennének. A figyelmeztetések ellenére a felhasználók számára a kényelem az első: egyetlen jelszót megjegyezni sokkal egyszerűbb, mint minden egyes fiókhoz új, összetett jelszót fejben tartani. Ez a megközelítés azonban növeli a támadásokkal szembeni sebezhetőséget, mivel a támadók a többször használt vagy gyenge jelszavakat kihasználva több fiókhoz is hozzáférnek a hitelesítési adatok feltöltését célzó támadások során. Ez a példa azt mutatja, hogy a felhasználóbarát lehetőségek gyakran győzedelmeskednek a biztonság felett, néha jelentős kockázatot is vállalva.

Magyarországon a fizetős védelmi termékek iránti kereslet viszonylag alacsony, és a felhasználók gyakran alkalmaznak olyan online viselkedési mintákat, amelyek egyszerűek, de nem feltétlenül biztonságosak. A megkérdezett szakértők szerint a végfelhasználó nem feltétlenül a leggyengébb láncszem, de szinte minden esetben a legutolsó. A technológia fejlődésével pedig egyre nagyobb nyomás nehezedik rájuk.

“Bár a tudatosság kulcsfontosságú, a gyakorlati ismeretek, például a jelszókezelők és hitelesítők egyszerű használatának bemutatása ugyanilyen fontos.”

Turányi Tatjana,
Kiberbiztonsági tanácsadó,
Quadron Cybersecurity

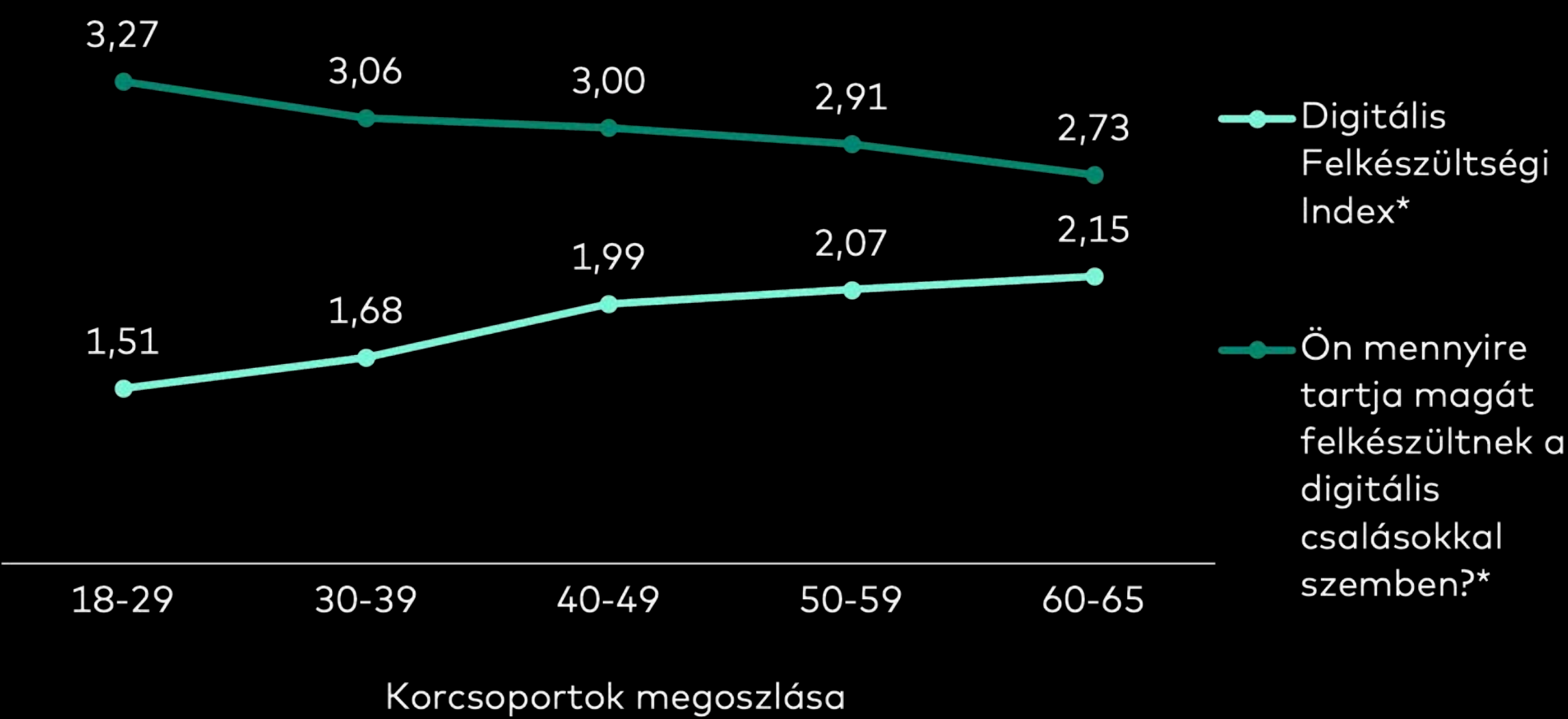


01.D.1.3

Oktatás



Magyarországon a fiatalok kibervédelmi ismeretei a Dunning-Kruger-hatást tükrözik: a korlátozott ismeretek túlzott önbizalomhoz vezetnek.



A magyar végfelhasználók - különösen a fiatalabb generáció tagjai – jellemzően túlzottan magabiztosak a kiberbiztonsági ismereteiket illetően.⁵ Ez a hamis biztonságérzet fakadhat az egyre széleskörűbb ismeretterjesztő törekvésekből és a digitális biztonságról folyó diskurzusokból.

FIATALABB GENERÁCIÓ:
Nem rendelkeznek még saját vagyonnal, de van veszélyérzetük, mert a téma a figyelmük középpontjában áll, ugyanakkor az online térben való mindennapos jelenlétük miatt túlságosan is magabiztosak a képességeikben.

IDŐSEBB GENERÁCIÓ:
Már rendelkeznek vagyonnal, de nem magabiztosak a technológiai újításokkal kapcsolatban és hiányzik belőlük a fenyegetettség érzése.

„Az oktatás hagyományos megközelítésének egyik kihívása, hogy a felhasználónak hatalmas mennyiségű információval van dolga, amelyet nem mindenki képes feldolgozni. Potenciálisan hatékonyabb, ha megmutatjuk nekik, hogyan tudják alkalmazni a munkájukban és a mindennapi tevékenységeikben, hogy ez viselkedésbeli változássá váljon.”

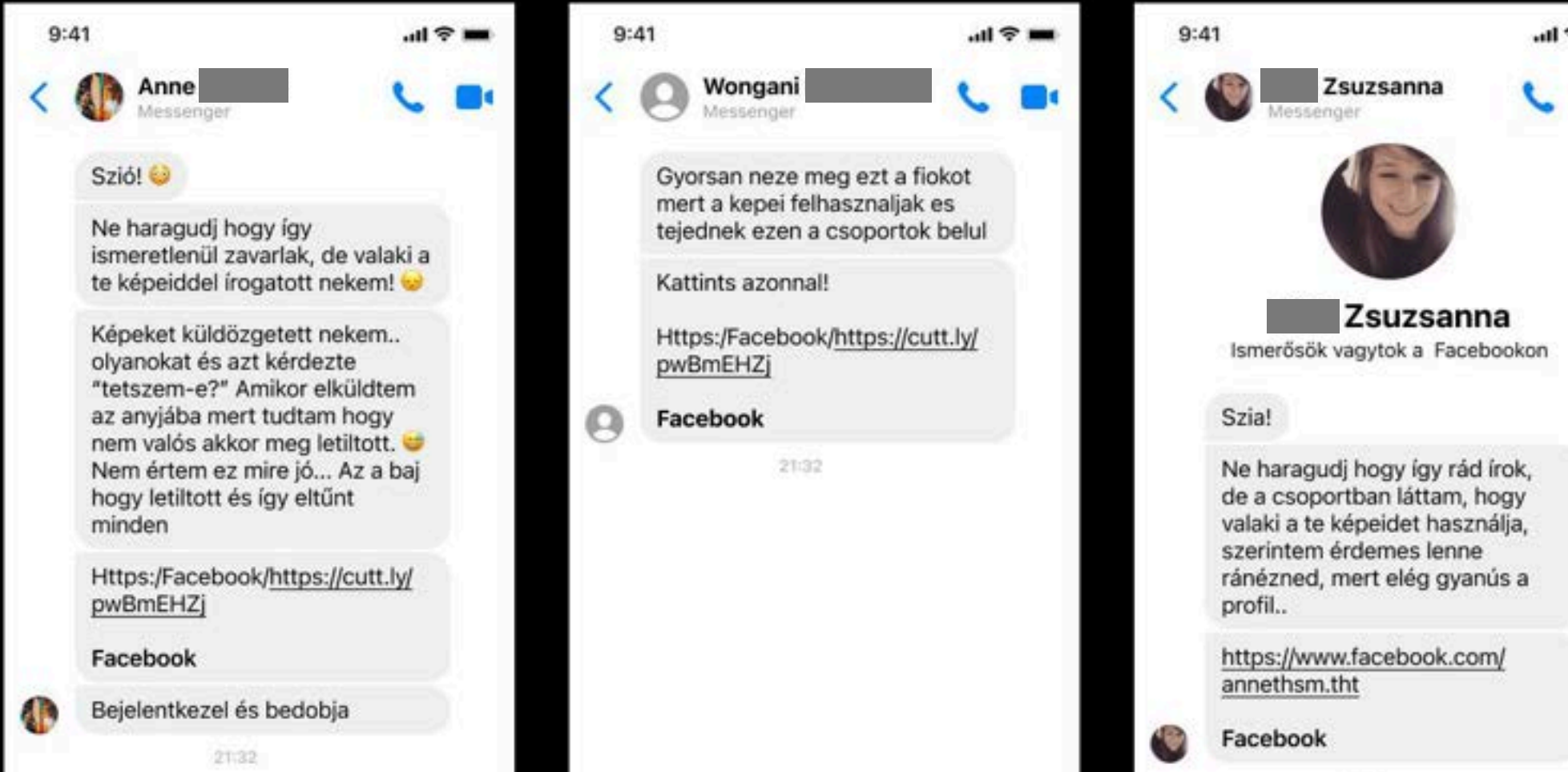
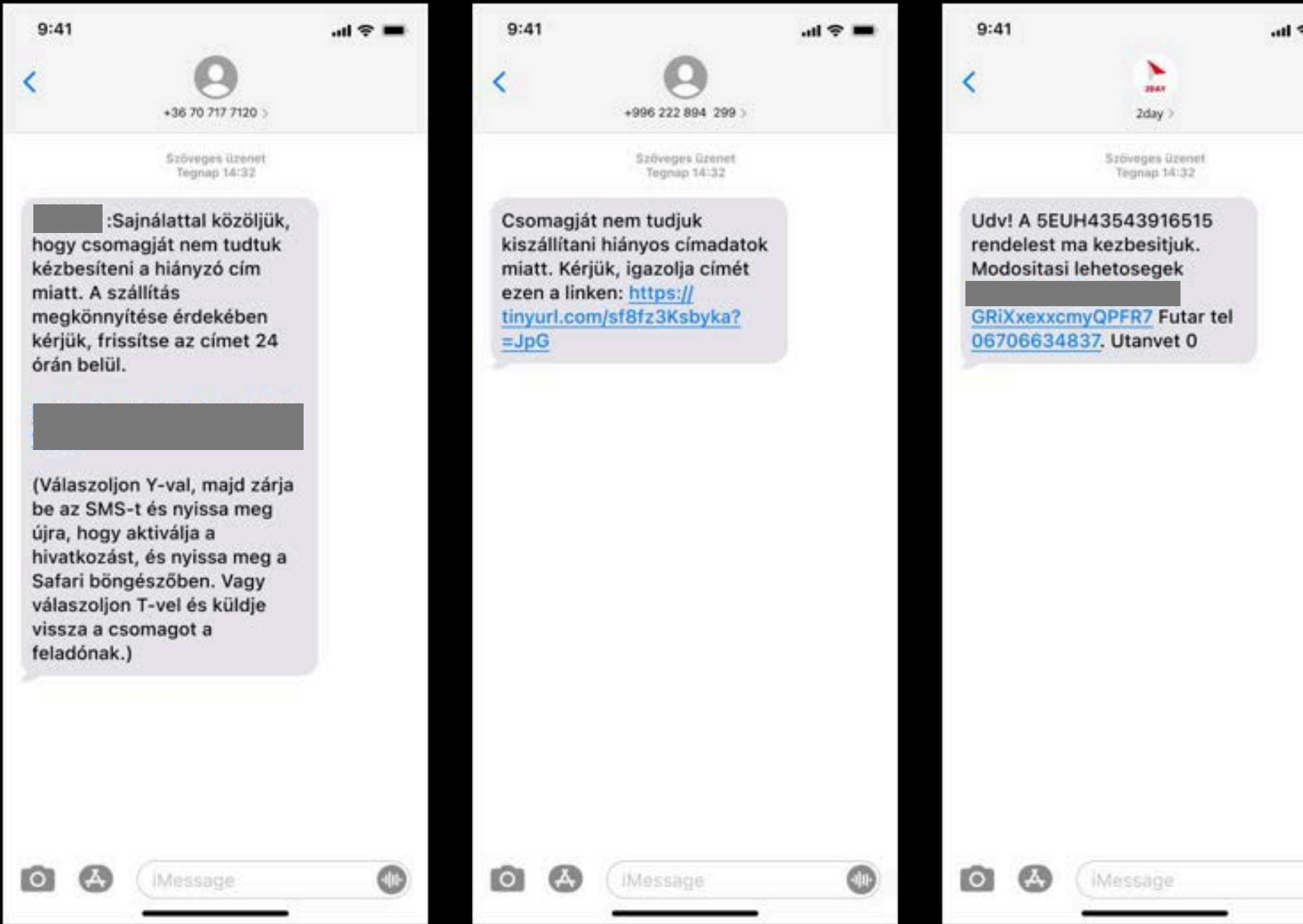
Turányi Tatjana,
Kiberbiztonsági tanácsadó,
Quadron Cybersecurity

A Mastercard felmérése szerint az emberek egyharmada nem tudja megkülönböztetni a valódi és a csalási szándékkal küldött üzeneteket.

A Mastercard felmérése⁵ során végzett gyakorlati feladatok rámutattak, hogy a felhasználók körülbelül egyharmada nem tudta megkülönböztetni a valós és a csalási célú üzeneteket, egyes scenáriókban pedig a résztvevők közel fele hibázott. Bár a 18–29 éves korosztály önbevallás alapján a legmagasabb szintű digitális biztonsági ismeretekkel rendelkezik, a 10 kérdésből álló elméleti tesztben mégis ők teljesítettek a leggyengébben a többi korcsoporthoz képest.

“Azt tapasztalom, hogy egyre több ember esik áldozatul, még olyanok is, akik rendelkeznek tapasztalattal ezen a téren.”

Anonim szakértő



01.D.2

Vállalatokat érintő kihívások



01.D.2.1

Információ- megosztás



A kiberbűnözéssel szembeni hatékony küzdelemhez elengedhetetlen, hogy a védekező oldal ágazatközi és határokon átnyúló kezdeményezéseken keresztül fogjon össze.

A **tudás és az információ** megosztása nemcsak a fogyasztók, illetve a szolgáltató és a felhasználó között játszik jelentős szerepet, hanem a különböző ágazatok között is.

Azzal, hogy a különböző piaci szereplők felismerik a nagyobb jó érdekében való együttműködés értékét, elősegítik az eredményesebb védekezést is, mivel a **kollektív fellépés hatékonyabb az ökoszisztéma szereplőinek védelmére.**

Külföldön és Magyarországon is elindultak már erre irányuló kezdeményezések, de minél többet építünk fel, bővítünk és fejlesztünk, annál sikeresebbek lehetünk a védekezésben.

"Ebben az ágazatban az információmegosztás különböző fórumokon keresztül az egyik legfontosabb módja annak, hogy az emberek a lehető leggyorsabban értesüljenek. Ezeknek a fórumoknak kötelezővé kellene válniuk a kritikus ágazatokban."

dr. Palicz Tamás,
Stratégiai igazgatóhelyettes,
Semmelweis Egyetem

"A kiberbűnözés túlmutat az országok fizikai határain ezért fontos a határokon átnyúló együttműködés és adatmegosztás."

Amtmann Zénó András,
Osztályvezető, OTP Bank Nyrt.,
Vizsgálati Osztály

Példát kell vennünk a sikeres nemzetközi programokról, és meg kell erősítenünk a Magyarországon már aktív kezdeményezéseket.



A CCB negyedévente megrendezésre kerülő **Connect&Share** konferenciájával facilitálja a belga piac információcseréjét is.

Connect & Share konferencia

- A Connect&Share egy negyedévente megrendezésre kerülő konferencia.
- Minden megrendezett konferencia után készül egy jelentés, ami a kiberbiztonsági gyakorlatok javítására vonatkozó legfontosabb meglátásokat és ajánlásokat emeli ki.
A jelentés felvázolja a **jelenlegi kiberfenyegetettséget kiemelve a jelentős sebezhetőségeket és a megfigyelt tendenciákat.**
- Emellett részletezi a CCB stratégiáit a **nemzeti kiberbiztonsági ellenállóképesség fokozására és a kockázatok mérséklésére.**
- A CCB-konferenciák előadói jellemzően **politikai döntéshozók, kiberbiztonsági szakértők és iparági vezetők.**



A **KiberPajzs** kezdeményezés többek között a **kereskedelmi szektorban** is aktív **ahol a piaci szereplők közötti együttműködés ösztönzésére törekszik.**

"A Kiberpajzs együttműködés és a Nemzeti Kibervédelmi Intézet is folyamatosan frissíti a tartalmait a weboldalukon, valamint folyamatosan azon dolgozunk, hogy a lehető legtöbb csatornán eljuttassuk a kiberbiztonsággal kapcsolatos legfrissebb üzenetet a lakosság felé."

Marsi Tamás,
Igazgatóhelyettes, *NBSZ NKI*



A külföldi kezdeményezések inspirációként tudnak szolgálni Magyarországon már létező kezdeményezések tovább fejlesztésére



A CCB-hez hasonlóan a **Global Cyber Alliance (GCA)**¹³ is a megkérdezett szakértők által kiemelt külföldi jógyakorlat.

A GCA egy nemzetközi nonprofit szervezet, amely **közösségekkel együttműködve dolgozik az internet javításán**, és segít az embereknek és a szervezeteknek abban, hogy biztonságosabbá tegyék az online tevékenységüket. Ezt három módon érik el: a **végfelhasználói közösségekkel együttműködve** olyan kiberbiztonsági megoldásokat alkalmaznak, amelyek megfelelnek az igényeiknek; **bevonják az infrastruktúra tulajdonosait és üzemeltetőit** a legjobb gyakorlatok azonosításába és továbbfejlesztésébe, hogy mindenki számára javítsák a kiberbiztonságot; és **ösztönzik az ökoszisztéma elkötelezettségét** a kiberbiztonsággal kapcsolatos kollektív fellépés érdekében.

A globális szintű együttműködés facilitálása mellett a GCA olyan **ingyenes eszközöket és forrásokat is biztosít**, amelyek segíthetnek a szervezeteknek és magánszemélyeknek a kiberkockázatok csökkentésére irányuló intézkedések meghozatalában.

A GCA globális partnerei közé tartoznak:



Craig Newmark Philanthropies



01.D.2.2

Technológia

A védelem növelése érdekében a vállalatok gyakran alkalmaznak összetett védelmi rendszereket, amelyek összezavarják a felhasználókat, és az árnyék-IT terjedéséhez vezetnek.

Ahogy az adatok egyre nagyobb értéket képviselnek és a rendszerek egyre összetettebbé válnak több beszállító bevonásával, úgy nő az adatmennyiség is, amelyet védeni kell. Azonban a túlzottan bonyolult biztonsági intézkedések megkönnyíthetik a támadók számára az emberi hibák kihasználását. A megoldás az egyszerű, intuitív, mégis hatékony védelmi rendszerek tervezésében rejlik.

\$258 k

Egy túl komplex védelmi rendszer az adatlopás okozta átlag veszteséget 258.000 USD-vel emelheti.⁹

\$2.9 m -
\$3.3 m

Az 500 fő alatti szervezetek jelentései szerint egy adatlopás átlag vesztesége 2.9 millióról 3.3 millióra (USD) emelkedett – ami 13%-os emelkedést jelent.¹⁰

FORRÁS: ⁹IBM (2024) COST OF DATA BREACH REPORT, ¹⁰IBM (2023) COST OF DATA BREACH REPORT

A szakértői interjúk szerint a vállalatok **nem feltétlenül vannak tisztában az ellenük elkövetett kiberincidensek** teljes számával. Ez a tendencia azt jelzi, hogy elsősorban reaktív, nem pedig proaktív kiberbiztonsági intézkedéseket alkalmaznak, ami magasabb költségekhez vezethet.

ÁRNYÉKADAT

Az árnyékadat olyan **ellenőrizetlen, nem kezelt adatok összessége**, amelyek a szervezet hivatalos adatkezelési folyamatain kívül esnek. Gyakran tartalmaznak érzékeny információkat, és biztonsági kockázatot jelentenek az IT- és biztonsági csapatok felügyeletének hiánya miatt. Ilyenek lehetnek **pl. a helyben tárolt érzékeny dokumentum-másolatok vagy régi biztonsági mentések**.

„Csak azok vásárolnak kibervédelmi termékeket, akiket már megtámadtak, vagy akiknek a versenytársait már érte támadás.”

Anonim szakértő

KÖZÖSSÉGI MÉDIA CSAPATOK

Számos vállalat tiltja a közösségi média alkalmazások használatát a munkahelyi mobilokon, figyelmen kívül hagyva, hogy bizonyos munkavállalóknak – például a közösségi média csapat tagjainak – szükségük van ezekre a munkavégzéshez. Ez gyakran ahhoz vezet, hogy a csapat tagjai saját eszközeiket használják a vállalat közösségi média platformjainak monitorozásához, ami nem nyújt biztonságos hozzáférést.

“Amellett, hogy cégek nem osztják meg az információt még rosszabb, hogy nagyon sok támadás van amiről maguk sem tudnak.”

Anonim szakértő



01.D.2.3

Oktatás



Az edukáció növelheti a tudatosságot, de fontos, hogy mindezt empátiával tegyük.

A felhasználók oktatása és tudatosítása alapvető fontosságú, **ebben pedig a szolgáltatóknak kulcsszerepet kell vállalniuk.** A megvalósítás módja azonban még ennél is fontosabb. A végfelhasználók oktatása során **kerülnünk kell az olyan kommunikációt, amely az áldozatot hibáztatja az elszenvedett támadásért.** Az ilyen hozzáállás kontraproduktív lehet: erősíti a szégyenérzetet, ami miatt kevesebben mernek segítséget kérni és bejelenteni az eseteket. Ha a szolgáltatók hatékonyan szeretnék edukálni a felhasználókat, olyan megközelítést kell alkalmazniuk, amely **gyakorlati eszközöket ad a felhasználók kezébe.**



Az Áldozatsegítő Központok azzal a céllal jöttek létre, hogy az áldozatot – a szükségletének megfelelő módon és mértékben – INGYEN hozzásegítsék alapvető jogai érvényesítéséhez, tanácsadással, információval és érzelmi támasz nyújtásával.

Az Áldozatsegítő Központ ennek érdekében:

- tájékoztatást,
- jogi tanácsot,
- érzelmi segítséget nyújt.

A magyar piacon a vállalatok reaktívan járnak el és csak az éppen felmerülő problémákat kezelik, ahelyett, hogy megelőző intézkedéseket tennének. Ez hosszú távon magasabb költségekhez vezethet.

A kiberbiztonsági szakértők számos módszert javasoltak a szervezeten belüli alkalmazottak oktatására. Leggyakrabban az e-learning modulok és az erre épülő felmérők, valamint a szimulációk kerültek említésre. Felmerült az is, hogy azokat az alkalmazottakat, akik nem teljesítik a követelményeket kötelezhetik további oktatási anyagok elvégzésére.

„Inkább az oktatással, mint a technológiával tudjuk felkészíteni a vállalatokat a támadásokra, hiszen ez segít a szűrésben és a védelemben is. Nem nem elég, ha van egy jó technológia, hiszen azt használni is kell, valamint szabályokkal és oktatással kell rendelkezni hozzá.”

Anonim szakértő

“Komoly szégyenérzet van a sértettekben, amik leküzdésében bizonyos kampányok kommunikációja nem segít, sőt csak növeli azt emiatt kevésbé jelentik az ügyet a rendőrségen.”

Anonim szakértő

„Egy előre gondolkodó vezetőnek mindenképpen meg kell tennie az ilyen kiadásokat, mert ez így is sokkal kevesebb, mintha támadásra kerül sor, és akkor kell megfizetnie a következményeket.”

Müller Péter,

IT - Fejlesztési és biztonsági vezető,
Ecofamily

Irányelvünk: Egy ellenálló ökoszisztéma

A kiberbiztonság globális kihívás, **amely minden érintett számára megköveteli, hogy megtalálja a képességeinek és körülményeinek leginkább megfelelő felelősségi szintet. Ha biztosítjuk, hogy a végfelhasználóktól kezdve a szolgáltatókig minden szereplő a lehető legjobb tudása szerint védekezzen és megossza ismereteit, jelentősen növelhetjük a védelmi oldal ellenállóképességét.**



02

A digitális ellenállás útjai

Stratégiai irányok
a kibertérben



02.A

TTP

keretrendszer

A fenyegetések sikeres kezeléséhez elengedhetetlen megérteni azok működését.

A támadások alaposabb megértéséhez olyan modelleket és keretrendszereket célszerű alkalmazni, amelyek feltárják 0a támadók viselkedését és a támadási fázisok mögötti indítékokat.

A **TTP keretrendszer** különösen hatékony a támadások egyes lépései közötti eltérések pontos leírására. Ennek kiemelt jelentősége van, mivel a kiberbűnözés elleni hatékony fellépés alapfeltétele a támadások dinamikájának alapos megértése. Ezáltal képesek vagyunk célzottan reagálni a fenyegetésekre.

**TAKTIKÁK:**
A támadó általános stratégiája és céljai, amelyek irányítják a cselekedeteit a támadás különböző szakaszain keresztül.

**TECHNIKÁK:**
A taktikák végrehajtásához használt konkrét módszerek, mint például a beszivárgás vagy egy specifikus technológiai megoldás.

**PROCEDÚRÁK:**
A taktikák és technikák precíz, lépésről lépésre történő végrehajtására.



TTP EGY PÉLDÁN KERESZTÜL

Egy autótolvaj egy drága autót tervez ellopni egy népszerű étterem parkolójából. A gyanú elkerülése érdekében parkolóőrnek adja ki magát ezzel megtévesztve az autótulajdonost, aki átadja a kulcsait.

TAKTIKÁK A tolvaj átfogó stratégiája, hogy észrevétlenül ellopja az autót pszichológiai manipuláció segítségével, erőszak alkalmazása nélkül, beleolvadva a környezetébe, azért, hogy minél jobban elterelje a figyelmet a büntettről.

TECHNIKÁK A tolvaj olyan technológiai eszközöket választ, melyek megakadályozzák az autó nyomon követését.

PROCEDÚRÁK A tolvaj hamis parkolóőr egyenruhát viselve várakozik a parkolóban, magabiztosan megközelíti az autó tulajdonosát és udvariasan megszólítja, hogy elnyerje a bizalmát.



A TTP rendszer minden eleme eltérő ütemben változik. Ez azt jelenti, hogy nem tudunk mindegyikre egyformán reagálni.

A TTP egyes elemei nem ugyanúgy változnak. Például a taktika nagyon ritkán tér el a kezdeti tervtől, míg a procedúrák olyan gyorsan változnak, hogy mind a szolgáltatói, mind a fogyasztói oldalon nehéz vele lépést tartani.

A TTP keresztrendszer minden egyes eleme más-más megoldást igényel.

TAKTIKÁK

LEGLASSABB >

A csalás átfogó stratégiai rétege nagyon ritkán és nagyon lassan változik.

TECHNIKÁK

LASSABB >

A technikák lassabban változnak, mivel a procedúrák naprakészen tartása biztosítja, hogy a technikák se váljanak elavulttá.

PROCEDÚRÁK

LEGGYORSABB >

Ez a leggyorsabban változó tényező. A támadók folyamatosan új szcenáriókat alakítanak ki, reagálva az aktuális eseményekre és trendekre.

A kiberbűnözők jelentős erőforrásokat fordítanak arra, hogy minél gyorsabban reagáljanak a globális eseményekre. Tehát a fogyasztóknak is a lehető leggyorsabban hozzá kell jutni friss információkhoz.

"A támadók renkívül gyorsan képesek reagálni. Amint valamilyen sebezhetőséget találnak, vagy új trendeket észlelnek a hírekben, már másnap tömeges támadásokat építenek ezekre."

Anonim szakértő

CROWDSTRIKE ÁTVERÉSEK

2024 júliusában egy **hibás CrowdStrike frissítés globális zavarokhoz vezetett**, ami a Microsoft Windows eszközök összeomlásához és „kék halálhoz” vezetett. Az „Global Microsoft Meltdown”-nak is nevezett incidens **több kritikus infrastruktúrát is érintett**, mint az egészségügy, légi közlekedés és sürgősségi szolgáltatások.

A kiberbűnözők gyorsan kihasználták a kialakult káoszt: **adathalász támadásokat** és magukat CrowdStrike-nak vagy Microsoft-nak kiadó **hamis támogató oldalakat** indítottak. Ezek az oldalak olyan "hotfix"-eket ajánlottak, amik segítség helyett olyan káros programokat telepítettek az áldozatok eszközeire, mint a HijackLoader. A támadók hamis domaineket regisztráltak, és még kriptopénzfizetést is követeltek az állítólagos sürgős javításokért ezzel kihasználva a kialakult káoszt.

Ez az eset jól szemlélteti, hogy a támadók legnagyobb erőssége a gyors reakcióidő és a globális események folyamatos monitorozása.



A TTP keretrendszer iránytűként szolgálhat, amely segít megtalálni a leghatékonyabb megoldást egy-egy problémára.

Amikor kibervédelemről beszélünk, hajlamosak vagyunk külön kezelni a végfelhasználók oktatását és a vállalat technológiai érettségét. Ez mindaddig hatékony volt, amíg a vállalatok elleni támadások többsége az infrastruktúrát és nem az emberi tényezőt célozta.

Most, hogy a támadók kezében a legnagyobb fegyver maga az adat, nem tudunk ilyen egyértelmű határokat húzni: már nem fedhetünk le mindent a végfelhasználók felelősségével vagy az infrastruktúra védelmével önmagában.

	Procedúrák	Technikák	Taktikák
 felhasználók	Helyzeti tudatosság	Általános biztonsági hozzáállás reflex szinten	Oktatás
 vállalatok	Jobb design a szolgáltatók részéről	A saját felület gyengeségeinek folyamatos monitorozás	Technológiai innovációk, AI alapú monitorozás és felismerés

A hatékony védekezés különböző megoldások ötvözése és azok legoptimálisabb allokációja. Ha képesek vagyunk a TTP keretrendszert felhasználni ezen megoldások azonosítására, és megtalálni a legjobb felhasználási módjukat, azzal az egész ökoszisztéma rezilienciáját növelhetjük.

A következő fejezetben a TTP keretrendszer képezi alapját a megoldási javaslatoknak:

- Helyzeti tudatosság
- Általános biztonságos hozzáállás
- Oktatás
- Technológiai innováció
- Jobb és biztonságosabb design
- Saját kitettségek monitorozása





02.B

Felhasználó szintű megoldások

02.B.1

Információ- megosztás



Ahhoz, hogy a kiberbiztonsági ismeretek organikusan terjedjenek a felhasználók között, fontos, hogy minden kapcsolati hálóban, közösségben legyen legalább egy hozzáértő személy.

"Egy jól képzett felhasználó az utolsó pont a védekezési láncban, és láthatjuk, hogy a jobb digitális készségekkel rendelkező felhasználó tudatosabb."

Koczka Ferenc,
Informatikai Igazgató,
Eszterházy Károly Egyetem

"Biztonságtudatosság szempontjából fontos az informatikai ismeret, felkészültség és hogy mennyire játszik szerepet az illető életében az online tér, épp ezért nem lehet eléggé hangsúlyozni az információmegosztás szerepét."

Kalcsó Gyula Péter,
Humán- rendszerbiztonsági szakértő

A **szakértelem szociális hálózatokba való integrálása kulcsfontosságú** a kiberbiztonsági ismeretek végfelhasználókhoz való eljuttatásában. Ha valakinek van **legalább egy hozzáértő ismerőse vagy családtagja**, máris **nagyobb eséllyel kap releváns és közérthető tanácsokat** a biztonságos online viselkedéshez.

Ez a megközelítés természetes kommunikációs csatornákat hoz létre a tudás terjesztésére így növelve a biztonságot egy adott közösségben. Ehhez **szükségesek olyan találkozók és események is, ahol a kiberbiztonság iránt érdeklődők megoszthatják egymással tapasztalataikat és bővíthetik tudásukat**, megfelelő keretek között, szakmai iránymutatással. **Ez a fajta tapasztalatcsere pedig elősegítheti hosszútávon egy általános biztonságos hozzáállás kialakulását.**



Cyber Islands: Magyarország kiberbiztonsági ökoszisztémájának megerősítése kollaboráción, innováción és megosztott erőforrásokon keresztül



A **Cyber Islands** egy olyan **kollaboratív tér**, ami kibervédelmi szakértőknek, vállalatoknak, startupoknak és diákoknak nyújt kapcsolódási pontot.

A **Cyber Islands célja**, hogy **közös tér és erőforrások biztosításával** támogassa az eredményes partnerségek kialakulását és **elősegítse a nemzeti kibervédelmi ökoszisztéma növekedését**.

Támogatók:



Szakmai együttműködések:



A **Cyber Islands célja**, hogy a **kiberbiztonsági közösségen belül a résztvevők széles skáláját támogassa**:

- Kiberbiztonsági Szakértők
- Cégek és Startupok
- Diákok és Fiatal Tehetségek
- Kiberbiztonság Iránt Érdeklődők
- Oktatók és Trénerek
- Befektetők

„A Cyber Islands-et azért hoztuk létre, hogy összefogjuk, inspiráljuk, és egy fizikai helyszínnel támogathassuk azokat a már létező kiberbiztonsági közösségeket, akik jelenleg elszigeteltebben működnek.”

Csertán Ákos,
Alapító,
Cyber Islands

Cyber Islands számos erőforrást es lehetőséget kínál a résztvevőknek:

- Hálózatépítést
- Együttműködési tereket
- Oktatási erőforrásokat
- Közösségi eseményeket
- Hozzáférést az eszközökhöz
- Karrierépítést

„A kiberbiztonság kihívásait csak együttműködéssel lehet hatékonyan kezelni, ezért a Cyber Islands célja, hogy teret adjon a tudásmegosztásnak és a közösség alapú fejlődésnek.”

Illés Gábor,
Alapító,
Cyber Islands

„A magyar kiberbiztonsági innováció és képességfejlesztés közös érdek, ezért tartjuk fontosnak egy olyan közösségi tér létrehozását, ahol a két terület iránt elkötelezett szakmabeliek kötetlenül tudnak találkozni és kapcsolatokat építeni.”

Krasznay Csaba,
Alapító,
Cyber Islands





02.B.2

Technológia

Ha a felületeket úgy tervezzük, hogy a korlátozott ismeretekkel rendelkezőknek is biztonságos felhasználói élményt nyújtsanak, az már egy lépés a megoldás felé.

A „usable security” olyan biztonsági rendszerek, eszközök és protokollok tervezését jelenti, amelyek egyszerűbbé és intuitívabbá teszik a felhasználók számára a használatukat.

A cél, hogy a biztonsági intézkedések ne okozzanak zavart a felhasználók számára és ezáltal nagyobb valószínűséggel kövessék a biztonságos gyakorlatokat és kerüljék a kockázatos viselkedést.

A használhatóság előtérbe helyezése csökkenti a felhasználókat érő kognitív terhet, ezzel egyszerűbbé téve a biztonsági folyamatok kezelését. Ez a megközelítés alkalmazkodik ahhoz, hogy a felhasználók különböző szintű kiberbiztonsági ismeretekkel rendelkezzenek, ezzel pedig fokozza az általános biztonságot.

USABLE SECURITY PÉLDÁK

Biometrikus Azonosítás:

Belépés fiókokba vagy eszközökbe ujjlenyomat, arcfelismerés, vagy hangfelismerés használatával anélkül, hogy jelszavakat kellene megjegyezni.

Két-faktoros Hitelesítés (2FA):

A jelszó megadása után a felhasználók egy SMS vagy email formájában kapott kóddal tudnak belépni, ezzel plusz egy réteg biztonságot szerezve.

Jelszókezelő:

Eszközök, amik elmentik és automatikusan kitöltik a jelszavakat különböző fiókokhoz, ezzel minimalizálva a megjegyzendő jelszavak számát és biztosítva az erős és egyedi jelszavakat minden fiókhoz.

Single Sign-On (SSO):

A felhasználó több szolgáltatóhoz is bejelentkezhet egy hitelesítő adattal, ezzel egyszerűsítve a bejelentkezési folyamatot anélkül, hogy a biztonság rovására menne.

„A fogyasztói döntéshozást elsősorban a kényelem, az ügyfélméltány valamint az adott szolgáltatás költsége befolyásolja, a kiberbiztonság csak kisebb mértékben.”

Anonim szakértő

„Szolgáltatóként a felhasználó és a támadó közötti út megszüntetése az egyik legfontosabb lépés, amit tehetünk.”

Krasznay Csaba,

Egyetemi docens,

Nemzeti Köszolgáltatati Egyetem

02.B.3

Oktatás



A felhasználók oktatásakor a helyzeti tudatosságra érdemes fókuszálni, valamint annak a megértésére, hogy a globális trendek hogyan befolyásolják a kibereseményeket, ezzel felkészítve a felhasználókat az adaptív és proaktív védekezésre.

A hagyományos végfelhasználói oktatás gyakran nem képes lépést tartani a támadási módszerek gyors fejlődésével. A kiberincidensek dinamikáját a globális események, a technológiai fejlődés és a támadók változó stratégiái alakítják. **Merev gyakorlatok tanítása helyett rugalmas szemléletre van szükség, amely felkészíti a felhasználókat az új fenyegetések felismerésére és kezelésére.**

A helyzeti tudatosságot középpontba helyező megközelítés segíti a felhasználókat a fenyegetések felismerésében és a kontextus megértésében. **Lényeges, hogy tisztában legyenek azzal, hogyan befolyásolják a globális trendek, geopolitikai feszültségek, gazdasági változások és technológiai újítások a kibervédelmi incidensek alakulását.**

A helyzeti tudatosság nemcsak a gyakori támadási jelek felismerésére összpontosít, hanem a támadást megelőző alapvető mintákra és jelzésekre is.

Példák a helyzeti tudatosság fejlesztésére

Trendek ismertetése: a legújabb globális kiberfenyegetésekről és támadási trendekről szóló hírek megosztása, hogy a felhasználók naprakészlegyenek.

Szenáriós képzés: interaktív szenáriók, melyek segítenek a felhasználóknak felismerni az adathalászatot és egyéb gyakori támadásokat, valamint megtanulják, hogyan érdemes ezekre reagálniuk.

Mintázat felismerés: megtanítja a felhasználóknak az alapvető támadási módszereket és segít felismerni a mintázatokat (pl.: social engineering),

Tudásmegosztás: workshopok szervezése felhasználók részére, ahol megoszthatják tapasztalataikat vagy biztonsági tippjeiket, ezzel növelve a tudatosságot.

Kontextuális kockázati workshopok: felhasználók oktatása arról, hogy a fenyegetések hogyan illeszkednek a globális trendekbe vagy szervezeti rizikókba.

Felhasználóként is sokat tehetünk saját kiberbiztonságunkért. Mindenkinek ki kell alakítania egy alapvető kiberhigiénias képességet, amelyeknek reflexnek kell lenniük. Ha hazamegyünk, kezet mossunk. Ha pedig az internetet használjuk, és szembe jön valami, ami túl szép, ahhoz, hogy igaz legyen, akkor azonnal gyanakonunk kell, hogy az valószínűleg nem az.

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI





02.C

Vállalat szintű megoldások

02.C.1

Információ- megosztás



A szolgáltatók számára egyre sürgetőbb, hogy lépéseket tegyenek, mivel a támadások közvetlenül érinthetik üzleti tevékenységüket.

94% 12.6%

A megkérdezettek (USA) 94%-a egyetért abban, hogy a cégeknek felelősséget kell vállalniuk az adataik védelméért.

A jogszabályok figyelmen kívül hagyása 12.6%-kal növeli a szervezetek számára az adatbiztonság megsértésének költségeit.¹⁰

43%

Az adatvédelmi incidensek áldozatainak 43%-a nem lép többé kapcsolatba az érintett szolgáltatóval.¹¹

„A szolgáltató oldaláról a helyzeti tudatosság segítheti a védekezést, hiszen a támadók is folyamatosan monitorozzák a szolgáltatók viselkedését.”

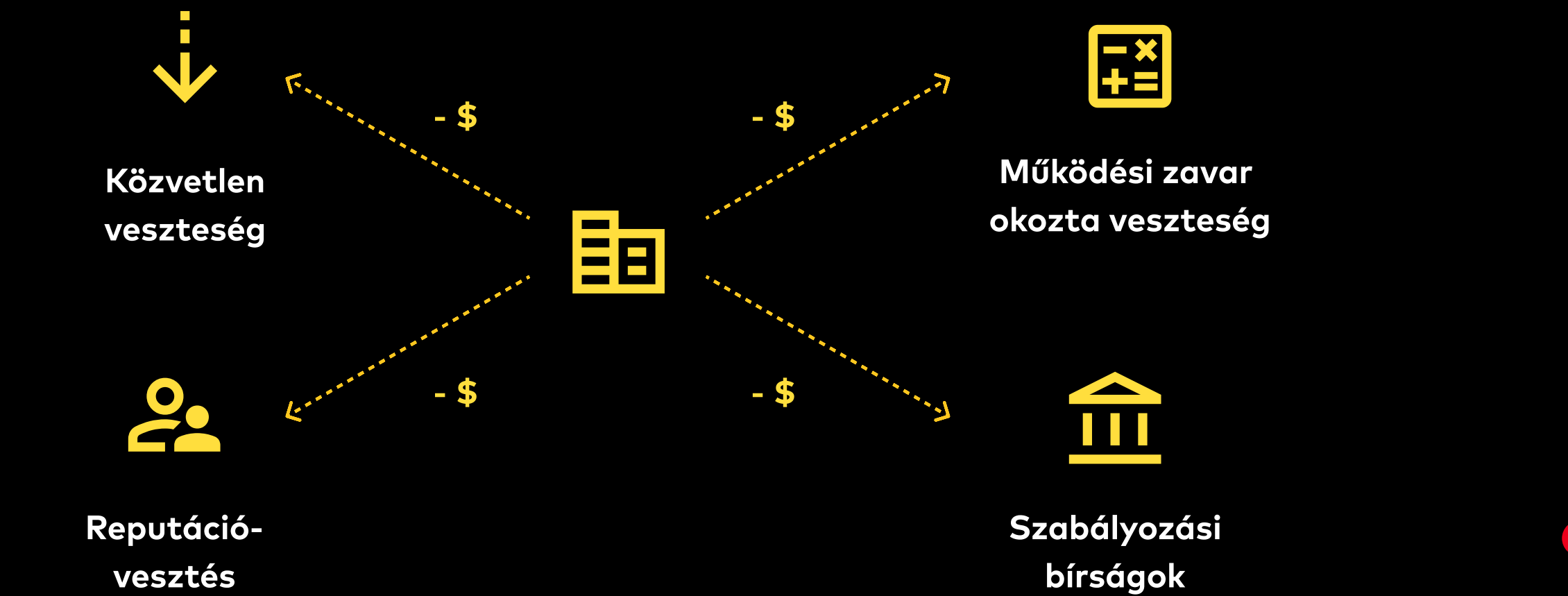
Anonim szakértő

FORRÁS: ¹¹TELESIGN (2024): STATE OF FRAUD, ¹⁰ IBM (2023): COST OF DATA BREACH

A fogyasztók és a hatóságok egyre nagyobb elvárásokat támasztanak a szolgáltatókkal szemben. A hamarosan megjelenő jogszabályok, mint például a NIS2 vagy a DORA egyre nagyobb nyomást gyakorolnak majd a piaci szereplőkre, azáltal, hogy a kiberbűnözés költségei többszöröződni fognak. Az ilyen szabályozási keretek szilárd struktúrát kínálnak a CISO-k és kiberbiztonsági szakemberek számára a védelmi stratégia rangsorolásához és üzleti és megfelelési vezetők számára a beruházási igények pontos meghatározásához.

A védekezés elmulasztása nem csupán közvetlen, hanem közvetett veszteséggel is jár majd a szolgáltatóknak. A fogyasztók elvárják, hogy a szolgáltatók védjék adataikat és tranzakcióikat. Ha a szolgáltató ezt elmulasztja, akkor az nemcsak közvetlen veszteséget fog okozni, hanem a reputáció csökkenésén keresztül közvetett veszteséget is.

Tehát a fogyasztók védelme nemcsak kötelezettségként jelenik meg, hanem pénzügyileg is kifizetődőbb.





02.C.2

Technológia

A szolgáltatóknak tisztában kell lenniük saját gyengeségeikkel, azért, hogy megfelelő döntéseket hozhassanak saját védelmük érdekében.

A komplex rendszerektől és ellátási láncoktól való függés egyre nagyobb kitettséget jelent a vállalatok számára, ami közvetlenül a felhasználóikat is érintheti.

A szolgáltató feladata, hogy tisztában legyen ezzel a kitettséggel és monitorozza saját, valamint beszállítójának gyengeségeit, hogy minél hamarabb észleljék a támadásokat, és a lehető leggyorsabban elzárják az utat a támadó és a felhasználó között.

100 nap

Azok a vállalatok, akik használtak AI-t és automatizációt, 100 nappal korábban észlelték és fékeztek meg az adatvédelmi incidenseket.

FORRÁS: IBM (2024): COST OF DATA BREACH

\$6 millió

Azok a vállalatok akik nem használtak AI-t és automatizációt, átlagosan 6 millió dolláros veszteséget szenvedtek, ami 45.6%-kal több, mint azok vesztesége akik használtak.

A rendszerek folyamatos monitorozása megelőzheti a potenciális támadásokat és mérsékelheti az okozott károkat.

63%

Egy 2024-es felmérés szerint a vállalatok 63%-a fektetne be védelmi eszközökbe egy adatvédelmi incidens után. Ez a 2023-as adatokhoz képest 23.5%-os emelkedést jelent.⁹

„Bár folyamatosan monitorozzuk a legújabb trendeket, támadásokat és incidenseket, ezeket érdemes (és sok szereplőnek kötelező is) bejelenteni a Nemzeti Kibervédelmi Intézetnek. Ezek az információk sosem maradnak felhasználatlanul, többek között ezek segítségével erősítjük a kibertér biztonságát a Kiberpajzs együttműködés keretein belül is.”

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI



Mastercard RiskRecon: A RiskRecon célja, hogy segítse a vállalatokat a kiberbiztonsági kockázatok feltárásában és csökkentésében azzal, hogy részletes értékelést nyújt saját és ellátási láncuk biztonsági helyzetéről. AI vezérelt technológiát alkalmazva folyamatosan szkenneli és elemzi a vállalat digitális lábnyomát, kiemelve az esetleges gyengepontokat a rendszerben.

A legtöbb szakértő egyetért abban, hogy a szolgáltatóknak rutinszerűen nyomon kell követniük tevékenységüket, hogy biztosítsák a minél gyorsabb válaszreakciót.

02.C.3

Oktatás



Egy ellenálló kiberbiztonsági ökoszisztéma építéséhez a vállalatok és felhasználók együttműködésére van szükség.

MUNKÁLTATÓI OKTATÁS:

A munkáltatók kulcsszerepet játszanak az ellenálló és együttműködő biztonsági kultúra kialakításában. Ez helyzeti tudatosságot fejlesztő képzésekkel érhető el, amelyek megtanítják a munkavállalókat a fenyegetések felismerésére a kiberbiztonsági környezet összefüggésében.

A csapatok közötti együttműködés, az információmegosztás és külső partnerekkel közös gyakorlatok erősítik a vállalatok védekezési képességét. A képzéseknek túl kell mutatniuk a technikai készségeken, és azonosítási, valamint kockázatfelismerési szemléletet kell előtérbe helyezniük az egységes válaszkészség érdekében

FELHASZNÁLÓK OKTATÁSA:

A végfelhasználóknak tisztában kell lenniük szerepükkel a biztonsági ökoszisztémában. A helyzeti tudatosságot fejlesztő képzések segítenek megérteni a folyamatosan változó fenyegetettségi környezetet, valamint felismerni a kiberbűnözés korai jeleit. **Fontos, hogy megtanulják, miként befolyásolhatják az egyéni tevékenységek – például gyanús e-mailek megnyitása vagy gyenge jelszavak használata – a kollektív biztonságot.** Az együttműködés ösztönzése a felhasználók között, akár vállalaton belül, akár kívül, növeli a tudatosságot és erősíti a közös felelősségérzetet a digitális környezet védelmében.



A KULCS TE VAGY!

A Magyar Nemzeti Bank és a Magyar Bankszövetség által támogatott **AKulcsTeVagy!** kezdeményezés célja a tudatosság növelése és a közvélemény oktatása.

A Mastercard Magyarország "BEYONDBAU EDUCATION" kezdeményezésének célja:

- **Gimnazisták oktatása** saját szerkesztésű oktatási anyagokkal a kiberbiztonságról (és más témákról)
- **Tanárok képzése** a témában
- Oktatási anyagok **ellenőrzése és javítása**

Ez az önkéntesek által vezetett kezdeményezés 2023-ra **1500 diákot** ért el 10 magyar gimnáziumban.

A Kiberpajzs program célja a magyarországi kiberbűnözés elleni hatékony fellépés az ágazati és szektor szinten érintett üzleti- és hatósági szereplők együttműködésének erősítésével, illetve a lakosság pénzügyi és digitális tudatosságának növelése, az áldozattá válás megelőzésének elősegítése széleskörű, összehangolt edukációs kampányok révén.



A Kiberpajzs célja a magyarországi kibervédelmi képességek erősítése **proaktív kommunikációs** kampányokkal, tudásmegosztással és külföldi jó gyakorlatok adaptálásával.

Az **egyszerűsége és elérhetősége**re alapozott megközelítésük segíti a szervezeteket és egyéneket az **emberi hibák kockázatának csökkentésében**. Az ilyen kezdeményezések kulcsfontosságúak egy ellenálló digitális közösség kialakításához és a változó kiberfenyegetésekkel szembeni védelemhez.

A Kiberpajzs átfogó támogatást nyújt a kiberbűnözés elleni küzdelemhez:

- Oktatási kampányokkal
- Partnerségek erősítésével
- Bejelentő csatornákkal
- Biztonsági intézkedésekkel
- Áldozattámogatással

A KiberPajzs folyamatosan figyeli a kibertérben megjelenő új fenyegetéseket, és ezekre gyorsan reagálva edukációs anyagokkal, figyelmeztetésekkel és gyakorlati tanácsokkal segíti a felhasználókat és a vállalatokat.

“A Kiberpajzs egy óriási tudáskészlet is. Az ott helyet foglaló szakértők az ország legjobb szakemberei, akik folyamatosan azon dolgoznak, hogy hatékonyan előzzük meg a régi és a legújabb támadásokat, így óvjuk meg a lakosság megtakarításait. Kiberpajzs példát mutat együttműködésből egy társadalmilag is fontos cél elérése érdekében.”

Marsi Tamás,
Igazgatóhelyettes,
NBSZ NKI

„A digitális evolúció erősödésével a sokarcú online világban a bűnözők is megjelentek. A KiberPajzs célja, hogy több ezer szakértő tudását összefogva elősegítse, hogy 10 millió magyar ember tudatossága jelentse a masszív védelmet. Lehetetlen mindenkihez bekapogtatni! Mindannyiunknak ajtót kell nyitnunk a tudásnak – kiélesíteni a szemünket, a fülünket, a figyelmünket!”
www.kiberpajzs.hu

Sütő Ágnes,
Magyar Bankszövetség főtitkárhelyettes,
KiberPajzs társ-projektgazda



Függelék



Szójegyzék

Név	Rövidítés	Definíció
Centre for Cybersecurity Belgium	CCB	A belgiumi nemzeti kiberbiztonsági hatóság, ők felelnek a belga kiberbiztonsági strratégia felügyeléséért, koordinálásáért és monitorozásáért
Digital Operational Resilience Act	DORA	Uniós szabályozás melynek célja a pénzügyi szervezetek IT biztonságának megerősítése, biztosítva hogy ellenálljanak a súlyos támadásoknak és helyreálljanak azokból
Network and Information Security Directive	NIS2	EU-s szabályozás, melynek célja a hálózati és információs rendszerek biztonságának növelésével a kiberbiztonság magas szintjének elérése a tagállamok körében
Payment Services Directive 3	PSD3	A pénzforgalmi szolgáltatásokat szabályozó uniós irányelv legújabb változata, amely a pénzügyi szektor biztonságának, hatékonyságának és innovációjának javítására összpontosít.
Tactics, Techniques & Procedures	TTP	Kiberbiztonságban használt keretrendszer a támadók viselkedésének leírására. A taktikák magas szintű stratégiák, a technikák a módszerek ezeknek a stratégiáknak a véghezviteléhez a procedúrák pedig a konkrét tevékenységek
Opportunity		A lehetőség a támadási célpontokat jelenti
Hook		A hook az indított támadásokat jelenti
Jutalom		A jutalom a sikeresen összegyűjtött adatokat jelenti
Végjáték		A végjáték a sikeresen végrehajtott támadásokat jelenti

Elkövetők jegyzéke

Név	Forrás
Black Hat	Önállóan operáló egyéni vagy kisebb elkövetői csoport. Főként a pénzügyi és személyes haszonszerzés motiválja őket, és viszonylag kifinomult támadásokat alkalmazva állami és magánszervezeteket céloznak. Limitált erőforrásokkal de fejlett készségekkel rendelkeznek. Ez az elkövető csoport tartalmaz csalókat is.
Cyber Warrior	Egy elkövetői csoport akik közvetve egy állam által szponzorálva vagy kontrollálva lehetnek. A motivációik politikaiak és/vagy ideológiaiak, és kifinomult támadásokkal vagy titkos kiberkémkedéssel nemzetállamokat céloznak (bizonyos esetekben azt is amelyikből működnek). Bőséges erőforrásokra és fejlett készségekre támaszkodhat. Ez az elkövetői csoport típus tartalmaz kiber-zsoldos csoportokat. Gyakran az Advanced Persistent Threat (APT) kategóriába esnek.
Hacktivist	Egyének vagy elkövetői csoport amely kapcsolatban állhat egy állammal, de főleg egyénileg operálnak. A motivációik ideológiaiak és megzavaró támadásokkal az állami vagy privát szektort célozzák. Limitált erőforrásokkal és közepes képességekkel rendelkeznek.
Szervezett bűnözés	Egy elkövetői csoport amely kapcsolatban állhat egy állammal, de főleg egyénileg működnek fizikai bűnözői csoportokhoz hasonló hierarchiábn és struktúrában. A motivációik főleg pénzügyiek de bizonyos esetekben lehetnek ideológiaiak, kifinomult támadásokkal céloznak állami és magánszervezeteket is. Gyakran az Advanced Persistent Threat (APT) kategóriába esnek.
Államilag Támogatot	Egy közvetlenül az állam által szponzorált elkövetői csoport, általában az állam kormányzati vagy katonai infrastruktúrájának részeként. A motivációi politikaiak és kifinomult támadásokat és kiberkémkedést alkalmazva más nemzet államokat támadnak Bőséges erőforrásokkal és fejlett készségekkel rendelkeznek. Gyakran az Advanced Persistent Threat (APT) kategóriába esnek.
„Script Kiddie”	Alacsony technológiai fejlettséggel rendelkező egyén, aki kívülről biztosított támadási TTP-ket használ. (taktikák, technikák és procedúrák). A személyes haszonszerzés motiválja őket és állami vagy privátszervezeteket céloznak bomlasztó vagy romboló támadásokkal. Limitált erőforrásokkal és alap képességekkel rendelkeznek. Ez az elkövető típus tartalmazza a kibervándálokat és a „script kiddie”-ket.



Források

Név	Forrás
AKULCSTEVAGY!	https://www.akulcstevagy.hu/
Áldozatsegítő központ	https://vansegitseg.im.gov.hu/
Black Hat Middle East and Africa	https://insights.blackhatmea.com/do-cybercriminals-collaborate-and-build-community/
Bloomberg	https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger
CCB	https://ccb.belgium.be/en
CCB	https://ccb.belgium.be/en/news/ambitions-and-achievements-field-cyber-security-belgium
CCB	https://ccb.belgium.be/en/news/feedback-ccb-connect-share-quarterly-cyber-threat-report-qctr-quarter-q4-2022
DORA	https://www.digital-operational-resilience-act.com/Article_45.html
eSentire	HTTPS://WWW.ESENTIRE.COM/RESOURCES/LIBRARY/2023-OFFICIAL-CYBERCRIME-REPORT
GCA	https://globalcyberalliance.org/
IBM	IBM cost of a data breach report 2023
IBM	IBM cost of a data breach report 2024
Kiberpajzs	https://kiberpajzs.hu/



Források

Név	Forrás
Magyar Nemzeti Bank	https://statisztika.mnb.hu/publikacios-temak/penzforgalmi-adatok/penzforgalmi-adatkozlesek/tajekoztato---penzforgalom
Mastercard	https://www.mastercard.hu/hu-hu/mastercard-uzleti-megoldasok/bankok-es-penzugyi-szolgaltatok/digitalis-fizetesi-index-2023.html
Mastercard	Age of Cybercrime report
Mastercard	Digital security awareness survey among the Hungarian population
MÁTRIX projekt	https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt
NIS2	https://www.nis-2-directive.com/NIS_2_Directive_Article_29.html
SecurityScorecard & Cyentia	https://securityscorecard.com/wp-content/uploads/2024/01/Research-Close-Encounters-Of-The-Third-And-Fourth-Party-Kind.pdf
STATIONX	https://www.stationx.net/data-breach-statistics
Telesign	https://www.telesign.com/whitepaper/2024-state-of-fraud
Statista: Global cybercrime estimated cost 2029	https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

