

Kicsik vagyunk – mégis célpont

Fenyegetések, szabályozás és az a néhány lépés, amivel egy kis- és középvállalkozás a legtöbbet nyeri

Trendig Plus - Kiberbiztonság

Interreg
AUSTRIA-HUNGARY



Co-funded by
the European Union

Trendig Plus

AN INTEGRATED BORDER REGION



MENETREND

120 perc, hét blokk, egy közös gyakorlat

Idő	Blokk	Perc
0:00	Kezdés – károk itthon és a világban, valós esetek (JLR, lengyel energiahálózat)	18
0:18	Fenyegetéstérkép, IoT/OT + közös adathalász-levél elemzés	24
0:42	Szabályozás és szabványok – GDPR, NIS2, CRA, ISO 27001, AI Act	18
1:00	Szünet	10
1:10	10 lépés, amivel jelentősen nő a biztonság	20
1:30	AI és a jövő – AI-támadások, shadow AI, kvantumveszély és PQC	13
1:43	Emberi tényező – tudatosság, jelentési kultúra, otthoni munka	8
1:51	Q&A + egyoldalas önellenőrző lista	9

A LEGGYAKORIBB TÉVHIT

„Minket ki akarna feltörni? Nincs nálunk semmi érdekes.”

A támadók nem válogatnak, hanem automatizáltan pásztáznak. Aki nyitva hagyja az ajtót, az felkerül a listára – mérettől függetlenül.

VILÁGSZINTEN

Ha a kiberbűnözés ország lenne, a világ 3. legnagyobb gazdasága lenne

10 500 mrd \$

becsült éves globális kár
2025-ben, 2031-re 12 200
mrd \$

4,44 M \$

egy adatvédelmi incidens
átlagos költsége; felismerés
és megfékezés: 241 nap

20,9 mrd \$

csak az FBI-nak bejelentett
kár 2025-ben – egy év alatt
+26%

60%

az EU-ban vizsgált
behatolások ennyi része
adathalászattal kezdődött

Másodpercenként kb. **333 000 dollár** kár – amíg ezt a mondatot kimondom, több mint egymillió.

MIÉRT CÉLPONT A KKV IS?

A számok magyar cégekről szólnak

minden 5.

magyar vállalatot ért
zsarolóvírus-támadás 2023-
ban

32%

ezeknél az adathalász üzenet
volt a belépési pont

46%

a cégeknek csak ennyi része
készít biztonsági mentést

~2×

nőtt 2025-ben a cégeket ért
utalási csalások kára; átlag >5
M Ft/cég

Olcsó célpont

Automatizált támadások, kevés védelem, nincs
saját biztonsági csapat.

Kapu a nagyokhoz

A beszállító hozzáférése és levelezése
ugródeszka a megrendelő felé.

Van pénz és adat

Utalások, ügyféladatok, bérlisták – mind
eladható vagy zsarolható.

Adatlopás titkosítás nélkül: 8,5 TB a darkweben

A **World Leaks** zsarolócsoporthoz egy nagy magyar médiacég rendszeréből **csaknem 15 millió fájlt** szerzett meg, majd – mivel nem kapott választ – közzétette a darkweben.

- Kikerült: bérjegyzékek, szerződések, kimutatások, belső üzenetek
- Érintett lehet: előfizetők neve, e-mail-címe, lakcíme, telefonszáma
- A cég hatósági bejelentést tett; a NAIH hivatalból vizsgálatot indított

TANULSÁG

Ma már nem kell titkosítani a zsaroláshoz – **elég ellopni.**

A mentés a leállítás ellen véd, az adatszivárgás ellen nem. Ez ellen a hozzáférések szűkítése, a naplózás és a gyors észlelés véd.

Egy hiányzó kétfaktoros belépés ára: 110 millió Ft

2022-ben hekkertámadás érte a közoktatási **KRÉTA** rendszer fejlesztőjét. A NAIH vizsgálata után **110 millió Ft** adatvédelmi bírságot szabott ki.

- A hatóság szerint az incidens megelőzhető lett volna, ha a belső rendszerekhez **kétfaktoros hitelesítés** kell
- Az MFA-t csak az incidens nyilvánosságra kerülése után vezették be
- Az érintett iskolákat sem értesítették késedelem nélkül

TANULSÁG

Az MFA a **legolcsóbb biztosítás**, amit ma köthetünk.

A bírságot nem csak a támadás, hanem a hiányzó alapvédelem és a késlekedő értesítés is növelte.

„Megváltozott a bankszámlaszámunk”

~1,2 mrd Ft

Számlaváltós csalóhálózat (BRFK)

43 sikeres csalás és 51 kísérlet. A partner nevében jelezték, hogy új a bankszámlaszám. Sértettek: kórház, színház, múzeum, önkormányzat, sportegyesület, közmű.

~47 M Ft

„Kiberbiztonsági munkatárs” hív (2026)

A csaló gyanús mozgásra hivatkozva „víruskeresőt” telepítettett, majd a beszélgetés alatt négy részletben leemelte a pénzt.

TANULSÁG

Nem a technika bukik el, hanem a **folyamat**.

Számlaszám-változást csak ismert számon visszahívva fogadunk el. Telefonra soha nem telepítünk semmit.

Egy támadás, ami egy teljes beszállítói láncot leállított

~6 hét

állt a gyártás a JLR brit és
külföldi gyáraiban

1,9 mrd £

becsült kár a brit
gazdaságnak – az eddigi
legdrágább kiberesemény ott

5 000+

érintett szervezet, főként
beszállítók a láncban

1,5 mrd £

állami hitelgarancia, hogy a
beszállítók ne menjenek
csődbe

TANULSÁG

Nem kell, hogy minket támadjanak meg: elég, ha a **legnagyobb vevőnk** áll le. Az üzletmenet-folytonossági tervben a vevő és a beszállító kiesése is szerepeljen.

Összehangolt támadás az energiarendszer ellen

Célpontok

- **30+ szél- és naperőmű** alállomása
- Kapcsolt erőmű, amely **közel félmillió** fogyasztó hőellátását adja
- Egy gyártó magáncég

Így jutottak be

- Internetről elérhető VPN, **MFA nélkül**
- Vezérlő **gyári jelszóval**
- Admin jog a tűzfalon → hozzáférés minden hálózati szegmenshez

Amit tettek

- PLC-k leállítva és jelszóval kizárva
- Vezérlő tönkretéve, eszközök gyári állapotra
- Adattörölő kártevő (wiper)

TANULSÁG

Áramkimaradás nem lett, az erőműben a végpontvédelem (EDR) megállította a kártevőt. A betörés módja viszont **bármelyik KKV-nál ismerős**: MFA nélküli VPN és gyári jelszó.

2025 TOVÁBBI ESETEI

A kiskereskedelemtől a sörgyáron át az óvodáig

Egyesült Királyság · 2025. április

Marks & Spencer

~300 M £

várható profitkiesés. Az online rendelés hetekig állt. A támadók egy **külső vállalkozón** keresztül jutottak be.

Japán · 2025. szeptember

Asahi sörgyár

~1,5 M

ügyfél adata érintett. Zsarolóvírus (Qilin), a japán gyárakban leállt a termelés és a rendelésvétel.

London · 2025. szeptember

Kido óvodalánc

8 000+

kisgyermek neve, fényképe és lakcíme kerülhetett a zsarolókhöz. Nincs olyan ágazat, ami „nem érdekes”.

02

Fenyegetésterkép

Hat kockázat, ami egy KKV-nál ténylegesen előfordul, az IoT-eszközök – és egy közös adathalász-levél elemzés

24 perc

Hat kapu, amin a baj bejön

Adathalászat / BEC

Hamis számla, hamis vezető, hamis bank. A leggyakoribb belépési pont.

Zsarolóvírus

Titkosítás és adatlopás együtt: kettős zsarolás, napokig álló működés.

Jelszavak

Egy máshol kiszivárgott, újrahasznált jelszó minden fiókot kinyit.

Beszállítói lánc

Az IT-partner, a könyvelő, a felhő hozzáférése a mi kockázatunk is.

Belső hiba

Rossz címzett, nyilvános link, kidobott papír – szándék nélkül.

Elveszett eszköz

Titkosítatlan laptop vagy pendrive = bejelentendő adatvédelmi incidens.

CEO-csalás – ma már hamis hanggal is

Árulkodó jelek

- **Sürgetés:** „egy órán belül kell”
- **Titoktartás:** „ne szólj senkinek, bizalmas”
- **Elérhetetlenség:** „most nem tudok beszélni”
- **Kivétel a szabály alól:** térjünk el a megszokottól
- **Új vagy külföldi számlaszám**
- Kényes téma: felvásárlás, adóellenőrzés

HANGKLÓNOZÁS, MAGYAR SZÁLLAL

Egy brit energetikai cég vezetőjét „a német anyacég vezérigazgatója” hívta – mesterségesen utánozott hanggal. Sürgős utalást kért egy magyar beszállítónak.

220 000 €

~72 M Ft ment egy magyar számlára, onnan azonnal tovább Mexikóba. A harmadik hívásnál gyanakodott meg.

ZSAROLÓVÍRUS

A titkosítás az utolsó lépés, nem az első

1

Belépés

adathalász levél,
ellopott VPN-jelszó,
frissítetlen rendszer

2

Lappangás

napokig, hetekig
észrevétlenül

3

Terjedés

admin jog, belső
hálózat bejárása

4

Mentések törlése

a hálózaton elérhető
mentés is célpont

5

Adatlopás

a zsarolás második
lába

6

Titkosítás, zsarolás

ekkor vesszük észre

241 nap

átlagos „lappangás”

Ennyi idő telik el átlagosan egy adatvédelmi incidens felismeréséig és megfékezéséig. Minden nap, amivel korábban észleljük, pénzben mérhető megtakarítás – ezért kell naplózás, riasztás és EDR.

CSENDES KOCKÁZATOK

Nem kell hozzá hekker, hogy baj legyen

Kockázat	Valós példa	Ellenszer
Beszállítói lánc	2025 szept.: a Collins Aerospace check-in rendszerét ért zsarolóvírus több európai repülőtéren bénította az utasfelvételt	Beszállítói hozzáférések listája, szerződéses elvárások
Belső hiba	500 ezer Ft NAIH-bírság egy könyvelőnek: ügyféladatos listát „fújt a szél” egy járókelőhöz a kidobott papírral	Iratmegsemmisítő, tiszta asztal szabály
Elveszett eszköz	Elhagyott, adatokkal teli pendrive – az egyik leggyakoribb gondatlansági incidens	Eszköztitkosítás, távoli zárolás
Jelszavak	Máshol kiszivárgott jelszó kipróbálása a céges fiókon (credential stuffing)	Jelszókezelő + MFA

IOT ÉS OT

A hálózat elfelejtett eszközei

+400%

IoT-kártevő támadás egyetlen év alatt (2023)

+387%

az energiaszektorra ért IoT-támadás egy év alatt (2025)

40%

az IoT-támadásoknak gyártó és szállítmányozó cégek ellen

~75%

a kártevőknek 3 családból (Mirai és társai) – gyenge jelszóra építenek

Mi van egy átlagos KKV-nál?

IP-kamera, router, NAS, nyomtató, beléptető, okos fűtés, napelem-inverter, távfelügyelt gyártógép vagy hűtőkamra – sokszor évek óta frissítés és gazda nélkül.

Védekezés

Leltár · gyári jelszó cseréje · firmware-frissítés · **külön hálózati szegmens** · ne legyen közvetlenül az interneten · távoli karbantartás csak MFA-s VPN-en · beszerzéskor: frissítési idő és CE/CRA-megfelelés

Feladó: Kovács Acél Kft. – Pénzügy <penzugy@kovacs-ancel-kft.co>

Válaszcím: kovacs.ancel.finance@gmail.com

Tárgy: SÜRGŐS – bankszámlaszám-változás, 2026/0912 számla

Melléklet: Szamla_2026-0912.pdf.html

Tisztelt Partnerünk!

Bankváltás miatt korábbi számlaszámunk megszűnt. Kérjük, a lejárt 4 860 000 Ft-os számlát MA 14:00-ig az alábbi új számlára utalják, különben a szállítást felfüggesztjük:

LT51 3250 0xxx xxxx xxxx

Az ügyet kérjük bizalmasan kezelni, telefonon jelenleg nem vagyunk elérhetők. Az új adatokat itt erősítheti meg: kovacs-ancel-kft.co/megerosites

Üdvözlettel:

Kovács Péter, pénzügy

GYAKORLAT

Hány árulkodó jelet talál?

Párban, 5 perc. Írják fel, mi gyanús, és mit tennének, ha ez a levél ma reggel az ő pénzügyesükhöz érkezne.

A cég és a levél kitalált – a minta valós esetekből épül.

MEGOLDÁS

Hét jel egyetlen levélben

- 1 Hasonmás domain:** kovacs-acek-kft.co a megszokott .hu helyett
- 2 Eltérő válaszcím:** a válasz egy gmail-fiókba megy
- 3 Sürgetés és fenyegetés:** „MA 14:00-ig”, „felfüggesztjük”
- 4 Számlaszám-változás e-mailben,** ráadásul külföldi (LT) számlára
- 5 Titoktartás + elérhetetlenség:** az ellenőrzést akadályozza
- 6 Dupla kiterjesztés:** a „.pdf.html” valójában weboldal
- 7 „Megerősítő” link:** adatahalász űrlap a hamis domainen



Helyes reakció: nem válaszolunk, nem kattintunk. Visszahívjuk a partnert a **korábbi ismert** számon, és jelentjük a levelet.

03

Szabályozás és szabványok

GDPR, kiberbiztonsági törvény (NIS2), CRA, ISO 27001 és társai – és az AI Act érintőlegesen

18 perc

Hat uniós szabály – melyik érint minket?

Szabály	Kire vonatkozik?	Mit kér röviden?	Mikortól?
GDPR	személyes adatot kezelők	adatbiztonság, 72 órás bejelentés	2018. máj. 25.
NIS2 / Kbtv.	kiemelt ágazat, jellemzően 50+ fő	kockázatkezelés, SZTFH, audit	2025. jan. 1.
CRA	digitális termékek gyártói, forgalmazói	biztonságos tervezés, frissítés, CE	jelentés: 2026. szept. 11. teljes: 2027. dec. 11.
RED	rádiós, netre kötött eszközök	EN 18031: nincs közös gyári jelszó	2025. aug. 1.
DORA	pénzügy és IKT-beszállítói	IKT-kockázat, incidens, tesztelés	2025. jan. 17.
AI Act	AI-t fejlesztők és alkalmazók	tiltások, AI-jártasság	2025–2028

Négy dokumentum, amit egy ellenőrzés elsőként kér

30. cikk

Adatkezelési nyilvántartás

Milyen adatot, miért, mennyi ideig, ki fér hozzá. Táblázat is lehet – de legyen naprakész.

13–14. cikk

Adatkezelési tájékoztató

Ügyfélnek, munkavállalónak, jelöltnek, kamerás megfigyeléshez – közérthetően.

33–34. cikk

72 órás incidensbejelentés

A NAIH felé a tudomásszerzéstől számítva. Minden incidenst belső nyilvántartásba is veszünk.

28. cikk

Adatfeldolgozói szerződés

Könyvelő, bérszámfejtő, IT-partner, felhő, hírlevélküldő – mindegyikkel írásban.

AZ ÓRA ELINDUL AZ ÉSZLELESKOR

Incidens után: ki, kinek, mikor jelent?

0 óra

Észlelés

Rögzítjük az időpontot. Elkezdjük a belső nyilvántartást.

24 óra

NIS2: korai figyelmeztetés

Csak a kiberbiztonsági törvény hatálya alá tartozóknak, az NKI felé.

72 óra

GDPR: NAIH-bejelentés

Ha személyes adat érintett. NIS2-érintetteknel ekkor jön az NKI-bejelentés is.

1 hónap

NIS2: zárójelentés

Ok, hatás, megtett intézkedések.



Magas kockázat esetén az **érintetteket is** késedelem nélkül tájékoztatni kell. Ha a 72 óra nem tartható, a késés okát is meg kell indokolni.

Érintett vagyok – vagy a partnerem?

1. Érintettség

Kiemelt vagy kritikus **ágazat** (pl. energia, közlekedés, egészségügy, gyártás, élelmiszer, digitális szolgáltatás) **és** jellemzően középvállalati méret: 50 fő felett, vagy 10 M € feletti árbevétel és mérlegfőösszeg.

2. Nyilvántartásba vétel

Az **SZTFH**-nál: kapcsolattartó, rendszerek biztonsági osztályba sorolása, kockázatkezelés, vezetői felelősség és képzés.

3. Audit

Kétévente, SZTFH-nál nyilvántartott auditorral. Az első kör határideje **2026. június 30.** volt; új belépőknek a nyilvántartásba vételtől 2 év.



Közvetett érintettség: a NIS2 kötelezi az érintett cégeket a beszállítói lánc biztonságának kezelésére. Kis beszállítóként a követelmények **szerződésben, kérdőívben, auditban** érkeznek hozzánk.

Mostantól a termék is felel a biztonságért

2024. dec. 10.

Hatályba lépett, átmeneti időszak

2026. jún. 11.

Tanúsító szervezetek kijelölése

2026. szept. 11.

Már él: kihasznált sérülékenységi és súlyos incidens jelentése (24 ó / 72 ó / 14 nap)

2027. dec. 11.

Teljes alkalmazás: CE-jelölés nélkül nincs piac

Ha terméket gyártunk

Biztonságos alapbeállítás (nincs gyári jelszó), sérülékenységszempontok kezelése a teljes támogatási időben, ingyenes biztonsági frissítés, szoftverjegyzék (SBOM), jelentés az ENISA platformján.

Ha terméket vásárolunk

Kérdezzük meg: meddig kap frissítést? Van-e CE-megfelelőség és sérülékenységi-bejelentési csatorna? Bíróság a gyártónak: akár 15 M € vagy az árbevétele 2,5%-a.

SZABVÁNYOK

A megfelelés közös nyelve

ISO/IEC 27001:2022

Információbiztonsági irányítási rendszer, tanúsítható. 93 kontroll 4 témában: szervezeti, emberi, fizikai, technológiai.

IEC 62443

Ipari automatizálás és OT: zónák és csatornák, követelmények gyártónak, integrátornak, üzemeltetőnek.

ETSI EN 303 645 · EN 18031

Fogyasztói és rádiós IoT: egyedi jelszó, frissíthetőség, sérülékenységi-bejelentési csatorna.

ISO/SAE 21434 · R155

Járműipar: kiberbiztonság a teljes életcikluson át – a beszállítóknak is kötelező elvárás.

CIS Controls – IG1

56 alapintézkedés kis szervezeteknek: a legjobb ingyenes kiindulópont.

Hol kezdjük?

CIS IG1 vagy a mai 10 lépés → ha a vevő kéri, ISO 27001 → ágazati szabvány.

Ami egy KKV-t ma ténylegesen érint

Mikortól	Mi
2025. febr. 2.	Tiltott gyakorlatok; AI-jártasság támogatása a munkatársaknál
2026. aug. 2.	Átláthatóság: az ember tudja, ha géppel beszél
2027. dec. 2.	Magas kockázatú rendszerek (pl. HR-szűrés)
2028. aug. 2.	Termékbe épített magas kockázatú AI

A magas kockázatú határidőket a 2026 nyarán elfogadott Digital Omnibus tolta ki.

BIZTONSÁGI OLDALRÓL

- Ügyfél- és személyes adatot, üzleti titkot ne másoljunk nyilvános chatbotba
- Egyoldalas AI-házirend: mire, melyik eszközzel szabad
- Céges fiók, kikapcsolt tanítás az adatainkon
- Deepfake hang és videó: a hívó személye nem bizonyíték

Szünet – 10 perc

Házi feladat a kávé mellé: nézze meg a telefonján, be van-e kapcsolva a kétlépcsős belépés a céges e-mail-fiókjában.

04

10 lépés, ami a legtöbbet hozza

Nem drága termékek, hanem beállítások és szokások – a legtöbb meglévő eszközzel megoldható

20 perc

ÁTTEKINTÉS

A tíz lépés egy képen

01

MFA mindenhol

e-mail, bank, távoli
elérés

02

Jelszókezelő

egyedi, hosszú jelszavak

03

Automatikus frissítés

gép, telefon, router,
plugin

04

3-2-1 mentés + teszt

visszaállítás próbája

05

Minimális jogosultság

nincs napi admin fiók

06

SPF, DKIM, DMARC

a domainünk védelme

07

Titkosított eszközök

laptop, telefon, pendrive

08

Kilépők hozzáférése

aznap letiltva

09

Kettős jóváhagyás

utalás és számlaszám-
csere

10

Alap incidensterv

ki, mit, kit hív

MFA és jelszókezelő: a fiókok két zárja



Többfaktoros belépés

- Sorrend: e-mail → bank → távoli elérés (VPN, RDP) → admin fiókok → felhő
- Hitelesítő app vagy hardverkulcs az SMS helyett
- „Fáradtság-támadás”: kéréstlen jóváhagyó kérést **soha** nem fogadunk el



Céges jelszókezelő

- Minden szolgáltatáshoz más, hosszú jelszó – fejben csak egy mesterjelszó
- Közös jelszavak megosztása Excel és post-it helyett
- Kilépéskor egy helyen látszik, mit kell cserélni

A mentés annyit ér, amennyit a visszaállítási teszt

3

példány

Az éles adat és két mentés.

2

különböző tároló

Pl. NAS és felhő – ne ugyanaz a hiba vigye el mindkettőt.

1

offline vagy törlésvédett

Amit a támadó a hálózatról nem tud törölni.

+

negyedéves teszt

Egy fájl és egy teljes gép visszaállítása, stopperrel mérve.

Kérdés, ami eldönti: **ha hétfő reggel minden gép titkosítva van, hány óra múlva tudunk újra számlázni?**

Négy beállítás, ami szinte ingyen van

Lépés	Miért számít?	Hogyan egy KKV-nál?
Automatikus frissítés	A támadások jelentős része ismert, már javított hibát használ ki	Automatikus frissítés gépen, telefonon; routert, NAS-t, webes plugint is
Minimális jogosultság	Amit a felhasználó nem érhet el, azt a kártevő sem	Napi munka sima fiókkal, külön admin fiók; mappák szerepkör szerint
Titkosított eszközök	Elveszett, de titkosított laptop jellemzően nem bejelentendő incidens	BitLocker / FileVault bekapcsolva, kulcs a cégnél; telefonon képernyőzár
Kilépők hozzáférése	A volt munkatárs és volt beszállító fiókja nyitott ajtó	Kilépési checklist: fiókok, jelszavak, eszközök, közös fiókok aznap

Ne lehessen a mi nevünkben levelet küldeni

SPF

A „feladói névsor”

Mely szerverek küldhetnek levelet a domainünkről.

DKIM

A „viaszpecsét”

Digitális aláírás: a levél tényleg tőlünk jött, és útközben nem módosult.

DMARC

A „házirend”

Mit tegyen a címzett a hamisítvánnyal – és küldjön róla jelentést.

DMARC bevezetése:

p=none · figyelünk



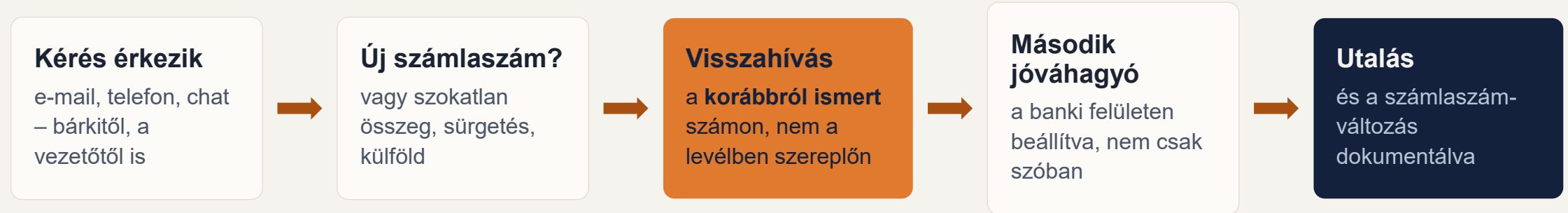
quarantine · spambe



reject · elutasítva

Kiegészítés: a külső levelek jelölése a tárgysorban, pl. [KÜLSŐ] – a hasonló domaineket ez is leleplezi

Az a folyamat, ami 1,2 milliárdot megfogott volna



Ha már elment a pénz: azonnal a bank csalásmegelőzési vonala, majd rendőrségi feljelentés. A visszahívás esélye órákban mérhető.

Az első 60 perc egy oldalon, papíron is

- | | |
|--|---|
| 1 Izolálás: a gépet le a hálózatról – de ne kapcsoljuk ki | 2 Riasztás: IT-partner és a kijelölt vezető |
| 3 Napló: mi, mikor, ki észlelte, mit tettünk | 4 Fiókok: érintett jelszavak cseréje, munkamenetek letiltása |
| 5 Pénz: ha utalás érintett, azonnal a bank | 6 Bejelentés: NAIH 72 órán belül; NKI, ha NIS2-érintett |
| 7 Kommunikáció: egy szóvivő, előre megírt üzenetváz | 8 Tanulság: egy héten belül, hibáztatás nélkül |

TELEFONLISTA – KINYOMTATVA

IT-partner (0–24): [szám]

Bank csalásmegelőzés: [szám]

Kiberbiztosító: [szám]

Adatvédelmi tanácsadó / jogász: [szám]

NAIH online bejelentő · NKI: incidens.nki.gov.hu

Rendőrség: 112

05

AI és a jövő kockázatai

Az AI a támadók kezében, a shadow AI a saját cégünkben – és a kvantumszámítógép, amely a mai titkosítást is megtörheti

13 perc

Olcsóbb, gyorsabb, hihetőbb támadások

80%+

a manipulációs kampányoknak AI-támogatott (ENISA, 2025 eleje, globálisan)

893 M \$

AI-hoz köthető csalási kár ~22 000 panaszból (FBI, 2025)

- **Hibátlan magyar nyelvű** adathalász levél, személyre szabva
- **Hangklón** néhány másodpercnyi nyilvános felvételből
- **Deepfake videóhívás** több „kollégával” egyszerre
- Automatizált sérülékenység-keresés és kártevőírás

HONGKONG, 2024 · ARUP

~25 M \$

Egy pénzügyes munkatárs videóhívásban „a pénzügyi igazgatóval és kollégákkal” egyeztetett – **mindenki deepfake volt**. 15 utalásban küldte el a pénzt.

Az arc és a hang már nem azonosítás.

SHADOW AI

Amit a cég nem lát, azt nem tudja védeni

59%

munkavállaló használ jóvá nem hagyott AI-eszközt

~3/4

ezek közül adott már meg neki érzékeny adatot

1 az 5-ből

szervezetnél volt már shadow AI-hoz köthető incidens

+670 e \$

többletköltség incidensenként, ha sok a shadow AI

Mi kerül ki tipikusan?

Szerződés és árajánlat „fogalmazd át”-ra, ügyféllista, forráskód, bérlista, megbeszélés-átirat AI-jegyzetelő bottal, böngészőbővítmény, ami minden oldalt „összefoglal”.

Samsung, 2023

Mérnökök forráskódot és belső jegyzetet másoltak egy nyilvános chatbotba. A cég ideiglenesen betiltotta a generatív AI-eszközöket.

Engedélyezni okosan, nem tiltani

Nyilvános adat

Marketingszöveg, publikus anyag →
bármely jóváhagyott eszköz

Belső adat

Ajánlat, folyamatleírás → csak céges
fiókos, nem tanító eszköz

Bizalmas adat

Személyes adat, ügyféltitok, forráskód →
nem kerül AI-ba, csak saját zárt rendszerbe

1. **Leltár:** mit használnak a kollégák?
2. **Céges eszköz:** SSO, MFA, adatmegőrzés
3. **Egyoldalas AI-házirend,** három színnel
4. **AI-jegyzetelő, bővítmény** csak jóváhagyással
5. **Az ember dönt:** AI-kimenet ellenőrzése
6. **Deepfake-protokoll:** visszahívás



Prompt injection: a dokumentumba rejtett utasítás átveheti az AI-ügynököt – utalás és adatküldés csak emberi jóváhagyással.

Ma gyűjtik, holnap fejtik meg

A mai nyilvános kulcsú titkosítás (**RSA, ECC**) védi a TLS-t, a VPN-t, a digitális aláírást és a firmware-frissítést. Egy elég nagy kvantumszámítógép (Shor-algoritmus) ezeket **órák-napok alatt** feltöri.

„Harvest now, decrypt later”

A lehallgatott, titkosított adatcsomagokat már ma tárolják. Ha megjelenik a gép, a régi forgalom – szerződés, terv, egészségügyi adat – visszamenőleg olvashatóvá válik.

Hány fizikai qubit kell az RSA-2048 feltöréséhez?

2012 · ~1 milliárd



2019 · ~20 millió



2025 · kevesebb mint 1 millió (Google)



2026 · kevesebb mint 100 ezer (szimuláció)



Logaritmikus skála – a becslés 13 év alatt kb. 10 000-szeresére csökkent

A megoldás már szabvány – az átállás évekig tart

NIST · 2024. augusztus

Az első PQC-szabványok

ML-KEM (FIPS 203) – kulcscsere

ML-DSA (FIPS 204), **SLH-DSA** (FIPS 205)
– aláírás

Már használatban

Hibrid kulcscsere

Klasszikus + PQC együtt: Chrome,
Cloudflare, Signal, iMessage – sokszor
észrevétlenül.

EU-ütemterv

2026 · 2030 · 2035

2026 végéig leltár és terv · 2030-ig a
magas kockázatú rendszerek · 2035-ig a
többi

Mit tehet ma egy KKV?

- 1. Kriptoleltár:** VPN, TLS, aláírás, IoT
- 2. Beszállító:** mi a PQC-ütemterve?
- 3. Beszerzés:** PQC-képes firmware-aláírás
- 4. Kriptoagilitás:** cserélhető algoritmus
- 5. Prioritás:** a 10+ évig titkos adat

06

Az emberi tényező

Az ember nem a leggyengébb láncszem – hanem a leggyorsabb riasztó, ha hagyjuk

8 perc

Nem a kattintást mérjük, hanem a jelentést



Kattintási arány

Hány százalék kattintott a szimulált levélre. Csökkenjen – de soha nem lesz nulla.



Jelentési arány

Hányan jelezték gyanúsnak. Ez a legfontosabb szám: ebből él a védekezés.



Jelentési idő

Hány perc telik el az első jelzésig. Minél rövidebb, annál kisebb a kár.

Program egy KKV-nál

Negyedévente 10–15 perces képzés · havonta egy szimulált levél, változó nehézséggel · kattintás után azonnali, rövid tanítóoldal · egy kattintásos „Gyanús levél” gomb · eredmények csak összesítve, név nélkül.

Ugyanaz a kattintás, két különböző hétfő

Ahol szólni szabad

9:05 Kata rákattint egy linkre, beírja a jelszavát.

9:07 Rájön, és azonnal szól: „Azt hiszem, hibáztam.”

9:20 Jelszócsere, munkamenetek letiltva, a levél törölve mindenkinél.

Kár: egy kellemetlen negyedóra.

Ahol félnek a büntetéstől

9:05 Ugyanaz a kattintás.

9:07 Kata szégyelli, reméli, hogy nem lesz baj. Hallgat.

+2 hét A támadó a fiókból hamis számlát küld az ügyfeleknek, és bejut a szerverre.

Kár: utalások, titkosított szerver, bejelentés.

A szabály egyszerű: **aki szól, azt megköszönjük** – a hibát a folyamatban keressük, nem az emberben.

OTTHONI MUNKA ÉS SAJÁT ESZKÖZ

Az iroda ma ott van, ahol a laptop



Otthoni router: gyári jelszó cseréje, frissítés, külön vendéghálózat a gyerekeknek és okoseszközöknek



Céges gép céges munkára: a család nem használja, nem telepít rá játékot



Saját telefon (BYOD): képernyőzár, frissítés, céges adat csak kezelt alkalmazásban, távolról törölhetően



Nyilvános wifi: kávézóban és hotelben céges VPN vagy a telefon saját hotspotja



Fájlok: céges felhőben, nem a saját Gmailben, WhatsAppon vagy pendrive-on



Képernyő és beszélgetés: vonaton, videóhívásban figyeljünk, ki lát és ki hall

14 kérdés – hány „igen” van?

12–14 jó · 7–11 közepes · 0–6 sürgős

- ☐ Az e-mailen, a bankon és a távoli elérésen **mindenkinél MFA** van.
- ☐ Céges **jelszókezelőt** használunk, nincs közös jelszó Excelben.
- ☐ Gépek, telefonok, router, NAS **automatikusan frissülnek**.
- ☐ Minden laptop és telefon **titkosított**, képernyőzárral.
- ☐ A domainen él az **SPF, DKIM és DMARC**.
- ☐ Megvan az **adatkezelési nyilvántartás**, a tájékoztató és az adatfeldolgozói szerződések.
- ☐ Kamerán, routeren, NAS-on **nincs gyári jelszó**, és külön hálózaton vannak.
- ☐ Van **offline vagy törlésvédett mentés**, és az elmúlt negyedévben teszteltük.
- ☐ Számlaszám-változást csak **visszahívással**, utalást **két jóváhagyóval** fogadunk el.
- ☐ Senki nem dolgozik naponta **admin fiókkal**.
- ☐ Kilépőnél és lezárt beszállítói munkánál **aznap** megszűnik a hozzáférés.
- ☐ Van **papíron is elérhető incidensterv** és telefonlista.
- ☐ Mindenki tudja, **kinek szóljon**, ha rákattintott – és nem fél szólni.
- ☐ Van **AI-házirend**, és tudjuk, milyen AI-eszközöket használnak a kollégák.

Ha csak hármat visz haza:

1

MFA az e-mailen és a bankon –
még ezen a héten

2

Offline mentés és egy kipróbált
visszaállítás

3

**Visszahívás és kettős
jóváhagyás** minden utalásnál

Ahol az adatok utánanézhettek

Mediaworks-incidens: Telex, 2026. 04. 30., 05. 01., 05. 04.; HVG, 2026. 04. 30.

KRÉTA NAIH-bírság: HVG / Telex, 2024. 02. 21.

Számlaváltós hálózat: BRFK / police.hu (Adózóna)

Telefonos csalás, 47 M Ft: Economx, 2026. 06. 09.

Hangklónozásos csalás: Telex G7, 2019. 09. 03.

JLR-leállítás: Economx / ESET, 2025. 11. 22.

Collins Aerospace: ICTglobal, 2025. szept.

Könyvelői NAIH-bírság: Adózóna, GDPR-esetek

Kiberbiztonsági audit: SZTFH / MTI, Adózóna, 2026. júl.; Telex, 2025. 05. 06.

Incidensbejelentés: MKIK NIS2 jogi állásfoglalások 2026/3–4
(nis2.mkik.hu)

AI Act + Omnibus: Gibson Dunn; Future of Privacy Forum; Rencore (2026)

Magyar zsarolóvírus-adatok: Sophos-felmérés, Infostart, 2024. 08. 04.

Csalási összeg 2024: MNB-adat, Telex, 2026. 01. 31.

Kitettség: Microsoft Digital Defense Report 2025

CEO-csalás jelei: OTP Bank ügyféltájékoztató

Hasznos oldalak: nki.gov.hu · naih.hu · sztfh.hu · kiberpajzs.hu

FORRÁSOK 2/2

Nemzetközi esetek, statisztikák, AI, PQC, szabályozás

Globális kár: Cybersecurity Ventures, Official Cybercrime Report 2025

Incidensköltéség, shadow AI: IBM Cost of a Data Breach 2025

USA-kár, AI-csalás: FBI IC3 2025 (Help Net Security, 2026. 04.)

EU behatolási vektorok: ENISA Threat Landscape 2025

Vállalati csalás 2025: MNB-adat, Economx, 2026. 04. 27.

JLR: Cyber Monitoring Centre (Business Insurance, 2025. okt.)

Lengyel energiahálózat: CERT Polska (Industrial Cyber); Dragos

M&S, Asahi, Kido: LBC/FT; Infosecurity Magazine; ICTglobal

Shadow AI: Cybernews-felmérés (Journal of Accountancy, 2025. 11.)

Arup deepfake-eset: nemzetközi sajtó, 2024. május

Kvantum-erőforrásbecslés: Gidney 2025; The Quantum Insider, 2026. 03. 31.

PQC-szabványok: NIST FIPS 203, 204, 205 (2024. aug.)

EU PQC-ütemterv: NIS Cooperation Group, 2025 (PQShield)

CRA: (EU) 2024/2847; Finite State idővonal

RED kiberbiztonság: SGS / TÜV SÜD összefoglalók (2025)

IoT-támadások: Zscaler ThreatLabz IoT/OT Threat Report 2023, 2025

BLUESTELLAS

Trendig Plus - Kiberbiztonság

Interreg
AUSTRIA-HUNGARY



Co-funded by
the European Union

Trendig Plus

AN INTEGRATED BORDER REGION



Papp Zsolt

Társalapító, ügyvezető

zsolt.papp@bluestellas.com · +36 20 508 7407

BlueStellas Kft. · 9700 Szombathely, Puskás Tivadar utca 7/A · info@bluestellas.com ·
www.bluestellas.com

