ISO 9000 FÓRUM Egyesület

Regionális minőségügyi ISO-tudásprogram vállalkozásoknak

EU új kihívásai - NIS2 megfelelés, Kiberbiztonság, Információbiztonság

Joó Gabriella – Információbiztonság vezető, BKK

ISO 9000 FÓRUM Egyesület

A minőség szolgálatában

1994 óta működő szakmai közösség
2003 óta közhasznú egyesület
ISO 9001 szabvány szerint tanúsított, ISOCRM rendszerrel automatizált, online folyamatokkal megvalósított működés

Több mint 400 tagunk között megtalálhatók

Tagjaink elkötelezettek a minőségszemlélet terjesztése, illetve a minőségfejlesztési eszközök gyakorlatba ültetése iránt

Fő tevékenységeink rendezvények szervezése, szakmai előadások, párbeszédek és tapasztalatcsere programok biztosítása.

Célunk

- Erős, támogató szakmai közösséget építeni
- Céglátogatásokkal, programokkal és konferenciákkal segíteni a fejlődést
- Tudásmegosztást és értékes tapasztalatcserét biztosítani
- Összefogni a minőség iránt elkötelezett vállalatokat és szakembereket

Regionális minőségügyi ISO-tudásprogram vállalkozásoknak

5 vármegyei helyszín – 19 alkalom

Témák

KKV vezetőfejlesztő sorozat 2 blokkban

- Kockázatkezelés, projektmenedzsment, Irányítási rendszerek használata
- Folyamatszabályozás és folyamatoptimalizálás, minőségügyi problémamegoldások, minőségtudatosság és változásmenedzsment

Belső auditor képzés

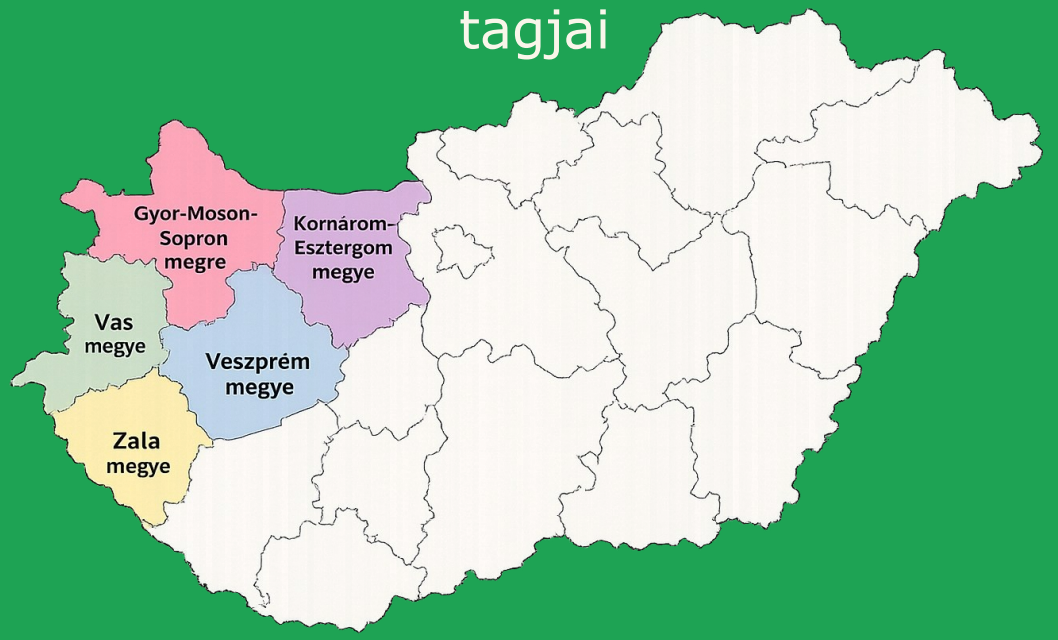
EU új kihívásai tematikus nap 2 témacsomagban

- ESG, energiahatékonyság
- Információbiztonság, NIS2, kiberbiztonság

Best Practice tapasztalatok megismerése - céglátogatás

Előadók

ISOFÓRUM Egyesület tapasztalt szakemberei, tagjai



ISO 9000 FÓRUM Egyesület

Legyen tagunk!

- Kedvezményes részvétel a Nemzeti Minőségügyi Konferencián
- Ingyenes részvétel céglátogatásokon
- Szakmai tudás megosztás, tanácsadás a tagok között
- Közvetlen kapcsolatépítés a minőség iránt elkötelezett szakemberekkel
- Szakmai elismerés és láthatóság a legfontosabb hazai fórumokon, weblapunkon
- Inspiráló, támogató közösség, amelyben minden tag számít

+36 30 161 7152

info@isoforum.hu

isoforum.hu

Joó Gabriella

Tedd a biztonságot üzleti előnnyé!

AI

Az előadás egyes vizuális elemei **generatív mesterséges intelligencia** segítségével készültek.

Joó Gabriella

Információbiztonság vezető – BKK

Információbiztonsági szakértő, BCM szakértő,
Oktató, Szerző

SZAKMAI HÁTTÉR

- Információbiztonsági szakmérnök
- Mérnök - informatikus
- Biztonságszervező menedzser
- ISO 22301 Lead Auditor
- ISO 27001 Lead Auditor
- ISO 27701 Lead Auditor

SZAKMAI TAPASZTALAT

- 10+ év információbiztonsági és BCM területen
- Oktató – Óbudai Egyetem és BCM Akadémia
- A *Válsághelyzetből versenyelőny – Üzletmenet-folytonosság lépésről lépésre* című könyv szerzője

> *Hiszem, hogy a biztonság nem csak a nagyvállalatok kiváltsága.*

TE MIT GONDOLSZ?

Mennyire tartod valószínűnek, hogy a vállalkozásodat kibertámadás éri?

A) NEM GONDOLOM

„A mi vállalkozásunkat valószínűleg nem éri támadás.”

VS

B) BIZTOSAN LESZ PRÓBÁLKOZÁS

„Nem az a kérdés, hogy lesz-e, hanem hogy mikor.”

Miért lett üzleti kérdés a kiberbiztonság?

01

A digitalizáció előnyei és kockázatai

A digitalizáció ma már nem választás, hanem a vállalkozások működésének alapja. Ahogy egyre több folyamat kerül online térbe, úgy nő a kibertámadások és az üzleti leállások kockázata is.

Előnyök

- ✅ Gyorsabb ügyintézés
- ✅ Online értékesítés
- ✅ Felhőszolgáltatások
- ✅ Távoli munkavégzés

Kockázatok

- ⚠️ Több adat
- ⚠️ Több támadási felület
- ⚠️ Nagyobb függőség az IT-tól
- ⚠️ Egy hiba is leállást okozhat

Lássunk egy példát!

Valós hazai kibertámadás
alapján készült esettanulmány

ADATHALÁSZAT

HOZZÁFÉRÉS

ZSAROLÓVÍRUS

ADATVESZTÉS

Hétfő reggel. 09:12. Minden rendben volt...

Egy teljesen átlagos hétfő reggel minden a megszokott rendben indul. A kollégák dolgoznak, a megrendelések érkeznek, a számlázás működik.

Néhány órával később azonban a vállalkozás működése teljesen megbénul.

Nézzük meg, hogyan jutottak el idáig...

09:12

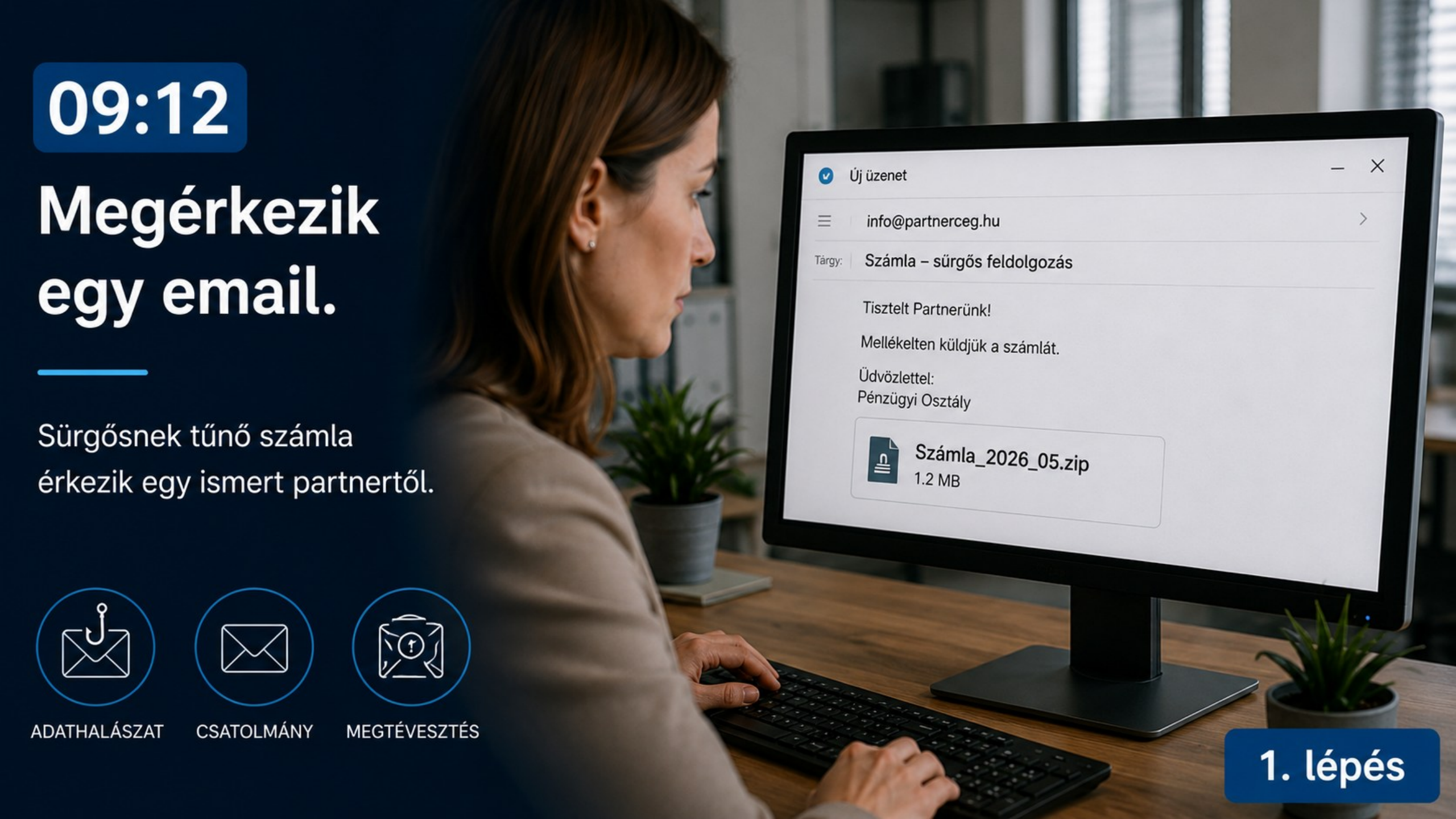
Megérkezik egy email.

Sürgősnek tűnő számla érkezik egy ismert partnertől.

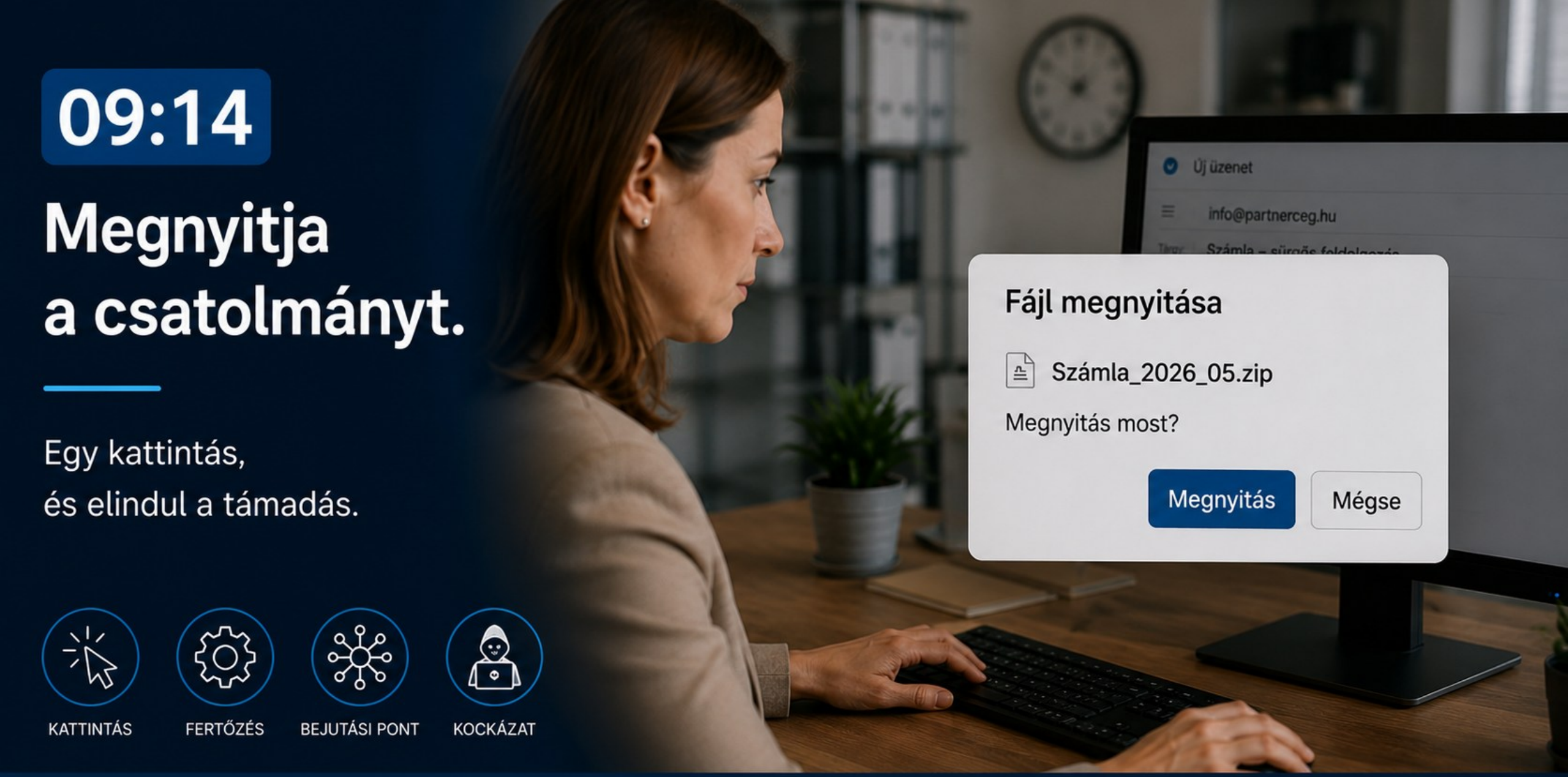
ADATHALÁSZAT

CSATOLMÁNY

MEGTÉVESZTÉS



1. lépés



09:14

Megnyitja a csatolmányt.

Egy kattintás,
és elindul a támadás.

KATTINTÁS FERTŐZÉS BEJUTÁSI PONT KOCKÁZAT

A támadók adathalász e-mailekkel jutnak be a rendszerbe.
Sokan nem gyanakodnak, ha az üzenet hitelesnek tűnik.

2. lépés

09:14

Megnyílik a csatolmány.

A csatolmányban lévő fájl megnyitásával elindul a ransomware.

A fájl megnyitásakor a ransomware elindul, és megkezdi a rendszer ellenőrzését és **titkosítását**.

3. lépés

10:20

Furcsán működnek a rendszerek.

A munkatársak hibákat tapasztalnak, lassul a munka.

LASSULÁS

HIBAJFLENSÉGEK

GYANÚ

Az első jelek gyakran aprók.
Fontos időben felismerni őket!

4. lépés


11:00
Leáll
a számlázás.
A rendszer nem engedi
megnyitni az állományt.
RENDSZERHIBA
ELÉRHETŐSÉG
KIESÉS
A rendszer nem elérhető,
a munka nem folytatható.
Hiba
Nem sikerült megnyitni
az állományt.
OK
5. lépés

14:00

Megjelenik a zsarolóüzenet.

A támadók titkosították az adatokat,
és váltságdíjat követelnek a feloldásért.

Az üzletmenet leállt.
Minden perc számít.

Az incidens súlyos hatással van a vállalat működésére,
és **azonnali beavatkozást** igényel.

6. lépés

15:00

Incidenst észlelünk / megkezdődik az incidenskezelés.

Értesítjük az informatikai és információbiztonsági csapatot, és elindítjuk az incidenskezelési folyamatokat.

- INCIDENS ÉSZLELVE
- CSAPAT ÉRTESÍTVE
- INCIDENSKEZELÉS ELINDÍTVA
- HATÁS FELMÉRÉSE

Gyors reakcióval minimalizáljuk a károkat és helyreállítjuk a rendszereket.

7. lépés

17:30

Sikeresen helyreálltunk, nem fizettünk.

A rendszereket a mentésből visszaállítottuk,
az adatok épségben megmaradtak,
és a működés helyreállt.
Nem fizettünk a támadóknak.

MENTÉSBŐL VISSZAÁLLÍTVA

ADATOK ÉPSÉGBEN

RENDSZEREK MŰKÖDNEK

NEM FIZETTÜNK A TÁMADÓKNAK

Az incidens sikeresen lezárva.
Tanultunk belőle, hogy még ellenállóbbak legyünk a jövőben.

Miért lett ma már minden vállalkozás célpont?

Régen a támadók kiválasztották az áldozatot. Ma már a támadások jelentős része automatizált: a támadók azt keresik, hol találnak könnyen kihasználható hibát. Ezért ma már minden internetkapcsolattal rendelkező vállalkozás potenciális célpont.

Miért támadnak?

Pénzt akarnak szerezni - Zsarolóvírussal vagy adatszivárgással próbálnak váltságdíjat kicsikarni.

Értékesek az adataid - Ügyféladatok, szerződések, számlák, üzleti tervek – ezek mind pénzt érhetnek a támadóknak.

Könnyebb célpontnak tűnsz - Sok kisvállalkozásnál nincs többfaktoros azonosítás, rendszeres mentés vagy naprakész védelem.

Számítanak arra, hogy gyorsan fizetsz - Ha napokig áll a számlázás vagy a termelés, nagy a nyomás, hogy minél előbb helyreálljon a működés.

A támadások nagy része automatizált - Nem téged választanak ki személyesen. Programok keresik folyamatosan a sérülékeny rendszereket az interneten.

A kibertámadások nem informatikai, hanem üzleti kockázatot jelentenek

Sokan azt gondolják, hogy egy kibertámadás...

- ❌ a számítógépekről, szerverekről szól.
- ❌ csak a nagyvállalatokat érinti.
- ❌ az informatikusok problémája.

Valójában a vállalkozás problémája.

- ➢ Leáll a számlázás és a pénzügyi folyamatok.
- ➢ Akadozik vagy leáll az ügyfélkiszolgálás.
- ➢ Megszakad a szolgáltatás, a napi működés.
- ➢ Ellehetetlenül a kommunikáció a munkatársakkal és az ügyfelekkel.
- ➢ Sérülhet a vállalkozás hírneve és az ügyfelek bizalma.

Információbiztonság – Mit és miért védünk?

02

TE MIT GONDOLSZ?

Az alábbiak közül melyik okozna nagyobb problémát a cégednek?

A) A RENDSZEREK LEÁLLÁSA

„Nem tudnánk dolgozni, számlázni, kiszolgálni az ügyfeleket.”

VS

B) ÉRZÉKENY ADATOK KISZIVÁRGÁSA

„Bizalmas vállalati, ügyfél- vagy munkatársi adatok kerülhetnének illetéktelenekhez.”

Egy kibertámadás története - esettanulmány

Fotó: Forbes

Mi történt?

2015. július 13.

Az **Impact Team** feltörte az Ashley Madison rendszerét, és hozzáférést szerzett a vállalat felhasználói adataihoz.

Nem egyetlen fájlt vittek el. A teljes adatvagyont veszélybe sodorták.

Ezután jött a zsarolás.

A támadók közölték:

„Állítsátok le az Ashley Madisont – vagy nyilvánosságra hozzuk az adatokat.”

A vállalat **nem tett eleget a követelésnek.**

2015. augusztus

A fenyegetés valóra vált.

A támadók közzétették a megszerzett adatokat.

Több mint 36 millió felhasználó személyes, fiók- és számlázási adatai kerültek nyilvánosságra.

A támadás néhány hét alatt egy informatikai incidensből személyes és társadalmi válsággá vált.

Ashley Madison – a támadás számokban

36+ millió
érintett felhasználói profil

~10 GB
első nagy adatdump, 20 GB további vállalati adat

11,7 MILLIÓ
feltört jelszó

31 M / 5,5 M
férfi / női profil (85%/15%)

A 3 leggyakoribb jelszó:

1. 123456
2. 12345
3. password

És voltak ilyenek is...

ishouldnotbedoingthis – ezt nem kellene csinálnom

ithinkilovemywife – azt hiszem, szeretem a feleségem

thisiswrong – ez helytelen

whatthehellamidoing – mi a fenét csinálok?

kb. 630 000 fióknál a felhasználónév és a jelszó megegyezett.

Milyen adatok kerültek ki?

- Nevek
- e-mail-címek
- lakcímhez kapcsolódó adatok
- születési dátum
- kapcsolati státusz
- Nem
- testmagasság, testsúly, testalkat
- szexuális preferenciák és fantáziák
- fényképek és szabad szöveges profiladatok
- biztonsági kérdések és válaszok
- jelszóhash-ek
- számlázási és tranzakciós adatok
- részleges fizetési kártyaadatok

És mi lett a támadás eredménye?

Nem csak adatok kerültek nyilvánosságra.

Az incidens következményei több szinten jelentkeztek:

A vállalat számára

- súlyos reputációs kár
- hatósági vizsgálatok és jogi következmények
- jelentős bizalomvesztés
- a vállalat vezetésének komoly válságkezeléssel kellett szembenéznie

A későbbi vizsgálat szerint az Ashley Madisonnál nem volt megfelelő írásos információbiztonsági szabályzat, megfelelő hozzáférés-kezelés vagy megfelelő munkatársi biztonsági képzés.

A felhasználók számára

- személyes és intim adatok kerültek nyilvánosságra
- kapcsolatok és családok kerültek válságba
- zsarolási kísérletek indultak
- az érintettek közül sokan súlyos társadalmi és személyes következményekkel szembesültek

És volt ennél is súlyosabb következmény

2015. augusztus 24-én a torontói rendőrség arról számolt be, hogy **két, az incidenssel összefüggésbe hozott öngyilkossági esetet vizsgálnak**. Fontos: a rendőrség akkor ezeket **nem megerősített információként**, *unconfirmed reports*-ként közölte.

Ezért fontos megértenünk, hogy mit is jelent valójában az információ védelme.

Adat, információ és üzleti érték

Mitől lesz egy adat értékes egy vállalkozás számára?

ADAT
Önmagában még nem mond sokat.

↓

INFORMÁCIÓ
Segít megérteni egy helyzetet.

↓

ÜZLETI DÖNTÉS
Alapot ad a megfelelő döntéshez.

↓

ÜZLETI ÉRTÉK
Versenyelőnyt és üzleti eredményt teremt.

ADAT	INFORMÁCIÓ
5 250 000	A hónap legnagyobb vevője még nem fizetett.
350	Már csak 350 db termék van készleten.
2026.09.15.	Holnap lejár a szerződés.

Az információbiztonság minden olyan helyzetben jelen van, amikor a vállalkozás adatokat, információt kezel, tárol, oszt meg, így digitális rendszereket használ.

Az információbiztonság három alapelve

Ki láthatja az információt?
Csak az férhet hozzá, akinek valóban szüksége van rá.

Biztosan helyes az információ?
Az adat nem módosult jogosulatlanul vagy véletlenül.

Elérem akkor, amikor szükségem van rá?
Az információ rendelkezésre áll, amikor dolgozni kell vele.

Hogyan jelennek meg ezek a mindennapi működésben?

Mindennapi helyzet	Bizalmasság (B)	Sértetlenség (S)	Rendelkezésre állás (R)
E-mail küldése	Csak a megfelelő címzett kapja meg.	A tartalom nem módosul útközben.	A címzett időben megkapja az e-mailt.
Dokumentum megosztása	Csak a jogosultak férnek hozzá.	A dokumentum nem módosul jogosulatlanul.	A dokumentum bármikor elérhető, amikor szükség van rá.
Banki utalás	Csak a jogosult indíthat utalást.	A bankszámlaszám és az összeg helyes.	Az internetbank működik, amikor szükség van rá.
Felhőszolgáltatás használata	Az adatokhoz csak a jogosultak férnek hozzá.	A fájlok nem sérülnek és nem módosulnak jogosulatlanul.	Az adatok bárhonnan, bármikor elérhetők.
Biztonsági mentés	A mentéshez csak jogosultak férnek hozzá.	A mentett adatok változatlanok és helyreállíthatók.	Hiba esetén az adatok visszaállíthatók.

Minden egyes lépésnél egyszerre kell gondoskodnod arról, hogy az információ csak a megfelelő személyhez jusson el, ne módosuljon jogosulatlanul és mindig rendelkezésre álljon.

Miért az információ a vállalkozás egyik legnagyobb értéke?

A legtöbb vállalkozás működése ma már információkra épül.

Ha ezek elvesznek, sérülnek vagy illetéktelen kezekbe kerülnek, annak közvetlen üzleti következményei lehetnek.

A számítógépek pótolhatók. Az üzletileg értékes információk sokszor nem.

Ha holnap tönkremegy a laptopod, veszel egy újat.

De ha elveszik az elmúlt tíz év ügyfélkapcsolata, ajánlata és szerződése, azt már nem tudod egyszerűen újra megvenni.

TE MIT GONDOLSZ?

Melyik alapelv sérült?

Hétfő reggel egy zsarolóvírus miatt a vállalkozás nem fér hozzá a fájljaihoz és a számlázó rendszeréhez. Az adatok ugyan megvannak, de nem lehet hozzájuk hozzáférni.

A) BIZALMASSÁG

Nincs arra utaló jel, hogy illetéktelen személy hozzáfért vagy hozzájutott az adatokhoz.

VS

B) SÉRTETLENSÉG

Nincs arra utaló jel, hogy az adatok tartalma jogosulatlanul megváltozott vagy módosult volna.

VS

C) RENDELKEZÉSRE ÁLLÁS

Az adatok és a számlázó rendszer ugyan megvannak, de a vállalkozás a zsarolóvírus miatt nem tud hozzájuk hozzáférni és használni őket.

TE MIT GONDOLSZ?

Melyik alapelv sérült?

Egy munkatárs véletlenül egy több száz ügyfél személyes adatait tartalmazó Excel-fájlt küld el egy olyan partnernek, akinek nem lett volna szabad megkapnia.

A) BIZALMASSÁG

A bizalmasság sérül, mert a személyes adatokat olyan partner kapta meg, akinek nem lett volna jogosultsága hozzáférni az adatokhoz.

VS

B) SÉRTETLENSÉG

Az adatok tartalma nem változott meg, csak jogosulatlan személyhez kerültek.

VS

C) RENDELKEZÉSRE ÁLLÁS

Az adatok továbbra is elérhetők és használhatók a vállalkozás számára, nem váltak hozzáférhetetlenné.

TE MIT GONDOLSZ?

Melyik alapelv sérült?

Egy támadó hozzáfér egy vállalkozás e-mail-fiókjához, majd egy partnernek küldött számlán megváltoztatja a bankszámlaszámot. A vállalkozás a hibás adat alapján utal.

A) BIZALMASSÁG

A támadó jogosulatlanul hozzáfért a vállalkozás e-mail-fiókjához és az abban található információkhoz.

VS

B) SÉRTETLENSÉG

A támadó jogosulatlanul megváltoztatta a számlán szereplő bankszámlaszámot.

VS

C) RENDELKEZÉSRE ÁLLÁS

A számla és az e-mail-fiók továbbra is elérhető volt, az adatot meg lehetett tekinteni és fel lehetett használni.

Fizikai biztonság – nem csak a hackerekre kell figyelni

1. **Nyitva hagyott iroda vagy szerverterület**
   Ha bárki szabadon bejuthat olyan helyiségbe, ahol számítógépekhez, szerverekhez vagy érzékeny információkhoz férhet hozzá, az komoly biztonsági kockázat. **A fizikai hozzáférés ugyanúgy hozzáférés.**

2. **Elveszett vagy ellopott laptop, telefon, pendrive**
   Egy elveszett eszközön akár nagy mennyiségű vállalati vagy személyes adat is lehet. Ezért fontos például a **képernyőzár, az erős hitelesítés és az eszközök titkosítása**.

3. **Leselejtezett adathordozó – az adat ne maradjon rajta**
   Egy régi laptop, merevlemez vagy pendrive attól még nem lesz biztonságos, hogy már nem használjuk. **Az adathordozón lévő adatokat biztonságosan törölni vagy az adathordozót fizikailag megsemmisíteni kell.**

4. **Vendég hozzáférése – ne férjen hozzá ahhoz, amihez nem kell**
   Egy vendégnek vagy külsősnek csak ahhoz szabad hozzáférést biztosítani, amire valóban szüksége van. **A „csak nézz körül nyugodtan” nem jelenthet szabad hozzáférést a vállalkozás rendszereihez.**

5. **Közös vagy lezáratlan eszköz – ne legyen szabadon hozzáférhető**
   Ha egy gépet többen használnak, vagy valaki egyszerűen otthagyja bejelentkezve, más hozzáférhet az adatokhoz. **A képernyőt mindig zárjuk le, amikor elhagyjuk az eszközt, még akkor is, ha rövid időre megyünk el.**

Incidens észlelése – mit tegyek, ha gyanús?

3 lépés, amit mindenkinek tudnia kell

1. **ÁLLJ MEG!**
   Ne kattints tovább, ne törölj semmit, és ne próbáld egyedül megoldani a problémát.

2. **JELEZD!**
   Azonnal szólj a kijelölt kapcsolattartónak a meghatározott csatornán.

3. **KÖVESD AZ UTASÍTÁST!**
   A további lépéseket – például az eszköz hálózatról való leválasztását – az IT / kijelölt szakember utasítása szerint végezd el.

Kávészünet

15 perc

A leggyakoribb kibertámadások és azok felismerése

03

Adathalászat - amikor a támadó téged próbál becsapni

Mi az adathalászat?

Az adathalászat olyan megtévesztési módszer, amelyben a támadó **megbízhatónak vagy ismerősnek tűnő személynek, szervezetnek vagy szolgáltatónak adja ki magát**, hogy rávegyen valamire.

A célja lehet például:

- **felhasználónév és jelszó megszerzése**
- **banki vagy fizetési adatok megszerzése**
- **kártékony fájl megnyittatása**
- **hamis weboldalra történő beléptetés**
- **pénz átutaltatása**
- **további rendszerekhez vagy adatokhoz való hozzáférés megszerzése**

Hogyan próbál rávenni?

A támadó gyakran **sürgetéssel, félelemkeltéssel vagy kíváncsiság felkeltésével** próbál döntésre kényszeríteni:

„Azonnal erősítsd meg a fiókodat!”

„Gyanús bejelentkezést észleltünk.”

„A számlád felfüggesztésre kerül.”

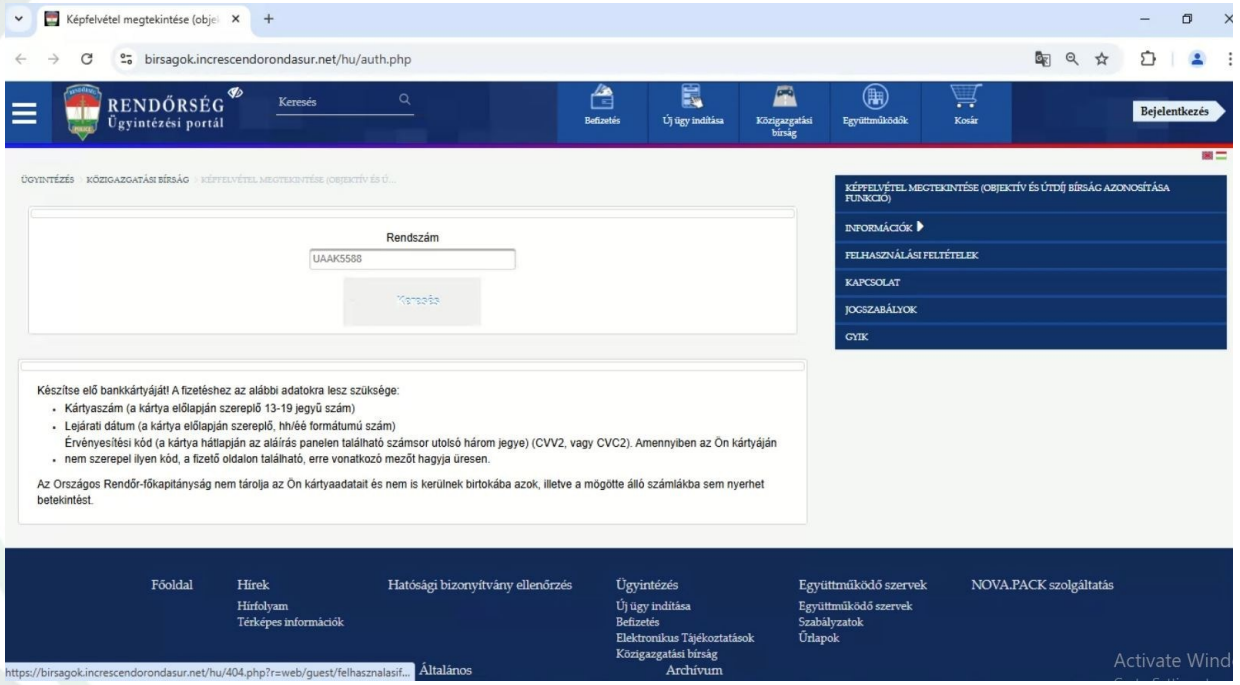
„A vezető ezt azonnal kéri.”

Adathalászat – valós példa

2026. 07. 01. – Szabálysértési bírság befizetésére hivatkozó adathalász üzenet – Forrás: NKI

A csalók most **e-mail üzenetekben** próbálják megtéveszteni a címzetteket. Az új változat a „Magyar Országos Központ” feladótól érkezik, és „Tisztelt lakos” megszólítással **szabálysértési bírság befizetésére próbálnak rávenni**, mobilkommunikációs eszköz közlekedés közbeni használata miatt. A levél végén az aláíró az „Országos Rendőrségi Főkapitányság”.

Az emailben lévő hivatkozás megnyitását követően egy **hamis Rendőrségi portál** jelenik meg, ahol a **rendszámunk megadását kérik**.



A csaló oldal célja, hogy a felhasználó a rendszám megadása után a „Keresés” gombra kattintva továbblépjen.

Ezt követően **megnyílik egy hamis Simplepay oldal**, rajta, „Bírságaim”: 6900 HUF befizetendő összeggel.

A csaló oldal a kártyaadatok megadása után a „Fizetés” gombra kattintást várja el a felhasználótól. Ezt a műveletet semmiképpen ne hajtsuk végre: ne adjunk meg bankkártya adatokat, és ne kattintsunk a fizetést indító gombra.

A fizetés gomb megnyomását követően egy **progress oldal jelenik meg**, mintha beindulna egy fizetési és hitelesítési folyamat a háttérben (ez sosem fejeződik be).

Fontos!

A támadók folyamatosan alakítják és finomítják módszereiket, ezért az ilyen üzenetek és a hozzájuk kapcsolódó felületek kezelése során **minden esetben fokozott körültekintés szükséges**. A gyanús tartalmú megkereséseket célszerű kritikusan vizsgálni, és minden esetben ellenőrizni azok hitelességét, mielőtt bármilyen műveletet végrehajtanánk.

Zsarolóvírusok - amikor egyszer csak nem férsz hozzá a saját adataidhoz

Mi az a zsarolóvírus (Ransomware)?

A zsarolóvírus olyan kártevő, amely titkosítja a vállalkozás fájljait vagy elérhetetlenné teszi a rendszereket, majd a támadó pénzt követel a hozzáférés helyreállításáért.

Egy támadás során például:

- Titkosítják a fájlokat
- Elérhetetlenné válnak a dokumentumok és adatok
- Leállhatnak a rendszerek és a munkafolyamatok
- Váltságdíjat követelnek
- Az adatokat akár ki is lophatják, majd közzététellel fenyegethetnek

Hogyan kezdődhet?

Egy zsarolóvírus sokféleképpen bejuthat a vállalkozásba:

- Adathalász e-mailből
- Kártékony csatolmányból
- Ellopott vagy gyenge jelszóval
- Sérülékeny, internet felől elérhető rendszerből
- Kompromittált felhasználói fiókon keresztül

Zsarolóvírusok – valós példa

2026. 03. 30. – Magyarország Ügyészségének nevével visszaélő adathalász kampány – Forrás: NKI

A támadók hivatalos megkeresés látszatát keltő e-maileket küldtek. Az üzenet egy **eljárási dokumentumra** hivatkozott, és arra próbálta rávenni a címzettet, hogy egy hivatkozásra kattintva töltsön le egy dokumentumot.

A fertőzés végső célja a végponton található dokumentumok, képek, archívumok és más állományok **titkosítása, majd váltságdíj követelése.**

Tisztelt [Címzett]!

Ezúton értesítjük, hogy a [Cégnév] Kft. (adószám: ***, székhely: ***) tekintetében a hatályos magyar jogszabályok alapján büntetőeljárás van folyamatban.

Az ügyhöz kapcsolódó iratok elektronikus formában az alábbi linken érhetők el:

[Ransomware letöltési linkje]

Kérjük, hogy a fenti hivatkozáson elérhető dokumentumokat megismerni szíveskedjen.

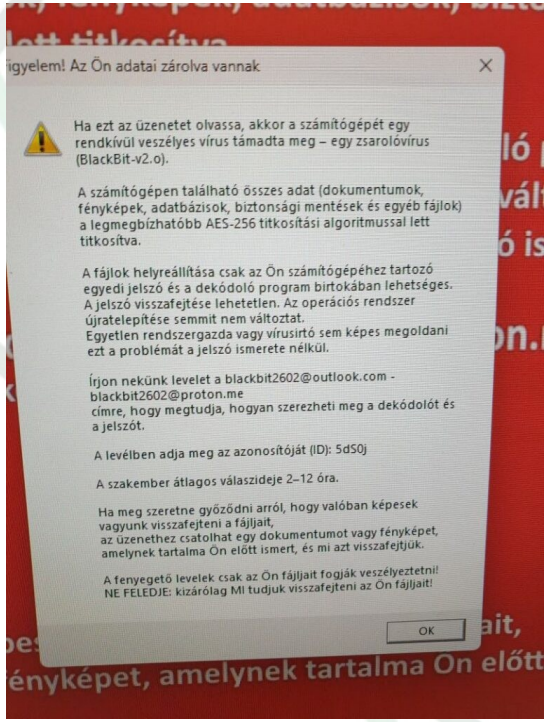
Amennyiben az ügyben nyilatkozatot kíván tenni, illetve észrevételt kíván előterjeszteni, azt a vonatkozó jogszabályi rendelkezések szerint, a meghatározott határidőn belül teheti meg.

Jelen értesítés kizárólag tájékoztatásul szolgál.

Tisztelettel:

xy

Magyar Ügyészség



Felismerési pontok

- Az ügyészség hivatalos e-mail címeinek végződése: **@mku.hu**. Gmail-es vagy más e-mail címről **nem érkezhet az Ügyészségtől levél**.
- Az üzenetben szereplő link látszólag hasonlíthat egy hivatalos oldalra, ténylegesen azonban **megtévesztő domainre mutat**.
- A hivatkozás megnyitása után **további kattintásra, dokumentum megtekintésére vagy letöltésre próbálják rávenni a felhasználót**.

Social Engineering - amikor a támadó az embert használja fel

Mi az a social engineering?

A social engineering olyan megtévesztési módszer, amelyben a támadó az emberi bizalomra, figyelmetlenségre vagy segítőkészségre épít, hogy információt, hozzáférést vagy pénzt szerezzen.

A támadó nem feltétlenül a technológiát próbálja feltörni. Megpróbál téged rávenni arra, hogy te nyisd ki neki az ajtót.

Hogyan próbálkozhat?

- **Telefonon** – például informatikusnak vagy banki ügyintézőnek adja ki magát.
- **E-mailben** – vezetőnek, kollégának vagy üzleti partnernek adja ki magát.
- **Üzenetben** – sürgős segítséget vagy adatot kér.
- **Személyesen** – például együtt érkezik be veled az irodába, arra hivatkozva, hogy elfelejtette a belépőkártyáját.
- **Megbízható személynek adja ki magát** – és kihasználja, hogy természetes módon megbízunk a kollégáinkban, vezetőinkben vagy szolgáltatóinkban.

Mit akar elérni?

- Hozzáférést szerezni
- Információt megszerezni
- Pénzt átutaltatni
- Kártékony programot elindíttatni

Social Engineering – valós példa

2026.07.28. A csalók ezúttal is a bizalomra építettek – Forrás: police.hu

Banki ügyintézőnek és rendőrnek adták ki magukat, majd a pénzének biztonságára hivatkozva vették rá áldozatukat többmilliós tranzakciókra.

A 64 éves csömöri nő július végén kapott egy telefonhívást. A vonal másik végén jelentkező ismeretlen a bankja ügyintézőjeként mutatkozott be, és azt állította, hogy veszélybe került a bankszámláján lévő összeg, ezért annak megóvása érdekében sürgősen intézkednie kell. A hívásba később egy másik személy is bekapcsolódott, aki rendőrként megerősítette a korábban elhangzottakat.

A telefonálók arra vették rá a sértettet, hogy azoknál a pénzintézeteknél, ahol számlával rendelkezik, hajtson végre átutalások az utasításaik szerint. A nő bízott bennük, és végrehajtotta a kért banki tranzakciókat. Mire kiderült, hogy bűncselekmény áldozatává vált, a közel 146 millió forint már eltűnt.

Mi tehetünk?

- Ha valaki telefonon azonnali intézkedést kér, legyen gyanakvó!
- Soha ne adja ki banki adatait, biztonsági kódjait vagy internetbanki hozzáférését ismeretleneknek!
- A bankok és a rendőrség telefonon soha nem kérik, hogy pénzt utaljon át vagy bankkártyás műveleteket hajtson végre a pénze védelme érdekében.
- Ha bizonytalan, szakítsa meg a hívást, és azonnal a bank hivatalos ügyfélszolgálatán érdeklődjön.

QR-kódos csalások - amikor egyetlen beolvasás rossz helyre vezet

Mi az a QR-kódos csalás?

A támadó egy QR-kód mögé rejti a megtévesztő hivatkozást, hogy rávegyen egy weboldal megnyitására, bejelentkezésre, adatmegadásra vagy akár egy alkalmazás letöltésére.

A QR-kód önmagában nem veszélyes.

Az számít, hogy hová vezet.

Miért veszélyes?

A QR-kód miatt nem látod előre olyan könnyen a webcímet, mint amikor egy számítógépen rámutatsz egy linkre.

Ráadásul a támadó egy teljesen valósághű bejelentkezési vagy fizetési oldalt is készíthet.

Hogyan működik?

QR-kódot küldenek
E-mailben, SMS-ben, plakáton, számlán vagy akár egy parkolási felületen.

⬇️

Beolvasod

⬇️

Megnyílik egy megtévesztő oldal

⬇️

Megadod az adataidat
például a felhasználónevedet, jelszavadat vagy banki adataidat.

QR-kódos csalások – valós példa

2024.09.10. - Quishing: QR fenyegetés az elektromos autósok számára – Forrás: NKI

Az EV töltőállomásokon gyakran QR kódok segítségével lehet kifizetni a megvásárolt áramot. A felhasználó csak beolvassa kamerája segítségével a töltőoszlopon elhelyezett QR-kódot, ami tovább irányítja őt egy weboldalra, ahol befejezheti a vásárlást.

Ezt a jelenséget használja ki egyre több kiberbűnöző. A 'quishing' a QR-kód, és a 'phishing' szavak kominációja, ami olyan csalást ír le, amelyben hamis QR kódokat használnak arra, hogy érzékeny információkat szerezzenek meg.

A támadás menete a következő:

- A csalók elkészítenek egy hamis adathalász weboldalt, ami megszólalásig hasonlít az eredeti fizető felületre
- A csalók készítenek egy QR kódot, amely a hamis oldalra mutat
- Ezt a QR kódot a csaló ráragasztja az oszlopon található eredeti QR kódra, ezzel letakarva az eredetit
- Amikor az áldozat beolvassa a hamis QR kódot, az ismerős fizetési felületen találja magát, ez azonban már a csaló által készített oldal
- Az áldozat beírja a bankkártya, vagy egyéb érzékeny adatait, amik így a csalóhoz kerülnek

Hogyan védekezzünk?

- Fizessünk (RFID) ügyfélkulccsal, feltöltőkártyával, érintésmentesen bankkártyával vagy applikáción keresztül!
- Ha mégis QR kódot használunk, ellenőrizzük a weboldal eredetiségét! A hamis weblap URL címében gyakran apró különbségek találhatók az eredeti címhez képest.
- Jelentsük a gyanús QR kódokat a töltőállomás üzemeltetőjének! Ezzel megelőzhetjük, hogy mások áldozatul essenek.

AI deepfake és hangklónozás - amikor már a látványnak és a hangnak sem hihetsz

Mi történik?

A mesterséges intelligencia segítségével a támadók ma már meggyőzően utánozhatják egy vezető, kolléga vagy üzleti partn[illegible]t és hangját, illetve hamis videót, képet vagy hangfelvételt készíthetnek.

A cél ugyanaz, mint sok korábbi social engineering támadásnál:

bizalmat kelteni → sürgetni → rávenni valamire.

Jelenleg Magyarországon magyar nyelven még nem egy elterjedt dolog, de egyszer megérkezik ide is…

Hogyan használhatják a támadók?

Deepfake videó: Egy vezető vagy üzleti partner arcát és mimikáját utánozzák.

Hangklónozás: Néhány másodpercnyi hangfelvételből megtévesztően hasonló hang készíthető.

AI-generált üzenetek: A korábbiaknál sokkal hitelesebb, személyre szabott e-maileket és üzeneteket készíthetnek.

Pénzügyi csalás: Például egy vezető hangján érkező sürgős kérés: „Most nem tudok beszélni, kérlek, azonnal utald el.”

Hozzáférés megszerzése: A támadó egy ismert személynek adva ki magát belépési adatokat vagy más érzékeny információt kérhet.

Ha egy szokatlan vagy sürgős pénzügyi kérés érkezik, ellenőrizd másik csatornán is – még akkor is, ha a hang vagy a videó teljesen valódinak tűnik.

AI deepfake és hangklónozás – valós példa

Mi történt?

2025 márciusában egy szingapúri **multinacionális vállalat pénzügyi igazgatója** egy látszólag rutinszerű Zoom-híváshoz csatlakozott a felsővezetői csapattal.

A pénzügyi igazgató és több vezető is jelen volt, a kommunikáció minden eleme hitelesnek tűnt. A pénzügyi igazgató **499 000 dolláros átutalást hagyott jóvá**, mielőtt a csalásra fény derült.

A hívásban résztvevők mind MI-vel generált entitások voltak…

Az eset nem egyedi.

2024 elején az Arup mérnöki vállalatot hasonló módszerrel támadták meg, amelynek során a támadók **egyetlen délután alatt 25,6 millió dollárt szereztek**. A technika széles körben terjed, miközben az azt lehetővé tevő eszközök folyamatosan olcsóbbá és könnyebben hozzáférhetővé válnak.

2025 első négy hónapjában a deepfake-alapú csalásokból származó kár meghaladta a 200 millió dollárt, míg 2024-ben ez az összeg 359 millió dollár volt, amelynek jelentős része az Egyesült Államokhoz köthető.

Az érintett szervezetek 61%-a 100 000 dollár feletti veszteséget jelentett, 19%-uk pedig 500 000 dollárnál is többet. A valós számok ennél vélhetően magasabbak.

Egy ilyen támadás végrehajtásához minimális erőforrás szükséges: egy név, egy rövid hangminta és egy olyan munkatárs, aki nem követi következetesen a hitelesítési eljárásokat.

A védekezés alapja a következetes ellenőrzés. Minden esetben szükséges a kérések hitelességének ellenőrzése, függetlenül azok sürgősségétől vagy forrásától.

Miért az ember a leggyengébb láncszem?

Az eddigi példáinkban mindig volt egy közös pont:

Adathalászat
Egy linkre **kattintasz**, mert az üzenet hitelesnek tűnik.

Zsarolóvírus
Megnyitsz egy kártékony csatolmányt, és a támadás elindul.

Social engineering
Megbízol valakiben, aki valójában nem az, akinek mondja magát.

QR-kódos csalás
Beolvasol egy QR-kódot, mert természetesnek tűnik, hogy ott van.

AI / deepfake / hangklónozás
Elhiszed, hogy valóban a főnököddel vagy üzleti partnereddel beszélsz.

Mi a közös bennük?

A támadó nem feltétlenül a technológiát akarja legyőzni.

Gyakran azt akarja elérni, hogy **te magad tedd meg helyette az első lépést.**

Az ember a leggyengébb láncszem?

Az ember nem azért a „leggyengébb láncszem”, mert nem tud hibázni.

Hanem azért, mert **a támadók tudatosan az emberi bizalomra, figyelemre és döntésekre építenek**.

Ezért a biztonság része az is, hogy tudjuk: mikor kell megállni, ellenőrizni és kérdezni.

Mit tehet egy vállalkozás már holnap?

04

TE MIT GONDOLSZ?

Ha holnap reggel kibertámadás miatt leállna a céged, tudnád, mit kell tenni?

A) IGEN

„Van tervünk, tudjuk, ki mit csinál.”

VS

B) NEM / NEM TUDOM

„Valószínűleg akkor kellene kitalálnunk.”

Értsd meg! Készülj fel! Cselekedj!

Nem az a kérdés, hogy lesz-e incidens. Hanem az, hogy mit teszel előtte és utána.

Egy KKV-nak vagy egyéni vállalkozónak nem kell mindent egyszerre megoldania.

Már néhány alapvető lépéssel is sokat lehet csökkenteni a kockázatot

Tedd tudatossá!
Te és a munkatársaid tudjátok felismerni az adathalászatot, a csalást és a gyanús helyzeteket.

Védd a hozzáféréseket!
Használj erős, egyedi jelszavakat és ahol lehet, többfaktoros hitelesítést (MFA).

Legyen mentésed!
A fontos adatokról legyen biztonságos, elkülönített és rendszeresen ellenőrzött biztonsági mentés.

Tartsd naprakészen!
Az operációs rendszerek, alkalmazások és eszközök frissítése csökkenti a kihasználható sérülékenységeket.

Tudd, mit teszel baj esetén!
Legyen meg, kit kell értesíteni, mit kell azonnal leállítani, és honnan tudod helyreállítani a működést.

Mi történik, ha egy incidens megakasztja a működésedet?

Egy kibertámadás következtében nemcsak az adatok kerülhetnek veszélybe:

- Leállhat a szolgáltatás.
- Megakadhat a termelés.
- Elérhetetlenné válhat a számlázás.
- Megszakadhat az ügyfélkiszolgálás.
- A munkatársak nem tudnak dolgozni.

Ezért kell tudnod előre:

- ✓ Mit csinálunk, ha nem érjük el az adatainkat?
- ✓ Mivel folytatjuk a munkát, ha egy rendszer leáll?
- ✓ Mi legyen az első lépés?
- ✓ Ki dönt? Ki intézkedik?

És közben a vállalkozásnak **tovább kell működnie!**

Nem az incidens az egyetlen probléma. Az igazi kérdés az, hogy képes-e a vállalkozás tovább működni közben.

Üzletmenet-folytonosság nem csak kibertámadás esetére

Mi történik, ha valami miatt egyszerűen nem tudunk dolgozni?

Áramszünet
Nincs áram → nincs internet, szerver, számítógép, pénztár stb.

Internet- vagy telekommunikációs kiesés
Nem érhető el a felhő, az e-mail, a telefon vagy az online ügyintézés.

Hardverhiba
Meghibásodik egy szerver, laptop, hálózati eszköz vagy más kritikus berendezés.

Felhőszolgáltatás kimaradása
Egy külső szolgáltató hibája miatt nem érjük el a rendszereinket vagy adatainkat.

Telephely elérhetetlensége
Tűz, csőtörés, műszaki hiba vagy más esemény miatt nem tudunk bemenni az irodába/üzembe.

Kulcsember tartós kiesése
Mi történik, ha az egyetlen ember, aki „mindent tud”, hetekig nem elérhető?

Hibás frissítés vagy véletlen törlés
Egy frissítés elront valamit, vagy valaki véletlenül töröl egy fontos adatot.

Nem az a kérdés, hogy történik-e valami.

Hanem az, hogy felkészültünk-e arra, hogy akkor is működjünk.

Miért nincs a legtöbb KKV-nál helyreállítási terv?

Nem azért, mert a vállalkozók nem tartják fontosnak a biztonságot. Gyakran egyszerűen mindig van valami sürgősebb.

Tipikus okok:

„Erre majd később lesz időnk.”
A helyreállítási terv addig nem tűnik sürgősnek, amíg valóban nincs szükség rá.

„Ez túl drága egy ekkora vállalkozásnak.”
Sokan egyből bonyolult, nagyvállalati megoldásban gondolkodnak, pedig az alapok ennél sokkal egyszerűbben is kialakíthatók.

„Nem tudjuk, hogyan kezdjünk hozzá.”
Mi a legfontosabb adat? Mi legyen az elsőként helyreállítandó rendszer? Ki döntsön? Kit kell értesíteni?

„Majd az informatikus megoldja.”
A helyreállítás azonban nem csak informatikai kérdés. Azt is tudni kell, hogyan folytatja az üzlet a működését, amíg a rendszerek helyre nem állnak.

„Van mentésünk, tehát rendben vagyunk.”
A mentés önmagában nem helyreállítási terv. Tudni kell azt is, hogy miből, hogyan és milyen sorrendben állítjuk helyre a működést.

A helyreállítási terv nem arra készül, hogy baj legyen. Arra készül, hogy amikor baj van, ne akkor kelljen kitalálni, mit csináljunk.

Mit tartalmazzon egy KKV helyreállítási terve?

Nem kell több száz oldalas dokumentum. A lényeg, hogy baj esetén mindenki tudja, mit kell tenni, milyen sorrendben és ki felel érte.

Egy jól használható helyreállítási terv választ ad legalább az alábbiakra:

1. ***Mi a legfontosabb?***
   Mely adatok, rendszerek és üzleti folyamatok nélkül nem tud működni a vállalkozás?

2. ***Mi történjen először?***
   Mely rendszereket és adatokat kell elsőként helyreállítani?

3. ***Ki mit csinál?***
   Ki dönt? Ki értesíti a munkatársakat, ügyfeleket vagy partnereket? Ki végzi a technikai helyreállítást?

4. **Miből állítjuk helyre?**
   Hol vannak a mentések? Mikor készült az utolsó használható mentés? Hogyan lehet hozzáférni?

5. **Mi az alternatíva?**
   Mit csinálunk addig, amíg a rendszer vagy az adat nem érhető el? Lehet-e átmenetileg manuálisan dolgozni, telefonon kommunikálni vagy más eszközt használni?

6. **Mikor mondjuk azt, hogy újra működünk?**
   Ki ellenőrzi, hogy az adatok és rendszerek helyreállítása valóban megfelelő, és vissza lehet térni a normál működéshez?

Nem az a cél, hogy mindent egyszerre állítsunk helyre. Az a cél, hogy először azt állítsuk helyre, ami nélkül nincs vállalkozás.

TE MIT GONDOLSZ?

Mikor teszteltétek utoljára, hogy a mentésből teljesen vissza tudtok állni?

A) TUDOM

„Rendszeresen teszteljük.”

VS

B) NEM TUDOM / MÉG NEM TESZTELTÜK

„Nem tudom, mikor volt utoljára.”

Biztonsági mentés és visszaállítás – legyen mihez visszanyúlni

Egy kibertámadásnál előfordulhat, hogy **az adatok törlődnek, titkosítva lesznek vagy egyszerűen elérhetetlenné válnak**. Ilyenkor a biztonsági mentés lehet az, ami lehetővé teszi, hogy a vállalkozás ne a nulláról kezdje újra.

De nem elég azt mondani: „Van mentésünk.”

Egy használható mentési megoldásnál tudnod kell:

Mit mentünk?
A vállalkozás működéséhez szükséges adatokat.

Milyen gyakran mentünk?
Egy heti mentés például teljesen mást jelent, mint egy óránkénti.

Hol van a mentés? (Georedundáns DR)
A mentés ne legyen ugyanúgy elérhető a támadó számára, mint az eredeti adatok.

Vissza tudjuk állítani?
A mentést rendszeresen tesztelni kell. Egy soha nem ellenőrzött mentésről nem tudhatod biztosan, hogy valóban használható.

Mennyi idő alatt állítható helyre?
Nemcsak az számít, hogy visszakapjuk-e az adatokat, hanem az is, hogy mikor tud újra működni a vállalkozás.

Egy fontos különbség

A biztonsági mentés nem ugyanaz, mint a helyreállítási terv.

A mentés azt mondja meg:

„Van honnan visszaállítanunk.”

A helyreállítási terv pedig azt:

„Tudjuk, mit, hogyan, milyen sorrendben és ki állít helyre.”

Van mentés. De vissza is tudunk állni?

Egy valós BCM audit tanulsága

1 AUDIT

Biztosítótársaságnál BCM auditot végeztünk.

Kiderült: nem rendelkeztek DR site-tal.

2 MIÉRT NINCS DR?

„Az adatokat át tudnánk tölteni a DR környezetbe. De nem tudjuk biztosan, hogy vissza is tudnánk állítani úgy, hogy minden megfelelően működjön."

→ A helyreállítást nem merték élesben kipróbálni.

3 BEÍRTUK A JELENTÉSBE

A kockázat bekerült a BCM audit jelentésébe.

Egy hónappal később...

4 MEGTÖRTÉNT AZ INCIDENS

Egy szerverben meghibásodott egy memória.

- A szolgáltatások leálltak
- 5 napig nem tudtak működni

A mentés önmagában nem helyreállítási terv.
A visszaállítást is tesztelni kell.

A felhő önmagában nem jelent biztonságot

„A felhőben van, tehát biztonságban van.” - **Ez az egyik leggyakoribb tévhit.**

A felhőszolgáltató biztosítja a szolgáltatás infrastruktúrájának és alapvető biztonságának egy részét, de **a vállalkozásnak is vannak saját biztonsági feladatai.**

Ezt nevezzük **megosztott felelősség elvének**.

Mit biztosít jellemzően a szolgáltató?

- **Az infrastruktúra védelmét**
- **A fizikai környezet és az alapplatform biztonságát**
- **A szolgáltatás rendelkezésre állását és technikai működését**

Mi marad a vállalkozás feladata?

Ki fér hozzá az adatokhoz?
Jogosultságok, MFA, felhasználói fiókok

Milyen adatokat tárolunk a felhőben?
Érzékeny adatok, megosztások, adatkezelés

Hogyan tudjuk helyreállítani az adatainkat?
Mentés és visszaállítás

Mit csinálnak a felhasználóink?
Tudatosság, adathalászat, hibás megosztás

Hogyan konfiguráltuk a szolgáltatást?
Hibás beállítások, túlzott jogosultságok

A felhőszolgáltató a felhő biztonságáért felel. A vállalkozás pedig azért, amit a felhőben csinál. A felhő használata nem helyettesíti a saját információbiztonságodat.

Négy alapvédelem, amit egy KKV már holnap bevezethet

A korábbi példákból már láttuk, hogy a támadók gyakran ellopott jelszavakkal, túlzott jogosultságokkal vagy nem megfelelően védett eszközökön keresztül jutnak be.

Ezért négy területre érdemes különösen figyelni

1. Többfaktoros hitelesítés (MFA)
Ne legyen elég önmagában a jelszó.
Ha egy támadó megszerzi a jelszavadat, az MFA egy újabb védelmi réteget jelent. Különösen fontos az e-mail, a felhőszolgáltatások, a távoli hozzáférések és a rendszergazdai fiókok esetében.

2. Jogosultságkezelés
Mindenki csak ahhoz férjen hozzá, amihez valóban szüksége van.
Ha egy felhasználói fiókot feltörnek, a támadó lehetőségeit jelentősen korlátozza, ha nem kap automatikusan hozzáférést a vállalkozás összes adatához és rendszeréhez. A jogosultságot nem azért adjuk, mert „hátha egyszer szüksége lesz rá”, hanem azért, mert a munkájához feltétlenül szükséges.

3. Mobileszközök biztonsága
A telefonod és a laptopod is a vállalkozás adatainak része.
Képernyőzár, titkosítás, automatikus frissítések, távoli törlés és az elveszett vagy ellopott eszközök gyors letiltása mind fontos védelmi intézkedések.

4. Végpontvédelem
Legyen minden gépen és mobileszközön naprakész, központilag kezelt végpontvédelem.
Vírusirtó / endpoint protection, automatikus frissítések, zsarolóvírusok és kártevők elleni védelem

Egyetlen ellopott jelszó, egy túlzott jogosultság vagy egy elveszett telefon is elég lehet ahhoz, hogy a támadó közelebb kerüljön a vállalkozás adataihoz. MFA + megfelelő jogosultságok + biztonságos eszközök = több akadály a támadó előtt.

Használd ki, amit már megvettél!

A Microsoft 365 és más felhőszolgáltatások számos beépített biztonsági funkciót és ajánlást kínálnak. Egy KKV-nak nem feltétlenül kell azonnal újabb biztonsági rendszereket vásárolnia – először érdemes megnézni, mit tud a már használt szolgáltatása.

Mire érdemes figyelni?

Többfaktoros hitelesítés (MFA)
Kapcsold be a felhasználói és különösen a rendszergazdai (admin) fiókoknál.

Jogosultságok felülvizsgálata
Ne legyenek felesleges vagy régi hozzáférések.

Biztonsági riasztások
Használd ki a szolgáltatás által jelzett gyanús bejelentkezéseket és biztonsági eseményeket.

E-mail-védelem
A beépített spam-, phishing- és kártevőszűrés megfelelő konfigurációja sok támadást már a felhasználó előtt megállíthat.

Eszközbiztonság
Ellenőrizd, milyen eszközökről férnek hozzá a vállalati adatokhoz, és hogy az eszközök megfelelnek-e a biztonsági követelményeknek.

Biztonsági ajánlások rendszeres ellenőrzése
A szolgáltatás által jelzett hiányosságokat ne hagyd figyelmen kívül: ezek gyakorlatilag egy személyre szabott teendőlistát adhatnak a vállalkozás biztonságának javításához.

Mielőtt új biztonsági eszközt vásárolsz, nézd meg, mit tudnak már azok a szolgáltatások, amelyekért fizetsz. A beépített biztonsági funkciók bekapcsolása gyakran az egyik leggyorsabb és legolcsóbb biztonsági fejlesztés.

A kiberbiztonság nem kizárólag az informatikus feladata

Az IT lehetőséget ad a technikai védelemre, de a biztonságos működéshez az egész vállalkozás együttműködésére szükség van.
Egy informatikus beállíthatja az MFA-t, a vírusvédelmet vagy a mentést.

De ő nem tudja egyedül eldönteni:

- Milyen információ a vállalkozás számára kritikus?
- Kinek milyen adatokhoz kell hozzáférnie?
- Mekkora kockázatot vállalunk egy üzleti döntéssel?
- Mit teszünk, ha incidens történik?
- Mennyire vesszük komolyan a biztonságot a mindennapi munkában?

A vezetés feladata

A vezetésnek kell **irányt mutatnia, erőforrást biztosítania, szabályokat meghatároznia és példát mutatnia**.

Ha a vezető azt mondja: „Nekünk erre nincs időnk.” akkor a munkatársak is azt tanulják meg, hogy a biztonság másodlagos.

Ha viszont a vezető azt mondja: „**A biztonság a működésünk része**.” akkor ebből idővel **szervezeti kultúra** lesz.

A kiberbiztonság nem egy ember feladata. Közös felelősség – de a példát felülről kell mutatni.

Nyilvános weboldal: keresd meg a hibát, mielőtt más találja meg

Ha a weboldalad vagy webalkalmazásod az internet felől elérhető, folyamatos támadási felületet jelent. Ezért érdemes rendszeresen ellenőrizni, hogy található-e rajta kihasználható sérülékenység.

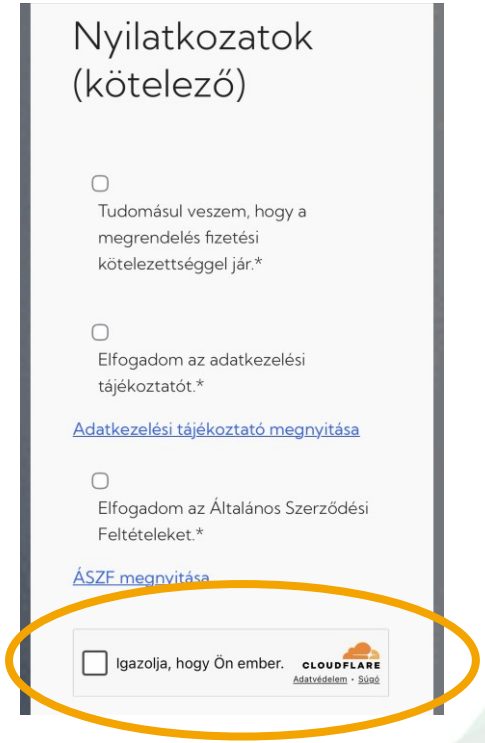
Mit tehet egy KKV?

Automatizált sérülékenységvizsgálat
Például Qualys Web Application Scanning (WAS) segítségével automatizáltan vizsgálhatók a webalkalmazások és API-k olyan sérülékenységek után, mint például az XSS vagy SQL injection. A vizsgálatok ütemezhetők, így rendszeresen megismételhetők.

Penetrációs teszt
Egy biztonsági szakértő ellenőrzött körülmények között megpróbálja kihasználni a feltárt sérülékenységeket, és azt vizsgálja, hogy egy valódi támadó meddig tudna eljutni.
Különösen indokolt lehet, ha a weboldal:

- személyes adatokat kezel,
- bejelentkezést biztosít,
- pénzügyi tranzakciót kezel,
- üzletileg kritikus funkciókat tartalmaz.

Automatizált visszaélések elleni védelem
Érdemes védeni például a bejelentkezést, regisztrációt, kapcsolatfelvételi és egyéb űrlapokat a botok és automatizált támadások ellen.
Cloudflare Turnstile
A Cloudflare Turnstile egy CAPTCHA-alternatíva, amelynek van ingyenes csomagja, és a weboldalakba beépítve segíthet megkülönböztetni a legitim felhasználókat az automatizált forgalomtól.



A kiberbiztosítás szerepe a pénzügyi kockázatok csökkentésében

Egy kibertámadásnak nemcsak informatikai következménye lehet, hanem közvetlen pénzügyi veszteségeket is okozhat.

Egy incidens után felmerülhet például:

- Pénzügyi veszteség – csalás, jogosulatlan utalás, üzleti kiesés
- Helyreállítás költsége – rendszerek, adatok és eszközök helyreállítása
- Szakértői költségek – IT-forenzik, incidenskezelés
- Kommunikáció és értesítés – ügyfelek, partnerek és hatóságok tájékoztatás
- Jogi és szabályozási költségek – bizonyos esetekben bírságok és jogi eljárások
- Üzleti kiesés – ha a támadás miatt a vállalkozás átmenetileg nem tud működni

Mit adhat ehhez a kiberbiztosítás?

A megfelelő biztosítási fedezet **az incidens egyes pénzügyi következményeit átvállalhatja**, például a helyreállítás, szakértői segítség vagy bizonyos üzleti veszteségek költségeit.

De nem helyettesíti a kiberbiztonságot. A kiberbiztosítás nem védelem a támadás ellen. Pénzügyi védőháló arra az esetre, ha a megelőzés ellenére mégis bekövetkezik az incidens.

KKV-ként ezt nézd meg:

Mit fedez a biztosítás?

Mekkora az önrész?

Milyen kizárások vannak?

Milyen biztonsági feltételeket kell teljesítened a biztosításhoz?

Ebédszünet

45 perc

NIS2 megfelelés egyszerűen – Miért érdemes akkor is foglalkozni vele, ha nem kötelező?

05

NIS2 – Miért érdemes akkor is foglalkozni vele, ha nem kötelező?

Mi az a NIS2, és miért született meg?

A **NIS2 az Európai Unió új kiberbiztonsági irányelve**, amelynek célja, hogy az EU-ban egységesen magasabb szintű kiberbiztonságot biztosítson.

A szabályozás abból indul ki, hogy a digitalizációval egyre több vállalkozás és szolgáltatás működése függ az informatikai rendszerektől, ezért egy kibertámadás már nemcsak informatikai, hanem **gazdasági és társadalmi kockázatot is jelent**.

Miért kellett új szabályozás?

A korábbi NIS-irányelvhez képest a NIS2:

- több ágazatra és több szervezetre terjeszti ki a kiberbiztonsági követelményeket,
- nagyobb hangsúlyt helyez a kockázatkezelésre és az incidensekre való felkészülésre,
- erősíti a vezetői felelősséget,
- és szigorúbb felügyeleti és szankcionálási keretet alakít ki.

Az EU-s NIS2 irányelvet Magyarország a **2024. évi LXIX. törvénnyel, Magyarország kiberbiztonságáról szóló Kiberbiztonsági törvénnyel** ültette át a magyar jogba.

A törvény 2025. január 1-jén lépett hatályba.

Kapcsolódó jogszabályok:

- 418/2024. (XII. 23.) Korm. Rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról,
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

NIS2 – Miért érdemes akkor is foglalkozni vele, ha nem kötelező?

A NIS2 célja és alapelvei

A NIS2 nem egyszerűen egy újabb „IT-s szabályozás”. A célja, hogy a szervezetek **tudatosabban kezeljék a kiberbiztonsági kockázataikat**, és képesek legyenek megelőzni, felismerni és kezelni a biztonsági eseményeket.

Mit akar elérni?

A kiberkockázatok csökkentését
Ne akkor kezdjünk védekezni, amikor már megtörtént a támadás.

A kockázatok tudatos kezelését
Legyen világos, milyen információkat, rendszereket és folyamatokat kell védeni, és milyen veszélyek fenyegetik őket.

A gyorsabb reagálást
Ha mégis bekövetkezik egy incidens, a szervezet tudja, mit kell tennie.

A működés helyreállítását
A cél nem csak az, hogy megállítsuk a támadást, hanem hogy a szervezet minél gyorsabban vissza tudjon térni a működéshez.

A vezetői felelősség erősítését
A kiberbiztonság nem pusztán informatikai kérdés: a vezetésnek is szerepet kell vállalnia a kockázatok kezelésében.

NIS2 – Mikor vonatkozik egy vállalkozásra Magyarországon?

Milyen tevékenységet végez?

Elsőként azt kell megnézni, hogy a vállalkozás **a törvény 2. vagy 3. mellékletében meghatározott ágazatba és szervezettípusba** tartozik-e.
Tehát önmagában az nem elég, hogy valaki például „gyártó” vagy „élelmiszeripari cég”. A konkrét tevékenységnek is szerepelnie kell a jogszabályban.

Mekkora a vállalkozás?

A 2. és 3. melléklet szerinti szervezeteknél főszabály szerint:

- középvállalkozásnak minősül, vagy
- eléri az 50 fő foglalkoztatotti létszámot, vagy
- az éves nettó árbevétele meghaladja a 10 millió eurónak megfelelő forintösszeget és a törvényben meghatározott esetben a mérlegfőösszegre vonatkozó feltétel is teljesül.

A hatóság bizonyos esetekben külön is azonosíthat egy szervezetet

A törvény lehetőséget ad arra is, hogy a nemzeti kiberbiztonsági hatóság bizonyos szervezeteket alapvető vagy fontos szervezetként azonosítson, ha a jogszabályban meghatározott feltételek fennállnak.

Vannak mérettől függetlenül érintett szervezetek is

A törvény alapján mérettől függetlenül a hatály alá kerülhet például:

- elektronikus hírközlési szolgáltató
- bizalmi szolgáltató
- DNS-szolgáltató
- legfelső szintű doménnév-nyilvántartó
- doménnév-regisztrációt végző szolgáltató.

Tehát itt nem kell megvárni az 50 főt vagy a 10 millió eurós küszöböt.

Vannak speciális szervezeti körök

A törvény külön kezeli többek között:

- közigazgatási szervezeteket,
- többségi állami befolyás alatt álló szervezeteket,
- honvédelmi érdekhez kapcsolódó gazdasági társaságokat,
- valamint egyes speciális digitális szolgáltatókat.

Értsd meg! Készülj fel! Cselekedj!

NIS2 – Mikor vonatkozik egy vállalkozásra Magyarországon?

2024. évi LXIX. Törvény
Magyarország Kiberbiztonságáról
2. és 3. melléklete

Ágazat	**Alágazat**
Energetika	Villamos energia, Távfűtés és hűtés, Kőolaj, Földgáz, Hidrogén
Közlekedés	Légi közlekedés, Vasúti közlekedés, Közúti közlekedés, Vízi közlekedés, Tömegközlekedés
Egészségügy	-
Ivóvíz, szennyvíz	Víziközmű-szolgáltatás
Hírközlési szolgáltatás	–
Digitális infrastruktúra	–
Kihelyezett IKT-szolgáltatások	–
Űralapú szolgáltatás	–
Postai és futárszolgálatok	–
Élelmiszer	Előállítás, Feldolgozás, Forgalmazás
Hulladékgazdálkodás	–
Vegyszerek előállítása és forgalmazása	–
Gyártás	Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása
	Számítógép, elektronikai, optikai termék gyártása
	Villamos berendezések gyártása
	Máshova nem sorolt gépek és berendezések gyártása
	Gépjárművek, pótkocsik és félpótkocsik gyártása
	Egyéb szállítóeszközök gyártása
	Cement-, mész-, gipszgyártás
Digitális szolgáltatók	Online-piactér, Keresőszolgáltatás, Közösségi média szolgáltatási platform, Doménnév-regisztráció
Kutatás	Kutatóhely

TE MIT GONDOLSZ?

Kinek a felelőssége a vállalkozás információbiztonsága?

A) AZ INFORMATIKUS

„Ő kezeli a rendszereket, ezért elsősorban neki kell gondoskodnia a biztonságról.”

VS

B) A VEZETŐ

„A biztonsággal kapcsolatos döntések és a szükséges erőforrások biztosítása vezetői felelősség.”

NIS2 – A vezetői felelősség szerepe

A NIS2 egyik fontos üzenete, hogy a kiberbiztonság vezetői szintű kérdés. A vezetésnek nem kell informatikai szakértővé válnia, de **felelősséget kell vállalnia azért, hogy a szervezet megfelelően kezelje a kiberbiztonsági kockázatait**.

Mit jelent ez a gyakorlatban?

Irányt kell adni
A vezetésnek biztosítania kell, hogy legyen működő kiberbiztonsági kockázatkezelési keretrendszer és megfelelő felelősségi körök.

Erőforrást kell biztosítani
A biztonsághoz szükséges emberi, technikai és pénzügyi erőforrásokat nem lehet pusztán az IT-ra hagyni.

Tudni kell, milyen kockázatokat vállal a vállalkozás
A vezetésnek ismernie kell a szervezet kritikus rendszereit, adatait és a hozzájuk kapcsolódó kockázatokat.

Meg kell jelölni a felelőst
A szervezet vezetője kijelöli az elektronikus információs rendszer biztonságáért felelős személyt, vagy külső szakemberrel állapodik meg.

A vezetőnek is értenie kell a kiberbiztonsághoz (Kötelező képzés)
A magyar szabályozás a vezető saját és a munkatársak kiberbiztonsági képzéséről, továbbképzéséről is rendelkezik.

Ellenőrizni és felügyelni kell
A vezetőnek gondoskodnia kell a védelmi intézkedések rendszeres értékeléséről és a feltárt hiányosságok kezeléséről.

A kiberbiztonság végrehajtását rá lehet bízni szakemberre. A vezetői felelősséget azonban nem lehet kiszervezni.

Értsd meg! Készülj fel! Cselekedj!

NIS2 – Kockázatkezelés, incidenskezelés és beszállítói biztonság

Egy vállalkozás kiberbiztonsága nem csak arról szól, hogyan védekezünk a támadások ellen. Azt is tudnunk kell, hogy mi a legfontosabb számunkra, mi történik baj esetén, és milyen kockázatot jelentenek a partnereink.

Kockázatkezelés

Tudd, mit kell megvédened!
Azonosítsd a vállalkozás számára fontos adatokat, rendszereket és folyamatokat, majd gondold végig:

Mi történhet?
Mekkora kárt okozna?
Mennyire valószínű?

Nem minden kockázatot kell megszüntetni, de **tudni kell róla, és tudatosan kell kezelni**.

Incidenskezelés

Tudd, mit kell tenned, ha megtörténik a baj!

Legyen előre meghatározva:
- ki veszi észre és jelzi az incidenst,
- ki dönt az azonnali intézkedésekről,
- kit kell értesíteni,
- hogyan korlátozzuk a kárt,
- hogyan állítjuk helyre a működést.

A cél, hogy **ne az incidens közepén kelljen kitalálni, ki mit csinál**.

Beszállítói biztonság

Ne csak a saját kockázataidat nézd!

Ha a vállalkozásod egy külső szolgáltatótól függ – például felhőszolgáltatótól, könyvelőtől, rendszergazdától vagy webfejlesztőtől –, akkor az ő biztonsági szintjük is hatással lehet a te vállalkozásodra.

Ezért érdemes tudni:
Ki fér hozzá az adataidhoz?
Milyen rendszereket üzemeltet helyetted?
Mi történik, ha nála van incidens?
Milyen biztonsági követelményeket vállalt szerződésben?

A NIS2 kifejezetten előírja a közvetlen beszállítókkal és szolgáltatókkal kapcsolatos biztonsági szempontok kezelését.

NIS2 – mint ingyenesen használható, átfogó biztonsági keretrendszer

A NIS2-t érdemes úgy is szemlélni, mint egy kész biztonsági ellenőrzőlistát: végigvezet azon, hogy egy vállalkozásnak mely területeken érdemes felkészülnie a kibertámadásokra. Nem kell NIS2-kötelesnek lenned ahhoz, hogy ezeket az alapelveket alkalmazd.

Mit érdemes végignézni?

Hozzáférések és jogosultságok
Ki fér hozzá a vállalkozás adataihoz és rendszereihez?

Biztonsági mentések és helyreállítás
Vissza tudjuk-e állítani az adatokat, ha elvesznek vagy titkosítják őket?

Incidenskezelés
Tudjuk-e, mit kell tenni, ha megtörténik a baj?

Sérülékenységek kezelése
Ismerjük és javítjuk a rendszereink gyenge pontjait?

Munkatársak tudatossága
Felismerik-e az adathalászatot és más megtévesztési kísérleteket?

Beszállítói biztonság
Tudjuk-e, milyen kockázatot jelentenek a külső szolgáltatók?

Kockázatkezelés
Tudjuk-e, mi történne, ha elveszítenénk a legfontosabb adatainkat vagy rendszereinket?

És hogyan használhatja ezt egy KKV?

Nézd végig a területeket → azonosítsd, hol vannak hiányosságok → állíts fel prioritásokat → kezdd a legnagyobb kockázatokkal.

Nem kell mindent egyszerre megoldani.

Már az is nagy előrelépés, ha egy vállalkozás végre tudja, hol vannak a legnagyobb biztonsági hiányosságai.

NIS2 – Hogyan segíthet a követelménylista a saját hiányosságaink feltárásában?

A NIS2 követelményei egy KKV számára is jó kiindulópont lehet annak átgondolására, hogy hol vannak a saját kiberbiztonsági hiányosságai.

Használjuk önellenőrzésre!

Vegyük végig a követelményeket, és minden területnél tegyük fel a kérdést:

- **Megvan?**
- **Részben van meg?**
- **Nincs meg?**

Terület	Kérdés, amit feltehetünk magunknak
Hozzáférések	Tudjuk, hogy ki milyen adatokhoz és rendszerekhez fér hozzá?
Mentések	Ha holnap eltűnnének az adataink, vissza tudnánk állítani őket?
Incidenskezelés	Tudjuk, mit kell tennünk egy kibertámadás esetén?
Tudatosság	Felismerik a munkatársaink az adathalász üzeneteket?
Beszállítók	Ismerjük a külső szolgáltatóink jelentette kockázatokat?
Sérülékenységek	Rendszeresen ellenőrizzük és javítjuk a rendszereink hibáit?

A cél nem a „kipipálás”

A követelménylista akkor igazán hasznos, ha nem egyszeri megfelelési feladatként, hanem önellenőrzési eszközként használjuk.

Megnézzük, hol tartunk → feltárjuk a hiányosságokat → felállítjuk a prioritásokat → elkezdjük kezelni a legnagyobb kockázatokat.

Kávészünet

15 perc

Hogyan induljunk el? – Gyakorlati eszközök és mesterséges intelligencia a mindennapokban

06

Az első lépések: tudd, mid van, mit védesz és ki fér hozzá

Egy vállalkozás információbiztonságát nem egy drága biztonsági rendszerrel érdemes kezdeni.

Először meg kell ismernünk a saját működésünket.

1. **Eszközleltár – Mink van?**
   Legyen nyilvántartásunk a vállalkozás által használt eszközökről: számítógépekről, laptopokról, telefonokról, szerverekről és egyéb informatikai eszközökről.

2. **Adatvagyon – Mit kell megvédenünk?**
   Tudjuk, milyen adatokat kezelünk, hol vannak ezek az adatok, és melyek különösen értékesek vagy érzékenyek?

3. **Jogosultságok – Ki fér hozzá?**
   Nézzük át, hogy ki milyen adatokhoz és rendszerekhez fér hozzá, és valóban szüksége van-e ezekre a hozzáférésekre.

4. **Mentések – Vissza tudjuk szerezni?**
   Legyen olyan biztonsági mentésünk, amelyből egy támadás, törlés vagy meghibásodás után ténylegesen vissza tudjuk állítani a fontos adatokat.

5. **Munkatársak felkészítése – Tudják, mire figyeljenek?**
   A munkatársaknak fel kell ismerniük a leggyakoribb támadásokat – például az adathalászatot, a hamis számlákat vagy a megtévesztő telefonhívásokat –, és tudniuk kell, mit tegyenek, ha valami gyanúsat észlelnek.

Hogyan használható az MI a vállalkozások biztonságának támogatására?

A mesterséges intelligencia nem helyettesíti az információbiztonsági szakembert vagy a megfelelő védelmi rendszereket, de egy KKV számára olyan segítséget adhat, amely korábban sokszor csak drága szakértői munkával volt elérhető.

Gyanús e-mailek és üzenetek elemzése
Egy AI-eszközzel megvizsgáltathatjuk a gyanús leveleket, és segítséget kérhetünk annak felismeréséhez, hogy milyen jelek utalnak adathalászatra vagy csalásra.

Biztonsági szabályzatok és eljárások
Segíthet egy vállalkozás saját szabályzatainak, eljárásainak és ellenőrzőlistáinak elkészítésében vagy átnézésében.

Kockázatok és hiányosságok feltárása
Az AI segítségével végig lehet gondolni például:

- milyen információkat kell védenünk,
- milyen kockázatok fenyegetik a vállalkozást,
- milyen biztonsági intézkedések hiányozhatnak.

Munkatársak tudatosítása
Segíthet adathalászati példák, gyakorlóhelyzetek és oktatási anyagok készítésében, így a munkatársak biztonságtudatossága is fejleszthető.

Incidens esetén
Egy megtörtént vagy feltételezett incidens során segíthet összerendezni az információkat, elkészíteni egy teendőlistát, vagy végiggondolni a lehetséges következő lépéseket.

Hogyan használható az MI a vállalkozások biztonságának támogatására?

De van egy nagyon fontos szabály!

Az AI-nak ne adjunk be bizalmas vagy érzékeny vállalati adatot csak azért, hogy „nézze meg”.

Mielőtt vállalati adatot töltünk fel egy AI-eszközbe, tudnunk kell, **milyen adatkezelési feltételek vonatkoznak az adott szolgáltatásra, és mit engedélyez a vállalkozás saját szabályozása.**

A jó kérdés nem az, hogy „használjunk-e AI-t?”, hanem az, hogy mire és hogyan használjuk biztonságosan?

Gyakorlati példák – így segíthet az AI egy KKV-nak

1. Precíz-Gép Kft. – Beszállítói szerződés

Helyzet

A vállalkozás új felhőszolgáltatót választ, és szeretné ellenőrizni, hogy a szerződésben megfelelően jelennek-e meg az információbiztonsági követelmények.

Nem a szerződést töltjük fel az AI-ba!

Promt (kérdés) az AI-hoz

„Milyen információbiztonsági követelményeknek érdemes szerepelniük egy felhőszolgáltatóval kötött szerződésben? Térj ki a hozzáférésekre, incidensbejelentésre, mentésekre, adatkezelésre, szolgáltatáskimaradásra és a szerződés megszűnésére.”

Az AI segít

- ellenőrzőlistát készíteni
- azonosítani a vizsgálandó területeket
- összeállítani a szolgáltatónak felteendő kérdéseket

2. MintaWeb Kft. – Külső webfejlesztő

Helyzet:

A webshopot egy külső fejlesztő üzemelteti, aki hozzáfér a vállalkozás rendszeréhez.

Kérdés az AI-hoz:

„Készíts információbiztonsági követelménylistát egy olyan külső webfejlesztő számára, aki hozzáfér a vállalkozás rendszeréhez és ügyféladatokat kezelő alkalmazásához.”

Az AI segít:

- végiggondolni a szükséges hozzáféréseket
- meghatározni a minimális jogosultságokat
- összegyűjteni a mentéssel, frissítésekkel, sérülékenységekkel és incidensekkel kapcsolatos elvárásokat

3. Családi Építő Kft. – Nincs információbiztonsági szabályzat

Helyzet:

A vállalkozásnak nincs kialakított információbiztonsági szabályzata.
A munkatársak saját tapasztalatuk alapján kezelik a biztonsági kérdéseket.

Kérdés az AI-hoz:

„Készíts egy egyszerű, KKV számára érthető információbiztonsági szabályzat vázlatot!!
Térj ki a jelszavakra, hozzáférésekre, e-mailekre, mobileszközökre, mentésekre és az incidensek kecelésére.”

Az AI segít:

- elkészíteni az első vázlatot
- feltárni, milyen területekre nincs még szabályozás
- közérthetővé tenni a szabályokat

A végleges szabályzatot természetesen embernek kell felülvizsgálnia és a vállalkozás működéséhez igazítania.

4. SzámlaPro Kft. – Megváltozott bankszámlaszám

Helyzet:

Egy munkatárs e-mailt kap egy megszokott beszállítótól, amelyben azt kérik, hogy a következő számlát már egy új bankszámlaszámra utalják.

Kérdés az AI-hoz:

„Egy beszállító e-mailben bankszámlaszám-változást jelentett be. Milyen információbiztonsági kockázatok merülhetnek fel, és milyen ellenőrzéseket végezzünk el, mielőtt utalunk?”

Az AI segít:

- felismerni a lehetséges csalási forgatókönyveket
- összeállítani az ellenőrzési lépéseket
- kialakítani egy hasonló esetekre alkalmazható eljárást

5. Kis Kft. – „Hol vannak a gyenge pontjaink?”

Helyzet:

A vezető szeretné felmérni, hogy a vállalkozás mennyire felkészült egy kibertámadásra, de nincs saját információbiztonsági szakértője.

Kérdés az AI-hoz:

„Tegyél fel nekem 20 kérdést egy 15 fős vállalkozás információbiztonságának felméréséhez! Térj ki az eszközökre, adatokra, jogosultságokra, mentésekre, e-mailekre, mobileszközökre, beszállítókra és a munkatársak tudatosságára.”

Az AI segít:

- rendszerezni a hiányosságokat és prioritási sorrendet felállítani

Mire használható és mire nem használható a AI információbiztonsági területen?

Az AI hasznos információbiztonsági segédeszköz, de nem biztonsági rendszer és nem helyettesíti a szakember döntését. Akkor használjuk jól, ha gondolkodási és előkészítő munkát támogat, nem pedig kritikus döntéseket bízunk rá.

Mire használható?

Kockázatok feltárására
Segít végiggondolni, hogy egy folyamat, rendszer vagy üzleti helyzet milyen információbiztonsági kockázatokat hordozhat.

Ellenőrzőlisták készítésére
Például: „Milyen szempontokat ellenőrizzek egy új felhőszolgáltató kiválasztásakor?”

Szabályzatok és eljárások előkészítésére
Első tervezetet, struktúrát, kérdéssort vagy ellenőrzőlistát készíthet.

Gyanús e-mailek elemzésére
Segíthet felismerni az adathalászat tipikus jeleit és elmagyarázni, miért gyanús egy üzenet.

Oktatásra és tudatosításra
Adathalászati példákat, gyakorlóhelyzeteket, kvízeket és oktatási anyagokat készíthet.

Ötletelésre és szakmai gondolkodás támogatására
Segít olyan kérdéseket feltenni, amelyekre elsőre talán nem gondolnánk.

Mire nem használható?

❌ **Nem helyettesíti a szakembert**
A válaszait ellenőrizni kell, különösen biztonsági döntések esetén.

❌ **Nem adunk neki bizalmas vállalati adatot**
Jelszavakat, ügyféladatokat, üzleti titkokat, személyes adatokat vagy más érzékeny információt csak akkor kezelünk AI-eszközzel, ha annak használata megfelelően szabályozott és technikailag is biztonságos.

❌ **Nem bízzuk rá a végső biztonsági döntést**
Például nem az AI dönti el, hogy egy sérülékenység elfogadható-e, vagy milyen biztonsági intézkedést kell bevezetni.

❌ **Nem tekintjük automatikusan igaznak a válaszát**
Az AI **tévedhet, hiányos vagy akár magabiztosan hibás választ is adhat**.

❌ **Nem használjuk önmagában biztonsági vizsgálatra**
Egy AI-beszélgetés nem helyettesít egy sérülékenységvizsgálatot, penetrációs tesztet vagy szakértői auditot.

Összefoglalás és kérdések

07

A legfontosabb tanulságok

Az információbiztonság nem egy informatikai projekt, hanem **a vállalkozás működésének védelme**.

1. Tudd, mit védesz!
Az adatok és az információk a vállalkozás értékei. Először azt kell tudnunk, **milyen adataink vannak, hol találhatók, és mi történne, ha elveszítenénk őket.**

2. Védd a bizalmasságot, a sértetlenséget és a rendelkezésre állást!
Ne csak azt kérdezzük, hogy *„ki férhet hozzá?”*, hanem azt is, hogy **megváltozhat-e jogosulatlanul az információ, illetve elérhető lesz-e akkor, amikor szükségünk van rá.**

3. Az ember a védelem része
Az adathalászat, social engineering, QR-kódos csalások, zsarolóvírusok és deepfake-ek ellen **a technológia mellett a munkatársak tudatossága is kulcsfontosságú.**

4. Készüljünk fel arra is, ha megtörténik a baj!
A cél nem az, hogy azt higgyük: *„velünk úgysem történhet meg”*.
Legyen **mentésünk, helyreállítási tervünk és incidenskezelési folyamatunk.**

5. Ne csak a saját vállalkozásunkat nézzük
A beszállítók, felhőszolgáltatók és külső partnerek biztonsága **a mi működésünkre is hatással lehet.**

6. A NIS2 akkor is hasznos, ha nem vagyunk kötelezettek
A NIS2 követelményei jó **önellenőrzési keretet** adhatnak: segítségükkel feltárhatjuk a hiányosságainkat, és meghatározhatjuk, mivel érdemes kezdenünk.

7. Az AI lehet a segítségünk – de nem helyettünk dolgozik
A mesterséges intelligencia segíthet **kockázatokat feltárni, ellenőrzőlistákat és tervezeteket készíteni, illetve tudatosítani**, de a döntés és a felelősség továbbra is az emberé.

A kiberbiztonság üzleti előnyt is jelenthet

A kiberbiztonságra sok vállalkozás még mindig úgy tekint, mint egy **szükséges költségre**. Pedig a megfelelő védelem nemcsak a károk megelőzését szolgálja, hanem **üzleti értéket is teremthet**.

- ✓ **Nagyobb bizalom az ügyfelek részéről**
  Egy partner számára komoly előnyt jelenthet, ha egy vállalkozásról elmondható, hogy **tudatosan kezeli az adatokat és a kiberbiztonsági kockázatokat**.

- ✓ **Könnyebb bekerülni beszállítói láncokba**
  A nagyobb vállalatok egyre gyakrabban várnak el biztonsági intézkedéseket a beszállítóiktól. A megfelelő felkészültség ezért **új üzleti lehetőségeket nyithat meg**.

- ✓ **Kevesebb kiesés és kisebb veszteség**
  Egy jól védett és felkészült vállalkozás egy incidens után **gyorsabban képes folytatni a működését**, így kisebb lehet az üzleti kár.

- ✓ **Versenyelőny**
  Ha két hasonló szolgáltató közül kell választani, előnyt jelenthet az a vállalkozás, amely **biztonságosan, megbízhatóan és kiszámíthatóan működik**.

- ✓ **Tudatosabb működés**
  A kiberbiztonsági intézkedések gyakran a működés más területeit is javítják: **rendezettebb jogosultságok, átláthatóbb folyamatok, kevesebb hibalehetőség és tisztább felelősségi körök** alakulhatnak ki.

Mit érdemes már másnap megvalósítani?

1. Kapcsoljuk be a többfaktoros hitelesítést
Elsőként a **levelezés, Microsoft 365, felhőszolgáltatások és rendszergazdai fiókok** védelmét erősítsük meg.

2. Nézzük át a jogosultságokat
Ki fér hozzá a vállalkozás adataihoz és rendszereihez?
Töröljük a már nem szükséges hozzáféréseket, és ahol lehet, alkalmazzuk a legkisebb szükséges jogosultság elvét.

3. Ellenőrizzük a mentéseket
Nem elég, hogy *„van backup”*.
Próbáljuk ki, hogy valóban visszaállíthatóak-e a legfontosabb adataink.

4. Készítsünk egy egyszerű eszköz- és adatleltárt
Legalább nagy vonalakban legyen meg, hogy: **Milyen eszközeink vannak? → Milyen rendszereket használunk? → Milyen fontos adataink vannak? → Hol vannak ezek?**

5. Tartsunk információbiztonsági oktatást
Mutassuk meg a munkatársaknak a leggyakoribb támadásokat:
adathalászat, hamis számla, QR-kódos csalás, telefonos megtévesztés.
És legyen egyértelmű: **Ha valami gyanús, nem szégyen megkérdezni – az a probléma, ha valaki csendben továbbmegy.**

6. Írjuk le egy oldalban, mi történik incidens esetén
Kihez fordulunk?
Kit hívunk?
Ki dönt?
Hogyan állítjuk le a további károkozást?
Honnan állítjuk helyre a működést?

Nem kell első nap egy 50 oldalas incidenskezelési szabályzat. **Egy jól átgondolt egyoldalas teendőlista is sokkal jobb, mint a semmi.**

További hasznos források és ajánlások

Magyar kiberbiztonsági források

NBSZ Nemzeti Kiberbiztonsági Intézet (NKI)
Aktuális kiberbiztonsági hírek, riasztások, elemzések és szakmai ajánlások. NBSZ NKI

KiberPajzs
Közérthető információk és gyakorlati tanácsok magánszemélyeknek és vállalkozásoknak a leggyakoribb online csalások és kiberfenyegetések felismeréséhez. KiberPajzs

Európai forrás

ENISA – European Union Agency for Cybersecurity
Útmutatók, jó gyakorlatok, kockázatkezelési és kiberbiztonsági anyagok vállalkozások számára is. ENISA

Ha Microsoft 365-öt használ a vállalkozás

Microsoft Secure Score
Érdemes rendszeresen ellenőrizni, mert a Microsoft a saját környezetünk alapján **biztonsági javaslatokat és javítási lehetőségeket** ad.
MS Secure Score

TE MIT VISZEL HAZA?

Mi volt számodra a mai előadás legfontosabb tanulsága?

1

EMBER

A leggyengébb láncszem helyett a védelem első vonala.

- Adathalászat, social engineering
- QR-csalás, deepfake
- A tudatosság mindannyiunk védelme

2

INCIDENS

Nem az a kérdés, hogy lesz-e, hanem hogy mi történik utána.

- Valódi támadások, valós következmények
- Incidenskezelés, gyors reagálás
- Az idő, az adat és a bizalom a legnagyobb érték

3

HELYREÁLLÍTÁS

A mentés csak akkor ér valamit, ha vissza is tudunk állni belőle.

- Rendszeres mentés
- Visszaállítási teszt
- Üzletmenet-folytonosság biztosítása

4

FELKÉSZÜLÉS

Nem kell tökéletesnek lennünk – el kell kezdenünk.

- NIS2, MFA, jogosultságok
- AI, mint segítség
- Kis lépések, nagy hatás

Válaszd ki azt az egyet, amit leginkább magaddal viszel!

Értsd meg!
Készülj fel!
Cselekedj!

A legjobb idő a felkészülésre tegnap volt. A második legjobb idő ma van!

Köszönöm a figyelmet!

Joó Gabriella

+36 30 161 7152

info@isoforum.hu

isoforum.hu