A *„Futok a pénzem után”* podcast a Marketing Commando és

a K&H Bank Üzletet ide együttműködésében jött létre

a bajbajutott kisvállalkozók megsegítésére

---

## Még mindig ugyanaz a jelszavad? Akkor ez neked szól!

### Karkas Péter IT technológiai tanácsadó és Gärtner Dávid, a K&H Bank üzleti információbiztonsági vezetője segítenek biztonságossá tenni céges és magánéltünk kibertámadásoknak kitett pontjait

Mindenhonnan azt halljuk, hogy legyünk óvatosak, vigyázzunk az adatainkra, előzzük meg a bajt – de konkrétan hogyan??? A számtalan tanács és tájékoztatás özönében könnyű elveszni, főleg, hogy szabadszemmel láthatalan veszélyről beszélünk, sok felületen, sok védekezési és mégtöbb veszély- lehetőséggel.

Ebben az adásban szakértőinktől egy olyan csekklistát kértünk, amivel:

- tételesen számba tudjuk venni az életünk tehcnikai területeit,

- mérlegelhetjük, melyik területen mit érdemes / kell bebiztosítanunk,

- és aztán ezt hogyan tegyük meg,

- és hogyan tartsuk frissen.

A következő oldalakon található táblázatok ebben segítenek: érdemes kinyomtatni és kitöltve tárolni, hogy bármikor rá tudj nézni – de ne felejtsd el, hogy ezeket rendszeresen kell frissíteni! Egy kisvállalkozás számára ez egy ugyanolyan fajsúlyú dokumentum kellene legyen, mint bármelyik céges szerződés: baj esetén nem csak referenciaként szolgál, de a hatóságok felé azt is dokumentálja, hogy te, mint cégvezető, legjobb tudásod szerint tudatosan mindent elkövettél a biztonság érdekében. Már csak ezért is érdemes ezt a dokumentumot komolyan venni és elkészíteni!

---

Az adásban szakértő vendégeink Gärtner Dávid, a K&H Bank üzleti információbiztonsági vezetője és Karakas Péter, IT technológiai tanácsadó. Tapasztalataik megosztását, a tőlük kapott hasznos információkat, tanácsaikat ezúton is köszönjük!

Karakas Péter maga is vállalkozó, cége, a Techfore Sight Solutions Kft cégalapítóknak és növekvő kisvállalkozásoknak segítek eligazodni az IT technológiai kihívások között, sőt: akár cégeket felkészíteni befektetésre, vagy skálázható csapatokat építeni.

Péter közvetlen elérhetősége: https://peterkarakas.com/.

## Biztonsági checklist KKV-nak

Kockázati Mátrix

| Eszköz kategória | Kockázati szint | Ajánlott intézkedések | Rendszeres karbantartás |
|---|---|---|---|
| Munkaállomások (PC-k, laptopok) | Magas (adatszivárgás, adatvesztés, phishing, social engineering, ransomware, alkalmazás fiók ellopása) | ● Antivirus software telepítése (fontos)<br>● Erős jelszó használata (fontos)<br>● Automatikus képernyőzár (fontos)<br>● Jelszókezelő telepítése (ajánlott)<br>● Lemeztitkosítás bekapcsolása (ajánlott) | ● Software frissítések (hetente, automatikus)<br>● Biztonsági mentések készítése (hetente automatikus) |
| Mobil eszközök (mobil, tablet) | Közepes (adatszivárgás, adatvesztés, phishing, social engineering, alkalmazás fiók ellopása) | ● Kötelező PIN (fontos)<br>● Automatikus képernyőzár (fontos)<br>● Jelszókezelő telepítése (ajánlott)<br>● Lemeztitkosítás bekapcsolása (ajánlott)<br>● MDM (ajánlott) | ● Software frissítések (hetente, automatikus)<br>● Nem használt alkalmazások eltávolítása (havonta) |
| IoT, okos eszközök (okos csengő, kamera) | Alacsony (adatszivárgás) | ● Alapértelmezett jelszó megváltoztatása (fontos)<br>● Okos eszközök számának minimalizálása (ajánlott)<br>● Hálózat szegmentálás (ajánlott) | ● Software frissítések (havonta) |

# Eszköz független teendők

**Egyszeri:**

- MFA bekapcsolása ahol lehet (fontos)
- Dokumentumok és email-ek felhő alapú tárolása (ajánlott)

**Rendszeres:**

- Felhasználói oktatás (fontos)
- Eszköznyilvántartás karbantartása (fontos)
- Hozzáférések korlátozása (least privilege principle) (fontos)
- Beléptetési és kiléptetési checklist-ek karbantartása (ajánlott)
- Pandrive-ok és külső tárolók használatának leépítése (ajánlott)

# Magyarázat

**Kockázatok:**

**Adatszivárgás:** Bizalmas információk – például ügyféladatok, jelszavak vagy belső dokumentumok – illetéktelen kezekbe kerülnek. Ez történhet véletlenül (pl. rossz címzettnek küldött e-mail) vagy támadás miatt.

**Adatvesztés:** Fontos fájlok vagy információk végleg eltűnnek, például egy hibás merevlemez, emberi hiba vagy törlés miatt – és nincs róluk biztonsági mentés.

**Phishing (adathalászat):** Olyan átverés, amikor a támadó hamis e-mailt vagy weboldalt használ, hogy rávegye az áldozatot jelszó vagy banki adat megadására. Gyakran tűnik hivatalos levélnek (pl. „frissítsd a fiókod”).

**Social engineering (manipulatív támadás):** Amikor a támadó pszichológiai trükkökkel próbál rávenni valakit arra, hogy titkos információt adjon ki vagy valamilyen hibát kövessen el (pl. „az IT-s vagyok, add meg a jelszavad”).

**Ransomware (zsarolóvírus):** Egy olyan vírus, amely titkosítja a számítógépen lévő fájlokat, és csak pénzért (váltságdíjért) cserébe ígéri visszaállítani őket. A fájlok elérhetetlenné válnak.

**Alkalmazás fiók ellopása:** Valaki megszerzi és használja más személy bejelentkezési adatait egy online szolgáltatáshoz (pl. e-mail, Facebook, céges szoftver), és visszaél azzal.

# Fontos intézkedések

**Antivirus software telepítése**

Miért fontos: Felismeri és blokkolja a rosszindulatú kódokat.
Kockázat: Trójai, ransomware és más malware könnyen bejuthat.

Mi ellen véd: Phishing és social engineering

**Erős jelszó használata:**

Miért fontos: Az első védelmi vonal a jogosulatlan hozzáférés ellen.

Kockázat: Egy gyenge jelszót a támadók könnyen feltörhetnek feltörhetnek brute force vagy szótáras támadással.

Mi ellen véd: adatszivárgás, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás), ransomware

**Automatikus képernyőzár:**

Miért fontos: Ha egy eszközt felügyelet nélkül hagyunk, bárki hozzáférhet a rajta nyitva maradt alkalmazásokhoz és fájlokhoz.

Kockázat: Céges levelezés vagy fájlok átnézése/eltulajdonítása

Mi ellen véd: adatszivárgás

**Kötelező PIN:**

Miért fontos: PIN nélkül a készülék teljesen védtelen.

Kockázat: Üzleti vagy személyes információk kiszivárgása

Mi ellen véd: adatszivárgás, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

**Alapértelmezett jelszó megváltoztatása:**

Miért fontos: Sok IoT eszköz (pl. routerek, kamerák, nyomtatók) gyárilag egyszerű jelszavakkal érkezik, amelyeket a támadók jól ismernek.

Kockázat: Az eszköz távolról feltörhető, Belépési pont lehet a céges hálózatra

Mi ellen véd: adatszivárgás

**MFA bekapcsolása ahol lehet:**

Miért fontos: Az MFA egy extra biztonsági réteg, amely megnehezíti a támadók dolgát még akkor is, ha a jelszót már megszerezték

Kockázat: Egyetlen ellopott vagy gyenge jelszó teljes fiók hozzáférés adhat

Mi ellen véd: adatszivárgás, adatvesztés, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

**Felhasználói oktatás:**

Miért fontos: A felhasználók a leggyakoribb célpontjai a támadásoknak. Az oktatás csökkenti az emberi hibák arányát.

Kockázat: Továbbít bizalmas adatokat csalóknak, letölt és telepít fertőzött fájlokat, banki utalás csalóknak

Mi ellen véd: adatszivárgás, adatvesztés, phishing, social engineering, ransomware, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

**Eszköznyilvántartás karbantartása:**

Miért fontos: Egy naprakész eszközlista segít nyomon követni, hogy mely eszközök csatlakoznak a hálózathoz, milyen állapotban vannak, és kik használják őket.

Kockázat: Nincs rálátás a céges infrastruktúrára, elavult, nem frissített gépek maradhatnak a hálózaton

Mi ellen véd: Gyorsabb reagálás eszköz problémákra, sérülékenységekre, ellenőrizhetőség audit vagy incidens esetén

**Hozzáférések korlátozása:**

Miért fontos: A felhasználók csak azokhoz az adatokhoz és rendszerekhez férjenek hozzá, amelyekre a munkájukhoz feltétlenül szükség van.

Kockázat: Egy kompromittált fiókkal a támadó sokkal nagyobb kárt tud okozni, hibák vagy rosszindulatú szándék esetén több adat szivároghat vagy törlődhet

Mi ellen véd: Mi ellen véd: adatszivárgás, adatvesztés, phishing, social engineering, ransomware, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

# Ajánlott intézkedések

**Jelszókezelő telepítése:**

Miért fontos: Egy jelszókezelő segít erős, egyedi jelszavak létrehozásában és biztonságos tárolásában.

Kockázat: A dolgozók ugyanazt a jelszót használják több rendszerhez, vagy túl egyszerű jelszavakat jegyeznek meg.

Mi ellen véd: adatszivárgás, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

**Lemeztitkosítás bekapcsolása:**

Miért fontos: Ha egy eszköz elveszik vagy ellopják, az adattartalom titkosítása megakadályozza, hogy illetéktelenek hozzáférjenek a tárolt fájlokhoz.

Kockázat: fizikai hozzáférés esetén teljes adattartalom olvasható, GDPR-sértés személyes adatok illetéktelen kiszivárgása esetén

Mi ellen véd: adatszivárgás

**MDM (Mobile Device Management):**

Miért fontos:  A vállalat központilag tudja kezelni a dolgozók mobileszközeit: beállításokat, alkalmazásokat, biztonsági szabályokat.

Kockázat: Nem felügyelt eszközökön érzékeny céges adatok lehetnek, Eszköz elvesztése esetén nem lehet törölni a tartalmát távolról, Inkonzisztens biztonsági beállítások

Mi ellen véd: adatszivárgás, alkalmazásokkal való visszaélés (pl. banki app, Facebook fiók lopás)

**IoT eszközök számának minimalizálása:**

Miért fontos: Minél több IoT eszköz van, annál nagyobb a támadási felület

Kockázat: Biztonsági frissítései gyakran elmaradnak, sebezhetőségeket rejtenek.

Mi ellen véd: adatszivárgás, adatvesztés

**IoT eszközök hálózati szegmentálása:**

Miért fontos: Az IoT eszközöket külön hálózatba (pl. VLAN, vendéghálózat) helyezve elkülöníthetők a céges számítógépektől és adatforgalomtól.

Kockázat: Egy feltört IoT eszköz hozzáférhet a teljes belső hálózathoz

Mi ellen véd: adatszivárgás, adatvesztés

**Dokumentumok és email-ek felhő alapú tárolása:**

Miért fontos: A modern felhőszolgáltatások biztonságos, naprakész és elérhető környezetet biztosítanak fájlok, e-mailek és kollaborációs munkafolyamatok számára. A hozzáférés és módosítás nyomon követhető, a mentés automatikus.

Kockázat: Adatok elveszhetnek lokális gépleállás vagy meghibásodás miatt, Nehezített együttműködés, verziókezelési problémák, Nem visszakereshető adatvesztés (pl. egy pendrive elvesztésével)

Mi ellen véd: adatszivárgás, adatvesztés, ransomware

**Beléptetési és kiléptetési checklist-ek karbantartása:**

Miért fontos: minden jogosultság, eszköz és adatvagyon visszavonása kulcsfontosságú az adatbiztonság szempontjából

Kockázat: Volt dolgozó fiókja aktív marad és beléphet, Céges adatok megmaradhatnak privát eszközön

Mi ellen véd: adatszivárgás, adatvesztés

**Pendrive-ok és külső tárolók használatának leépítése:**

Miért fontos: A hordozható tárolók könnyen elveszhetnek

Kockázat: Fizikai adatlopás, Kontrollálatlan adatmásolás

Mi ellen véd: adatszivárgás

# Eszköznyilvántartó táblázatok

**Számítógépek és laptop-ok**

| Eszköz azonosító | Eszköz neve | Típus | Operációs rendszer | Antivirus telepítve | Jelszókezelő | Lemeztitko-sítás | Erős jelszó | Automatikus képernyőzár | Tulajdonos/ Felhasználó | Utolsó frissítés |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

## Példa:

| Eszköz azonosító | Eszköz neve | Típus | Operációs rendszer | Antivirus telepítve | Jelszókezelő | Lemeztitkosítás | Erős jelszó | Automatikus képernyőzár | Tulajdonos/ Felhasználó | Utolsó frissítés |
|---|---|---|---|---|---|---|---|---|---|---|
| PC-001 | SALES-PC | Asztali | Windows 11 Pro | Windows Defender | Igen | Nem | Igen | Igen | Közös, értékesítési csapat | 2025-06-04 |
| LAPTOP-001 | DEV-001 | Laptop | Linux | ClamAV | Igen | Igen | Igen | Igen | Szabó Tamás | 2025-06-06 |

# Mobil eszközök

| Eszköz azonosító | Eszköz neve | Típus | MDM | Jelszókezelő | Titkosítás | PIN/Jelszó beállítva | Automatikus képernyőzár | Tulajdonos/F elhasználó | Utolsó frissítés |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Példa:**

| Eszköz azonosító | Eszköz neve | Típus | MDM | Jelszókezelő | Titkosítás | PIN/Jelszó beállítva | Automatikus képernyőzár | Tulajdonos/ Felhasználó | Utolsó frissítés |
|---|---|---|---|---|---|---|---|---|---|
| MOB-001 | SALES-PHONE | Samsung A15 | Igen | Igen | Nem | Igen | Igen | Közös, értékesítési csapat | 2025-06-04 |
| TABLET-001 | FINANCE-TABLET | iPad gen 10. | Nem | Igen | Igen | Igen | Igen | Nagy Éva | 2025-06-04 |