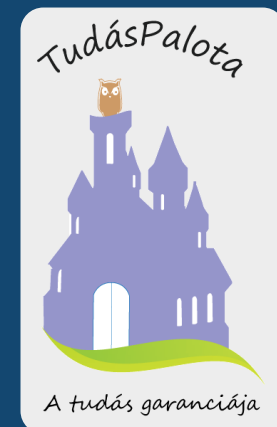


*VÁLLALKOZÁSUNK  
VÉDELME A  
DIGITÁLIS  
KORSZAKBAN*

# KIBERBIZTONSÁG





# Nyilas Gábor



[level@nyilasgabor.hu](mailto:level@nyilasgabor.hu)



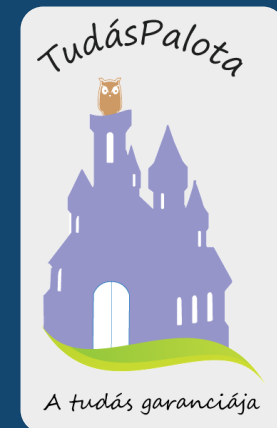
[nyilasgabor.hu](http://nyilasgabor.hu)



[linkedin.com/in/gabornyilas/](https://www.linkedin.com/in/gabornyilas/)



+36 30 6850657



# VÉGZETTSÉG



- Okleveles informatikus mérnök (MSc.)
- Okleveles közgazdász (MSc.)



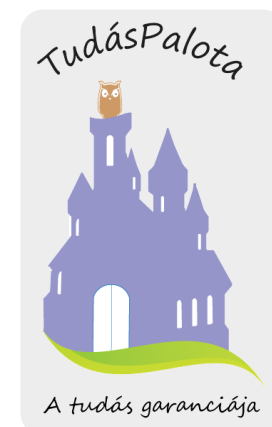
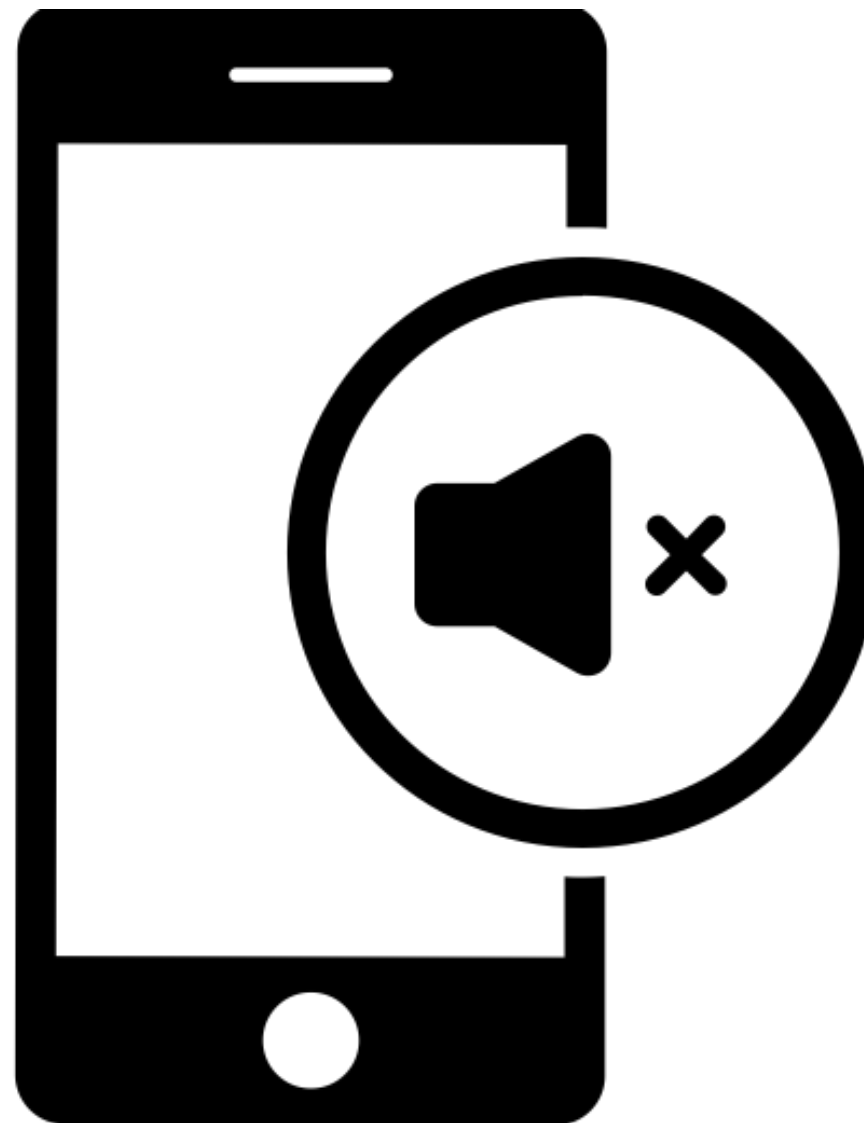
# TAPASZTALAT

- IT mentor (3 év)
  - Full-stack szoftverfejlesztők
  - Java Backend fejlesztők
  - Cybersecurity tanácsadók
  - Tesztautomtizálók
- Vezető szoftvermérnök (10+ év)
- IT csoportvezető (2,5 év)
- IT tréner (9 év)
  - Irodai alkalmazások
  - Infrastruktúra
  - Webdesign
  - Programozás

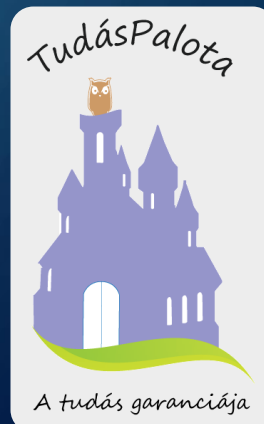


# KERETEK

- 75 perc előadás
- 15 perc kérdés-válasz szekció



# MENETREND



# BEVEZETÉS

## 01

Digitális világban élünk, ahol az adat olyan értékes mint egykor az olaj volt.

## 02

A kiberbiztonság már nem csak IT-kérdés, hanem **stratégiai üzleti prioritás**.

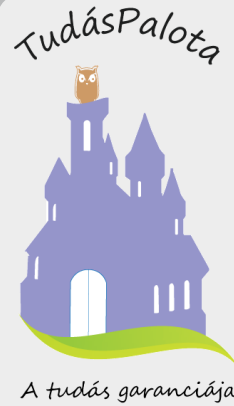
## 03

Előadásom bemutatja, hogyan védekezhetünk hatékonyan a kiberfenyegetések ellen, és miért elengedhetetlen a kiberbiztonság az üzleti sikerhez.



# 1. ADATVÉDELEM ÉS ÜGYFÉLBIZALOM MEGŐRZÉSE

SZEMÉLYES ADATOK, PÉNZÜGYI INFORMÁCIÓK,  
SZELLEMI TULAJDON

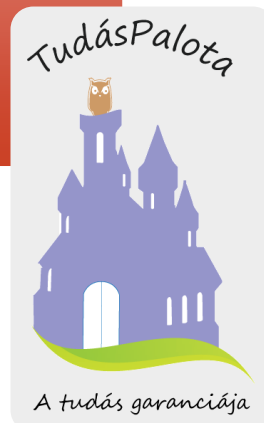


ADATVÉDELMI  
INCIDENSEK  
KÖVETKEZMÉNYEI

**Ügyfélbizalom elvesztése:**  
Nehezen visszaállítható

**Hírnév romlása:**  
Hosszú távú károkat okozhat

**Pénzügyi veszteségek:**  
Bírságok, kártérítések



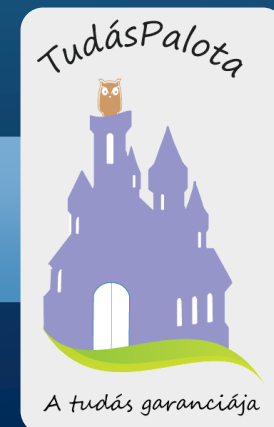
# STRATÉGIÁK AZ ADATVÉDELEMRE

**Titkosítás:** Adatok védelme tárolás és továbbítás során.

**Hozzáférési jogosultságok kezelése:** Csak a szükséges jogosultságok biztosítása.

**Adatmentés és helyreállítás:** Rendszeres mentés, incidens esetén gyors helyreállítás.

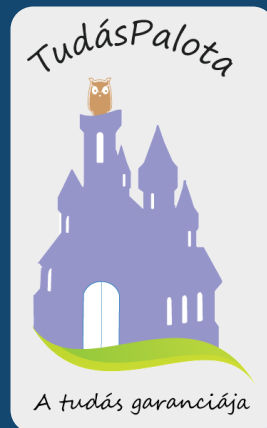
**Adatvédelmi szabályzatok:** Világos irányelvek az adatkezelésre.



## 2. KIBERFENYEGETÉSEK ELLENI VÉDEKEZÉS

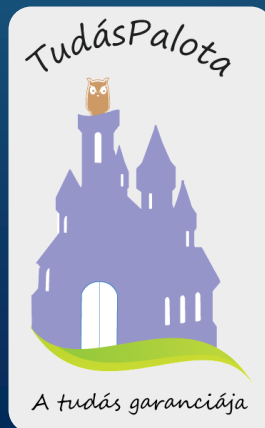
## GYAKORI KIBERFENYEGETÉSEK

- **Zsarolóvírusok (Ransomware):**  
Adatok titkosítása, a visszaállítás csak váltságdíj fejében lehetséges
- **Adathalászat (Phishing):**  
Hamis üzenetekkel érzékeny adatok megszerzése
- **DDoS támadások:**  
Szolgáltatások elérhetetlenné tétele
- **Rosszindulatú szoftverek (Malware):**  
Vírusok, férgek, kémprogramok



# VÉDEKEZÉSI STRATÉGIÁK

- **Tűzfalak és behatolásvédelmi rendszerek (IPS/IDS):**  
Védelmet nyújtanak a hálózat külső támadásaival szemben
- **Antivírus és végpontvédelem:**  
Eszközök védelme rosszindulatú szoftverek ellen
- **Biztonsági frissítések:**  
Szoftverek és rendszerek naprakészen tartása
- **Biztonsági mentések:**  
Rendszeres és megbízható adatmentések
- **Incident Response Plan:**  
Előre kidolgozott terv kiberbiztonsági incidensek kezelésére



### 3. SZABÁLYOZÁSOK ÉS JOGI MEGFELELÉS

TudásPalota



A tudás garanciája

## FŐBB SZABÁLYOZÁSOK

---

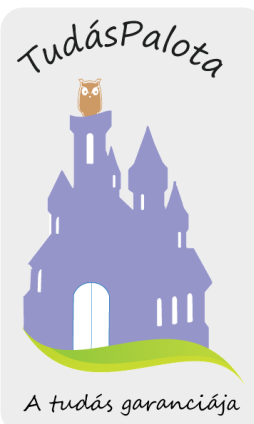
**GDPR (Általános Adatvédelmi Rendelet):**  
EU-s adatvédelmi szabályozás, amely szigorú előírásokat fogalmaz meg a személyes adatok kezelésére.

---

**NIS2 irányelv:**  
Az EU kiberbiztonsági irányelve, melynek célja a kritikus infrastruktúrák és digitális szolgáltatások biztonságának garantálása.

---

**Egyéb iparági specifikus szabályozások:**  
Például PCI DSS  
(bankkártya adatok kezelése).



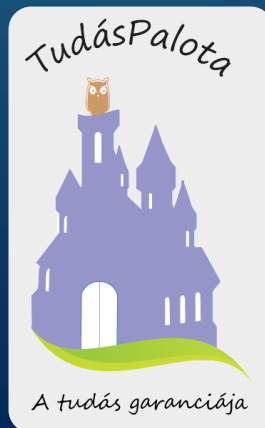
# A MEGFELELÉS FONTOSSÁGA

- **Bírságok elkerülése:** A szabályozások megsértése súlyos pénzügyi szankciókat vonhat maga után.
- **Jogi felelősség:** A vállalat vezetői és az IT szakemberek is felelősséggel tartoznak.
- **Üzleti partnerek elvárásai:** Sok partner megköveteli a jogi megfelelést.



# HOGYAN BIZTOSÍTHATÓ A MEGFELELÉS?

- **Jogi tanácsadás:** Szakértő bevonása a szabályozások értelmezéséhez.
- **Folyamatos auditálás:** Rendszeres ellenőrzések a megfelelőség fenntartásához.
- **Dokumentáció:** Az adatkezelési és biztonsági folyamatok részletes dokumentálása.



# 4. ÜZLETI FOLYAMATOK ZAVARTALANSÁGÁNAK BIZTOSÍTÁSA

# A KIBERBIZTONSÁGI INCIDENSEK HATÁSA

- **Működés leállása:** Pénzügyi veszteség, ügyfélvesztés.
- **Adatvesztés:** Elveszett vagy sérült üzleti adatok.
- **Szolgáltatás kiesés:** Elérhetetlenné váló weboldalak, rendszerek.



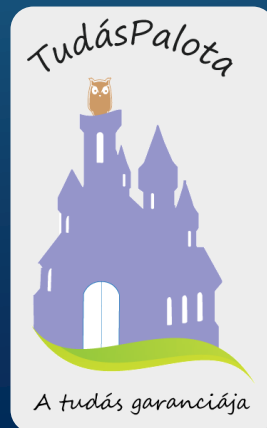
# ÜZLETMENET FOLYTONOSSÁGI TERV (BCP) ÉS KATASZTRÓFA- HELYREÁLLÍTÁS (DRP)

- **BCP:** Vészhelyzet esetére, az üzleti tevékenység fenntartására irányuló terv.
- **DRP:** Katasztrófa után az IT rendszerek és adatok helyreállítására vonatkozó terv.



# ESZKÖZÖK ÉS MÓDSZEREK:

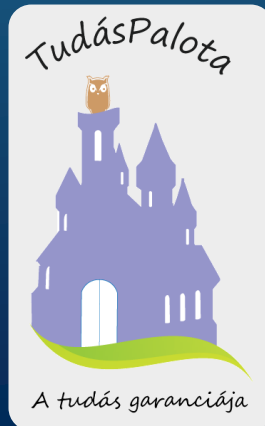
- **Redundáns rendszerek:** Többszörözött szerverek és hálózatok a kiesés minimalizálására.
- **Cloud alapú megoldások:** Magas rendelkezésre állás és rugalmasság.
- **Rendszeres tesztelés:** A BCP és DRP tervek hatékonyságának ellenőrzése.



# 5. KÖLTSÉGMEGTAKARÍTÁS ÉS PÉNZÜGYI VESZTESÉGEK ELKERÜLÉSE

# A KIBERBIZTONSÁGI BEFEKTETÉS MEGTÉRÜLÉSE

- **Incidenskezelés költségeinek elkerülése:** Helyreállítás, jogi díjak, PR költségek megtakarítása.
- **Bírságok elkerülése:** A jogi megfelelés hiánya miatti büntetések elkerülése.
- **Hírnévvesztés elkerülése:** A rossz hírnév közvetett pénzügyi hatásainak kiküszöbölése.
- **Adatvesztés megelőzése:** A gyakran pótolhatatlan értékű adatok biztonságban tartása.



# PÉNZÜGYI VESZTESÉGEK

- **Közvetlen költségek:** Helyreállítás, vizsgálatok, jogi díjak.
- **Közvetett költségek:** Elmaradt bevétel, ügyfélvesztés, márkáérték csökkenése.

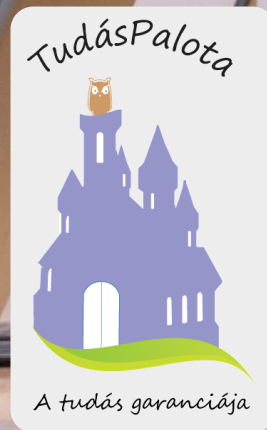


## KÖLTSÉGHATÉKONY MEGOLDÁSOK

- **Megelőzés:** Kevesebb pénzbe kerül a megelőzés, mint a helyreállítás.
- **Kockázatkezelés:** Azon területekre kell fókuszálni, ahol a legnagyobb a kockázat.
- **Biztosítás:** Kiberbiztosítás kötése a pénzügyi kockázatok csökkentése érdekében.

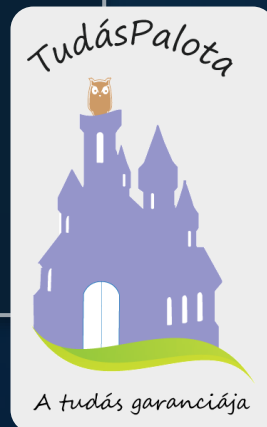


# 6. MUNKAVÁLLALÓI TUDATOSSÁG NÖVELTÉSE



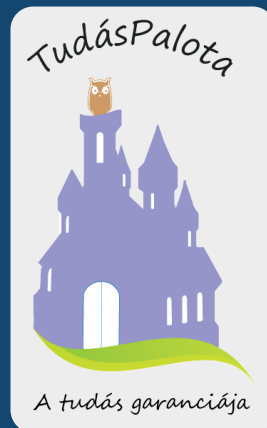
# AZ EMBERI TÉNYEZŐ

*A kiberbiztonsági lánc leggyengébb szeme és  
egyben a legerősebb védelmi vonala.*



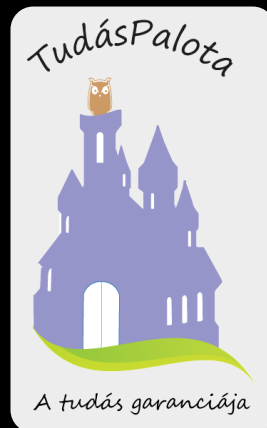
## GYAKORI HIBÁK:

- **Gyenge jelszavak:** Könnyen feltörhetők.
- **Adathalász levelekre kattintás:** Kártékony oldalakra vezető linkek megnyitása.
- **Nem biztonságos Wi-Fi használata:** Adatforgalom lehallgatásának veszélye.
- **Ismeretlen eszközök csatlakoztatása:** Vírusok behurcolása.



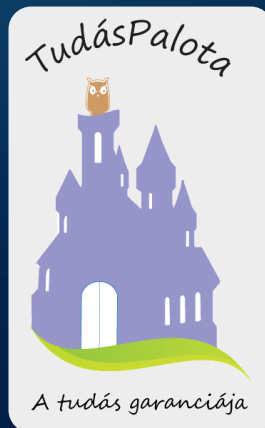
# KÉPZÉSEK ÉS TUDATOSSÁG NÖVEELÉS

- **Rendszeres tréningek:** Kiberbiztonsági alapok, friss információ aktuális fenyegetésekről.
- **Szimulált adathalász támadások:** A munkavállalók reakciójának tesztelése.
- **Biztonsági szabályzatok kommunikálása:** Világos és érthető iránymutatások.
- **Folyamatos tájékoztatás:** Hírek, figyelmeztetések a legújabb fenyegetésekről.
- **Pozitív megerősítés:**  
Jutalom a helyes viselkedésért.



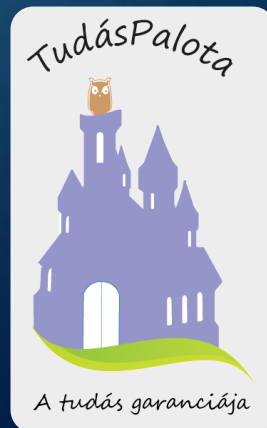
- A kiberbiztonság nem egyszeri feladat, hanem **folyamatos erőfeszítés**.
- A proaktív megközelítés kulcsfontosságú.
- Az egész szervezetnek együtt kell működnie a védekezésben.

# ZÁRÓ GONDOLATOK



KÉRDÉSEK?

és válaszok.



תודה  
Dankie Gracias  
Спасибо شكراً  
Merci Takk  
Köszönjük Terima kasih  
Grazie Dziękujemy Děkojame  
Ďakujeme Vielen Dank Paldies  
Kiitos Täname teid 谢谢  
**Thank You** Tak  
感謝您 Obrigado Teşekkür Ederiz  
Σας ευχαριστούμε 감사합니다  
Будьдуду  
Bedankt Děkuje vám  
ありがとうございます  
Tack

