white hat
IT SECURITY

Incidensek tanulságai

Fehér Sándor
CEO, White Hat IT Security

Sándor **FEHÉR**

- White Hat IT Security **CEO**
- Incidensreagáló menedzser
- Nemzetbiztonsági múlt és **20+ éves** IT biztonsági tapasztalat
- Egyetemi előadó
- **OSCP, OSCE, OSWP, CISM** tanúsítványok
- **ISO27001** vezető auditor
- Mérnök informatikus és programtervező matematikus diplomák
- a **HCC** alapítója
- a **CYAN** választott tagja
- a **GFCRC** vezetőségi tagja
- egy kisgyermek apukája

white hat
IT SECURITY

white hat

IT SECURITY

SOC as a Service

Incident Response

Penetration testing

NIS2 & ISO27001

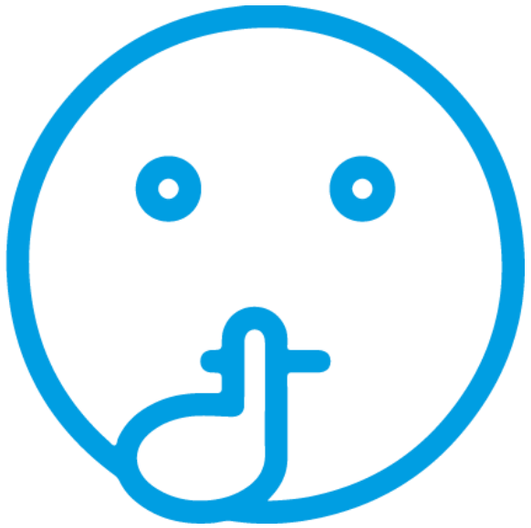
Egy kibertámadás költségei

- Árbevétel kiesése
- Incidens reagálók díja
- Integrátorok és egyéb partnerek díja
- Régóta halogatott ITB beruházások költsége
- Kártérítések rövid és közép távon
- Elvesztett üzletek
- Elvesztett ügyfelek
- Hatósági bírság
- Reputációs kár

Az éves árbevétel kb. 1-5%-a

white hat
IT SECURITY

Jogi nyilatkozat



- Az incidensreagáló szakemberek szigorú titoktartási megállapodás (NDA) hatálya alatt állnak
- Néhány tényt emiatt elfedtünk vagy megváltoztattunk
- Minden hasonlóság a valósággal pusztán a véletlen műve ;)

white hat
IT SECURITY

IR esettanulmány | A hiányzó MFA?

DACH

autóipari beszállító

zsarolóvírus

CEO-t adathalász támadás érte

A háttériroda hálózata leállt

Emaileket loptak el

4,5 napra leállt a logisztika

~700k EUR veszteség

A támadás oka:
hiányzó MFA

white hat
IT SECURITY

IR esettanulmány | Hamis felvásárlási folyamat

EU

turizmus

email fraud
/ CFO fraud

CEO nyaral (Facebookon posztolja)

CFO célzása péntek délután

Nyomás alatt 20k EUR-t utaltak át

A támadás oka:

belső biztonsági szabályok hiánya

white hat
IT SECURITY

IR esettanulmány | Belső támadó

CE

ipari beszállító

belső támadó

4 különböző ITS incidens 6 hónap alatt

A 3. incidens után hívtak incidensreagáló csapatot

Tűzoltó-szindrómával rendelkező rendszergazda

A veszteség mértéke ismeretlen

A támadás oka:
security kontrollok hiánya

white hat
IT SECURITY

IR esettanulmány | EU szintű GDPR incidens

EU

divatipar

zsarolóvírus +
kettős zsarolás

A háttériroda és a webshop kompromittálódott

Személyes adat + egészségügyi adat

12 ország hatóságait vonták be

22 ezer ügyfelet érintett 12 EU országban

A támadás oka:

emailbiztonság hiányosságai és frissítések hiánya

white hat
IT SECURITY

white hat
IT SECURITY

Incidens esetén:

+36 1 833 3866

Think like an adversary – act like a white hat.