

1 PERC VAGY 1 ÉV?

INFORMATIKAI TÁMADÁSOK KIVITELEZÉSE
NEM HOLLYWOODI MÓDSZEREKKEL



Veres-Szentkirályi András 2019-11-14



Veres-Szentkirályi András

- ▶ OSCP, GWAPT, SISE
- ▶ Silent Signal társalapító (2009-)
- ▶ IT biztonsági szakértő, *pentester*
 - ▶ webalkalmazások
 - ▶ Wi-Fi hálózatok
 - ▶ mobilalkalmazások (appok)
- ▶ 15+ év tapasztalat
- ▶ önálló szakmai kutatások

Menetrend

1 Bevezetés

- 1. célpont: sima ügy
- 2. célpont: kisebb nehézségek
- 3. célpont: kemény dió

Egy fontos gondolat előszó helyett



“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break.”

– Bruce Schneier (1998. október 15.)

<https://www.schneier.com/crypto-gram-9810.html#cipherdesign>

Grand Brighton Hotel, 1984



“Today we were unlucky, but remember **we only have to be lucky once. You will have to be lucky always.**”

– Provisional IRA (1984. október 13.)

Taylor, Peter (2001). *Brits: The War Against the IRA*. Bloomsbury Publishing. p. 265. ISBN 0-7475-5806-X.

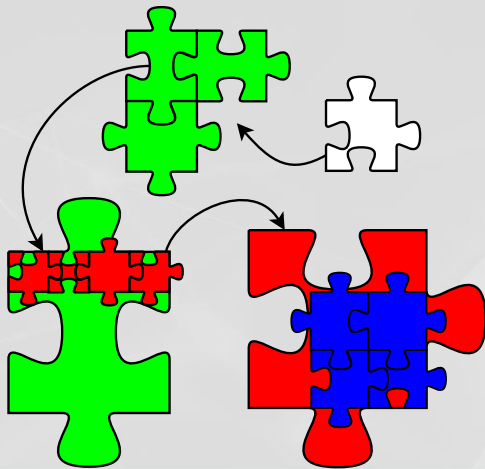
https://en.wikipedia.org/wiki/Brighton_hotel_bombing

Sérülékenységek forrásai



- ▶ Szervezeten kívülről
 - ▶ hosszú bizalmi lánc
 - ▶ szoftvergyártó hibát követ el
 - ▶ idővel kijavítja
- ▶ Szervezeten belülről $\Leftarrow$ **ezzel kezdjük**
 - ▶ kiszervezett IT is ide tartozik
 - ▶ hibás beállítások
 - ▶ nem (időben) telepített frissítések

Az **információ** nem fizikai áru:
tetszőleges példányszámban másolható,
ellopása nem feltétlenül kelt feltűnést.



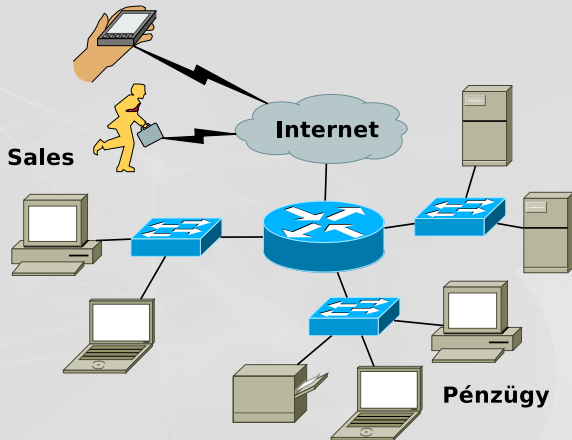
Menetrend

- Bevezetés
- 1. célpont: sima ügy
- 2. célpont: kisebb nehézségek
- 3. célpont: kemény dió

Cég IT-biztonsági érettségi szintje



- ▶ belső szolgáltatások saját szerveren
 - ▶ legyen elérhető futároknak és sales-eseknek kívülről bármikor
- ▶ biztonság nem visz magával csomagot
 - ▶ 0 költségvetés



- ▶ internet felőli felderítés
- ▶ gyenge pont azonosítása
- ▶ behatolás
- ▶ további védelem hiányában teljes hozzáférés

Intermezzo: Milyen a jó jelszó?



Szerinted melyik a legerősebb jelszó az alábbiak közül?

1. Micimacko2019!
2. correcthorsebatterystaple
3. SiX#e'9k

Hányat kellene próbálkozni?



- ▶ Micimacko2019!

$100.000 \text{ szó} \times 10.000 \text{ szám} \times 16 \text{ szimbólum} = 16.000.000.000 = 1,6 \cdot 10^{10}$ lehetőség

- ▶ correcthorsebatterystaple

$100.000^4 \text{ szó} = 100.000.000.000.000.000.000 = 10^{20}$ lehetőség

- ▶ SiX#e'9k

$96^8 \text{ karakter (kis-/nagybetű/szám/speciális)} = 7.213.895.789.838.336 \approx 7 \cdot 10^{15}$ lehetőség

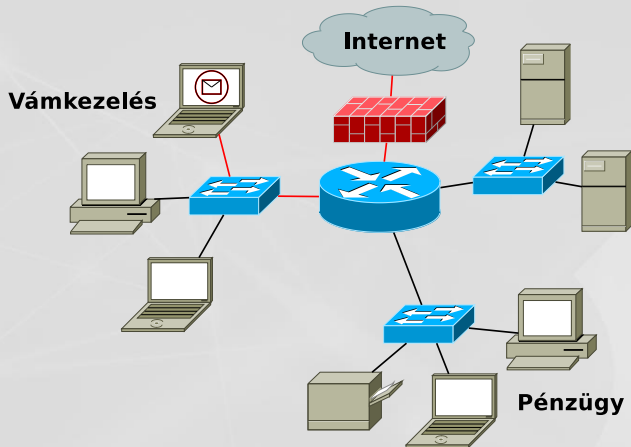
Menetrend

- 
- Bevezetés
 - 1. célpont: sima ügy
 - 3 2. célpont: kisebb nehézségek
 - 3. célpont: kemény dió

Cég IT-biztonsági érettségi szintje



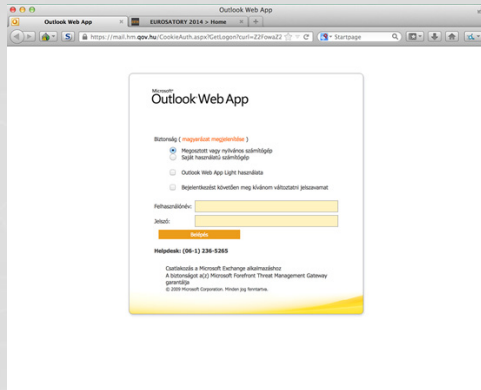
- ▶ internet felől semmi látnivaló
- ▶ munkatársak megfelelő jelszavakat használnak
- ▶ vámkezelés miatt e-mail lehetőség
- ▶ nincsenek belső „válaszfalak”



- ▶ alapos céges felderítés
- ▶ belépési pont azonosítása
- ▶ phishing oldal létrehozása
- ▶ phishing levél beküldése
- ▶ felhasználó megszemélyesítése

  <https://mail.hm.gov.hu/>

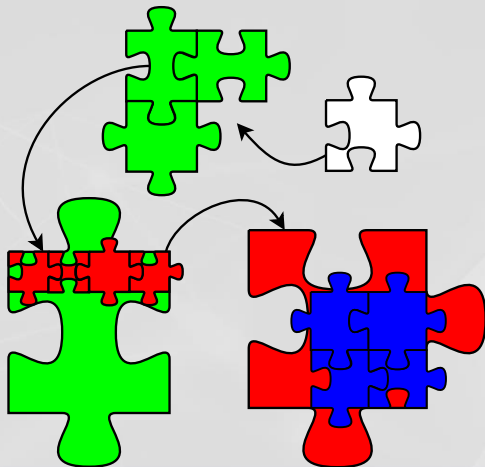
  <https://mail.hm.qov.hu/>



Sérülékenységek forrásai

- ▶ Szervezeten kívülről $\Leftarrow$ **itt folytatjuk**
 - ▶ hosszú bizalmi lánc
 - ▶ szoftvergyártó hibát követ el
 - ▶ idővel kijavítja
- ▶ Szervezeten belülről
 - ▶ kiszervezett IT is ide tartozik
 - ▶ hibás beállítások
 - ▶ nem (időben) telepített frissítések

Az **információ** nem fizikai áru:
tetszőleges példányszámban másolható,
ellopása nem feltétlenül kelt feltűnést.



Intermezzo: Mennyi időnk van?



Szerinted átlagosan mennyi idő egy gyártói javítás megjelenése után elkészíteni a javított sérülékenységet kihasználó támadást?

▶ **11 nap**

▶ **22 nap**

▶ **44 nap**

▶ **88 nap**

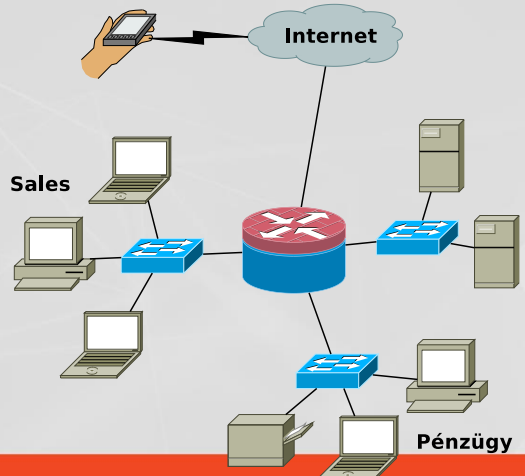
Menetrend

- Bevezetés
- 1. célpont: sima ügy
- 2. célpont: kisebb nehézségek
- ④ 3. célpont: kemény dió

Cég IT-biztonsági érettségi szintje



- ▶ hálózat izolált részekre van szedve
 - ▶ ezek között ellenőrzött átjárás
- ▶ modern kétfaktoros azonosítás
 - ▶ phishingnek esélye sincs



- ▶ lassú és nagyon alapos céges felderítés
 - ▶ rendszergazdák IT fórumokon azonosítható kérdései
 - ▶ álláshirdetéseken megjelölt technológiák
 - ▶ nyilvános sajtóbejelentések, beszállítói marketinganyagok
 - ▶ alacsonynak besorolt információszivárgás sérülékenységek
- ▶ sok-sok várakozás
 - ▶ mikor települ egy frissítés későn
 - ▶ mikor kerül engedélyezésre valami ideiglenesen
 - ▶ „A gép forog, az alkotó pihen.”
- ▶ lépésről-lépésre haladás
 - ▶ minden lépés és perc magában hordozza a lebukás esélyét

- ▶ ezek fikcionális cégek voltak
- ▶ mindenki máshol helyezkedik el ezen a skálán
- ▶ konkrétumok is hasznosak lehetnek...
- ▶ ...de mindenki a saját lehetőségein belül tud egy kicsit előre menni
- ▶ cél: támadói siker kockázat csökkentése

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu



facebook.com/silentsignal.hu



@SilentSignalHU



@dn3t

