# SICONTACT™

**biztonság** a digitális világban

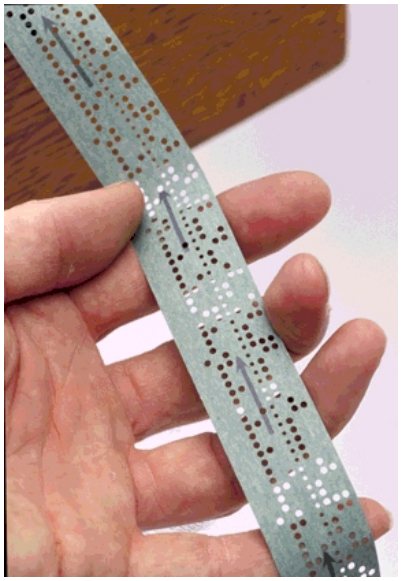
SICONTACT
biztonság a digitális világban

# Biztonsági megoldások helye a vállalati rendszerben

## Hol és mit kell mindenképpen védeni?

ESET Cyberoam AIDA64

# Bemutatkozás



Csizmazia-Darab István

Sicontact Kft., az ESET magyarországi képviselete
csizmazia.istvan@sicontact.hu
antivirus.blog.hu

1979-1980: FÜTI, R20/R40 nagygépes operátor
1981-1987: HUNGAROTON hanglemez stúdió, stúdiós
1988-1990: Volán Tefu Rt, programozó
1990-2000: ERŐTERV Rt, programozó + vírusadmin egy 400 gépes hálóban
2001-2003: 2F Kft, F-Secure és Kaspersky support, Vírus Híradó főszerkesztő
2003-2005: IDG, PC World online szerkesztő, újságíró
2006-2007: Virus Buster Kft, kártevő elemző, sajtóhír felelős
2007-2014: Sicontact Kft, IT biztonsági szakértő

Ha fiatal lennék, ma is ugyenezt a területet választanám...

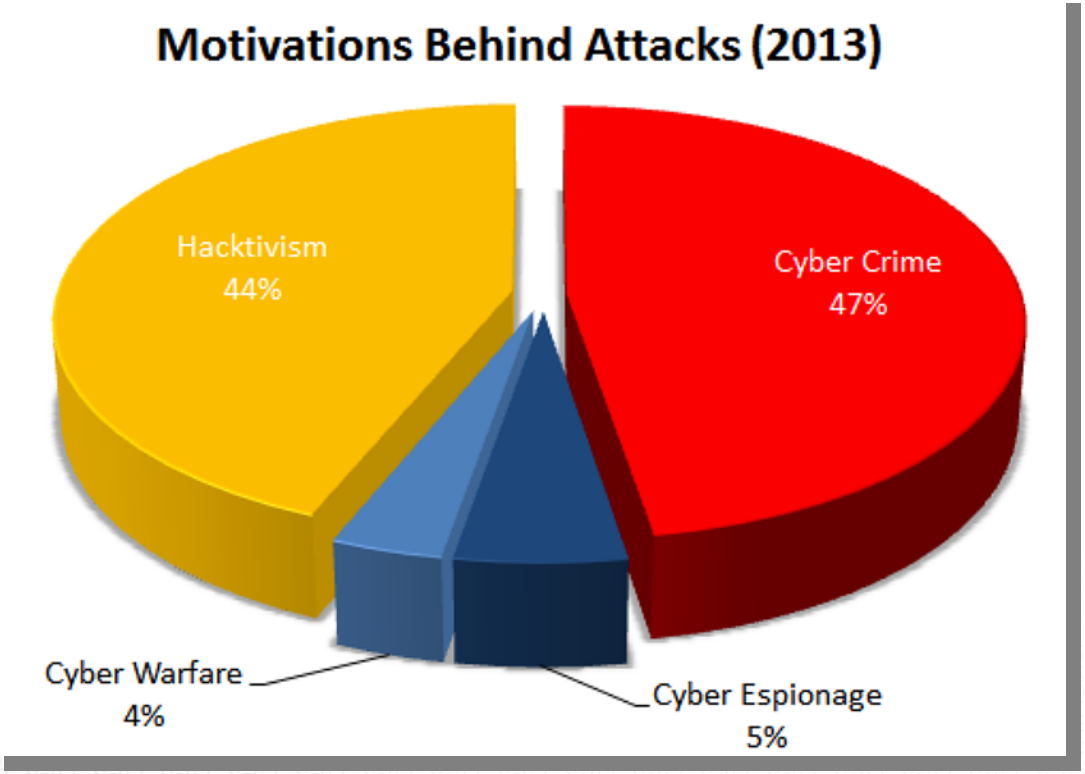
# Néhány friss adat a biztonságról

- A támadások száma, kifinomultsága nő (APT, folyamatos fenyegetések)

- Egyre olcsóbb támadó eszközök, botnetek

- Egyre kisebb vállalatok is célpontok

- Életünk része lett az állandó támadás

# A befektetés költsége VS. a káresemény költsége

- Az informatika a gazdasági teljesítés alappillére
- Az üzletfolytonosság kulcsfontosságú
- Nélküle nem lehet profitot termelni, ezért költeni kell rá

**Például**

- 2011-ben 20 támadás a SONY ellen
- elhallgatták, nem kezelték
- összességében 24 milliárd USD veszteség
- megfelelő védekezés 10 ezer dolláros költség lett volna

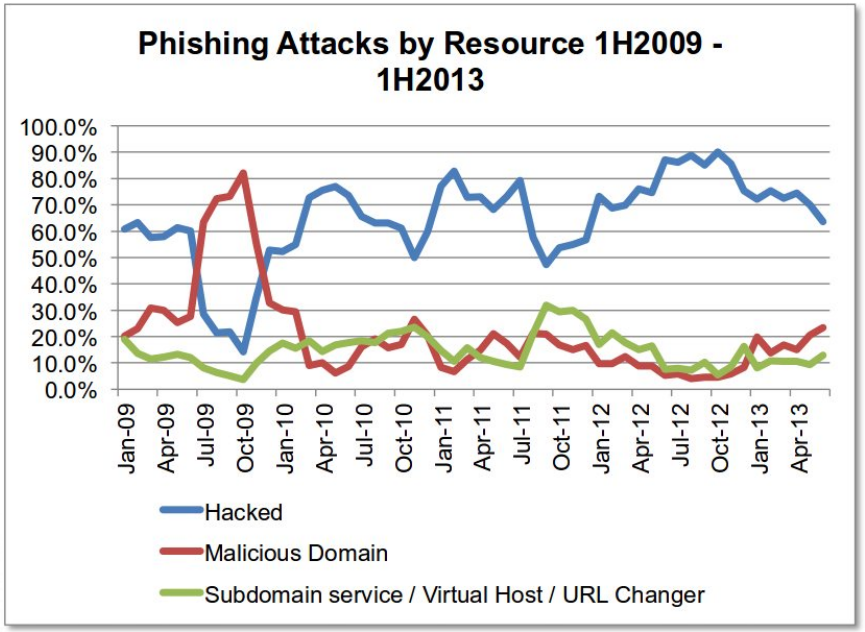
*(Shakeel Tufail, HP Enterprise Security Solutions)*

2008. USA
- Több pénz az elektronikus csalásokból, mint a drogkereskedelemből: 105 mrdUSD

# Kiemelten fontos a szerverek védelme

- **A spamek 27%-a feltört szerverről érkezik**
- **Az üzemeltetők gyakran maguktól nem is veszik észre**
- **Sokszor csak konkrét ügyfél panasz nyomán kezdenek el vizsgálódni**

*(Anti-Phishing Working Group 2013.)*




**Például**

- 2014. júliusban feltörték az Európai Központi Bank külső szerverét
- konferenciák, üzleti események regisztrációs és személyes adatok
- Az EKB mindvégig nem észlelte a beavatkozást
- a szerver feltöréséről egy üzenetből értesültek
- a támadók a lopott információk visszatartásáért cserébe pénzt követeltek

# Az Adobe incidens - Tanulságok

- 2013. október - Előbb „csak” 2.9, utána 38 elismert ellopott ügyféladat

- 2013. november - 130 millió és forrás (Acrobat, ColdFusion, CF Builder, Photoshop )

- Nyilvánosságra kerültek a jelszavak - “adobe.users.tar.gz.torrent”

- Sok felhasználó a jelszó-emlékeztetőkben egy az egyben megadta a jelszavát

1. "123456" - 2,000,000
2. "123456789" - 446,000
3. "password" - 345,000

# Az Adobe incidens - További nem várt mellékhatások

- Adobe-bal közös szerveren lévő Corporate-Car-Online-t is feltörték

- Luxus limuzin kölcsönző, 850 ezer ügyfél a nyilvántartási adatbázisban

- Cégvezetők, sztárok, politikusok: Donald Trump, Tom Hanks, stb.

- A fontos emberek útvonalai: emberrablás, merénylet, ipari kémkedés

- 241 ezer hitelkártya adata

- a lopott adatok alapján testre-szabottabb APT támadások, célzott adathalászat, stb.

# Tipikus cégek elleni támadási vektorok 1.

**Ipari kémkedés a Facebook-on**


1. Menedzser szerepelt egy korábbi konferencián

2. A Facebookon 2-3 héttel később jön egy „referens”

3. Általában elfogadja az ismerősnek jelölést

4. A „kolléga” felajánl neki:
   - Böngészőkiegészítő
   - PDF szakmai dokumentum (lásd New York Times, 2012. szeptember-december)
   - Link

**Például**

Csak Németországban az ilyen dokumentált esetekből évente több száz van

ESET Cyberoam AIDA64

# Tipikus cégek elleni támadási vektorok 2.

- Jelszavak, munkafegyelem, social engineering

- Nehéz elfogadni, elhinni a belső fenyegetés veszélyét (Kevin Mitnick)

- A támadások, adatszivárgások jelentős részében van belső szál


**Például**

Edward Snowden (2013) kollégák hozzáféréseit is használta, 20-25 account

# Hatékony védekezés 1.

**Biztonsági alkalmazások használata**

- végpont védelem

- szerver védelem

- nincs támadhatatlan platform


**Például**

2011-2012. 600 ezer Flashback botnetes fertőzött Macintosh gép

2013. április Linux/Cdorked.A Apache szervereket fertőző backdoor

ESET Cyberoam AIDA64

# Hatékony védekezés 2.

**Hibajavítás, frissen tartás, automatizált patchmanagement I.**

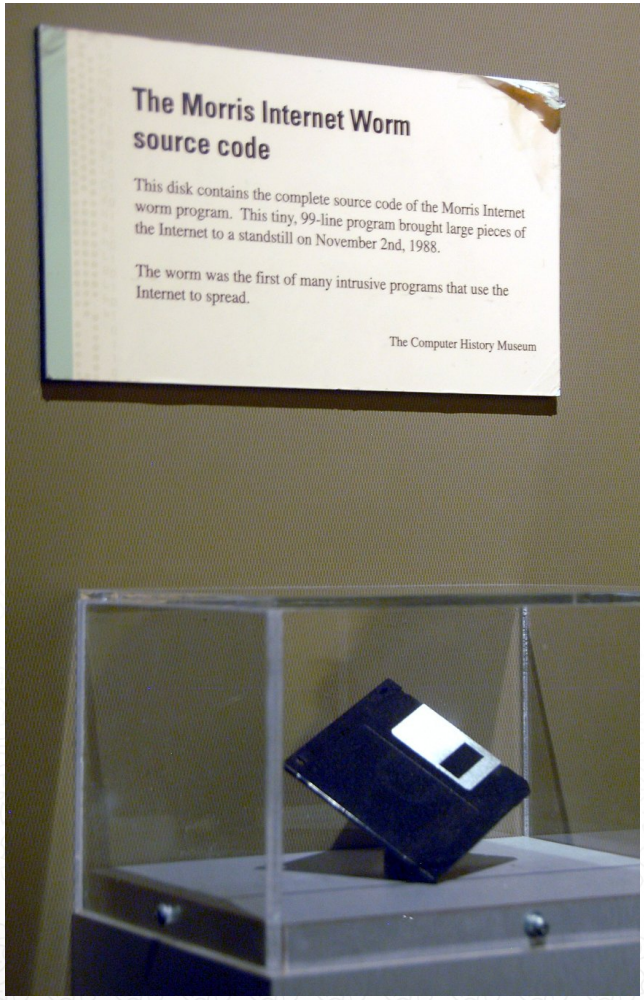
- 2013. november - 25 éves a Morris-worm

- 1988. puffertúlcsordulásos támadás,

- tetszőleges parancs végrehajtása a kompromittált gépeken

- Senki nem gondolta még akkor, hogy éppen a frissítés hiánya okozhat fertőzést

- Nem csak OS, hanem minden alkalmazás, és a virtuális környezetek is



# Hatékony védekezés 3.

**Hibajavítás, frissen tartás, automatizált patchmanagement II.**

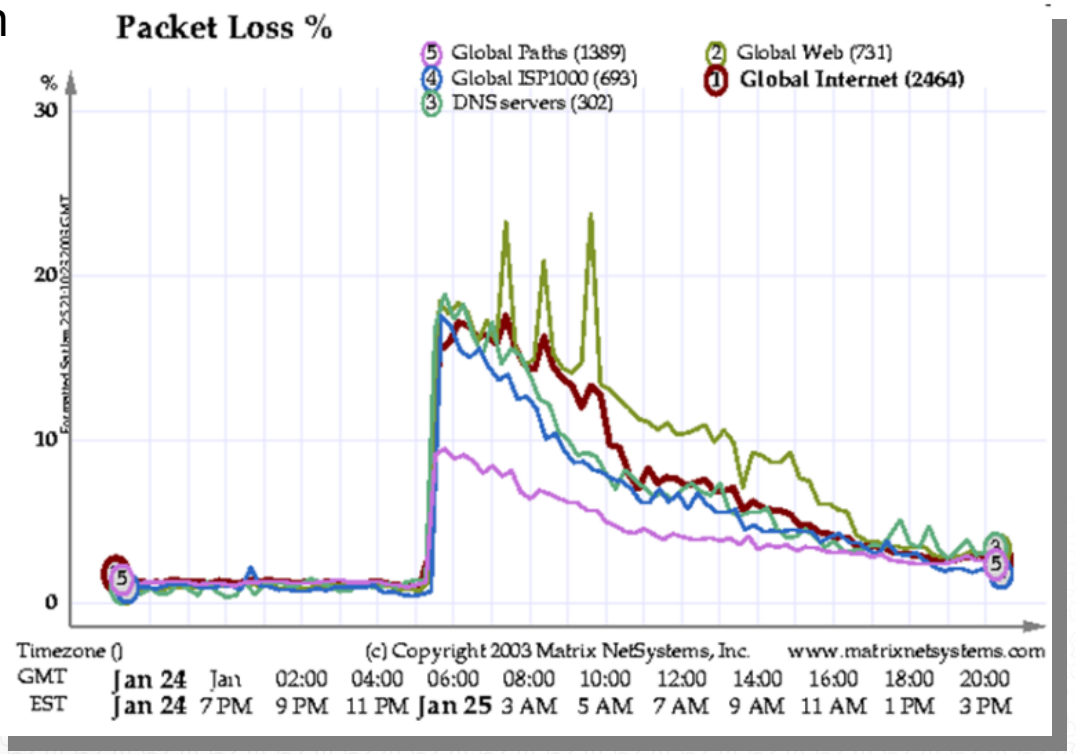
- 2003.01.25. - SQL Slammer/Zaphire

- MS SQL Server 2000 befoltozatlan hiba miatti puffertúlcsordulás

- az első félórában 75 ezer számítógép

- a megfertőződött szerverek 90%-a a járvány első tíz percében elesett

- becslések szerint a kár 750 millió USD



# Hatékony védekezés 4.

**Biztonságtudatosság, rendszeres képzések**

2012. ESET felmérés:

- 90% nem részesült biztonsági tréningben az utóbbi évben
- 68%-a még soha életében
- Folyamatos és rendszeres legyen
- Átfogó: titkosítás, mentés, BYOD, stb.
- Nem csak technikai, hanem social engineering is

# Mi könnyítheti meg egy CIO életét? I.

**Egy lehetséges megoldás - az UTM (Unified Threat Management)**

- költséghatékony és egyszerű

- egységes felületen minden biztonsági szolgáltatás

- tűzfal, IPS, vírusvédelem, spam, VPN, webszűrés

- Központi felügyelet, naplózás, riportok a hálózati tevékenységekről


**Példa**

- vírus- és kémprogram elleni védelem
- felhasználónként, csoportonkénti házirend
- internetes sávszélesség kontroll

ESET Cyberoam AIDA64

# Mi könnyítheti meg egy CIO életét? II.

**Egy lehetséges megoldás - AIDA 64 rendszer-diagnosztikai szoftver**

- Miklós Tamás 1995-től (korábban ASMDEMO, Everest)
- Automatizált hálózati hardver és szoftver leltár
- száz, vagy akár ezer gépes hálózatban
- testre szabható riportok, statisztikák, grafikonok készítése


**Példa**
riasztást (e-mail/SMS) kap a rendszergazda

- ellopják, kicserélik, elromlik bármely hardverelem
- nem engedélyezett programot telepítenek
- eltávolítják vagy lejárt a vírusirtó
- USB eszközök használatáról (adatszivárgás, Autorun)
- hány XP van még a cégnél?

ESET Cyberoam AIDA64

# Összegzés

**A hatékony IT védelem az igazi spórolás**

- nincs kényszerű leállás
- nincs reputáció vesztés
- nincs adatszivárgás
- a károk elhárítása, az incidens kivizsgálása, az adatok visszállítása költséges

**A tudatformálás fontossága**

- a vállalatvezetők szemlélete sok esetben hiányos (Viber, személyiségteszt)
- a dolgozók rendszeres biztonságtudatossági képzése
- a megelőzés az igazi cél