„VISZONTLÁTÁSRA MAGÁNTITOK!”

EMLÉK MŰSOR A ZÁRT HÁLÓZATOKRÓL AVAGY AZ INFORMATIKAI BIZTONSÁG KOCKÁZATAI A JELENBEN ÉS A JÖVŐBEN

Pécs, 2014.04.23

T · · Systems ·

„EGÉSZ NAP FOTÓZTAM, HOZZÁM NEM JÖTT IDE SENKI…”

Kép forrás: Internet, http://www.google.com

TARTALOM
HOVA JUTOTTUNK?

1. Az aktuális helyzet
2. Tévhitek és okaik
3. Mire ez a nagy felhajtás?
4. Technológiák és amit állítanak róluk
5. Kibertér víziók
6. Lehetséges jövőképek
7. T-Systems tapasztalatok
8. ITBN és KIBEV

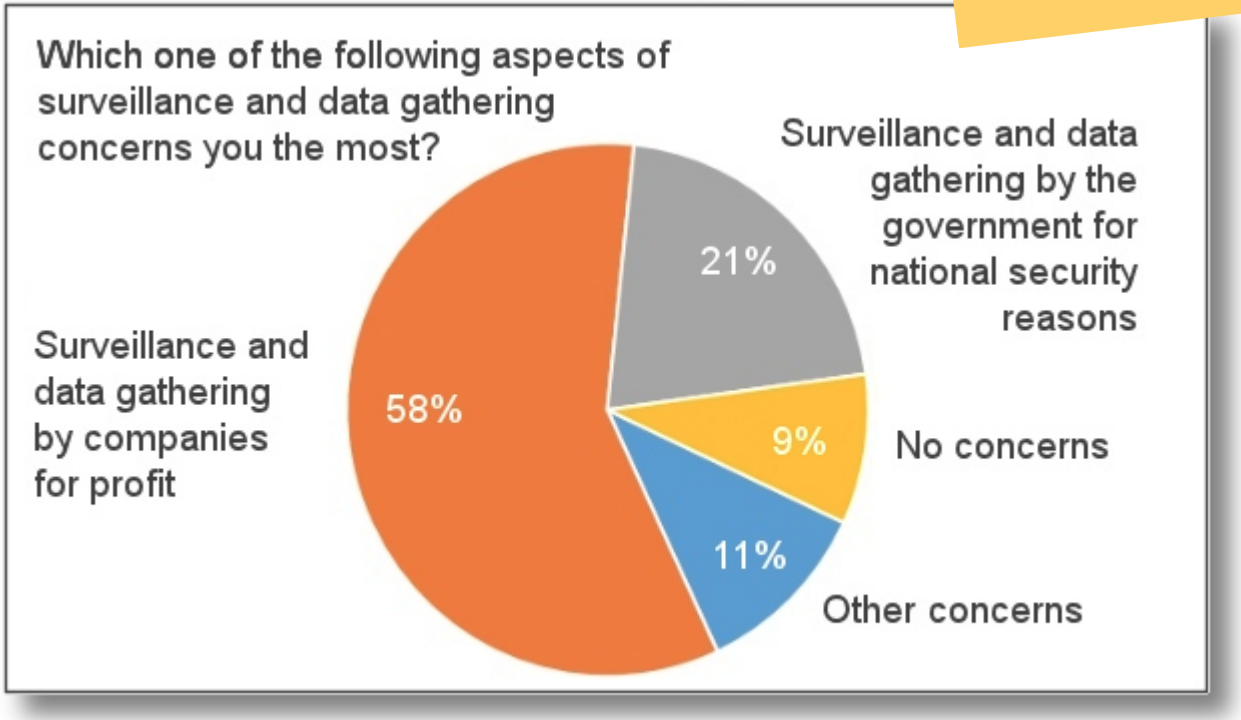
AZ AKTUÁLIS HELYZET

MIT MONDANAK AZ EMBEREK (FRISS FELMÉRÉS: USA)

I am now less trusting of technology companies (e.g. Internet service providers and software companies) as they may be assisting the government in surveillance of private citizens.

60% AGREE	40% DISAGREE

2014.04.09
HARRIS - ESET
AMERIKAI EGYESÜLT ÁLLAMOK



T · · Systems ·

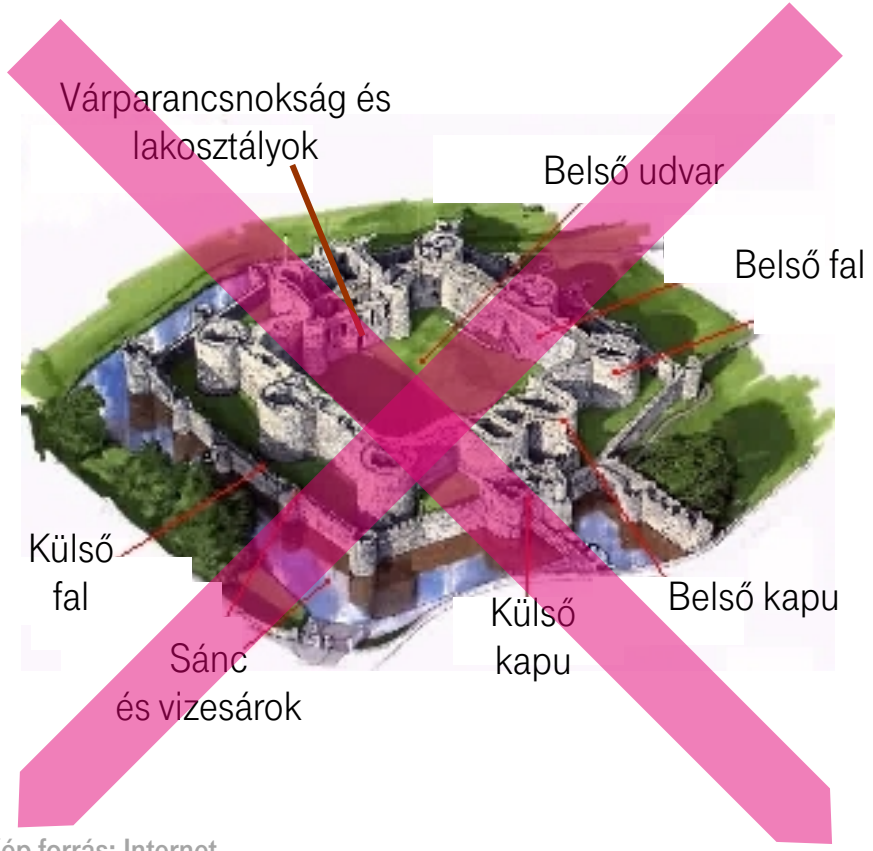
AZ AKTUÁLIS HELYZET
MA EZ TÖRTÉNIK

Kép forrás: Internet, http://www.forbes.com

- Pl. spy/malware-t írnak Androidra
- Tavaly tibeti aktivistákat célzó támadás
- Nem sokkal korábban a Kaspersky Lab is talált egyet
- Köthető a Kínai kormányhoz
- Komplex, célzott email és phishing támadás
- Amiket lop: kontakt adatok a telefonból és a SIM-ről, hívás adatok, SMS-ek, Geo lokációs adatok, telefon adatok
- A frissen talált verzió (képen) + telekommunikációs cégek adatai = pontos lokáció

AZ AKTUÁLIS HELYZET
TEMETHETJÜK A „VÁRFALAKAT”

- Már nincs olyan, hogy belső és külső védelem
- Várfal sincs, amin őrök lennének
- Már olyan sincs, hogy körkörös védelem
- Nincsen önvédő hálózat sem
- A védendő információk egyszerre vannak bent és kint
- Városromok másodpercenként vannak
- ...és nem láthatóak előre



Kép forrás: Internet, prezentáció 2007

T · · Systems ·

TÉVHITEK
ÉS OKAIK

TÉVHIT	OKOK
A tűzfal megvéd minket	Egyszerű és eddig jó volt
A vírusirtó megvéd minket	Gyorsan fölmegy és ingyenes
De hát van rajta jelszó	Elsőre jónak tűnik
Föl van téve a frissítés	A gyártók biztosan tudják...
A fejlesztő biztonságosra írta	Nem a mi dolgunk
Van mentés	Majd visszaállunk
Le van írva	A papír pajzs kitart
...	...

T · · Systems ·

TÉVHITEK
TŰZFAL ÉS VÍRUSIRTÓ

Forrás: http://nebezial.deviantart.com/

T · · Systems ·

VALÓJÁBAN PEDIG
EZ A VÁLASZTÉK

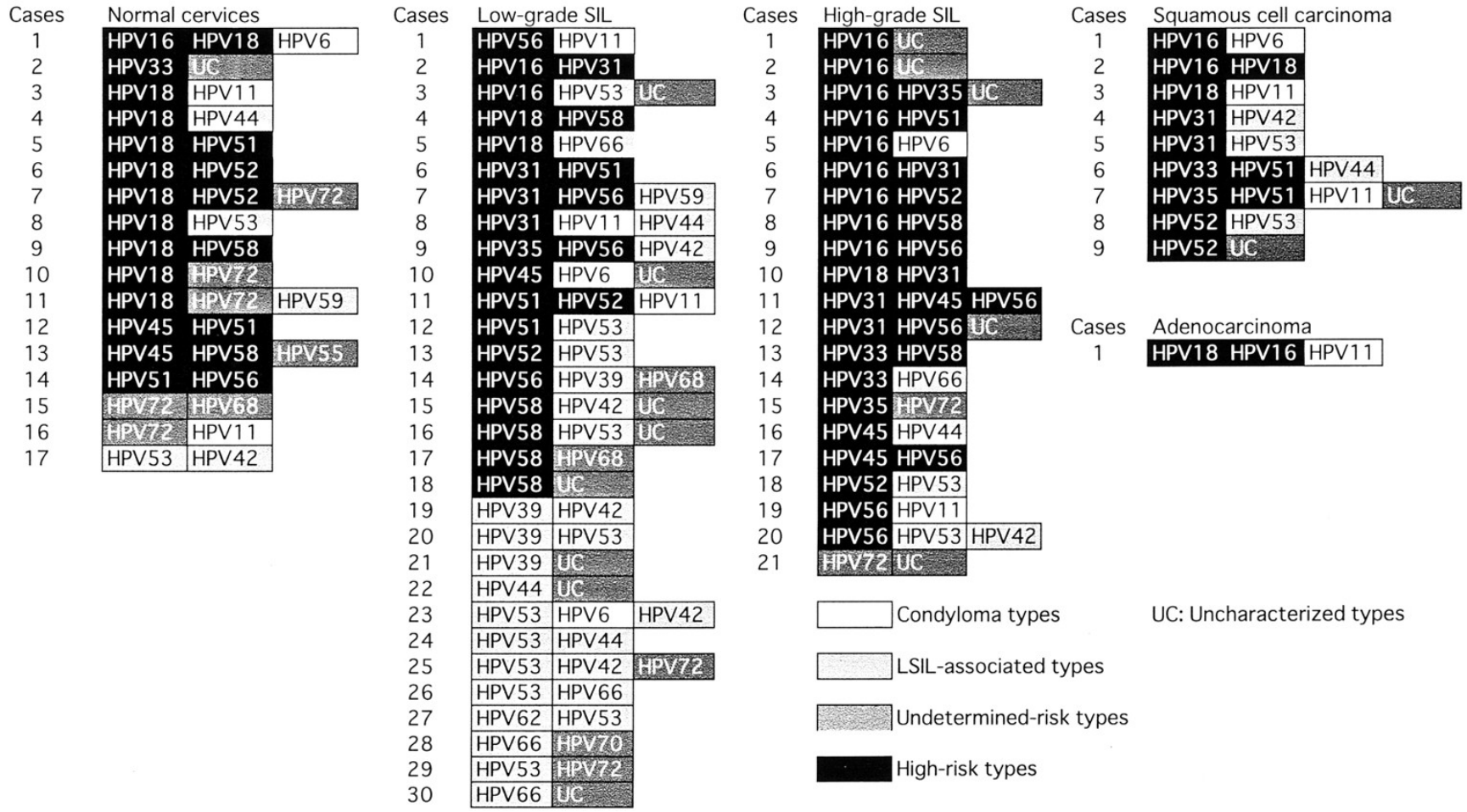
Forrás: http://http://stylefavor.com/

T · · Systems ·

DE MIÉRT VAN ERRE SZÜKSÉG?
MIRE EZ A NAGY FELHAJTÁS?

BONYOLULT AZ ÉLET

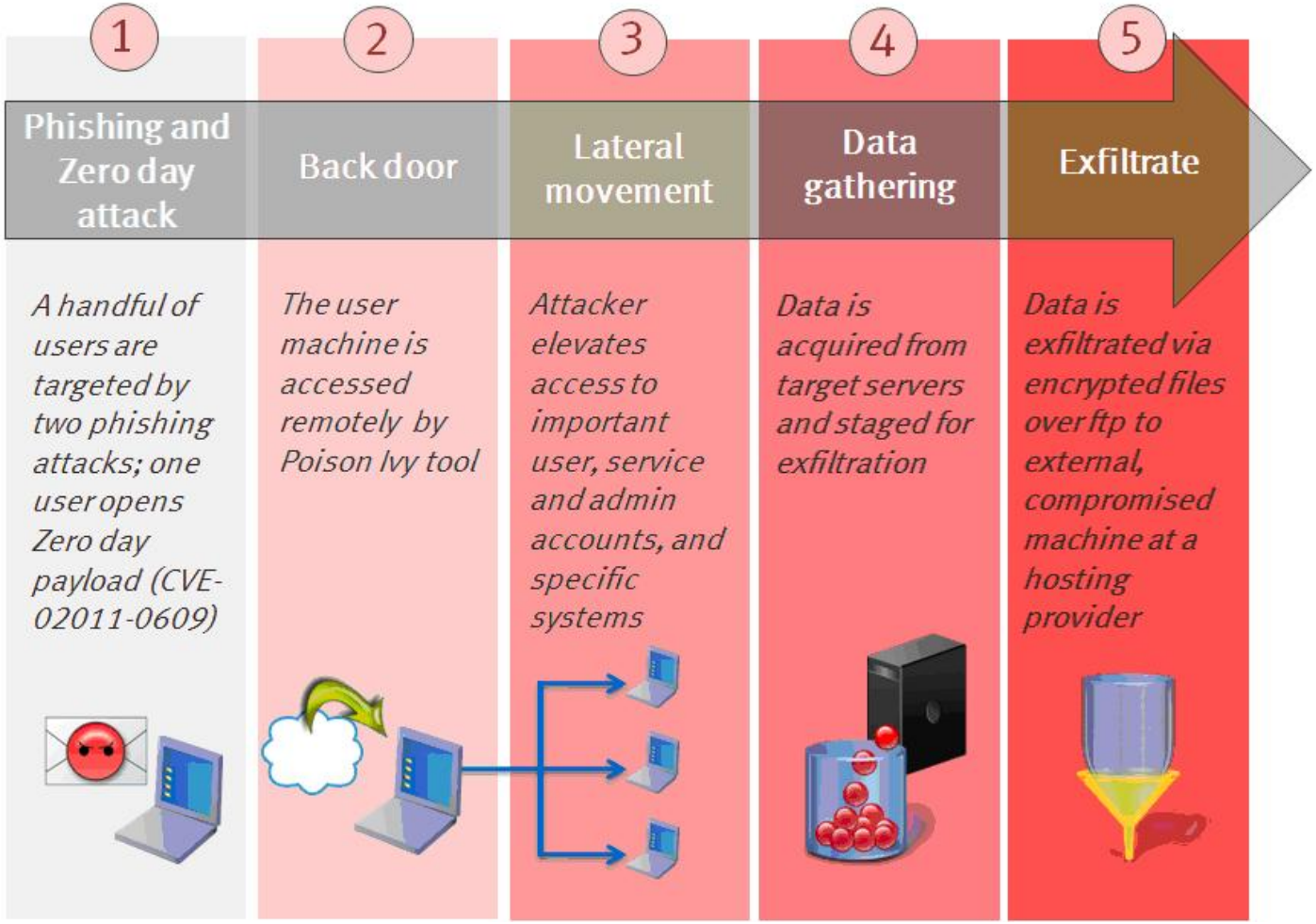
ÉS MOST MÁR AZ IT IS...



T · · Systems ·

HOL RONTJUK EL?

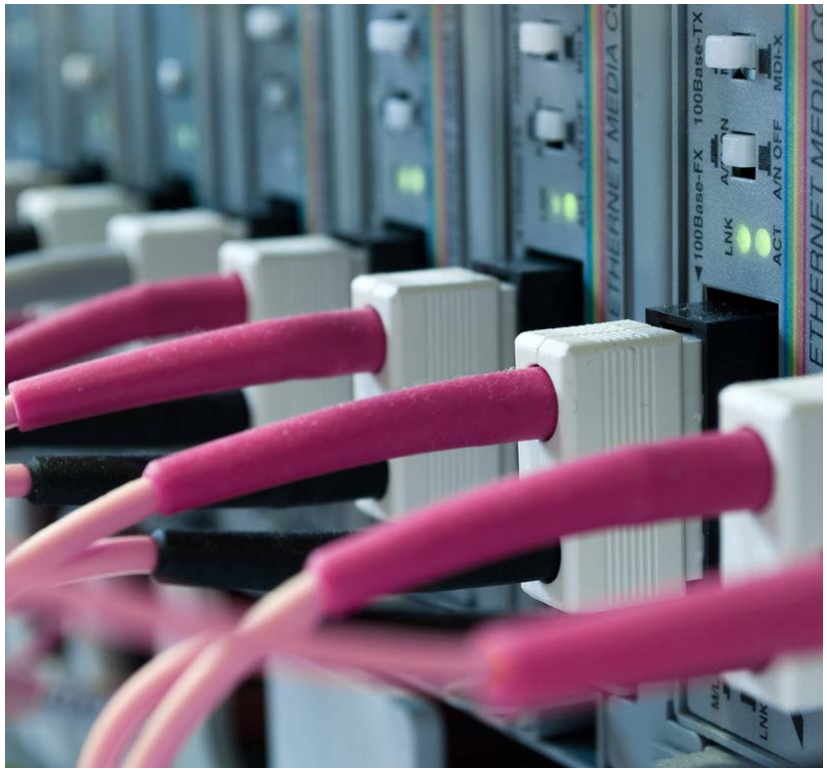
GYAKORLATILAG MINDENHOL...



Forrás: RSA blog

T · · Systems ·

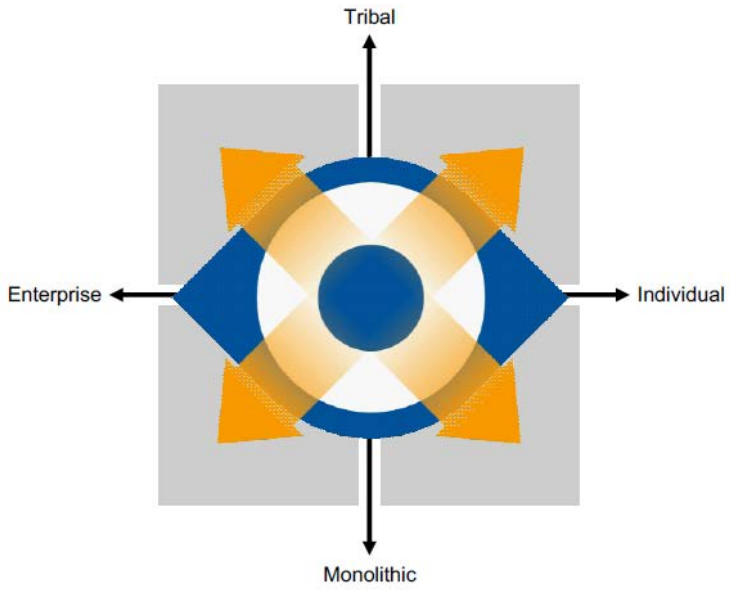
TECHNOLÓGIÁK
ÉS AMIT ÁLLÍTANAK RÓLUK



- APT védelem
- DDoS védelem
- DLP megoldások
- Mobil eszközök védelme
- Ipari védelem
- Hálózati megfigyelési technikák
- Naplóelemzés és hálózatelemzés
- SOC megoldások
- Malware laborok

T · · Systems ·

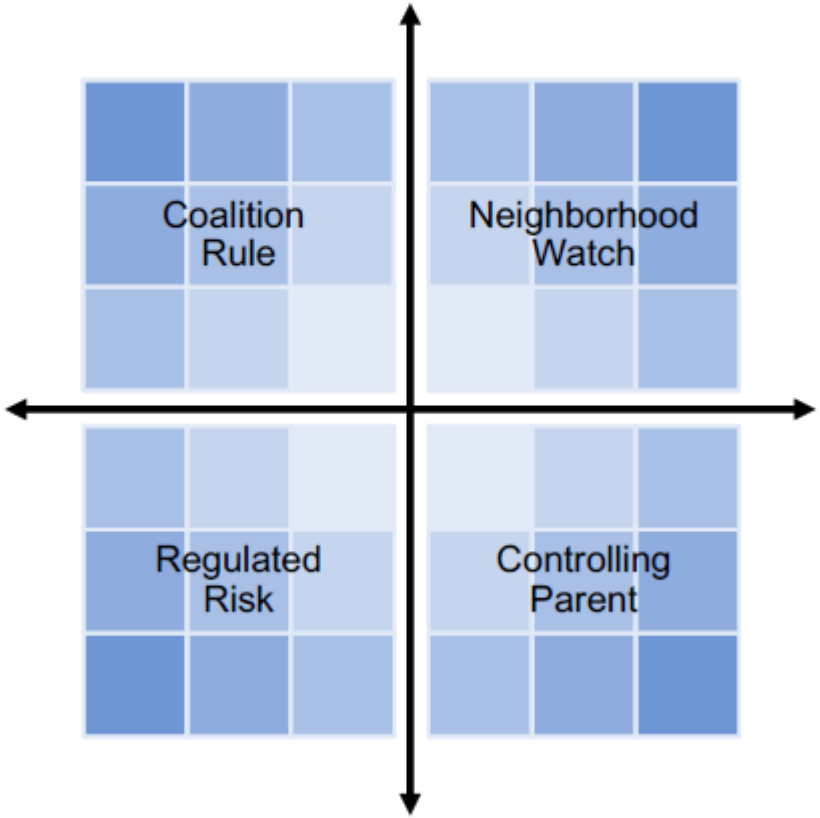
KIBERTÉR VÍZIÓK
GARTNER VARIÁNSOK – 2020-RA



Gartner expects overlap.

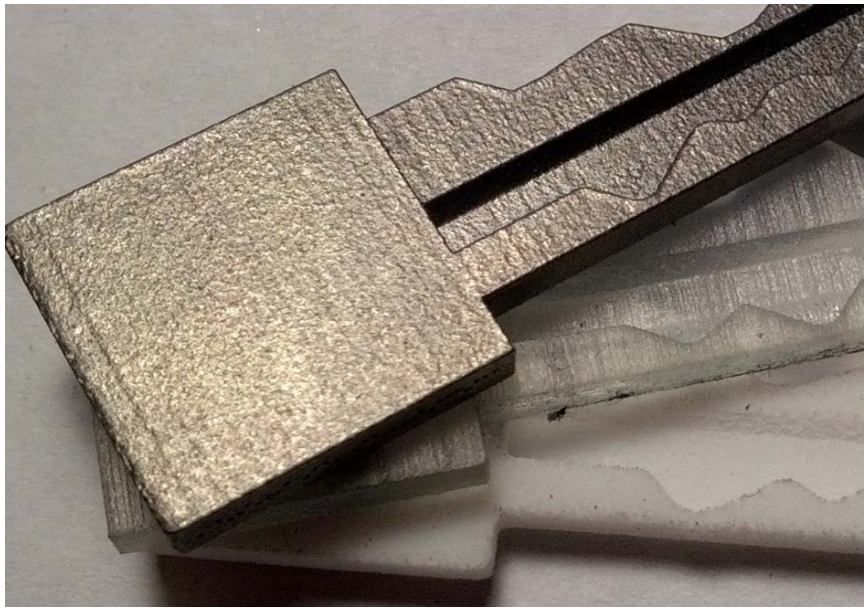
Figure 4. The Four Scenarios for 2020 on a Grid

How we select from and apply our four control strategies will depend on how the world changes for our organization.



Source: Gartner (May 2013)

LEHETSÉGES JÖVŐKÉPEK
MI VÁRHATÓ A KÖZELJÖVŐBEN – 3D NYOMTATÁS



- 2013.08
- MIT hallgatók projektje
- 3D nyomtatott kulcs (fényképről is)

T · · Systems ·

LEHETSÉGES JÖVŐKÉPEK
MI VÁRHATÓ A KÖZELJÖVŐBEN?

- A támadások sebessége és kifinomultsága exponenciálisan nő
- Egyre több hibát fedezünk fel az alkalmazásainkban = 0 day nő
- Az egyének célpontba kerülnek
- Kiderül, hogy mi lesz a cloud-al és annak biztonságával
- 3D printing, automatikus profilozás
- A gyártók sebességre, komplexitásra optimalizálnak (még több felvásárlás)
- A védekezők költségei nagyot nőnek
- Ukrajna:Hidegháború = kiberháború?

T · · Systems ·

T-SYSTEMS TAPASZTALATOK
MIBS – TÁVFELÜGYELET

- Naponta több száz millió biztonsági esemény feldolgozása
- Havi szinten több mint 20 milliárd esemény
- Az ügyfelek, vállalatok több ezer informatikai eszköze produkálja
- A biztonsági központ szakemberei és etikus hackerei elemzik a nap 24 órájában
- Informatikai betörések, hacker vagy biztonsági incidensek esetén akár perceken belüli értesítés

T · · Systems ·


Menedzselt Informatikai Biztonsági Szolgáltatás
Az incidensek alkonya
T · · Systems · · ·

T · · Systems ·

A MEGOLDÁS FELÉ
EGY FIGYELEMRE MÉLTÓ TECHNOLÓGIA

FireEye™

FireEye – APT védelem

- Virtuális futtató környezet
- Lépésenkénti elemzés
- Szimulációs viselkedés elemzés
- Minta/ujjlenyomat készítés
- Forensics képességek
- „a szokatlan” elemzése

T · · Systems ·

MIBEN TUD SEGÍTENI A T-SYSTEMS
VAGY ESETLEG JÓMAGAM?

A biztonságnak a T-Systemsnél 6 fő és 36 szakmai alterülete van

Ami ma **leginkább** foglalkoztat minket:

- Adatszivárgás elkerülése (egyedülálló módszertan)
- Napló- és hálózat elemzés, felügyelet és incidens menedzsment
- Alkalmazás biztonság,APT/Malware
- DDoS támadások elleni szolgáltatás
- Hálózatbiztonság és védelem

T · · Systems ·

MIBEN TUD SEGÍTENI A CIVIL SZFÉRA
ÉS A SZAKMAI KEZDEMÉNYEZÉSEK?

INFORMATIKAI BIZTONSÁG NAPJA

A régió legnagyobb ingyenes biztonsági rendezvénye

2500 szakember, 100 brand, 70 előadás és workshop, trade show, kapcsolatépítés, 2 nap

kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

Civilek a kiberbiztonságért

Magyarország első ilyen kezdeményezése

Közös munkalehetőség

T · · Systems ·

KÖSZÖNÖM!

Keleti Arthur
keleti.arthur@t-systems.hu

T · · Systems ·

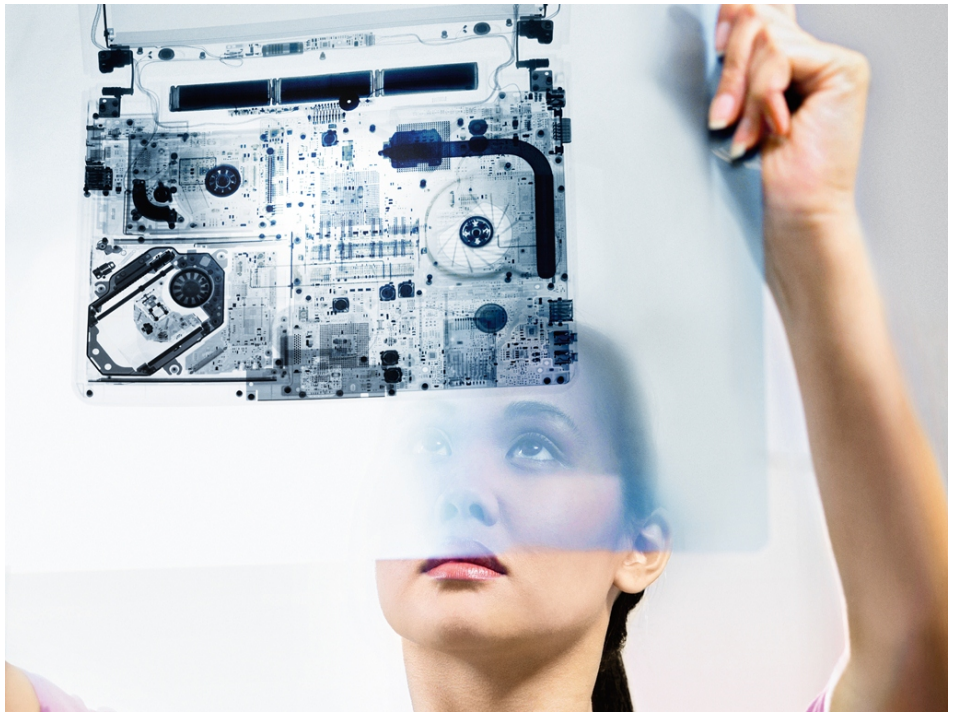
HOGY HALAD ÁT A KLASSZIKUS VÉDELMEN EGY APT?

- **Firewalls**: Firewalls allow generic http Web traffic. Next-generation firewalls (NGFW) usually no dynamic protection
- **IPS:** Signatures, packet inspection, DNS analysis, and heuristics will not detect anything unusual in a zero-day exploit + in heavy disguise
- **Anti-virus and Web malware filtering**: Malware and the vulnerability are unknown (zero-day), and the website: clean reputation they will let it pass
- **Email spam filtering**: Spoofed phishing sites use dynamic domains and URLs, blacklisting no-no
- **Web filtering**: Most outbound filtering blocks adult content etc. Less than a quarter of enterprises restrict social networking sites + dynamic vs. static problem
- **Data loss prevention (DLP):** DLP tools were primarily designed for personally identifiable information (PII)—strings like social security numbers, license numbers etc. — and these tools are only as good as their rules + encryption, callback problems
- ...

Forrás: FireEye

T · · Systems ·

GYÁRTÓK
A STRATÉGIÁK EREDŐJE



Big Data biztonság

Alkalmazás biztonság

Malware kezelés

Incidens kezelés

Sebesség és pontosság

SOC, emberek, folyamatok

T · · Systems ·

LEHETŐSÉGEK
A NEHÉZSÉGEK KÖZEPETTE IS

- Adatvédelmi kérdéseket lehet kezelni (adatosztályozások, kockázatok, DLP)
- Elérhető árú megoldások a hálózatbiztonságban, napló- és hálózat elemzésben (pl. DDoS, NAC)
- Törvényi megfelelősségért lehet tenni
- Alkalmazások bizt. követelményei!
- Operatív és védelmi szinten: malware képességek, CERT tapasztalatok, „hacker” tudás beszerzése
- FOLYAMATOSAN: menedzsment nyomasztása!

T · · Systems ·

KIBERTÉR VÍZIÓK
MERRE TART A KIBERBIZTONSÁG

- Fogalmunk sincs, hogy mi fog történni...
- Trendeket látunk (azokat is gyakran túlértékeljük)
- Kiberháborús helyzet van
- Sérülékenységek, 0 day-ek percenként kerülnek elő
- A biztonsági „AI” még nincs készen
- Kevés a biztonságban tapasztalt operatív szakértő (kevés SOC)

T · · Systems ·

KIBERTÉR VÍZIÓK
GARTNER VARIÁNSOK – 2020-RA

Regulated Risk: (Szabályzott biztonság)

- Alapvetően tömbösít, a kormányzat előír
- A cégek + államigazgatás együtt, biztonsági csapat fókusz (kiberháborús lépések?)
- A cégek felelősek a munkatársaikért
- Minden infrastruktúra = kritikus infrastruktúra

Coalition Rule: (Céges összefogás)

- Az előírások és compliance hatástalan
- A cégek saját erőforrásaikra támaszkodnak
- Fekete piaci, földalatti kiberkartellek
- Nagy cégek koalíciót és jól védett kiberdomaineket alkotnak (hadurak)

Controlling Parent: (Irányító szülő)

- Az egyének a fő támadási célcsoport
- Kétes adatbányászati módszerek, privát szféra?
- A kormányzat erre reagálva szigorúan szabályoz ÉS megfigyel
- A kereskedelem reagál a vevők problémái miatt

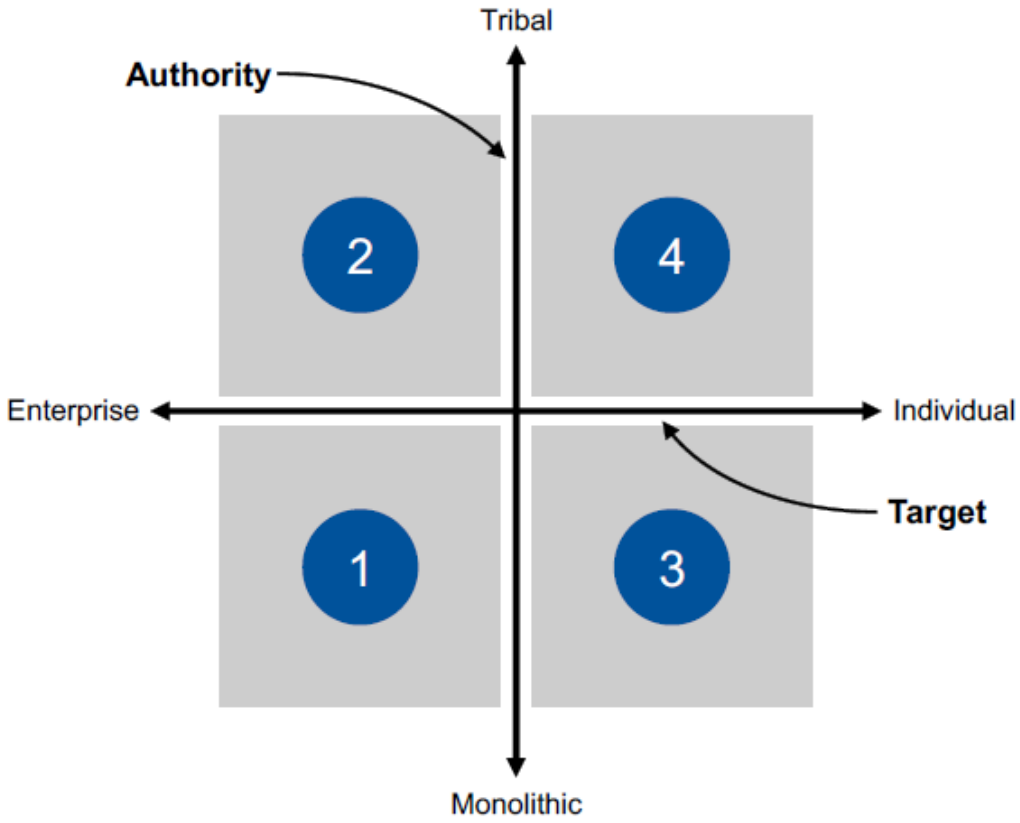
Neighborhood Watch: (Emberi összefogás)

- Anarchista jellegű helyzet
- A szabályzás és a kormányzati lépések nem működnek
- E-Polgárőrségek alakulnak a hacktivisták ellen
- Közösségi védelmi csapatok alakulnak

T · · Systems ·

KIBERTÉR VÍZIÓK
GARTNER VARIÁNSOK – 2020-RA

Figure 1. The Gartner Security and Risk Management Scenario



Source: Gartner (May 2013)

A valós kockázatok felmérése inkább meghatározó, mint az előírások

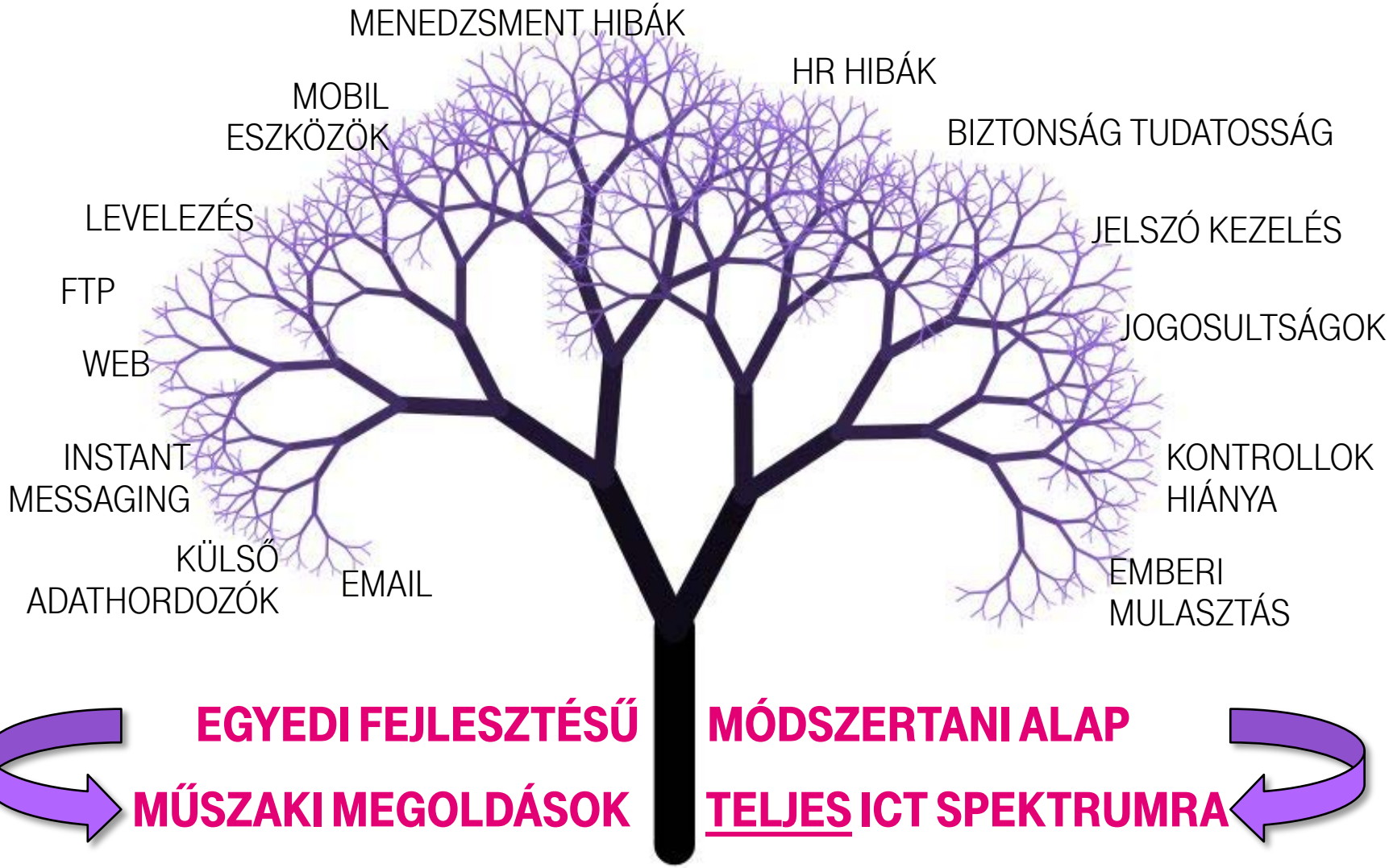
A nemzetközi vállalatok 25%-a foglalkoztat kiberháborús zsoldosokat

A Facebook felhasználóinak 30%-t veszti el „privacy” kérdések miatt

A Global 2000 nagyvállalat CEO-i közül 30%-ot már ért célzott kiberaktivista vagy kiberbűnözői támadás

T · · Systems ·

ADATSZIVÁRGÁS ELKERÜLÉSE – FA MODELL



Kép forrása: Internet

T · · Systems ·