NAGY SÁV, NAGY VÉDELEM A KIBERBIZTONSÁG MODERN FAKTORAI

Keleti Arthur
Kecskemét, 2014.10.08

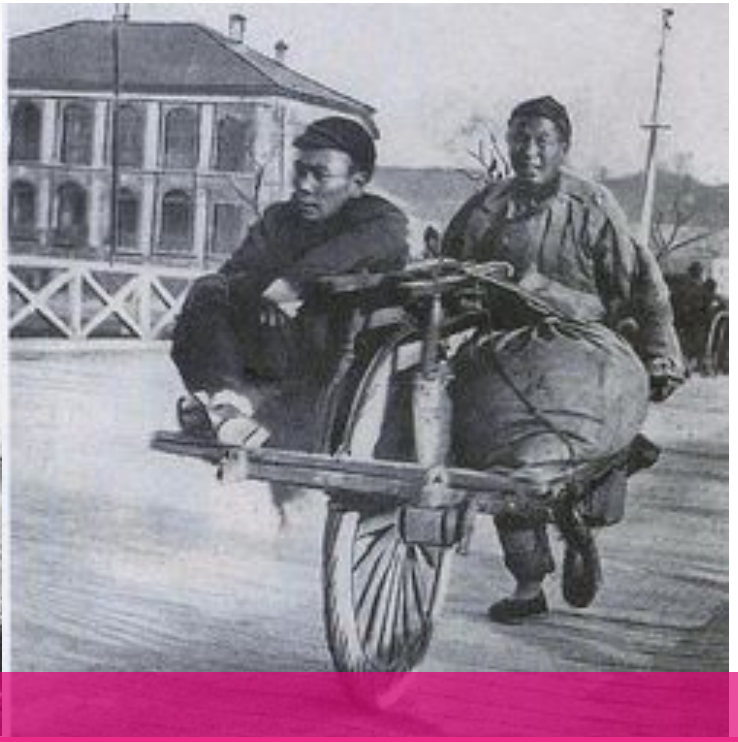
T · · Systems ·

TEMPÓ
SÁVSZÉLESSÉG
KOMPLEXITÁS

T · · Systems ·

Kép forrás: Internet, http://www.fbi.gov

T · · Systems ·



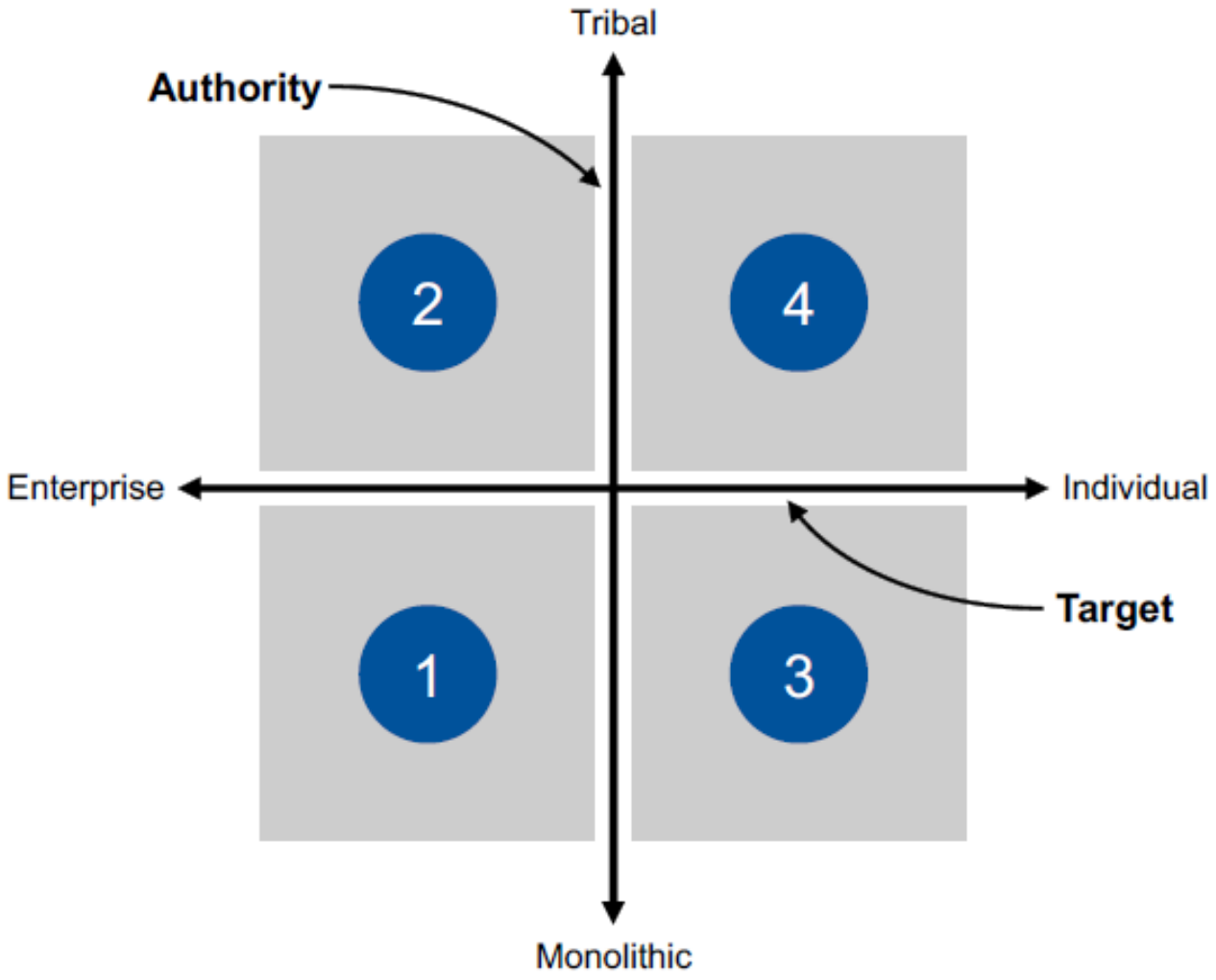
A KÍNAIAK JOBBAN CSINÁLJÁK

T · · Systems ·

HOVA LETT A „RÉGI” HACKER? ÉRTJÜK A MOTIVÁCIÓKAT?

T · · Systems ·

Figure 1. The Gartner Security and Risk Management Scenario

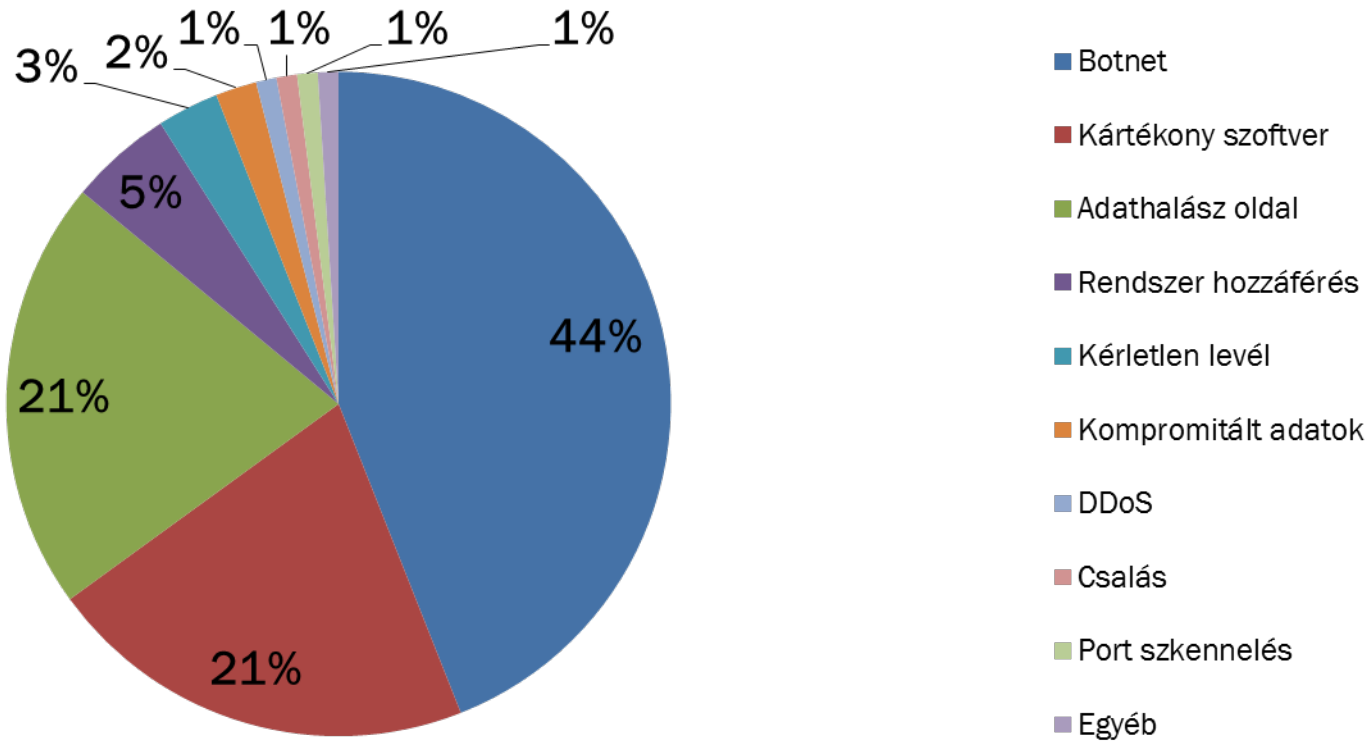


Source: Gartner (May 2013)

A DOLGOK INTERNETE

T · · Systems ·

NMHH RIPORT - ENISA
EZ VOLT 1,5 ÉVE – MI LEHET MOST?



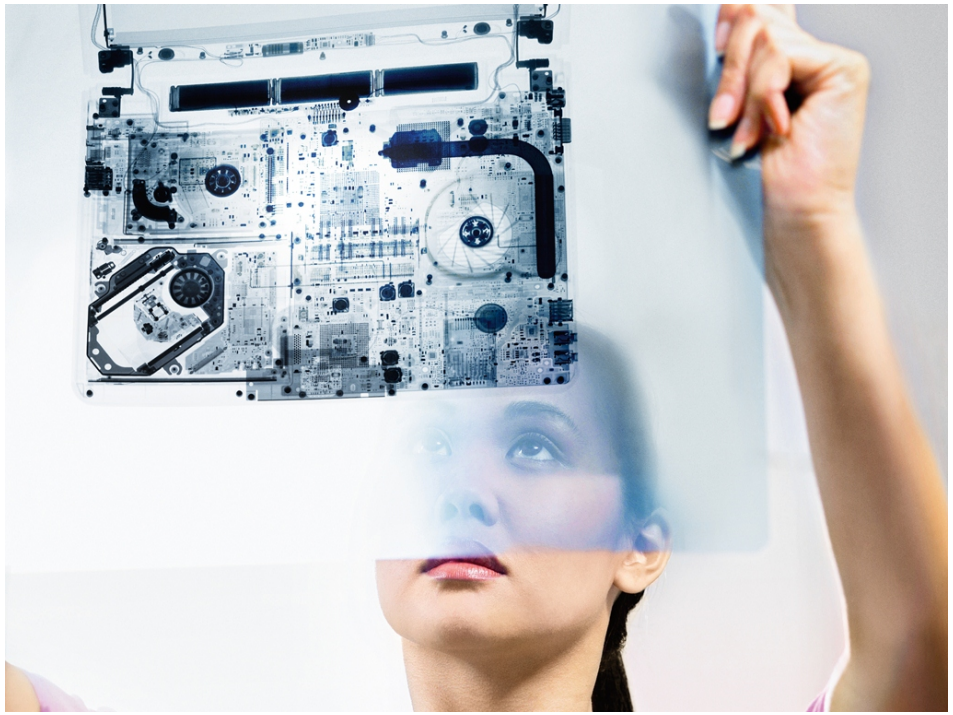
Forrás: NMHH riport az ENISA és a Bizottság számára, 2013. március

T · · Systems ·

A FEL- ÉS BEISMERÉS HIÁNYA

T · · Systems ·

GYÁRTÓK
A STRATÉGIÁK EREDŐJE



Big Data biztonság

Mobil? VoIP? Titkosítás?

Hálózati adatelemzés

Alkalmazás biztonság

Malware kezelés

Incidens kezelés, SOC

T · · Systems ·

A SZOLGÁLTATÓ DOLGA?

T · · Systems ·

ÉS A JÖVŐ?

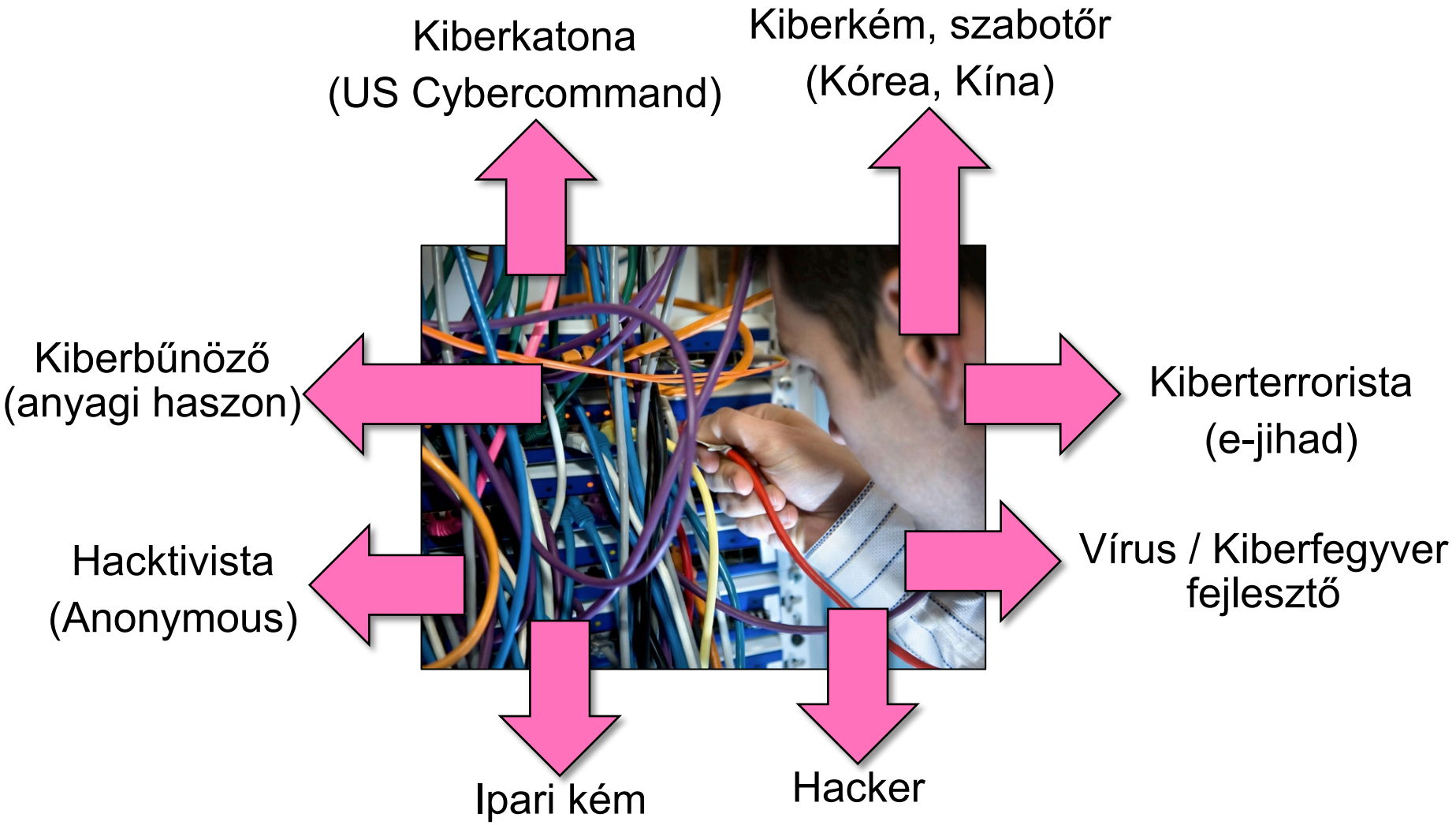
T · · Systems ·

KÖSZÖNÖM!

Keleti Arthur
keleti.arthur@t-systems.hu

T · · Systems ·

MI LETT AZ „EGYSZERŰ” HACKERBŐL



KIBERTÉR VÍZIÓK
MIT CSINÁLNAK A KORMÁNYOK

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

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?)

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

Coalition Rule: (Céges összefogás)

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

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 ·

GYÁRTÓK STRATÉGIÁK ÉS MEGKÖZELÍTÉSEK (NÉHÁNY PÉLDA)

- Balabit – Naplózni és SCB már nem elég, komplex megközelítés
- Cisco – Hálózati védelemből a komplex APT védelem felé, Big Data
- Checkpoint – Hálózati szegmentáció és APT kell
- FireEye – Alkalmazás biztonság – APT védelem
- Fortinet – Hálózati biztonságból – alkalmazás biztonságba
- HP – Összetett adatbányászat és elemzés a naplóelemzés helyett
- IBM – Naplóelemzés, Big Data biztonság és ipari biztonság
- Juniper – Big Data, Data Center biztonság
- McAfee – Vírusírtó nem elég, APT védelem és hálózatelemzés kell
- Radware ÉS Arbor – DDoS intelligencia képességek növelése

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

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

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

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 ·