



Információ biztonság

Áttekintés.

Magyar Telekom gyakorlat.

Hári Krisztián - ITB vezető - Magyar Telekom



Információ - Áttekintés

„Az információ hatalom, ha jól használod, győzelem!”

- Történelmi szerep
- Információs társadalom?
 - Lényegi szerep az információ feldolgozásnak
 - 5,4 milliárd GB / év, 800 MB / fő / év <- e-szemét kezelés
 - Értékes információ felezési ideje csökken – tanulás

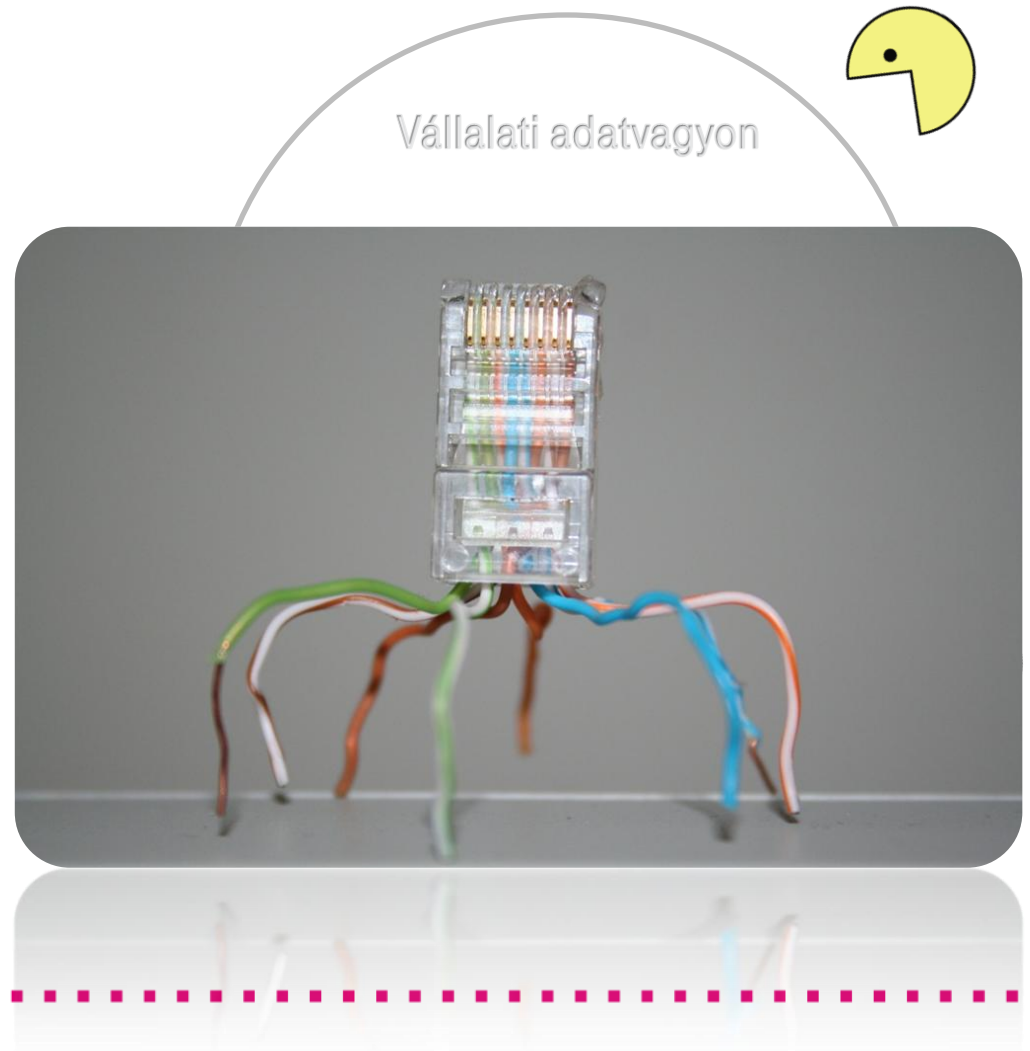
Adat: ismeretelen

Információ: értelemmel bíró adat



Hol találunk információt, adatot?

- Felhasználó programok
- Felhasználói környezet
- Szerver oldali programok
- Szerver oldali környezet
- Hálózatok
- Fizikai környezet
- Emberek
- Kütyük világa



Veszélyforrások

■ Külső:

- Vírusok, worm-ok, malware-ek (Stuxnet, Zeus)
- Botnet-ek (Storm, Rustock)
- 0-day sebezhetőségek
- Hackerek (HBGary)
- Script kiddie-k
- Konkurencia
- Szervezett bűnözés (Market)
- Elégedetlen ügyfelek

■ Belső:

- Szándékos és szándékolatlan programozási hibák (Mars, MySQL.com)
- Rossz üzemeltetési gyakorlat, folyamat (Comodo CA)
- Felhasználói hanyagság, rossz indulat
- Felhasználói bűncselekmények



A legnagyobb veszélyforrás

Az ember



Mit tehetünk?

Védjük az információt!

- De nem mindenáron!
A biztonság nem lehet öncélú!
- Kockázat és érték arányosan
- Biztonság része kell legyen a vállalat mindennapjainak
- Folyamatokba, keretrendszerbe integrálva



Kötelezettségek

- Törvények (Magyar és EU-s)
- Nemzetközi és nemzeti elvárások
 - SOX
 - BilMog
 - PCI DSS
 - Mátrix megfelelés



Mi segítheti a munkánkat?

- Nemzetközi módszertanok:
 - COBIT
 - CC
 - ISO27001
 - ITIL
- Tanúsítások, auditok
- JPÉ



Az információvédelem kihívásai a Magyar Telekomnál

Technikai környezet

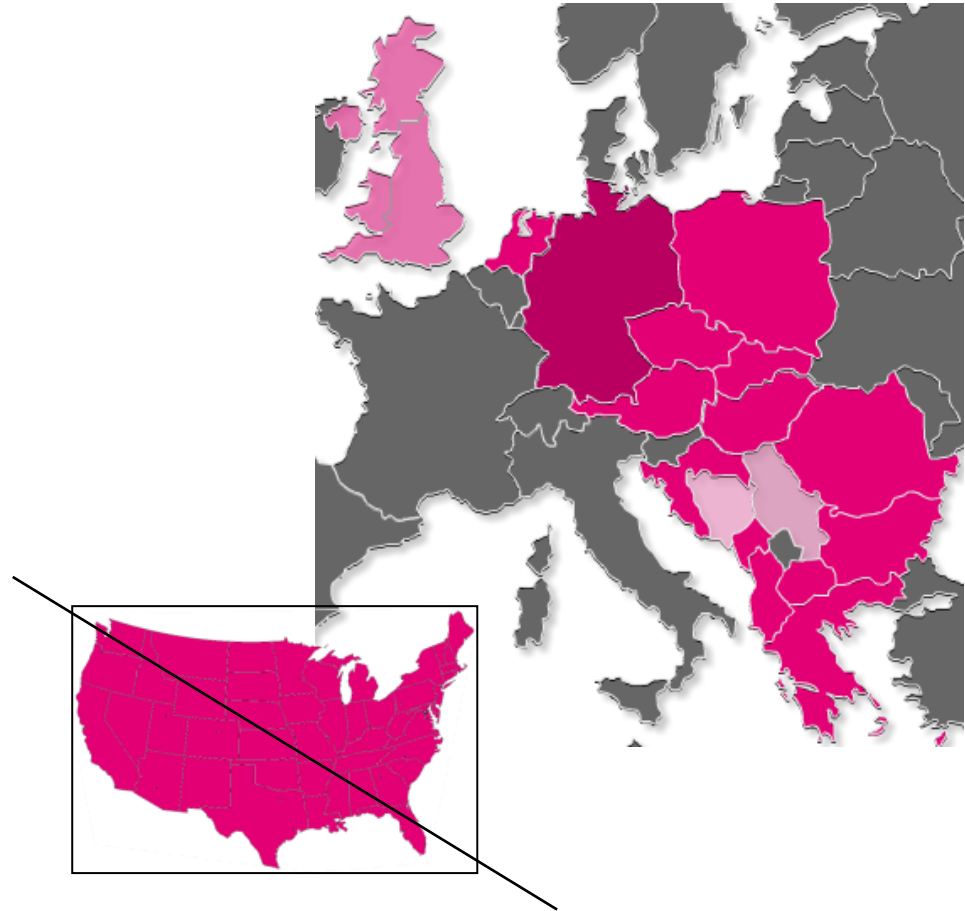
- Több mint 100.000 végpont több mint 100 telephelyen
- ~ 20.000 aktív végponti eszköz
- ~ 1.000 alkalmazás
- Sok millió ügyfél
- ~ 23.700 TB februári adatforgalom
- Több 100 TB tárolt adat



Az információvédelem kihívásai a Magyar Telekomnál

Politikai környezet

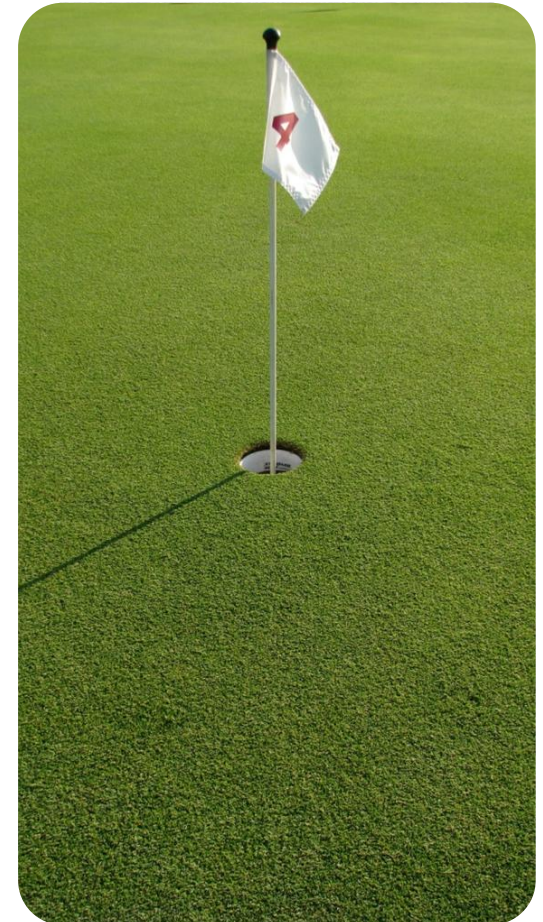
- T történelem
- >11 magyar leányvállalat
- >5 külföldi leányvállalat
- DT csoport



Magyar Telekom

Az út

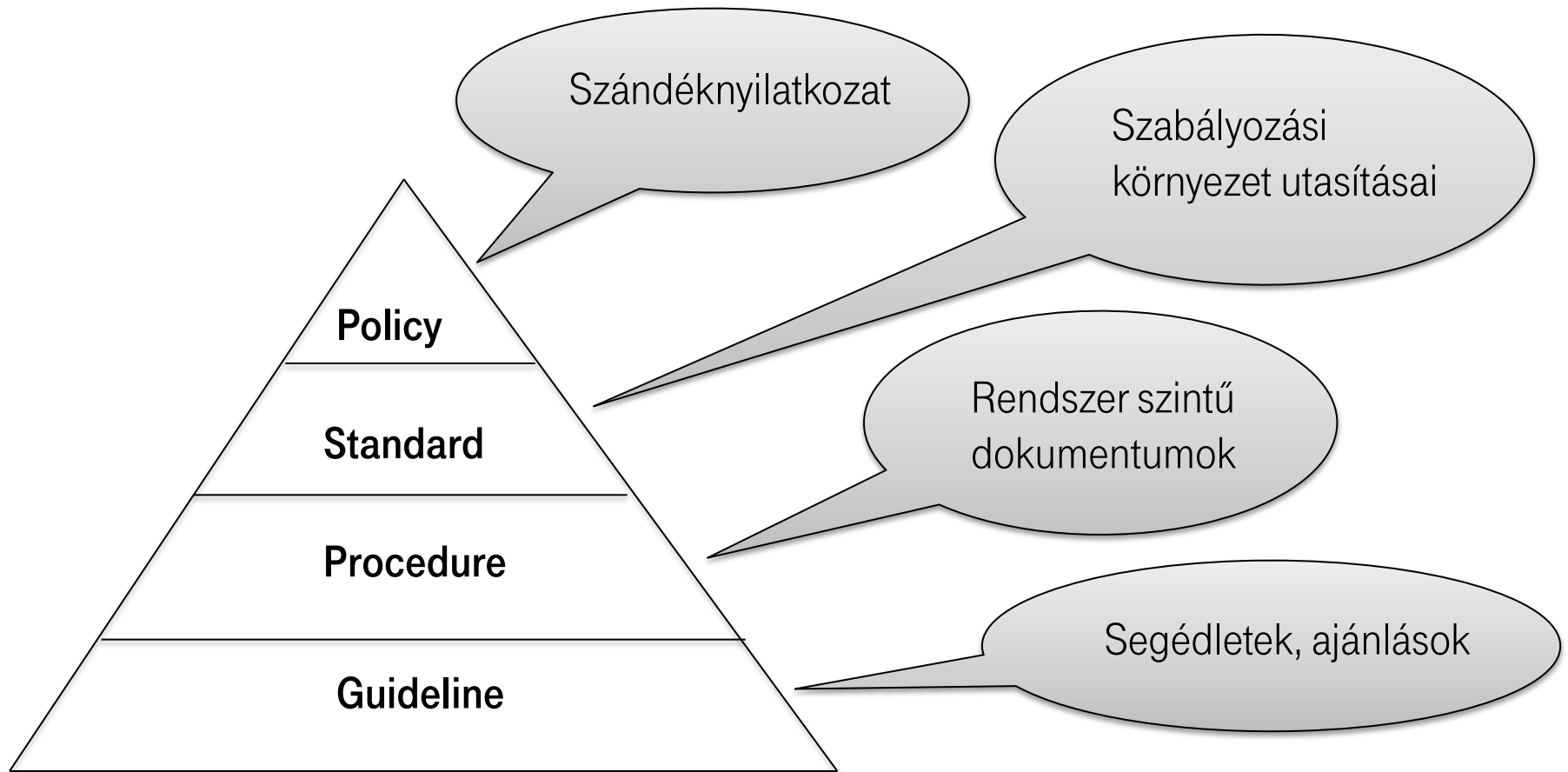
- Architektúra szabványosítás, tervezés, egységesítés
- Központi menedzsment
- Információbiztonsági Irányítási Rendszer (IBIR) bevezetése (ISO 27001)
 - Szabályozási környezet
 - Kockázat menedzsment, eltérésekkel
 - Minőségbiztosítás
- Megfelelőségi auditok
- Biztonsági közművek



- Tűzfal rendszer, IDS/IPS
- Szabályozott távoli elérés (VPN hozzáférés vezérléssel)
- CA – Belső PKI rendszer (tanúsítvány és időpecsét)
- IAM – Központi jogosultságkezelő rendszer és címtár
- Log elemző rendszer
- AD + Kerberos alapú autentikáció, autorizáció
- SSO – Single Sign On
- Sebezhetőség vizsgálat
- Biztonsági incidens menedzsment
- Katasztrófa adattár és központi mentő rendszer
- Adat és adathordozó megsemmisítés



Magyar Telekom - Szabályozási piramis



Összegzés



- Teljes vezetői támogatás szükséges
- Szabályozási és irányítási rendszer szükséges
- A kockázatokat azonosítani kell
- Eltéréskezelés
- Nincs 100%-os védelem
- JPÉ





Kütyük és a biztonság

avagy biztonságos, biztonságos?

...T.....

Mi az a kütyü?



Egy kis történelem

	Commodore 64	IBM PC XT	IBM PC AT	486 DX	iPad2
Released:	1982	1983	1984	1989	2011
CPU:	1MHz	4.77MHz	8 MHz	100 MHz	1 GHz dual
RAM:	64K	128 K	16 MB max		512 MB
Display:	25 X 40 text	640x480	640x480		1024x768
Storage:	None	10MB	20MB		16-64 GB
OS:	ROM BASIC	PC-DOS v2.0	PC-DOS v3.0		iOS



Jövőkép – Hype?



- PC veszélyben?
- Óriási felfutás várható
 - 2010 Q4 - >10.000.000 eladva
 - 2011 - Motorola, Samsung, LG, Lenovo, Asus, Panasonic, HTC, Cisco, Blackberry
- Akarom faktor
- Alkalmazás mindenre

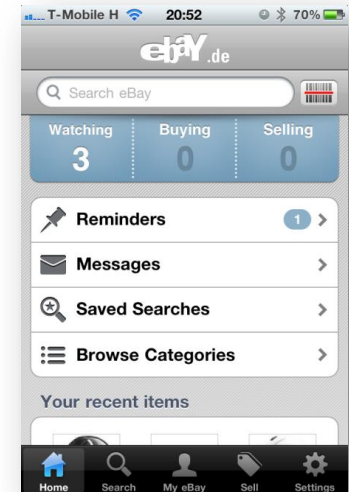
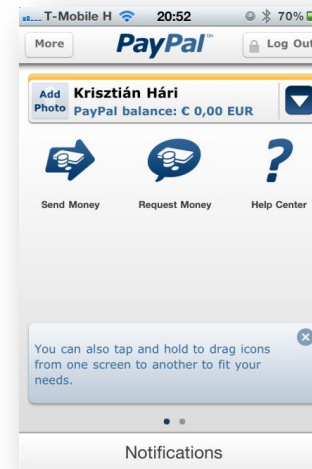


Kockázatok

A magánéletben

- Online élettér
- Magánszféra határai
- Személyes adatok kezelése
- Egy eszközben minden azonosító

- App hozzáférések:
 - 33% location
 - 14% contacts
- Malware-ek, trójaiak
- Felhő adatfeldolgozás



Kockázatok

Vállalati környezetben

- Felhasználói tulajdon
- Helyfüggetlen, kis méretű
- Mindenre van alkalmazás
- Program telepítés nem központilag menedzselt
- Távoli elérés
- Titkosítási és hitelesítési kérdések
- Vállalati adatok tárolása (levelezés, dokumentumok, alkalmazások)
- Magán és céges adatok keveredése
- Védelmi mechanizmusok kikerülése
- WiFi, BT megosztás
- „Cloud”



Mit tehetünk?

JPÉ és ökölszabályok

- Jelszavas védelem
- Titkosítás
- Biztonságos távoli elérés (VPN, RDS, cert)
- Bevizsgált operációs rendszer
- Bevizsgált hardverek
- Eszközmenedzsment
- Központi policy menedzsment
- Bevizsgált alkalmazások
- Vállalati appserver?
- Távoli törlés



IAESTE és Magyar Telekom akadémia

Következő előadás

Telekom Stratégia az innováció
tükrében és a Telekom gyakornoki
program

Kiss Adél

Kiss Annamária

2011.04.06.





Köszönöm a figyelmet!

Hári Krisztián

hari.krisztian.peter@telekom.hu

