Networkshop 2011

infota - ahol a gondolat testet ölt

DUNAÚJVÁROSI FŐISKOLA

IT és hálózati sérülékenységek tovagyűrűző hatásai a gazdaságban

Egy multidiszciplináris kutatás kezdetei

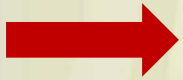
Dr. Horváth Attila

A kutatás kiindulópontja

- Az ICT technológiák elterjedése általános
  - Kormányzati szektor
  - Gazdaság
  - Háztartások
- E technológiákra bízzuk a teljes adatvagyont

- Biztonságos és folyamatos működésük fenntartása kritikus feladat

Mit vizsgáljunk?

- A meghibásodások, támadások biztonsági kockázatok komoly károkat okozhatnak
- Elhárításuk technológiai, informatikai feladat
- DE:
  - Mekkora pontosan az a kár, amelyet egy-egy hiba, szoftver-sérülékenység, vagy biztonsági kockázat okoz? 
  - Mennyi forrást kell allokálni a megelőzésre és az esetleges támadás vagy hiba elhárítására?
  - A döntéshozó sok esetben nem informatikus!

A projekt kezdeti résztvevői

- PTA-CERT-Hungary
- NMHH
- Magyar Posta
- Ecostat
- BellResearch
- Információs Társadalomért Alapítvány

DUNAÚJVÁROSI FŐISKOLA

A kutatási feladat

- Inputok:
  - A CERT-Hungary szoftver sérülékenységi adatbázisa
  - A Bellresearch szoftver-, eszköz- és biztonsági statisztikái
  - Szekunder kutatási források és a KSH adatbázisa
- A cél:
  - Megbecsülni ez alapján a potenciális fenyegetések és meghibásodások gazdasági hatásait felhasználás-, gazdaság-, szociális- és népességstatisztikai adatbázisok felhasználásával.

Miért új?

- Nincs egységes módszertan
- A legtöbb helyen még kísérleti fázisban sem jár a becslési modellek fejlesztése
- Siker esetén a CERT hálózatában a nemzetközi hasznosítás lehetőségei is adottak

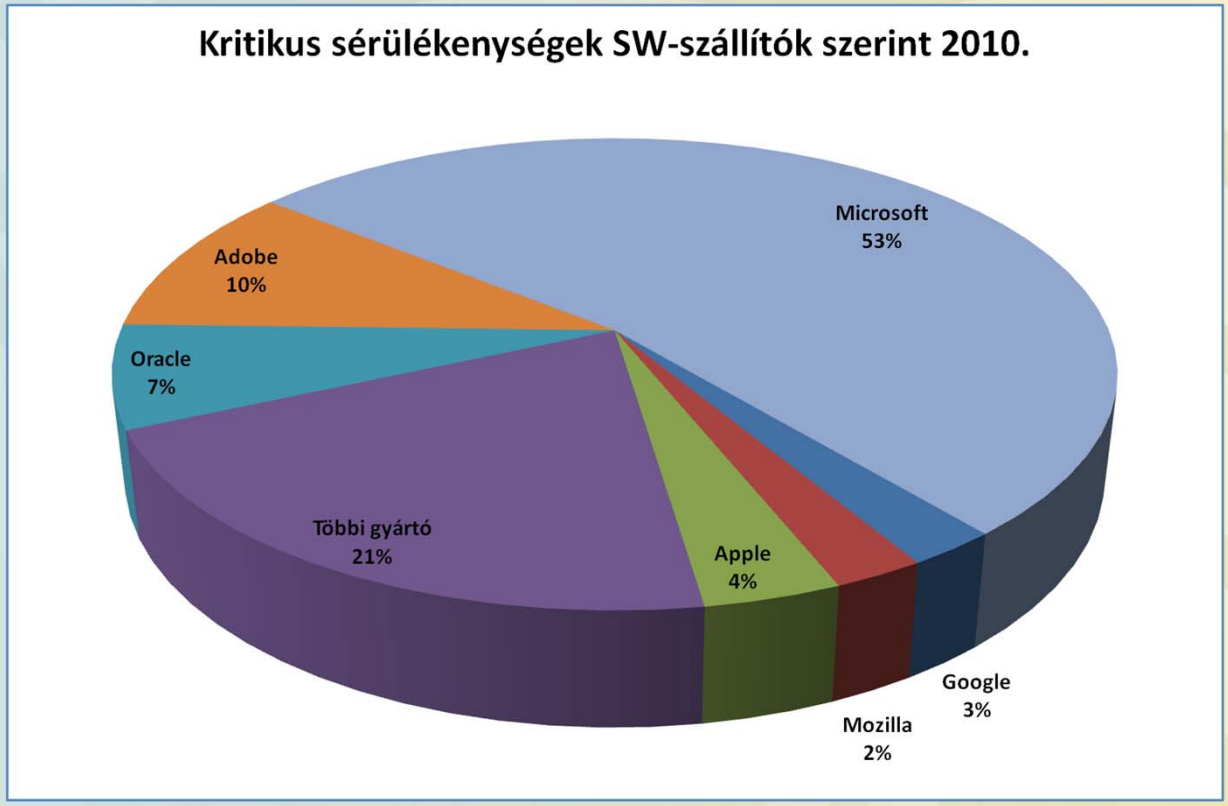
A kutatás ütemezése

- Negyedéves és éves adatelemzés készítése
- Megfelelő leválogatások létrehozása az egyes kormányzati és gazdasági döntéshozói csoportok támogatására.
- A PTA-CERT-Hungary éves és negyedéves jelentéseinek kiegészítése.
- Első ütem 2010. április 1 – december 31.

Az első ütem feladatai

- A lakossági és gazdasági szoftver-felhasználási statisztikák alapján azonosítani azon legkritikusabb szoftverek körét, amelyek sérülékenységei kritikusak lehetnek a teljes nemzetgazdaságra nézve.
- Összevetni ezeket a sérülékenységi adatokkal
- Megkezdeni a megelőzéshez szükséges befektetések becslését lehetővé tevő modell kidolgozását.

Sérülékenységek és előállítók



- Microsoft
  - Windows
  - Office
- Adatbáziskezelők
- Adobe:
  - Reader, flash
- Apple
  - iOS, iTunes, Safari
- Mozilla
  - Firefox
- Google
  - Chrome

- Ezen széles körben elterjedt szoftverek sérülékenységeinek kihasználása az egész nemzetgazdaság szintjén súlyos és nehezen elhárítható problémákat eredményezhet.

Jellemző sérülékenységi problémák 1.

- A sebezhetőségek három típusát különböztethetjük meg:
  - a rendszer nyilvánosan elérhető felületének hibáját kihasználó támadási forma („kapuhiba”), vagy
  - a rendszer hibáját kihasználó távoli forma („falhiba”), vagy
  - a rendszerbe bejuttatott kód futtatásával végrehajtott támadási forma („trójai”).

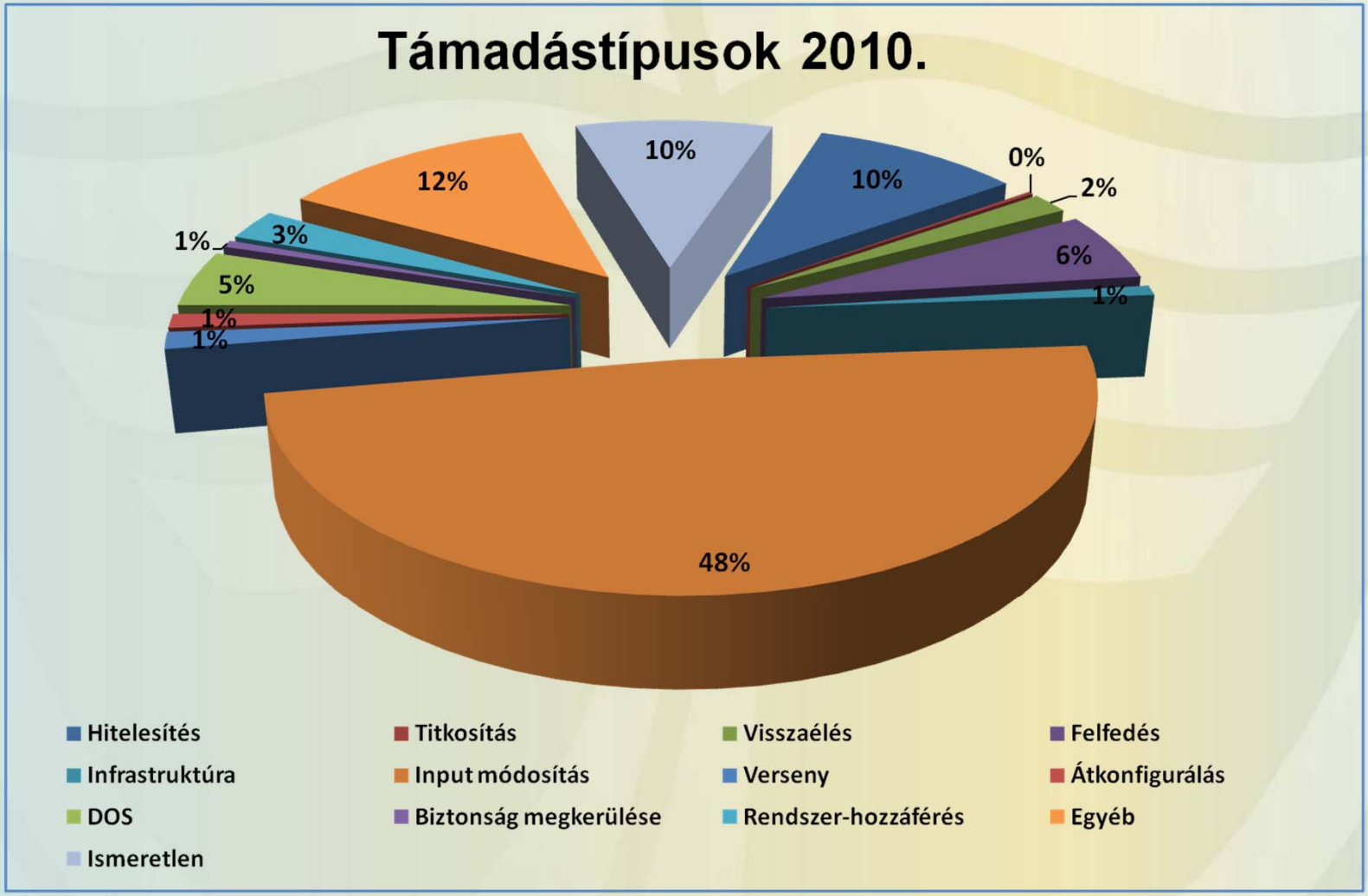
Jellemző sérülékenységi problémák 2.

Javítási forma	Százalékos megoszlás		
	2010. I-II. né.	2010. III. né.	2010. IV. né.
Nincs javítás	46%	47%	63%
Van javítás	0,2%	2%	7%
Van frissítés	20,8%	5%	6%
Egyéb javítás	25%	46%	24%

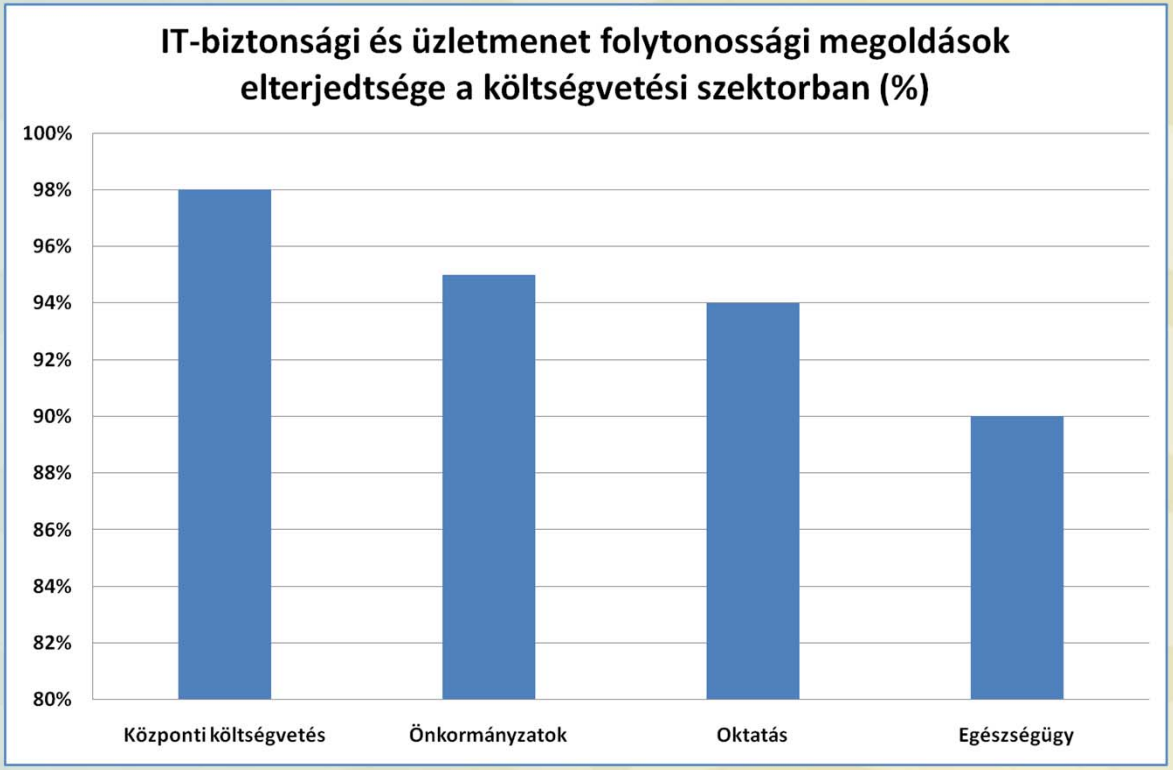
Jellemző sérülékenységi problémák 3.

- A távoli, interneten keresztül végrehajtható támadások túlsúlya (97%) a helyi támadásokhoz képest
- Támadási típusok
  - **Bemeneti adatok jogosulatlan módosítása**
    - ➡ Input kontroll
  - Hitelesítés
  - Titkosítási rendszerek elleni támadás nem volt
    - ➡ Hatékony kriptográfia

Jellemző sérülékenységi problémák 4.

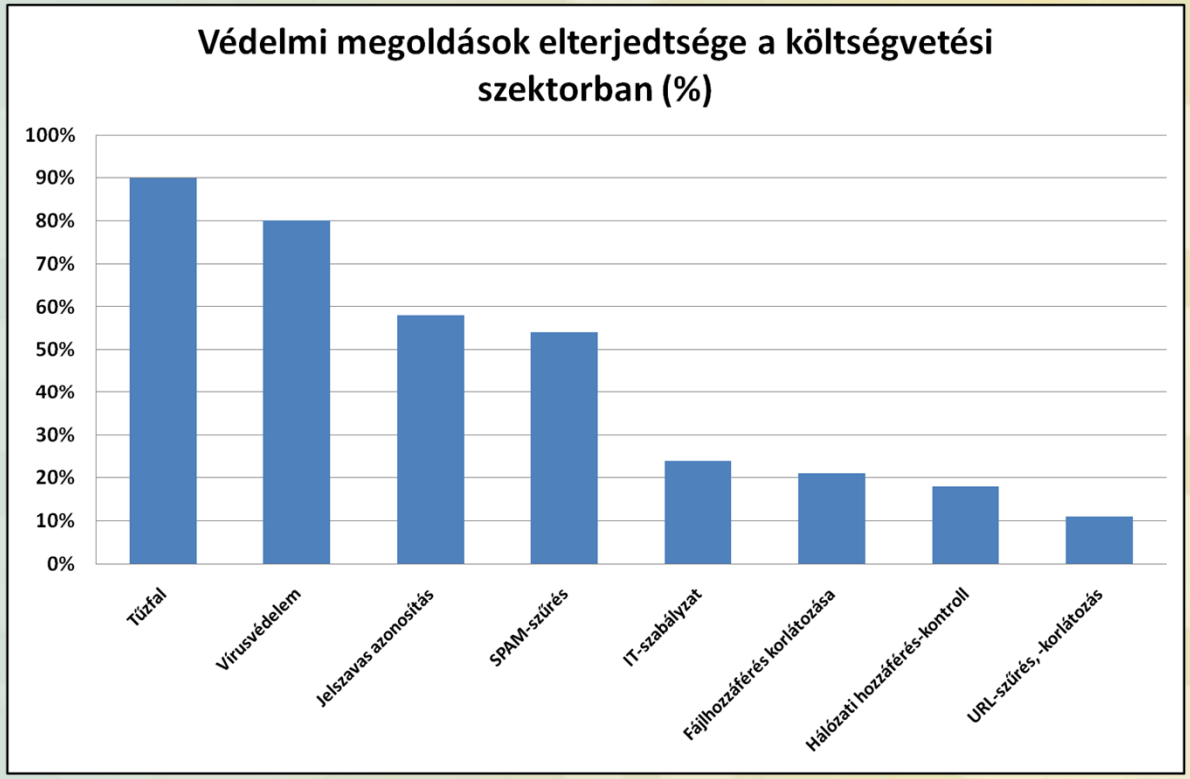


A kormányzati szektor biztonsága



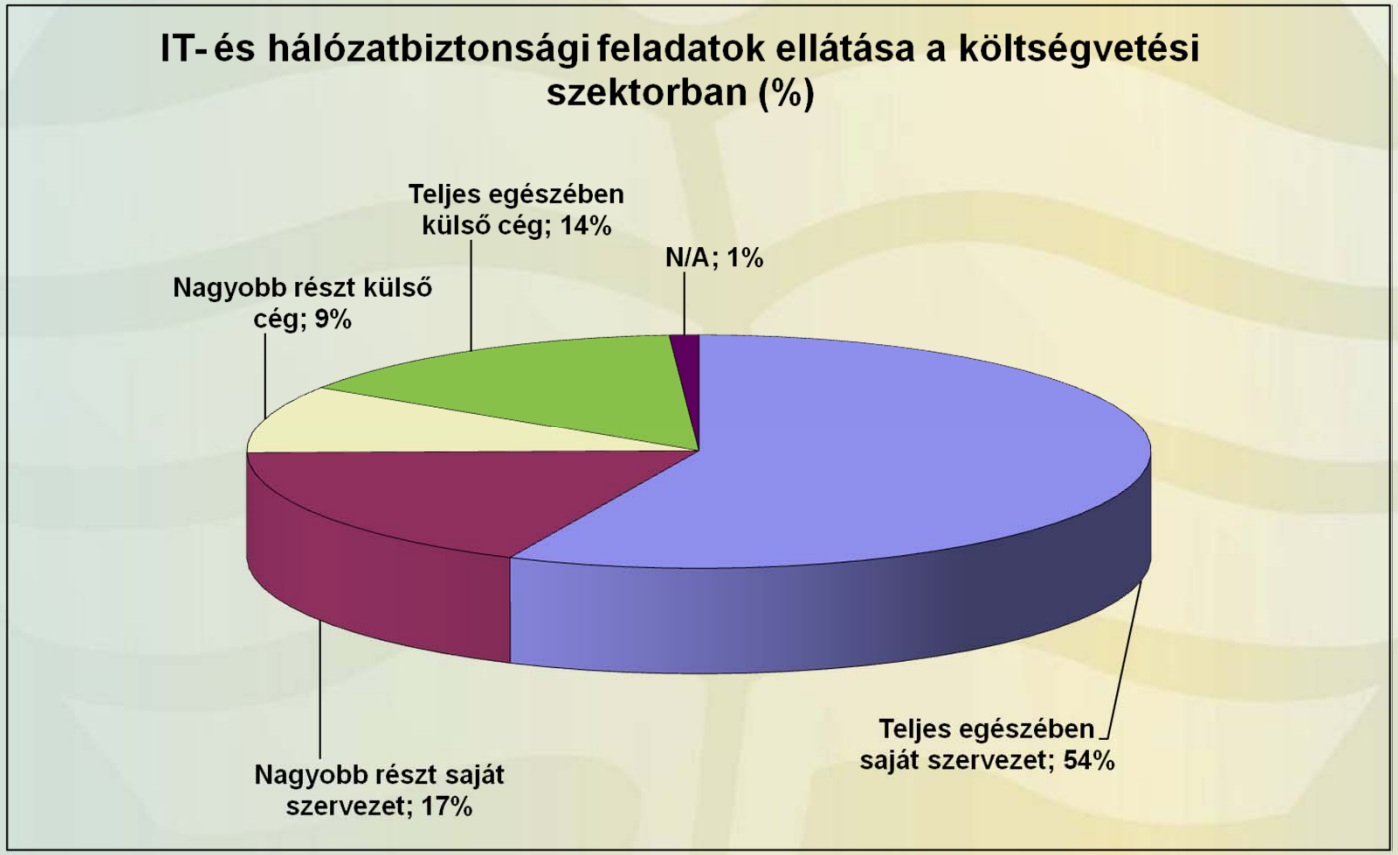
- **A rögzített szabályok, a megvalósítási lépések és az ellenőrzési eljárások hiánya megnehezíti vagy akár lehetetlenné is teszi a potenciális veszélyekre való tudatos és következetes felkészülést.**
- **Nincs a teljes államigazgatást és közigazgatást átfogó, azonos megbízhatóságú és kézben tartható kockázatú koncepción alapuló irányelv (szabvány csomag), emiatt nincsenek bevezetve és alkalmazva egységes biztonsági szempontokkal kézben tartható infokommunikációs (távközlési és számítástechnikai) védelmi rendszerek sem.**

A kormányzati szektor biztonsága



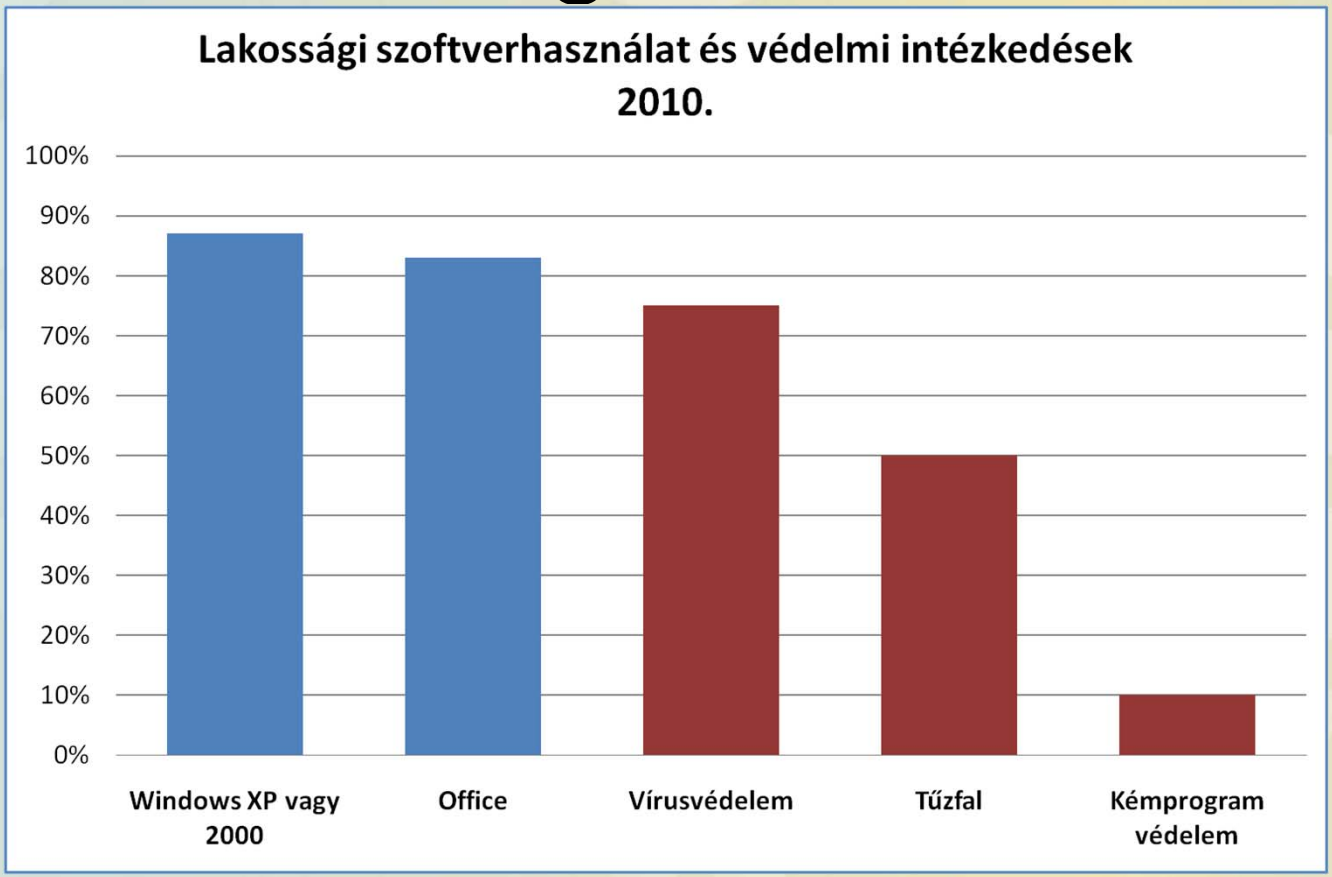
- **A magyarországi intézmények jellemzően csak a védelem legalapvetőbb elemeit alkalmazzák, míg a szervezet mélyebb rétegeit is átható stratégiai szemlélet igen ritka.**
- **Az intézményi szféra szereplőire kevés kivételtől eltekintve jellemző, hogy IT-biztonsági tudatosságuk sokkal inkább az alkalmazott eszközök halmazaiban ölt testet, mint hogy a szervezet működésének egészét befolyásoló filozófiában csúcsosodna ki.**

A kormányzati szektor biztonsága



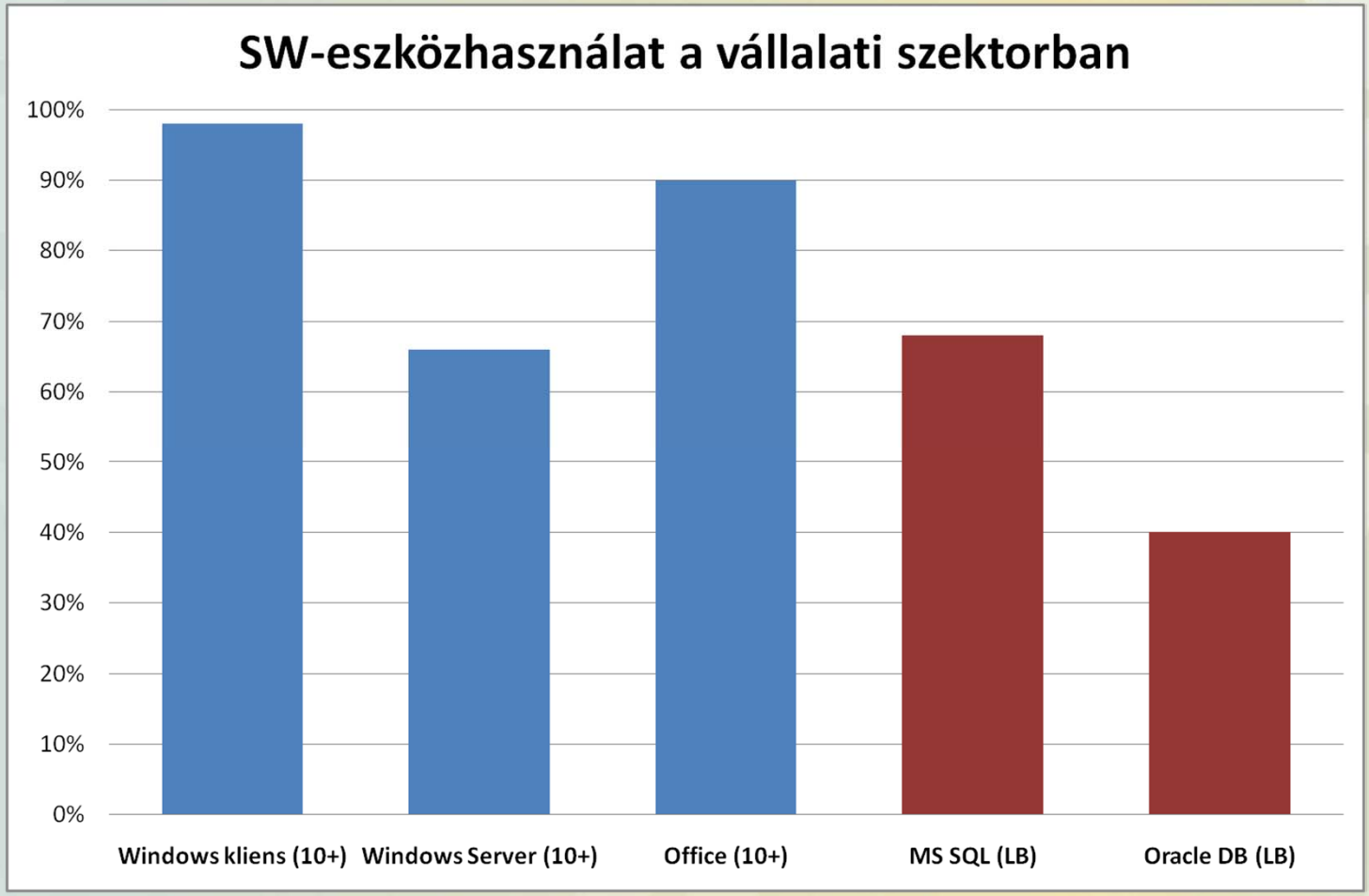
- **Anyagi okok miatt a közigazgatásban csak közepes képzettségű informatikai szakembereket lehet alapvetően alkalmazni.**
- **Tudomásul kell venni, ezért, hogy nagy rendszerek fejlesztéséhez szükséges professzionális és gazdaságosan működtethető informatikai fejlesztő és szolgáltató üzemeltető gárdával nem rendelkezhet.**

Lakossági eszközök



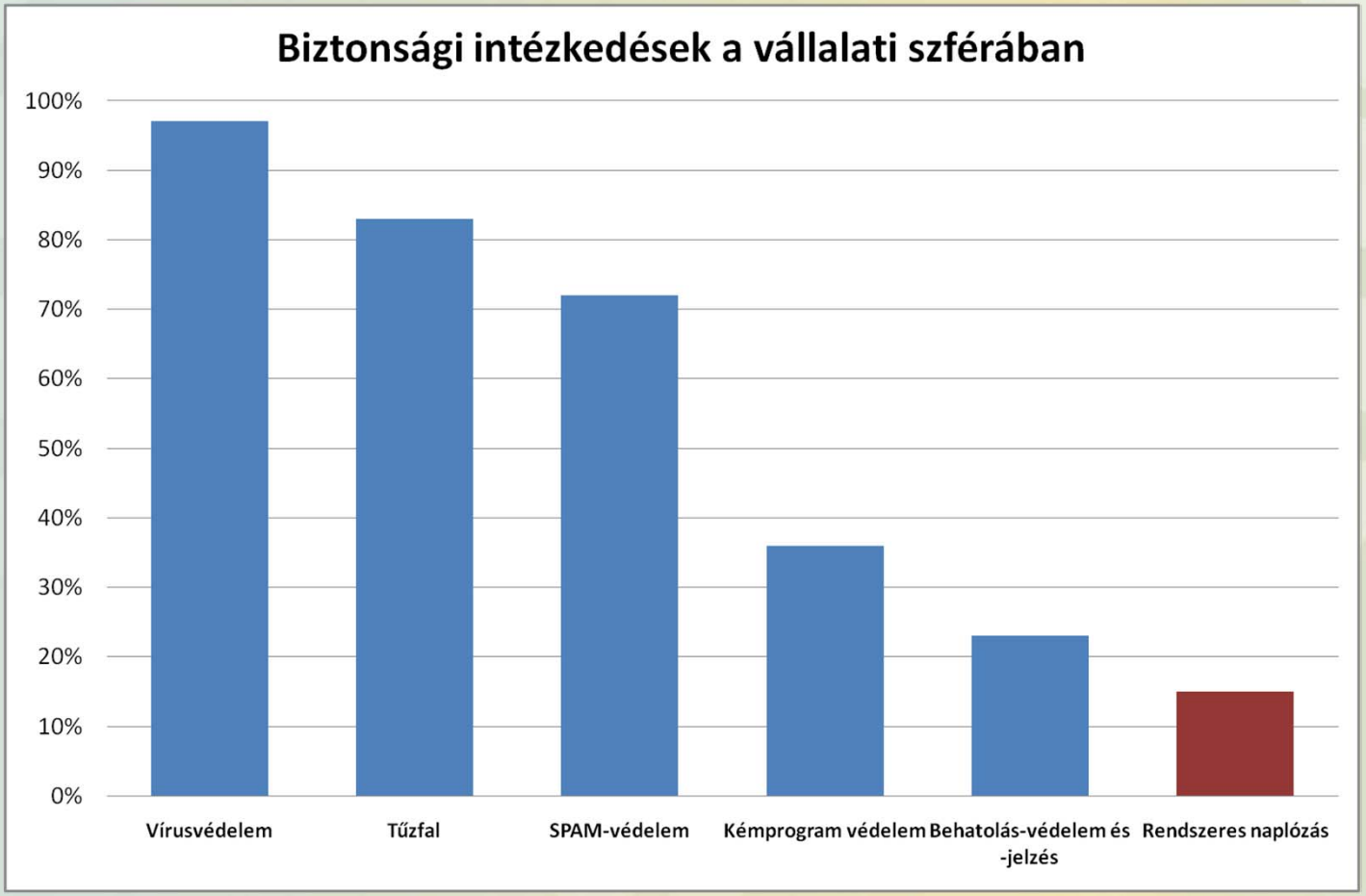
- Figyelembe véve a lakosság szoftverhasználati szokásait látható, hogy a hibákat hordozó Microsoft termékek széles körű használata, amely ráadásul a biztonsági eszközök nem megfelelő elterjedtségével jár együtt, így komolyan veszélyezteti az állampolgárok elektronikus ügyintézési lehetőségeit, adatbiztonságát és személyes adatainak védelmét, valamint az információs társadalom lehetőségeibe vetett bizalmát.

Vállalati eszközök



- **A vállalati szférában, is széles körben alkalmazzák a legkritikusabb sérülékenységeket hordozó szoftvereket, operációs rendszerként, a napi irodai munkához és a vállalat legfontosabb vagyonát jelentő adatbázisok kezelésére is.**

Vállalati biztonság



- **A vállalati szféra igen csekély mértékben van felkészülve egy komoly informatikai biztonsági támadás kezelésére és szakszerű, gyors elhárítására. A komplexebb kockázatokat leginkább az informatikai tevékenység megfigyelésével, naplózással lehet kiszűrni, amelynek a részesedése aggasztóan alacsony.**

Egy kiindulópont a ROSI (Return on Security Investments) modell

$$ROSI = \frac{(Kockázati\ kitettség \times \%\ csökkentés\ mértéke) - Védekezési\ költség}{Védekezési\ költség}$$

- Hogyan határozható meg a kitettség?
  - Iparági statisztikák, incidensek
    - Magyarországon nem érhető el reprezentatív adatbázis
    - Aktuáriusi becslés – a következő periódus feladata
  - Elmaradt bevételek számítása az incidensekből fakadó időkiesésekből

Teljesítménycsökkenés a vállalati szférában

- A különböző biztonsági incidensekből fakadó problémák naponta átlagosan egy óra (maximum akár 4 óra) hasznos munkaidő kihasználhatóságát korlátozzák.
- Rövidebb 10-15 perces kiesésekből áll össze
- Okai:
  - Biztonsági incidensek (60%)
  - Átgondolatlan védekezési szisztémák (40%)

Leállással járó informatikai kockázatok

Probléma	Átlagos időveszteség (perc)
Alkalmazáshoz és rendszerhez kötődő leállások	10
Email szűrés és SPAM	15
Sávszélesség hatékony kihasználása. Áteresztőképesség	10
Nem hatékony és hatástalan biztonsági politikák	10
Biztonsági politikák szigorúsága	10
Rendszerhez kötődő kiesések és frissítések az IT részéről	10
OS és alkalmazások biztonsági javításai	10
Nem biztonságos és nem hatékony hálózati topológia	15
Vírusok, vírus ellenőrzés	10
Férgek	10
Trójai, keylogger	10
Kémprogramok	10
Felugró hirdetések	10
Kompatibilitási problémák	15
Engedély alapú biztonsági problémák (felhasználónév/jelszó)	15
Fájlrendszer rendezetlensége	10
Sérült vagy elérhetetlen adatok	15
Rendszerinformációk és adatok illetéktelen elérése vagy eltulajdonítása	15
Biztonsági menztések visszaállítása	15
Alkalmzás használati problémák	15
Teljes idő	**240**

Az átgondolatlan védekezés hatásai

- A kiesések fakadhatnak:
  - Üzemidőben futtatott teljes biztonsági ellenőrzés (kapacitás kiesések),
  - Rosszul menedzselt sávszélesség és hálózati topológiák,
  - Frissítések és biztonsági patchek munkaidőben való telepítése,
  - Az ezekből gyakran adódó kompatibilitási problémák megoldása,
  - Túl szigorú beléptetés és jogosultságkezelés.

Makrogazdasági hatások

- Jelentős hatékonyság romlás
- Akár a megtermelhető GDP 10-15%-os vesztesége nem megfelelő IT-felkészültség esetén
- Áttételes hatások:
  - Ügyintézési és feldolgozási idők növekedése
  - A gazdaság többi részéből munkaidő elvonása
  - Bizalomvesztés az iparágban és egyéb áttételes hatások

Köszönöm a figyelmet!

Dr. Horváth Attila

Főiskolai docens

Dunaújvárosi Főiskola, Informatikai Intézet

horvath.attila@mail.duf.hu

DUNAÚJVÁROSI FŐISKOLA