EAGLEEYEOS™
ORGANIZED SECURITY

Technológia az adatszivárgás ellen

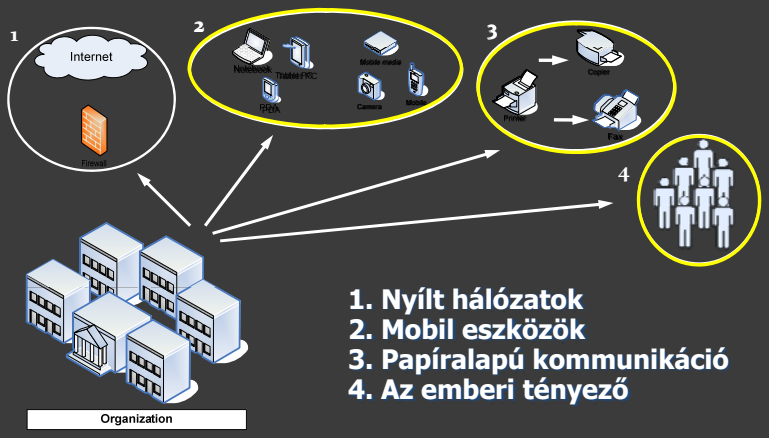
2008. november 17.

Fazekas Éva, Processorg Software 82 Kft.

Áttekintés

1. A probléma
2. Az elvárt eredmény
3. Megoldási lehetőségek
4. A technológia
5. Funkciók
6. Eredmények

Az adatszivárgási probléma
Veszély a kapukon belül



1. Nyílt hálózatok
2. Mobil eszközök
3. Papíralapú kommunikáció
4. Az emberi tényező

Incidens esetén

A múlt:

	Ráfordítás	***A sikeres támadás eredménye***
Védő	A védelem költségei: (-)	Kár: (-)
Támadó	A támadás költségei: (-)	Haszon: (+)

Sikeres támadás: A támadó az információt megszerezte, és nem hagyott maga után olyan bizonyítékot, amely beazonosíthatná a kilétét.

Incidens esetén

A jövő:

	Ráfordítás	***A ~~sikeres~~ támadás eredménye***
Védő	A védelem költségei: (-)	Kár: (-)
Támadó	A támadás költségei: (-)	Felelősségrevonás: (-)

Sikeres támadás: A támadó az információt megszerezte, és nem hagyott maga után olyan bizonyítékot, amely beazonosíthatná a kilétét.

Elméleti megközelítés: Ajánlások, szabályzatok, szabványok

KEHI
ÁSZ
ITIL
BASEL II
SOX
DRP
ISO 27001
BS 7799
COBIT
ISO 15408 - CC
PSZÁF
MEH ITB
MIBÉTS
TCSEC
CRAMM
BCP
INFOSEC
Common Evaluation Methodology
ISO 13335
Common Criteria

A védelem elve

EAGLEEYEOS™

1. **Mindent tiltsunk…!**

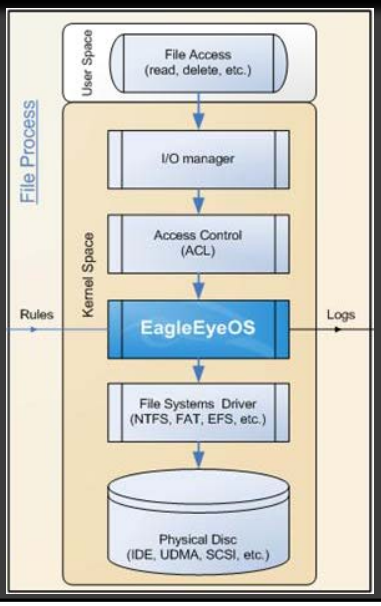
?

Kivéve, amire szükség van

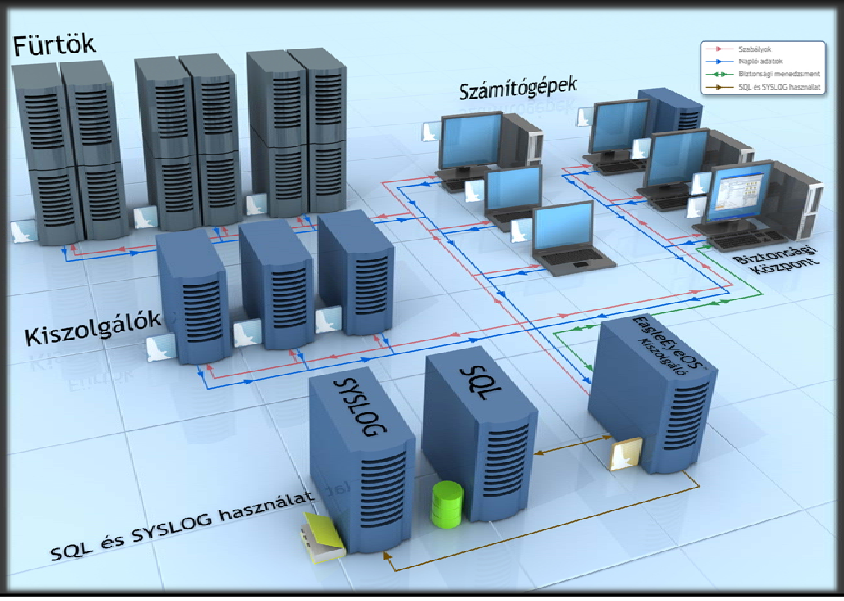
2. **Mindent naplózzunk…!**

?

Kivéve, amire nincs szükség



A rendszer működése



Naplózás

- **Valósidejű naplózás**
  - Specifikus naplózás: pozitív és negatív logszűrők
  - Egyedi titkosított adatbázis, vagy szabványos SQL
  - Syslog formátum az integráció elősegítésére
- **Különböző riporttípusok:**

Riport, AutoRiport, Riasztás, FLT, SLT, Pillanatképek

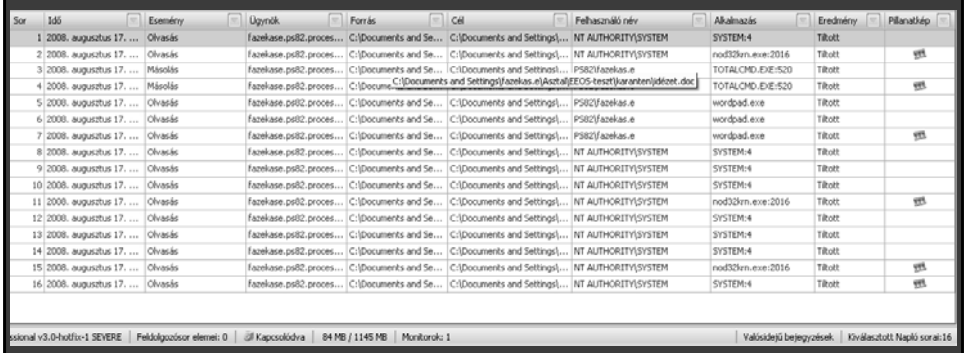
FLT: File Lifecycle Tracking: a fájlok teljes életútjának felrajzolása „Honnan jött? Hová ment?"

SLT: Storage Lifecycle Tracking: a tárolók aktivitásának követése egyedi azonosító alapján - „Kié?" „Melyik gépekhez csatlakoztatták?" „Milyen fájlok kerültek rá?"

Pillanatképek: képernyőmentés a fájlesemény pillanatáról (egyedi tömörítésben, a log mellé csatolva)

Naplózás

- **Valósidejű naplózás**



- **Naplóeredmények megtekintése: EagleEyeOS™ Viewer**

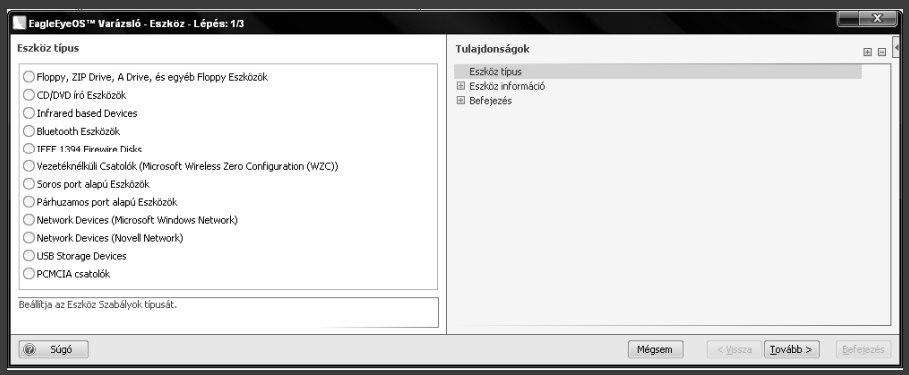
Szabálykialakítás

- **A vállalati informatikai szabályzat teljes leképezése a rendszer által:**
  - **Felhasználó alapú**
  - **Gép alapú**

  } **…és ezek kombinációja**

Eszköz- és tárolókezelés

- **Fájlrendszer alapú tárolók kezelése:**
  normál, read-only, tiltott
- **Mobil eszközök kezelése:**
  (MTP - Media Transfer Protocol, PTP – Picture Transfer Protocol)



Egyedi technológia

- **Fájlmegosztó Zónák kialakítása (Easy, One, Professional): A hálózat és alhálózat, valamint tetszőleges felhasználói csoportok védett fájlmegosztása**
- **Karanténok (Easy, One, Professional) : Az itt tárolt fájlok cél elérési útja pontosan meghatározható, így ellenőrizetlenül, véletlenül nem kerülhet ki fájl a gépről**
- **Könyvtár védelem (Easy, One): a kijelölt könyvtárak elérhetetlenné válnak a veszélyesnek minősített alkalmazások számára (pl. Skype sérülékenység)**

Üzemeltetés

Telepítés: tömegesen és észrevétlenül

Lincenszkezelés: kliensalapon

Javítások: lokális fájlból vagy online

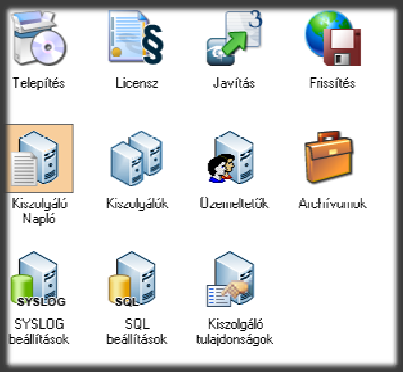
Frissítés: lokális fájlból vagy online

Szerverek: tetszőleges számú szerver lehet a rendszeren belül

Szerver naplózás: minden rendszeren belüli esemény naplózásra kerül

Üzemeltetők korlátlan számban, tetszőleges jogosultsági szinteken kinevezhetők

Archívumok: méretalapon vagy időalapon



EAGLEEYEOS™

Az elérhető eredmény

A bevezetés során:

megtörténik az adatvagyon és a kockázatok felmérése

A működés kezdetén:

A naplóállományok elemzésével megalkotásra vagy korrigálásra kerül a vállalat IT biztonsági szabályzata

A működés során:

A hozzáférések ellenőrizhetők, az incidensekről azonnal értesül a rendszergazda

Az üzemeltetés során:

A hozzáférés kezelés automatikussá válik, így az IT biztonsági szabályzat betartatása nem jelent plusz munkát

További információk

A prezentáció letöltése:
www.processorg.hu

A szoftverek letöltése és további dokumentációk:
www.eagleeyeos.com

Publikációk IT biztonság témakörben:
www.saveas.hu

Köszönöm a figyelmet!

Köszönöm a figyelmet!

Fazekas Éva

Processorg Software 82 Kft.
Mobil: +36 30 460 1085
E-mail: fazekas.e@processorg.hu

- w w w . processorg . hu -

Köszönöm a figyelmet!