Zabezpečení osobních údajů

Ing. Jan Bukovský

Praha, 1.2.2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Cíl semináře

- Nařízení GDPR v § 83 ukládá za porušení povinností správce a zpracovatele podle článků …25 až 39… správní pokuty až do výše 10.000.000 EUR…
- V tom je tedy i §32 „Zabezpečení zpracování“
- Dalo by se tedy očekávat, že „vhodná technická a organizační opatření pro ochranu dat“ budou v nařízení GDPR důkladně popsána.
- Bohužel, není tomu tak. Nařízení GDPR se praktickými opatřeními zabývá jen velmi málo.

- **Cílem tedy je popsat některá základní technická a organizační opatření a upozornit i na některá úskalí při jejich nasazení a používání.**

Povinnosti správců dle GDPR

- Nařízení GDPR požaduje zpracovávat data zabezpečeným způsobem (viz např. článek 5f) GDPR:
- „Osobní údaje musí být … **zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením** („integrita a důvěrnost“)“
- Dále např. § 25 odst.2: „Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, **jež jsou pro každý konkrétní účel daného zpracování nezbytné**. Tato povinnost se týká **množství** shromážděných osobních údajů, **rozsahu jejich zpracování**, **doby jejich uložení** a jejich **dostupnosti**. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.“

Zabezpečení zpracování - § 32 GDPR

- 1. Správce a zpracovatel … provedou vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
- a) pseudonymizace a šifrování osobních údajů;
- b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Zabezpečení zpracování - § 32 GDPR II.

- 2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
- 4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Povinnosti správců a zpracovatelů v oblasti zabezpečení a zpracování osobních údajů

- Jen nezbytné údaje a v nezbytném rozsahu zpracování
- Uložení a dostupnost jen v nezbytném rozsahu
- Ochrana před ztrátou, zničením a poškozením
- Ochrana před neoprávněným zpracováním
- Nesmí být zpřístupněno neomezenému počtu osob
- Odolné systémy včetně kontinuity v případě výpadků
- Analýza rizik a opakované testování
- Zpracování pouze na pokyn správce (nebo ze zákonných důvodů)

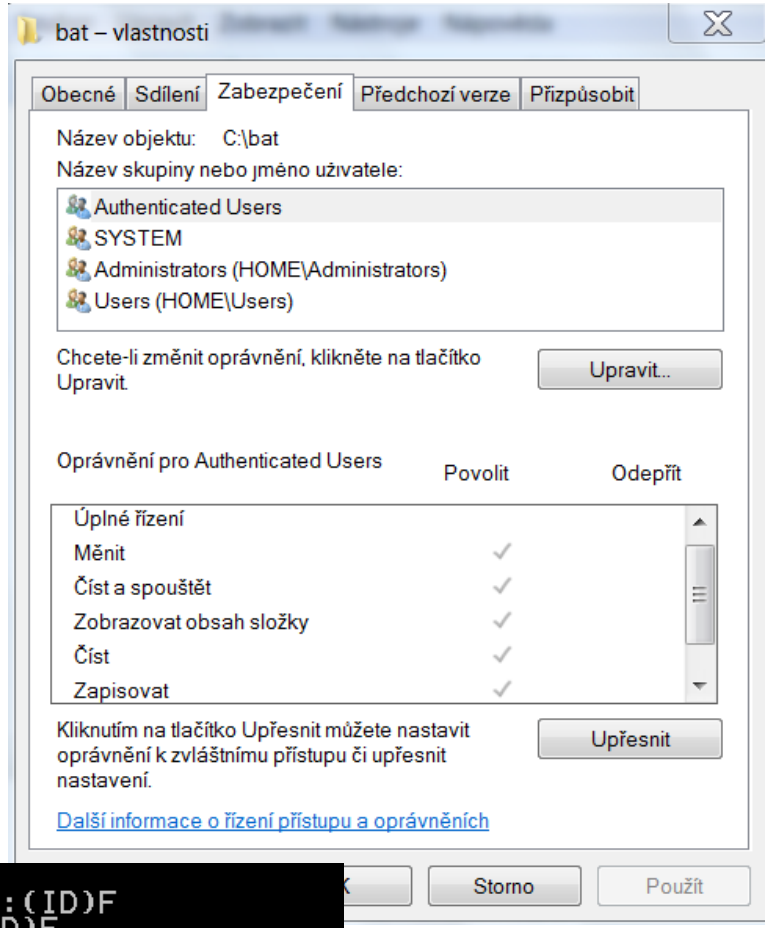
Úvodní (rozdílová, GAP) analýza

- Zjistit, kde všude se v organizaci nacházejí osobní data
- Na základě čeho se shromažďují (zákon, souhlas) a jak se zpracovávají
- Zda uložení a zpracování dat je v souladu s požadavky GDPR (zde se právě posuzuje onen „rozdíl“ uvedený v názvu analýzy)
- Jakými nápravnými opatřeními je soulad s GDPR možno dosáhnout

Osobní údaje	Na základě čeho sbírány	Kde uloženy	Jaké zpraco-vání	Zabezpe-čení dat	Soulad s GDPR	Nápravná opatření

Omezení přístupu

Zjistí se např.
CACLS C:\BAT*.*
F full, R read, W write




```
C:\bat\auto>cacls *.*
C:\bat\auto\AUTOMAT1.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT2.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT3.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT4.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C
```

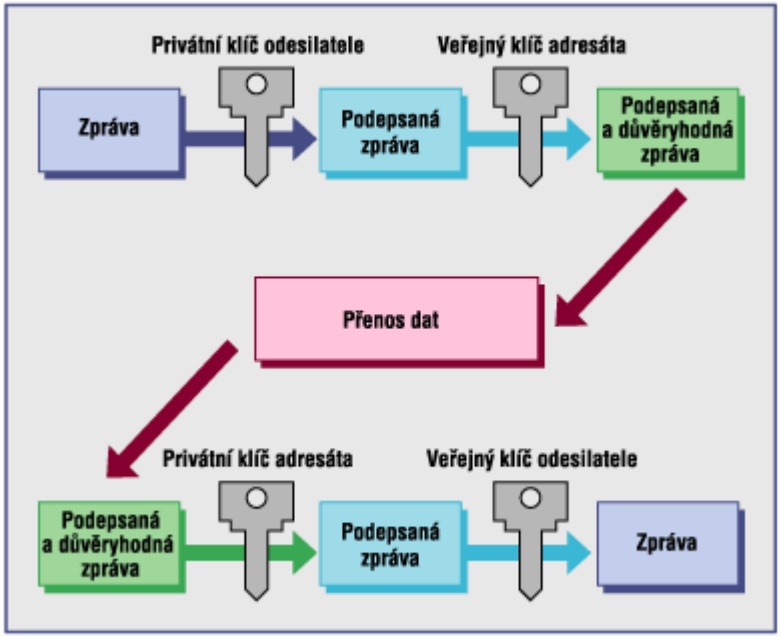
Šifrování

- **Šifrování dat** je proces, kterým se nezabezpečená elektronická data převádí za pomoci kryptografických postupů na data šifrovaná, čitelná ideálně pouze pro majitele dešifrovacího klíče. Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu včetně přenosu přes telekomunikační sítě nebo Internet.
- Symetrické
- Asymetrické

Asymetrické šifrování

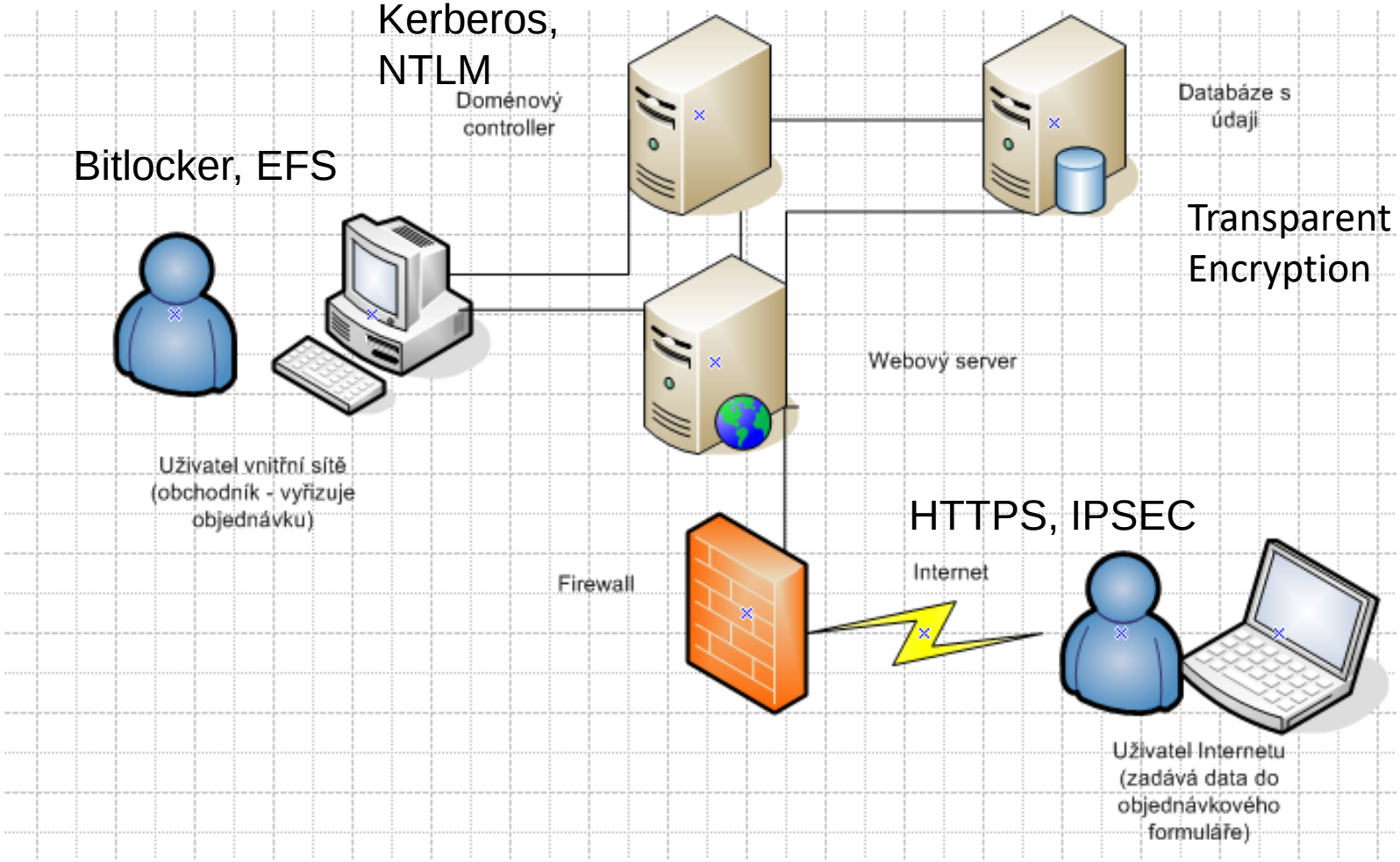
Snadný přenos klíčů, ale pomalé

Šifruje se veřejným klíčem příjemce



Dešifruje se soukromým klíčem příjemce

Co vše se dá šifrovat a jak



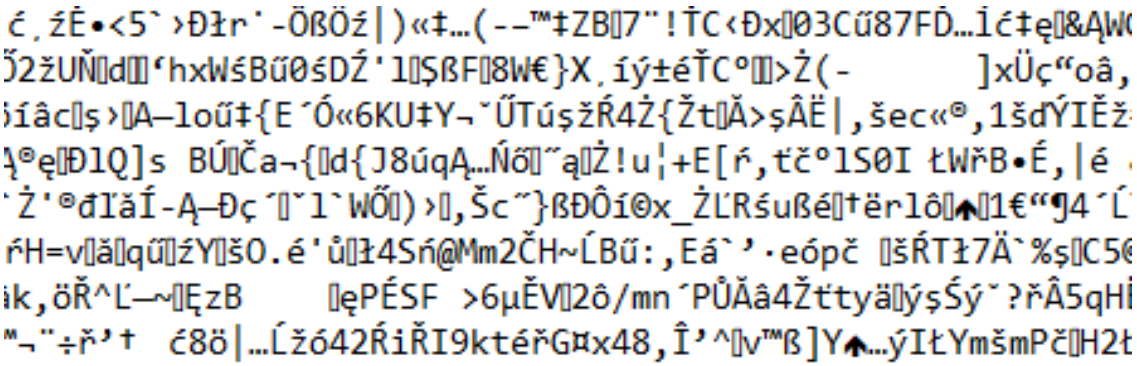
Anonymizace a pseudonymizace

- **Anonymizace** - Pojem se používá v českém prostředí již dlouhou dobu. Jejím principem je nahrazení pouze některých záznamů v databázi – pouze těch, kde jsou obsažena osobní data. Anonymizace je nevratný proces bez možnosti zpětné identifikace osoby. To znamená, že se data nedají v budoucnu dohledat.
- **Pseudonymizace** je procesem vratným. Vaše osobní údaje ve vybraných záznamech databáze jsou v tomto případě opět nahrazeny, ale je možné je v budoucnosti zrekonstruovat. K rekonstrukci (odhalení) osobních údajů je nutné mít "klíč" (obvykle nějakou převodní tabulku nebo znalost nějakého algoritmu).

Šifrování a pseudonymizace – rozdíl

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	Mach	18000	Praha 1 Štupartská 6
55	Milan	Zamrazil	25000	Praha 5 Na Bělidle 6
56	Karel	Winter	50000	Praha 8 Novákových 13
57	Milan	Páv	12000	Kladno Železničářů 12

Originál



Šifrování

Šifrování a pseudonymizace – rozdíl II.

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	Mach	18000	Praha 1 Štupartská 6
55	Milan	Zamrazil	25000	Praha 5 Na Bělidle 6
56	Karel	Winter	50000	Praha 8 Novákových 13
57	Milan	Páv	12000	Kladno Železničářů 12

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	XXX	18000	ZZZ
55	Milan	XXX	25000	ZZZ
56	Karel	XXX	50000	ZZZ
57	Milan	XXX	12000	ZZZ

ID	Jméno	Příjmení	Mzda	Adresa
54	Karel	BOGOJ	18000	99MAA
55	Milan	MAOAM	25000	14BRT
56	Karel	KUTUL	50000	55UVU
57	Milan	UUTAV	12000	18STR

Nahoře anonymizace,
Vlevo pseudonymizace

Velmi citlivým údajem je převodní tabulka nebo algoritmus!

Výhody a nevýhody způsobů zabezpečení dat

Způsob	Proti čemu chrání	Proti čemu nechrání
Přístupová práva	Přístup neoprávněných zaměstnanců nebo cizích osob (nemají přístup)	Odposlouchávání, ztráta médií (CD apod.), neoprávněné zpracování jinak oprávněnými zaměstnanci
Šifrování	Přístup neoprávněných zaměstnanců nebo cizích osob (neznají klíč), odposlech během přenosu, ztráta médií	Neoprávněné zpracování jinak oprávněnými zaměstnanci. Často zpomaluje zpracování (musí se zašifrovat všechna data)
Pseudonymizace	Přístup neoprávněných zaměstnanců nebo cizích osob (neznají systém pseudonymizace), odposlech během přenosu, ztráta médií (částečně). Rychlejší.	Neoprávněné zpracování jinak oprávněnými zaměstnanci (zejména adminy). Extrémní citlivost převodních mechanismů!

Bezpečnostní monitoring

- Slabina většiny technických řešení:
  - jejich neúčinnost na osoby, které byly organizací určeny jako oprávněné
  - nerozlišují, jestli se osobní data zpracovávají jen v potřebném, tedy minimálním možném rozsahu.
- Proto monitorování aktivit osob zpracovávajících osobní údaje.
  - Požadavky na takové monitorování - viz např. vyhláška 316/2014 Sb.
- Např. Monitoring na Active Directory
- Monitoring přístupů do Internetu nebo mailu
- DLP (Data Loss Prevention)

Vyhláška 316/2014 Sb. § 21

- ***Odst. 1*** a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti a
- *b)* ochranu získaných informací před neoprávněným čtením nebo změnou.
- **Odst.2** a) přihlášení a odhlášení uživatelů a administrátorů,
- *b)* činnosti provedené administrátory,
- *c)* činnosti vedoucí ke změně přístupových oprávnění,
- *d)* neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- *g)* přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
- *h)* použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

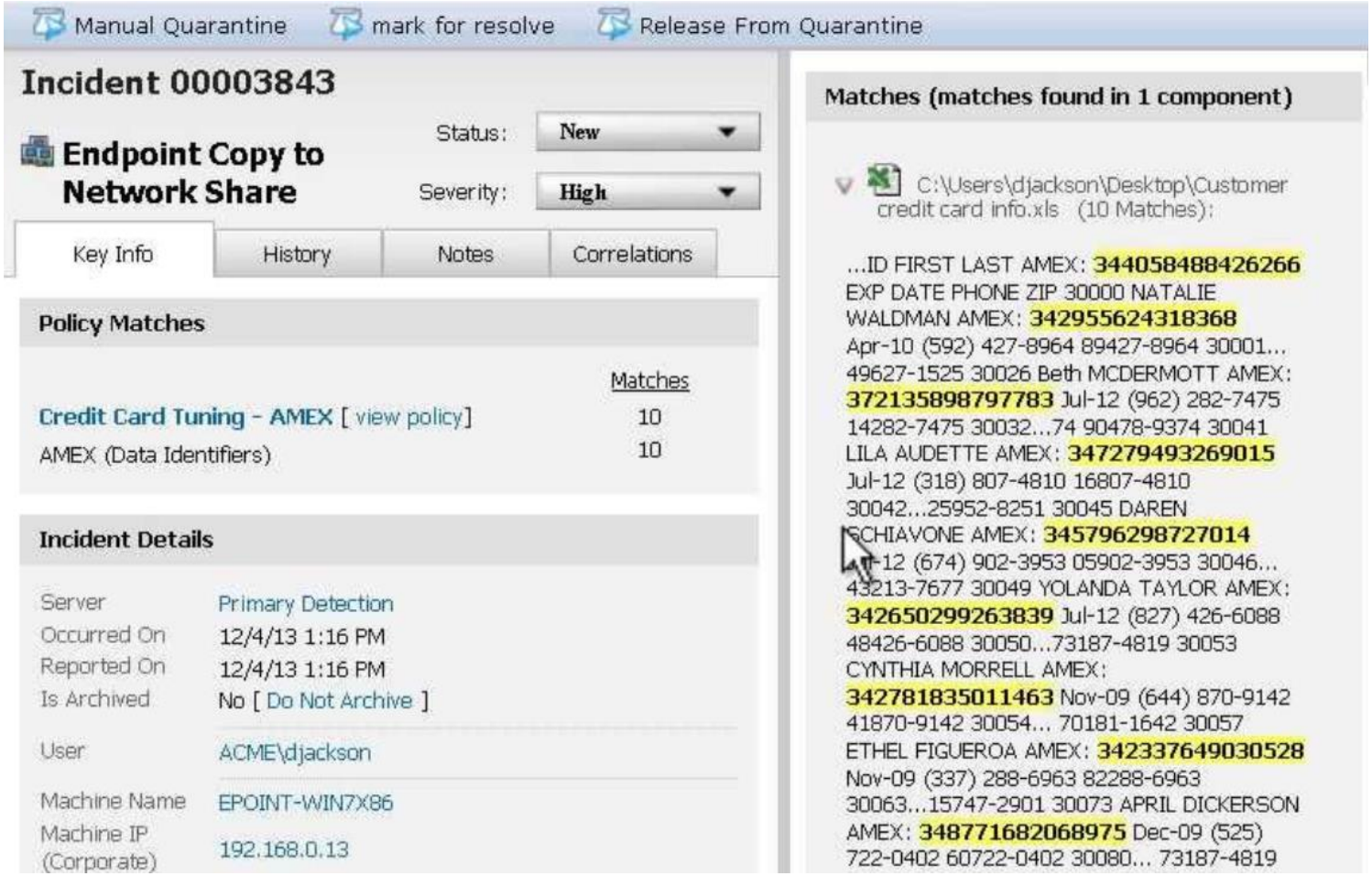
Log na Active Directory

- Spustit EVENTVWR na doménovém cntrolleru
- Co např. sledovat:
- Změny vlastního logu (ID 516, 517, změna času ID 520)
- Jakékoli změny group policy (ID 608 – 609)
- Jakékoli změny v založení a zrušení účtů (ID 624, 630, ale i 625 a dále sada ID k odemknutí účtů 621,626,628..)
- Jakékoli změny ve skupinách (ID 631, 634 a dále změny ve složení skupin ID 632 – 633)
- Více než 50 chybných přihlášení během deseti minut (ID 529 – 534, 537)
- Počty a časy úspěšných přihlášení (ID 528, 538)
- Četnost chybných přihlášení (ID 529 – 532, a zejména 644 – uzamčení účtu)

Funkce DLP monitoringu

- Pouze monitorovat (ukládat záznamy o uživ. aktivitách a příp. zneužití dat)
- Blokovat (tj. podezřelé aktivity se nezpracují),
- Šifrovat (tj. např. mail se odešle, ale zašifrovaný, a příjemce jej nepřečte, pokud šifru nezná),
- Varovat obsluhu systému (tj. hned, jak byla data zpracována, dozví se to určený specialista),
- Varovat uživatele (edukace zaměstnanců – tj. zaměstnanec se dozví, že jeho aktivita je sledována a zaznamenána).
- Nevýhody:
  - DLP systém sám zpracovává osobní data!
  - Aktivita se nezaznamená, dokud není nastaveno příslušné pravidlo DLP

Data Loss Prevention



Fyzická bezpečnost

- Velký význam – je v podstatě na úrovni vnější ochrany
- Zábrany, vrátnice, klíče, karty, zónování…
- EZS, EPS
- aktivní prvky, síťové zásuvky (bránit v připojení cizích PC!) uklízečky, návštěvy…
- stanice (bránit ve vyjmutí disků)
- notebooky (hrozí odcizení mimo organizaci! vždy NTFS, šifrování!), mobily
- média (diskety, CD, pásky – nesmí se volně povalovat bez ochrany!)
- Databáze: zajistit hlavně stanice administrátorů a jejich hesla
- Písemnosti: uzamčení, trezory, vědět, kde se nachází
- DMS, archiv, podatelna

Fyzická ochrana serveroven

- Uzamčení, přístup na karty pro omezený počet pracovníků IT, zaznamenávání průchodů
- Servery musí být i na lokální úrovni zaheslovány a opatřeny šetřičem nebo uvedeny na přihlašovací obrazovku
- Náhradní zdroje (UPS), klimatizace – zdroj potenciálních poruch a narušení fyz. bezpečnosti
- Racky by měly být uzamčeny
- Náhradní sály musí být uzamčeny až do doby použití
- Zabezpečit je třeba i tel. ústředny a komunikační prvky (kabelová hlava, antény, přenos na náhr. pracoviště…)
- Režimová opatření

Závěrečné shrnutí

- **Některá vhodná technicko-organizační opatření pro ochranu osobních údajů při jejich uložení a zpracování:**
- Omezení přístupu
- Šifrování
- Pseudonymizace
- Monitorování uživatelů a administrátorů
- Fyzická ochrana dat
- Odolné systémy
- Kontinuita podnikání
- Omezení rozsahu zpracovávaných dat
- Procesy a umístění dat analyzovány a aktuální
- …

Děkuji za pozornost!

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz