



**Aby vaše data boli v bezpečí
a vy ste mohli pokojne spávať**

Miroslav Kalinovský, HP Technology Services / November, 2014

„Privacy is not for the passive.“

Jeffrey Rosen

História bezpečnostných incidentov



- Za posledných 10 rokov sa výdavky na IT bezpečnosť zvyšovali o 11% ročne ^{*1}
- Podľa agentúry ENISA (European Union Agency for Network and Information Security) sa v 19 krajinách z 28 zúčastnených EU krajín udial závažný incident a iba v 9 sa neudial žiaden incident ^{*2}
- 94% organizácií niekedy utrpelo prienik aspoň jedného záznamu ₁

• *1 <http://www.ponemon.org/>

• *2 <https://www.enisa.europa.eu/>

Dôvody prečo sa zaoberať témou bezpečnosti



- Vo Veľkej Británii prieskum ukázal, že 43% spoločností nad 250 zamestnancov utrpelo za posledný rok krádež alebo neoprávnený prístup k dátam, a iba 30% tento útok verejne priznalo ^{*3}
- Zákazníci požadujú kontrolu nad svojimi dátami a zníženie hrozby úniku dát pri zachovaní primeraných nákladov a prácnosti

• ^{*3} <http://www.gov.uk>, INFORMATION SECURITY BREACHES SURVEY 2014

Potreby organizácií v kontexte bezpečnosti a súkromia dát



- Zabránenie neoprávneného prístupu k údajom – jednak k aktívnym (prístupy do systémov, heslá) ale aj k archívnym či záložným (sejť na páskové médiá)
- Procesy v súlade s lokálnymi právnymi predpismi a normami
- Potreba bezpečného odstránenia dát z vyradených nosičov, prípadne fyzické znehodnotenie nosičov údajov – v prípade fyzickej likvidácie je potrebný presný postup, aby bolo možné zabezpečiť opakovateľnosť a spoľahlivosť

Životný cyklus dát

Rôzne obdobia si vyžadujú rozdielne služby pre starostlivosť o bezpečnosť dát

Nasadzovanie

- overenie implementácie, penetration testing

Produkčné obdobie

- SIEM produkty
- Sieťová bezpečnosť
- Aplikačná bezpečnosť
- Závady hardvéru

Post-produkčné obdobie

- Presun zariadení na iné oddelenie, dcérsku firmu a podobne



Životný cyklus dát

Rôzne obdobia si vyžadujú rozdielne služby pre starostlivosť o bezpečnosť dát

Vyradenie zariadenia

- Zmazanie dát nepostačuje,
- Potreba znehodnotenia uložených dát (čí zariadenia), ako aj vymeniteľné médiá

NIST 800-88 Clear/Purge Method (I, II, I+II), DoD 5220.22-M ECE, NSA, Certified for Common Criteria (ISO 15408)

Čo robíme pre riešenie týchto výziev



- Softvér pre jednotlivé oblasti životného cyklu: TippingPoint, ArcSight, Fortify,
- Defective Media Retention
- Comprehensive Defective Material Retention
- Data Sanitization Services for Storage
- Data Sanitization Services for Servers
- Onsite Media Sanitization
- Asset Recovery

Čo ďalej a ako by to mohlo prakticky vyzerat'



- Dôraz na výber partnera pre bezpečnosť a súkromie dát
- Čakanie sa neopláca
- Venovať sa tejto oblasti ako celku

- Príklad IT oddelenia kde sa kladie veľký dôraz na bezpečnosť

Zdroje doplňujících informací



www.hp.com/services/dataprivacy

www.ponemon.org

www.nist.org

www.gov.uk

Ďakujem za pozornosť

