SECURITY 2012

20. ročník konference o bezpečnosti v ICT

DLP
a
ochrana osobních údajů

Miloš Šnytr

Úřad pro ochranu osobních údajů

Co chráníme

- **Direktiva 95/46/ES**
  - o ochraně fyzických osob v souvislosti se zpracováním osobních údajů …
- **Zákon č.101/2000 Sb**.
  - o ochraně osobních údajů…

Zpracování osobních údajů

- Osobní údaje
  - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů….
  - Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat …
- Zpracování
  - Jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. …

Zabezpečení údajů

- **§13 Zákona o ochraně osobních údajů**
  - Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, **neoprávněným přenosům**, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. ….

Zákoník práce

- **§316**
  - (1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

Zákoník práce

- **§316**
  - (2) Zaměstnavatel nesmí **bez závažného důvodu** spočívajícího ve **zvláštní povaze činnosti zaměstnavatele** narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

Zákoník práce

- **§316**
  - (3) Jestliže **je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele**, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, **je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.**

DLP a ochrana osobních údajů

- DLP v přenášené komunikaci (v obsahu i v metadatech /názvu, příjemci, . . .*)* cíleně vyhledává datové struktury, které s velkou pravděpodobností vypadají jako osobní údaje (jména, **RČ,** adresy, **...)** nebo …..
- **Jde tedy o zpracování osobních údajů**

DLP a ochrana osobních údajů

- Dojde-li k detekci porušujícího jednání, tj. je podle nastavené konfigurace důvodné podezření na porušení bezpečnostní politiky, je obsah komunikace zachycen a odeslán na centrální DLP server. Tam může správce DLP serveru provádět další investigaci nad výtahem vzorku, který odeslání reportu způsobil nebo i nad celým obsahem souboru.

DLP a ochrana osobních údajů

- Dojde-li k detekci porušujícího jednání, tj. je podle nastavené konfigurace důvodné podezření na porušení bezpečnostní politiky, je obsah komunikace zachycen a odeslán na centrální DLP server. Tam může správce DLP serveru provádět další investigaci nad výtahem vzorku, který odeslání reportu způsobil nebo i nad celým obsahem souboru.
- **Data tedy jsou dále zpracovávána!**

Zpracování osobních údajů

- Provozovatel DLP systému je jako správce povinen:
  - Stanovit rozsah nezbytný k naplnění účelu
  - Uchovávat pouze po dobu nezbytnou
  - Nesdružovat údaje
  - Zpracování řádně zabezpečit
  - …

DLP systémy

- Jsou jen jednou z forem zajištění bezpečnosti dat.
- Nacházejí data vyvolávající podezření, že zaměstnanec zpracovává data v rozporu s nastavenými pravidly.
- zaměstnavatel je povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění
- **Další zpracování jen v součinnosti se zaměstnancem!**

DLP systémy

- Lze je považovat za plnění právní povinnosti správce?
  - Jen jestliže je u zaměstnavatele dán **závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele**

DLP systémy

- Jedná-li se o plnění právní povinnosti správce.
  - Lze provádět zpracování bez souhlasu zaměstnanců.
  - **Není tedy třeba plnit oznamovací povinnost dle §16 ZOOU (registrace).**

DLP systémy

- Jedná-li se o plnění právní povinnosti správce.
  - Není sice třeba plnit oznamovací povinnost dle §16 ZOOU (registrace).
  - **Správce, je povinen zajistit, aby informace, týkající se zejména účelu zpracování, kategorií osobních údajů, kategorií subjektů údajů, kategorií příjemců a doby uchování, které by byly jinak přístupné prostřednictvím registru vedeného Úřadem, byly zpřístupněny, a to i dálkovým přístupem nebo jinou vhodnou formou.**

DLP systémy

- Pokud nejde o plnění právní povinnosti správce.
  - **Zpracovávat data pouze se souhlasem zaměstnance !**
  - **Je třeba plnit oznamovací povinnost dle §16 ZOOU.**

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Miloš Šnytr
ÚOOÚ
milos.snytr@uoou.cz