SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Hledání jistot při přípravě DLP řešení

Pavel Běhal

T-Mobile Czech Republic a.s.

Na počátku byla … idea DLP

- Výstupy analýzy rizik a několika auditů – riziko:
  - „Nedostatečně pokrýváte kontrolu nakládání s daty na externích médiích.“
  - „Nemáte přehled, zda emailovou komunikací neodchází i osobní, telekomunikační či jiné sensitivní údaje.“
- Špatné zkušenosti s ochranou dat na stanicích ze spřáteleného zahraničí
- Rostoucí hodnota kvalitních dat na trhu

Úskalí – budeme sledovat uživatele

- Ano i Ne … jak to vlastně bude?
- Otevřeny otázky:
  - Jak získat pro DLP našeho interního zákazníka?
  - Známe technické možnosti a omezení DLP řešení?
    - Nelze využít/nasadit něco jiného?
    - Reference – pozitivní i negativní?
    - Provozní dopady? Dostupnost? Náklady? Lidé?
  - Co na to český právní řád?
    - Přístup dalších osob k sensitivním údajům?
    - Soulad s právní ochranou soukromí zaměstnanců?
    - Kdo bude vlastníkem a provozovatelem řešení?
    - Utajit či zveřejnit sledování?

Jistota 1. – Osobní údaje

- Konzultovali jsme u nejpovolanějších = ÚOOÚ

- Klíčová zjištění dle z.č. 101/2000 Sb.:
  - Z titulu správce osobních údajů máme právo detekovat jednání osob porušujících bezpečnostní politiku při přístupu k osobním údajům.
  - DLP může být legitimním a legálním technickým prostředkem pro provádění kontroly nakládání s údaji.
  - Uživatelé musí být předem prokazatelně a závazně seznámeni se všemi souvisejícími interními pravidly.
  - I v rámci systému DLP musí být zajištěna zákonná ochrana údajů, a to zejména vymezením práv a povinností dohlížejících osob.
  - Není vyžadována zvláštní oznamovací povinnost pro používání nástroje.

Jistota 2. – Zákoník práce

- Využili jsme právní pomoci

- Klíčová zjištění dle §316 z.č. 262/2006 Sb.:
  - Naše Společnost naplňuje pojem „zvláštní povaha činnosti zaměstnavatele“ pokud jde o činnost zaměstnanců pracujících s daty obsaženými v databázích zákaznických údajů.
    - Shodně však lze toto aplikovat i pro práci s: know-how, obchodním tajemstvím a údaji zaměstnanců.
  - Zaměstnavatel je povinen informovat zaměstnance o rozsahu kontroly a o způsobu jejího provádění.
  - Musíme respektovat princip proporcionality, přiměřenosti a princip dobrých mravů.
    - Kontrolní mechanismy použité pro plnění účelu musí co nejméně narušovat soukromí zaměstnanců.

Výsledek … obdrželi jsme zelenou

- Pro projekt jsme stanovili mantinely:
  - Omezit cíle dohledu pouze na:
    - data charakteru osobních údajů a údajů o telekomunikačním provozu ve větším než malém množství,
    - velmi úzkou množinu citlivých dokumentů,
    - uživatele s prokazatelným přístupem k těmto datům,
    - předávaní dat externím emailem, webem a výměnnými médii.
  - Minimalizovat implementační i provozní náklady
    - Předejít dopadům na odezvu a dostupnost aplikací
    - Analýza business procesů bude až předmětem provozního ladění

Kde jsme nyní

- Zvolili jsme výrobce i dodavatele

- Pracujeme na implementaci DLP, včetně:
  - dohledové politiky vyhovující stanoveným cílům,
  - procesu řízení incidentů,
  - směrnice o sledování nakládání s daty a úpravy existujících personálních směrnic,
  - komunikační kampaně na zaměstnance.

- Více informací (možná) na „SECURITY 2013“ ☺

A na konci …

- Řešení DLP aktuálně chápeme primárně jako nástroj zvyšování uživatelského povědomí o ochraně údajů, nástroj na podporu prevence a teprve v poslední řadě jako zdroj indicií o činnosti v rozporu s interními směrnicemi Společnosti.

- DLP = Data Leak Prevention

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Pavel Běhal

T-Mobile Czech Rep. a.s.

pavel.behal@t-mobile.cz