Ochrana citlivých dat v praxi

Ing. Pavel Běhal, CISSP

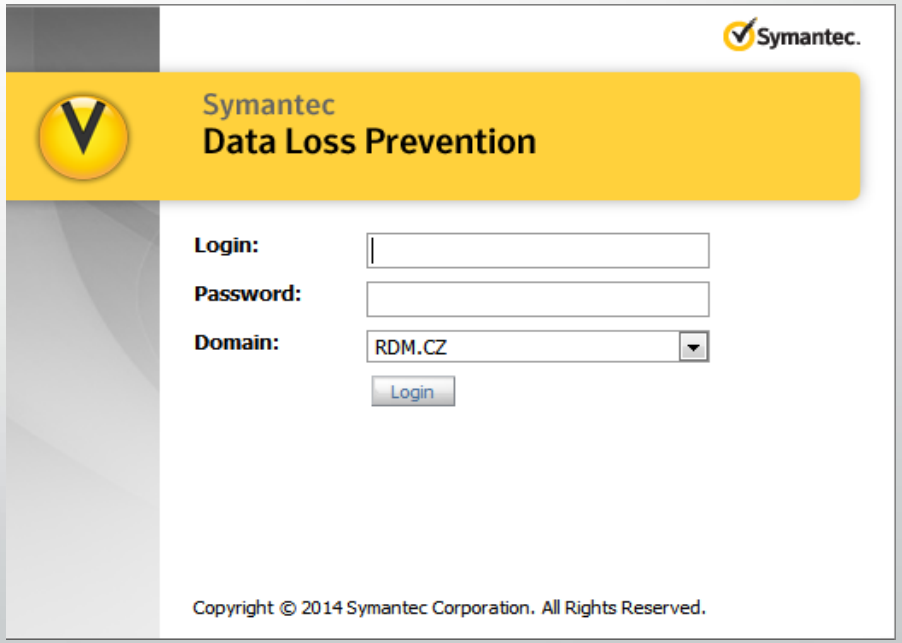
Vedoucí oddělení informační a datové bezpečnosti
T-Mobile Czech Republic a.s.

pavel.behal@t-mobile.cz

20. dubna 2016

Ochrana citlivých dat
versus
Data Loss/Leak Prevention (DLP) řešení

- Cílem prezentace je seznámit vás s praktickými úskalími implementace a provozu DLP řešení na ochranu dat z pohledu vlastníka jednoho takového řešení



DLP nefunguje

- …

DLP ne-funguje, pokud

- si nejsem jist, jaké mám povinnosti a jaké mám pravomoci
  - Základem je
    - Identifikace procesů/služeb, aktiv a analýza rizik
    - Klasifikace informací
  - Musím respektovat všechny relevantní právní a regulační rámce
    - Ochrana osobních údajů, Pracovní právo, Občanský zákoník, Kybernetická bezpečnost, Smlouvy, …
    - Řešení musí, v souladu s ochranou oprávněných zájmů Společnosti, automatizovaně sledovat zpracování citlivých dat, které probíhá v rozporu s deklarovanými pravidly Společnosti

DLP ne-funguje, pokud

- nemám jasně stanovené cíle a jejich měření/akceptaci
  - Musím přesně vědět co chci zvoleným řešením dosáhnout
    - Naplnit regulaci?
    - Blokovat zpracování či přenos?
    - Zvýšit povědomí?
    - Sbírat důkazy?
  - Krátkodobě i dlouhodobě

DLP ne-funguje, pokud

- nemám zájem a podporu vedení Společnosti
  - Opatření, o kterém vedení nic netuší si „nezaslouží podporu“
  - Strategie provozu a rozvoje Společnosti musí zohledňovat i rizika a dostupná opatření na ochranu informací
  - Organizace musí viditelně deklarovat strategii, cíle a prostředky ochrany dat
  - Technicky vynucená opatření na ochranu dat nejsou svévolí „bezpečáků“, ale ochranou uživatelů, vedení firmy i samotného businessu

DLP ne-funguje, pokud

- nemám kvalifikované pracovníky dohledu a řešení incidentů
  - Čerstvá událost se řeší snáze a s nejvyšším edukačním dopadem
  - Díky dlouhodobé zkušeností lze systém politik a opatření efektivně zlepšovat
  - Musí mít přehled v evidenci incidentů i výjimek
  - Bez dostupné podpory uživatelů nelze aplikovat tvrdé restrikce

DLP ne-funguje, pokud

- neřídím citlivá data u zdroje
  - Základem je vynucení principů „need-2-know“ a „least-priviledge“ (případně i „segregation of duties“)
    - Procesy a technologie řízení přístupů (IdAM) a privilegovaných přístupů (PAM)
  - Dokumenty musí být značeny stupněm citlivosti informací (klasifikovány)
  - Využívat maskování dat a omezení náhledu
    - Případně i pseudoanonymizaci a anonymizaci

DLP ne-funguje, pokud

- nemám pod kontrolou všechna koncová zařízení a elektronické kanály
  - DLP je pouze tak efektivní, v jak uzavřeném a řízeném prostředí je nasazeno
    - Komplexní endpoint security, řízení aplikací a elektronických médií/kanálů je základem
    - Podporované v. povolené formáty souborů
    - Jak na šifrování souborů?
    - … zůstává: otisk obrazovky, fotoaparát, papír + tužka
  - Přístup administrátorů a podpory třetí stranou nesmí zůstat bez dohledu
  - Práce v terénu (externí obchodní kanály, technici apod.)

DLP ne-funguje, pokud

- nereaguji včas na změny v infrastruktuře a službách
  - Inovace (např.: Cloud, BYOD, VDI, MDM, HomeWorking, DevOps, Outsouring, Managed Services, Remote support, …) mohou koncepci ochrany dat snadno a rychle rozbít
  - Omezování nákladů a požadavky na extra komfort pak vedou
    - k akceptaci rizika
    - k nutnosti monitoringu potenciálního zneužití
      - Musí se kombinovat se: Sandboxing, SIEM, Nahrávání terminálů, Misuse Detection (behaviorální sledování)

DLP ne-funguje, pokud

- neinformuji otevřeně dotčené pracovníky
  - Je nezbytné předem proškolit interní i externí pracovníky o důvodech, charakteru a rozsahu (potenciálního) automatizovaného sledování a dohledu zpracování citlivých dat
  - Doporučuje se, aby o proškolení existoval záznam s podpisem pracovníka

DLP ne-funguje, pokud

- nemám stanovena pravidla nakládání se zachycenými událostmi
  - Přístup k zachyceným událostem musí být jasně omezen (citlivé informace)
  - Nutno zohlednit možnost zachycení soukromých informací
    - (např. informace o pravidelné prohlídce u závodního lékaře)
  - Nastavit pravidelné promazávání již neaktuálních dat
  - Stanovit politiku a pravidla interního vyšetřování

DLP funguje

- …

DLP funguje

- Pomáhá nám identifikovat změny v procesech zpracování citlivých dat
- Odhalujeme s ním procedurální chyby uživatelů (méně závažná porušení pravidel)
- Slouží ke zvyšování povědomí uživatelů o ochraně dat
- Využíváme jako zdroj indicií / důkazů pro interní vyšetřování (závažná porušení pravidel)
- Společně s dalšími opatřeními přispívá k ochraně citlivých informací

Děkuji vám za pozornost