SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Proč ochrana dat a informací není běžnou součástí každodenního života?

Martin HANZAL

SODATSW spol. s r.o.

Obsah příspěvku

- Hledání odpovědí hlavně na otázky:
  - Co v současnosti běžně děláme pro ochranu dat a informací?
  - Kde jsou současné největší mezery v ochraně dat a informací?
  - Jaké odpovědnosti mají jednotliví pracovníci v organizaci zpracovávající citlivá data a informace?
  - Co můžeme udělat k tomu, abychom zvýšili ochranu zpracovávaným datům a informacím?

Představení autora

- Martin HANZAL je současným výkonným ředitelem společnosti SODATSW spol. s r.o., která od roku 1997 pomáhá technickými prostředky zvyšovat ochranu informací a to především:
  - Ochrana informací opouštějících chráněné prostředí organizace
  - Ochrana informací před neoprávněnou manipulací ze strany oprávněných uživatelů
  - Monitoring přístupů k citlivým informacím organizace

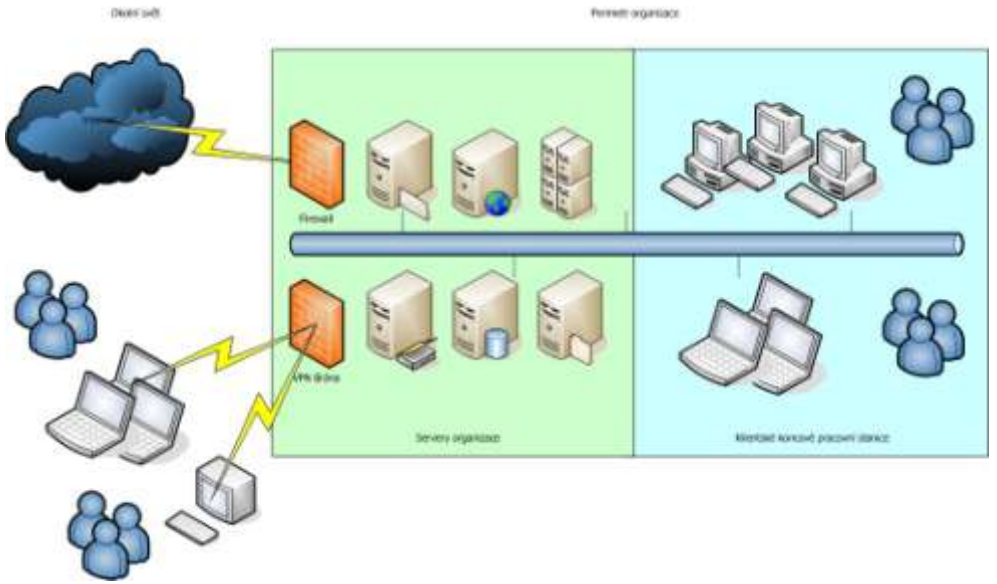
Pracovní role v organizaci

- Manažer
  - Ředitel, vedoucí pracovník odpovědný za určitou část organizace
    - IT manažer (CIO)
    - Bezpečnostní manažer (CISO)
- Správa IT
  - Technický pracovník zodpovědný hlavně za provoz a mnohdy rozvoj jednotlivých částí IS/IT, po technické stránce za bezpečnostní mechanismy
- Uživatelé – my všichni, uvnitř i vně organizace

Používané prostředky ochrany

- Identifikace a autentizace
- Řízení přístupů k jednotlivým entitám IS
- Antivirová kontrola
- Šifrování – pouze v rámci komunikačních protokolů
- Elektronický podpis
- Monitorování událostí (logování)

- A co šifrování uložených dat a informací?



Statistiky ukazují

- Šifrování uložených dat v ČR používá:
  - 16% organizací používajících notebooky nebo média, na kterých fyzicky data opouštějí organizaci
  - 4% organizací používají šifrování na data uložená uvnitř perimetru
- A přitom je uznávanou pravdou:
  - Naprostá většina úspěšných útoků znamenajících ztrátu organizaci je vedena na uložená data a ne na data přenášená komunikačními protokoly
- Absence šifrování uložených dat je časovanou bombou pro zpracovatele i poskytovatele

Ochrana dat v organizaci

- Běžný uživatel
  - Svým chováním může značně ohrozit způsob ochrany dat, ale sám od sebe nezačne ani nemůže použít technické prostředky na zvýšení ochrany
- Správci IS/IT
  - V rámci celkové ochrany dat organizace je provozovatelem IS/IT a tedy i provozovatelem technických prostředků k ochraně dat
- Manažeři
  - Jsou odpovědni za způsob ochrany dat v organizaci

Běžná praxe v organizaci

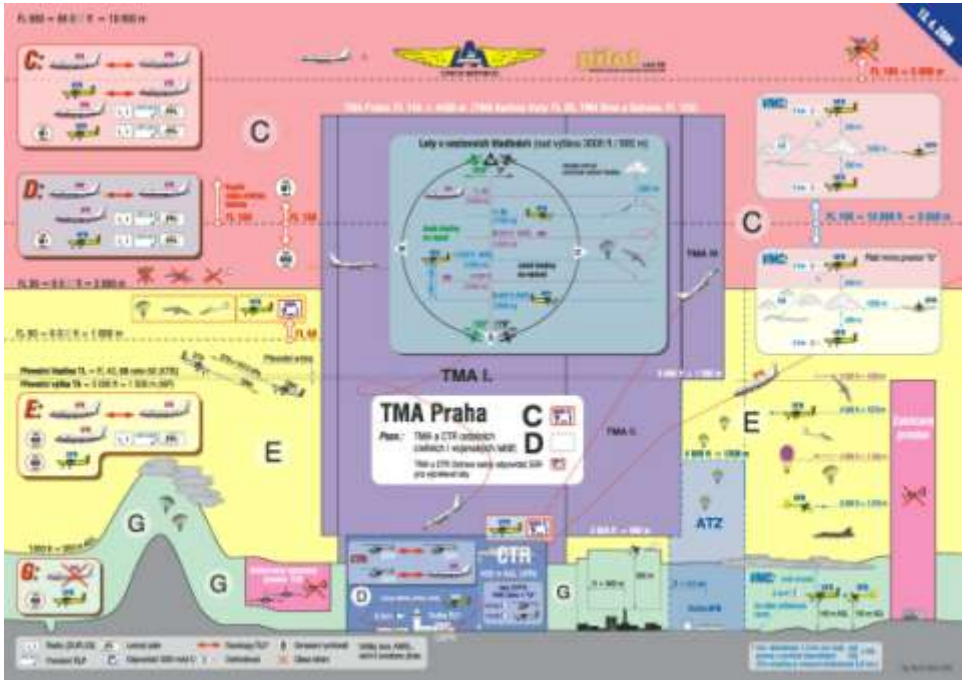
- Běžný uživatel
  - Většinou nepochybuje o tom, že by data byla nedostatečně chráněna, protože to přece řeší správa IT
- Správci IS/IT
  - Většinou nepřichází s návrhy řešící problematiku zvýšení ochrany dat, jejích hlavním cílem je udržet celý IS/IT systém organizace v provozu
- Manažeři
  - Zapomínají, že oni vytváří strategii pro ochranu dat v organizacích

Zákon na ochranu informací

- Neexistuje ucelený zákon, kterým by se obecně řídily pravidla provozování IS/IT zpracovávající citlivá data a informace
  - Pro organizace platí zákon na ochranu osobních údajů 101/2000 Sb. (hlavně §13), obchodní zákoník 513/1991 Sb. (hlavně §17, §271)
- Způsob ochrany je na zodpovědnosti řídících pracovníků zodpovědných za vedení organizace
- Vhodným průvodcem je norma ISO 27001 – Information Security Management System (ISMS)

Srovnání s bezpečností v letectví

- Mezinárodní organizace pro civilní letectví (ICAO) ustanovená Chicagskou dohodou z dne 7. prosince 1944
- Hlavní cíl: „Bezpečnost a plynulost civilního letectví“



Kdo připravuje ochranu dat

- Bezpečnostní manažer
- Bezpečnostní manažer nebývá běžně samostatnou pracovní pozicí. V praxi se setkáváme:
  - Manažer kvality se stane i manažerem bezpečnosti
  - HR oddělení případně právní oddělení
  - Vnitřní kontrola
  - Některý z ředitelů
- Důležité je, aby se ochrana dat řešila v rámci managementu organizace

Informační mapa

- Vytvořte seznam všech typů informací, které se v organizaci nachází
- Každému typu náleží zodpovědná osoba
- Určete klasifikaci jednotlivých informací podle jejich hodnoty
- Vytvořte seznam všech možných úložišť, na kterých se mohou informace nacházet
- Vytvořte vztahovou matici mezi klasifikací a jednotlivými úložišti

Datový audit

- Většina IS/IT je nějakou dobu provozována bez klasifikace informací a pravidel k jejich ukládání
- K přesnému zorientování může sloužit datový audit, který zjistí typ ukládaných dat do jednotlivých úložišť
- V praxi se ukazuje, že až 60% všech dat organizace je uloženo na jiných datových úložištích, než v původních databázích

Politika ochrany dat

- Důležitý výchozí dokument, který musí být akceptovaný managementem organizace
- Politika by měla obsahovat:
  - Prostředky pro ochranu pracovních nástrojů – jedná se o desktopy, notebooky, mobilní a přenosná zařízení používaná pracovníky organizace
  - Prostředky na ochranu sdílených dat uvnitř organizace a mezi spolupracujícími organizacemi
  - Kontrolní mechanismy zajišťující spolehlivost použití systému ochrany dat v organizaci

Pracovní nástroje

- Bezpečné zpracování dat na desktopech a noteboocích pracovníků
  - Šifrování lokálně zpracovávaných dat – dokumenty, exporty a importy reportů apod.
- Bezpečný přenos dat mezi jednotlivými pracovníky a spolupracujícími subjekty
  - Emailová výměna dat
  - Výměna dat přes výměnná média a sdílená úložiště

Sdílení dat

- Možnost šifrování sdílených dat v rámci pracovních skupin, které zpracovávají pro organizaci data s nejvyšší klasifikací (nejcitlivější data)
- Jednoznačně prokazatelné přístupy a případně důvody přístupů k zpracovávaným datům organizace
- Bezpečná výměna dat, která jsou zpracovávána ve více organizacích (propojování více systémů)

Kontrola organizace

- Kontrola z pohledu organizace zabezpečuje prokazatelně správnou funkčnost celého systému ochrany dat
  - Monitorování přístupů
  - Manipulace ze strany obsluhy (modifikace, kopírování, přenos apod.)
  - Stav bezpečnostní mechanismů (co bylo, je a jak chráněno)
- Pokud dojde k úniku dat, pak mohl selhat jednotlivec, nikoli však celý systém

Ochrana dat - šifrování

- Nejedná se o produkt, který se nasadí v IS/IT organizace a pak už běží sám
- Jedná se o proces, který prolíná celou organizaci a týká se většiny pracovníků a pracovních pozic
- Ochranu dat správci IS/IT provozují, nemůžou být však jako jediní odpovědni za správnost provozu

Závěr

- Manažeři
  - Nečekejte, že správci IS/IT zavedou systém na ochranu dat sami od sebe – požadavek musí přijít z vedení organizace
- Správci IS/IT
  - Je pravděpodobné, že pokud nastane ztráta či únik dat, tak se bude odpovědnost házet na vás
- Uživatelé
  - Zkuste někdy popřemýšlet, jestli vaše organizace dostatečně chrání zpracovávaná data

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Martin HANZAL
SODATSW spol. s r.o.
martin@sodatsw.cz