SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Zavádění PKI infrastruktury v organizaci - procesní aspekty

Vlastimil Červený, Kateřina Minaříková

Deloitte Advisory, s.r.o.

Agenda

- Zavádění PKI v organizaci – úvod
  - Proč je procesní bezpečnost někdy náročnější než technická?
- Bezpečnostní standardy PKI
  - Které normy v oblasti PKI můžeme využít?
- Procesy zavádění PKI v organizaci
  - Na jaké kroky bychom určitě neměli zapomenout?
- Nejčastější problémy z praxe
  - Na co si dát při zavádění PKI pozor?

Zavádění PKI v organizaci - úvod

- Technická vs. Procesní náročnost zavádění PKI
- Vybudování PKI infrastruktury nám automaticky neřeší problémy
  - Použití certifikátů v uživatelských aplikacích
  - Začlenění správy životního cyklu certifikátů mezi ostatní IT procesy dané organizace
  - Uživatelská přívětivost v použití certifikátů
- Velké nároky na procesní bezpečnost při zavádění i provozu PKI

Bezpečnostní standardy PKI

- Existuje řada mezinárodních norem v oblasti PKI
  - **ETSI TS 101 456** - Policy requirements for certification authorities issuing qualified certificates
  - **ETSI TS 102 042** - Policy requirements for certification authorities issuing public key certificates
  - **CWA 14167-1 -** Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
  - **WebTrust for Certificate Authorities**
  - **ISO 21188:2006** - Public Key Infrastructure for financial services -- Practices and policy framework

Procesy zavádění PKI

I. Definice bezpečnostních služeb PKI

II. Kategorizace uživatelů a bezpečnostní role

III. Návrh technického řešení PKI

IV. Stanovení bezpečnostních požadavků na PKI

V. Stanovení požadavků na životní cyklus certifikátů

VI. Instalace PKI a ceremoniál generování kryptografických klíčů CA

VII. Školení koncových uživatelů

Procesy zavádění PKI I.

I. Definice bezpečnostních služeb PKI

- Které „služby“ PKI v naší organizaci potřebujeme?
  - elektronický podpis e-mailů,
  - šífrování e-mailů,
  - autentizace technických zařízení,
  - šifrování datových úložišť,
  - atd.
- Jaké aplikace bude PKI podporovat?
  - E-mail
  - Přístupový systém
- Požadavky na poskytované PKI služby (certifikáty) by měly vždy vyplývat z řídící dokumentace organizace v oblasti klasifikace dat!

Procesy zavádění PKI II.

II. Kategorizace uživatelů a bezpečnostní role

- Kdo bude poskytované PKI služby v naší organizaci používat?
  - Interní zaměstnanci (všichni zaměstnanci vs. vybrané skupiny uživatelů)
  - Externí subjekty (problémy se vzdálenou identifikací a autentizací, bezpečné předání žádosti o certifikát, atd.)
  - Technické zařízení (je potřeba určit vlastníky těchto zařízení)
- Kdo bude zastávat jednotlivé bezpečnostní role v rámci PKI?
  - Je třeba obsadit technické a procesní bezpečnostní role PKI (Bezpečnostní úředník PKI, Administrátor CA, Správce certifikátů, Auditor CA, atd.)
  - Požadavky SOD (Segregation Of Duties)

Procesy zavádění PKI III.

III. Návrh technického řešení PKI

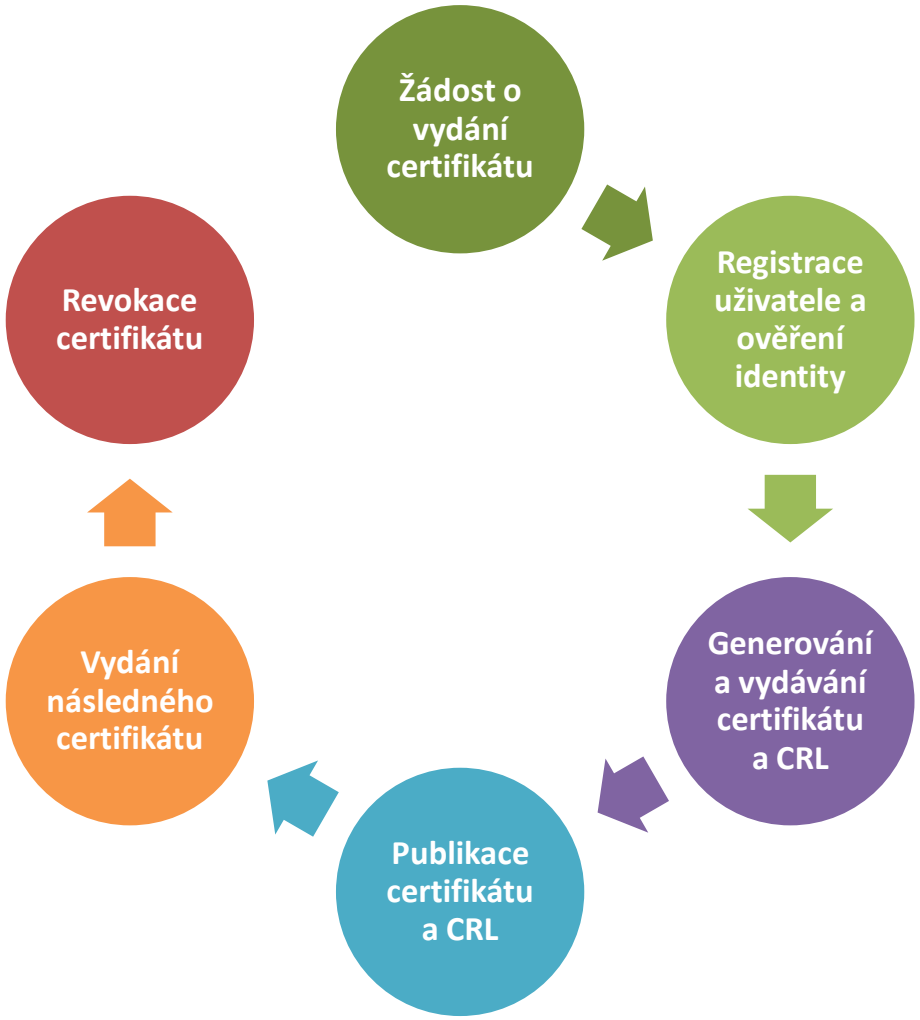
- Volba technologie PKI
  - Microsoft Certification Authority VS. Jiné řešení
- Návrh architektury PKI
  - Jedno, dvou, tří vrstvá architektura CA
  - Napojení PKI na další ICT systémy (LDAP, webové rozhraní, card management system, HSM, atd.)
- Návrh úložišť kryptografických klíčů
  - Uložení soukromých klíčů CA (HSM, souborový systém)
  - Uložení soukromých klíčů uživatelů (souborový systém, chipové karty, USB token, ..)

Procesy zavádění PKI IV.

IV. Stanovení bezpečnostních požadavků na PKI (Systémová bezpečnostní politika CA)
- Parametry kryptografických klíčů a použitých algoritmů
- Personální bezpečnost (bezpečnostní role, SOD)
- Uložení soukromých klíčů CA a soukromých klíčů uživatelů
- Řízení přístupu
- Síťová bezpečnost
- Zajištění dostupnosti PKI infrastruktury a PKI služeb
- Zálohování a obnova dat a soukromých klíčů
- Fyzická a environmentální bezpečnost PKI

Procesy zavádění PKI V.

V. Stanovení požadavků na životní cyklus certifikátů a kryptografických klíčů
   - Certifikační politika (CP)
   - Certifikační prováděcí směrnice (CPS)
   - Struktura CP, CPS např. dle RFC 3647



Procesy zavádění PKI VI.

VI. Instalace PKI a Ceremoniál generování kryptografických klíčů CA

- Cílem ceremoniálu je řízeným procesem za účasti osob v bezpečnostních rolích vytvořit základy PKI infrastruktury:
  - Instalace CA
  - Vygenerování klíčového páru CA
  - Zálohování soukromých klíčů CA
  - Bezpečné uložení záloh klíčů a CA
- Jedná se o klíčový moment v důvěryhodnosti celé PKI infrastruktury!

Procesy zavádění PKI VII.

VII. Školení koncových uživatelů

- Vytvoření pravidel použití certifikátů pro uživatele
  - Psáno jazykem koncových uživatelů
- Koncoví uživatelé by měli mít jasně dáno, kdy mají danou PKI službu (certifikát) použít (vyplývá z klasifikace dat)

PKI – nejčastější problémy z praxe

- Budování PKI bez provedené identifikace a klasifikace informačních aktiv
- Chybějící bezpečnostní požadavky na nakládání s informačními aktivy (dle jejich klasifikace)
- Nejasné požadavky na použití PKI služeb
- Chybějící podpora vedení organizace pro vybudování PKI nebo při implementaci => vyplývá z nejasných požadavků na PKI služby

PKI – nejčastější problémy z praxe

- Problémy s obsazením do bezpečnostních rolí PKI
  - Role se netýkají pouze oddělení IT
- Chybějící ceremoniál generování klíčů
  - Instalaci PKI provádí interní IT nebo externí dodavatel – a co důvěryhodnost PKI??
- Nedostatky v procesní dokumentaci (CP, CPS)
- Problémy se zaváděním certifikátů do užívání koncovými uživateli
  - Jak přesvědčit koncové uživatele k používání certifikátů?
- Chybějící školení koncových uživatelů

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Vlastimil Červený, CIA, CISA
vcerveny@deloitteCE.com
Kateřina Minaříková, CISA, CISSP
kminarikova@deloitteCE.com
Deloitte Advisory, s.r.o.