Bezpečnost: kontroly, bezpečnostní politika, standardy; Internet a vybraná bezpečnostní řešení

PV080

Vašek Matyáš

Zásadní kroky pro zajištění bezpečnosti

1. Analýza hrozeb

2. Specifikace bezpečnostní politiky a architektury

3. Popis bezpečnostních mechanismů

Kontroly

- Co vlastně dělat? (Analýza rizik)
- Jak to budeme dělat? (Bezpečnostní politika)
- Jaký systém použít? (Kritéria hodnocení bezpečnosti)
- Děláme to dobře? (Interní audit)
- Dělají to špatně? (Externí, příp. i vynucený audit)

Audit IT

- Naplánování auditu
- Dokumentace a posouzení kontrol
  - Důraz na dokumentaci, ne technologie!
- Výběr testů souladu a jejich provedení
  - Je dokumentace správná?
- Výběr a provedení speciálních testů
  - Skutečná kontrola funkčnosti
- Celkové posouzení systému

- Interní audit: Oddělení nezávislé na IT oddělení!

Od zranitelnosti k riziku

- ***Zranitelnost*** – slabé místo v systému
- ***Hrozba*** – akce/událost, která může ohrozit bezpečnost
  - potenciální využití zranitelnosti
- ***Riziko*** – pravděpodobnost, že se hrozba uplatní (zranitelnost využije)
  - Dva aspekty – pravděpodobnost a výše škody
- ***Útok*** – akt využití zranitelnosti (realizace hrozby)

Analýza rizik v IS obecně

- Často podle standardu (BS7799)
- Srovnání rizik a kontrol
  - Použití definované stupnice
  - Neoceňuje hodnoty
- Přístup odhadu podle informačních aktiv
  - Vhodnější pro společnosti kriticky závislé na IT a také společnosti se složitější kontrolou. Živnostníkovi stačí v méně formální postup srovnání rizik a kontrol.

Analýza rizik

- Zvážit, co všechno by mělo být chráněno
- Vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám.
  - Často nelze než vycházet z analýzy empirických poznatků o problémech v okolí, jiných útocích na podobné hodnoty atd.
- Chybně provedená analýza rizik má za důsledek téměř vždy chybně navržená bezpečnostní opatření. Hodnoty pak mohou být chráněny velmi nákladným, ale naprosto nesmyslným a neúčinným způsobem.

Analýza rizik

- Častěji spíše proces odhadu rizik – méně formální a podrobný než skutečná analýza
- Kvantitativní vs. kvalitativní
- Kvantitativní
  - Výstup je velmi srozumitelný
  - Nejčastěji výstup v $$$ (vystavení rizikům)
- Kvalitativní
  - Diskrétní stupnice (ne $$$)
  - Jednodušší postup, automatizovatelný, ale výsledky nejsou lehce srozumitelné

Analýza rizik – metoda ALE

- Annual Loss Expectancy
- ALE = SLE x ARO
- SLE – Single Loss Exposure
- ARO – Annualized Rate of Occurrence

Analýza rizik – BPA

- Business Process Analysis
- Širší pojetí rizik, nejen IT
  - Některá IT rizika tak mohou zůstat neidentifikována (pokud neovlivňují obchodní proces)
- Výstupy
  - Mapa procesů a jejich popisy.
  - Tabulka rizik (kvalitativní) a kontrol
  - Doporučení

CRAMM

- 1985 – Vláda UK – Risk Analysis and Management Method
- Strukturovaný přístup ve třech fázích:
  - Identifikace a ocenění hodnot.
  - Odhad hrozeb a zranitelností hodnot.
  - Výběr vhodných protiopatření.
- Analýza vcelku složitá, používá se zvláštní software a je zde velká časová náročnost, potřeba školených specialistů.

Několik poznámek k analýze rizik

- Sběr informací – dotazníky, pohovory atd.
- Kontrola úplnosti – formální kontroly, ale hlavně zkušenost hodnotitelů!!!
- Zpracování vstupních dat
  - polo/automatizované
- Zpráva s návrhy pro snížení rizik

Bezpečnostní politika

- Co a jak mají dosáhnout ochranná opatření.
- Cíl – minimalizace (kontrola) rizik.
- Strategie – jak dosáhnout cíle – použití bezpečnostních funkcí
  - Zahrnuje požadavky, pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami.
- Většinou psána normálním jazykem, lze ale použít i nějaký druh formalismu.

Bezpečnostní politika

- Celková bezpečnostní politika
  - Určitá míra nezávislosti na použitých IT.
  - Citlivá data, zodpovědnosti, základ infrastruktury.
  - Horizont nad 5 let.
- Systémová bezpečnostní politika
  - Zohledňuje použité IT, konkretizace CBP.
  - Horizont obvykle cca 2-3 roky.
- Příp. další, specifické, politiky – provozní, personální, intranetová...

Bezpečnostní (IT) standardy

- Motivace
  - Kompatibilita, cena implementace a změn
  - Minimalizace problémů
- Standardy oficiální (vyžadovány zákonnými normami) – ČSNI, ISO
- Standardy průmyslové
- Kritéria hodnocení bezpečnosti

Kritéria hodnocení bezpečnosti

- USA – konec 60. let a 70. léta – potřeba minimalizovat výdaje na jednotlivá hodnocení kupovaných systémů
- Jednotné měřítko hodnocení bezpečnosti
- 1985 – Trusted Computer System Evaluation Criteria – "Oranžová kniha"
  - D – žádná bezpečnost (nevyhověl vyšší třídě)
  - A1 – nejvyšší úroveň (matematický formalismus)
- ITSEC (Evropa), CTCPEC (Kanada)
- Common Criteria (CC)

Common Criteria

- Target of evaluation (TOE) – co se hodnotí
- Protection profile (čipové karty, firewally)
  - Katalogizován (aplikace kritérií v dané oblasti)
- Security target (ST) – teoretický cíl
- Hodnocení TOE – odpovídá realita teorii (ST)?
- Požadavky funkčnosti (co) a záruk (jak dobře koncepčně)

Význam kritérií

- Zjednodušují použití bezpečných systémů
  - Jednodušší vzájemné srovnání
  - Jednodušší odhad, zda systém splňuje požadavky
- Zjednodušují specifikaci požadavků
- Zjednodušují návrh a vývoj bezpečných systémů

BS7799

1. Code of Practice for Information Security Management – 1995
2. Specification for Information Security Management Systems – 1998

- Oba doplněny v roce 1999
- ISO/IEC standard 17799, i jako česká norma

Úloha manažera bezpečnosti IT

- Zkušenost s bezpečností důležitá, ale...
- Umění přesvědčovat je zásadní!
- Zkušenost: 60 % manažer, 40 % expert
- Místo velmi náročné
  - Kritizován za bezpečnostní incidenty
  - Kritizován za obstrukce “normálnímu” chodu
  - Jak může být oceněn za “nic se neděje!”? ☺

Internet a bezpečnost

- Důvěrnost a integrita emailu
  - S/MIME (Netscape, Outlook) – stejný certifikát jako pro SSL – viz přednášku k podpisu
  - PGP (ale i další – disk, ICQ atd.)
- Důvěrnost a integrita WWW komunikace
- Anonymita
- Firewally
- Odmítnutí služby
- Eternity server

Anonymní web browsing

- Spojení do skupiny „nerozlišitelných jedinců“
- Slabiny
  - Velikost skupiny
  - Správce skupiny
- www.anonymizer.com (připojení na proxy)
  - průkopník ve svém oboru, nyní ze situace komerčně těží
- Další projekty (např. Crowds) s vlastní uživ. proxy

Anonymní email I.

- Broadcastové sítě – filozofie doručení zpráv všem, lze šifrovat pro vybrané(ho)
  - Anonymita příjemce
- („anonymní“) remailery třídy 0
  - V podstatě pseudonymita a nespojitelnost příjemce s odesilatelem, udržování tabulky pseudonymů
- („anonymní“) remailery třídy 1 – řízení činnosti příkazy
- Více článek T. Beneše (DSM 2/2001)

Anonymní email II.

- Remailery – neochrání před statistickým rozborem komunikace (délka zpráv, frekvence atd.)
- Mixy – cibulovité schéma (symetrická vs. asym. kryptografie)
  - Generování klamných zpráv.
  - Doplňování délky
  - Možnost míchání okruhů
  - Více příští přednáška...

Pretty Good Privacy

- Umožňuje šifrování a digitální podpis (+ jiné)
- Kombinace sym. a asym. kryptografie
  - Šifrování – veřejným klíčem příjemce se šifruje vždy nově generovaný klíč pro sym. šifru
  - Podpis – soukromým klíčem se podpíše haš zprávy
- Autor Phil Zimmermann, už přes 15 let od v1!
- Integrace – elm, mutt, Eudora, Outlook...
- Nyní výraznější vývoj přes Gnu Privacy Guard (GPG / GnuPG)
- Více na www.gpg.cz (dříve www.pgp.cz)

PGP klíč

- RSA (2.6.x) a Diffie-Hellman/DSS
- Délka klíče
- *UserID* – obvykle jméno a email
- Otisk (fingerprint)
- Úroveň důvěry – zachovávat opatrnost!!!
- A další: KeyID, datum vytvoření, platnost (novější verze PGP)...

Klíče PGP

- Klíčenka (keyring)
- Revokování – problém ztráty hesla nebo narušení integrity
- Tranzitivita důvěry
- Servery klíčů
  - Také přes www.gpg.cz

Podepisování klíče

- Podepsat vlastní klíč!!!
  - Integrita
- Cizí klíče jen při důvěryhodném předání!!!
  - Zaslání emailem nebo web link NEJSOU DŮVĚRYHODNÉ!
  - Osobní předání na disketě
  - Ověření otisku před podpisem (telefon, papír ap.)
  - Důvěryhodný zprostředkovatel (!)

Další vylepšení PGP

- Šifrování disku
- Dokonalejší mazání dat (wipe)
- Práce s certifikáty X.509 a PKI vůbec
- Rozdělení klíče (prahová kryptografie)
- Problém s odvoláním klíče - designated revoker
- ICQ plugin
- Fotografie k *UserID*

...atd

TLS (Transport Layer Security), dříve jako SSL (Secure Sockets Layer)

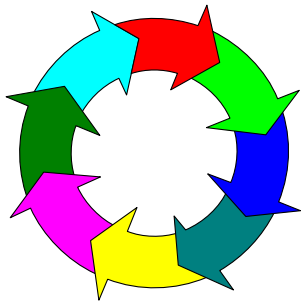
- Protokol pro
  - Autentizaci entit (klient, server)
  - Kontrolu integrity
  - Důvěrnost komunikace
- Vyvinut firmou Netscape, široce podporován
- Běží na protokolech jako TCP a je transparentní pro vyšší HTTP, FTP...
- Certifikáty X.509, WWW prohlížeče

O TLS/SSL

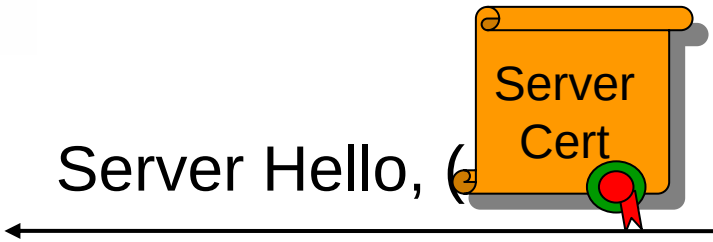
- TLS/SSL Record Protocol
  - Základní vrstva
- TLS/SSL Handshake Protocol
  - Pro úvodní autentizaci a nastavení parametrů spojení
  - Autentizace serveru default (lze zrušit), klienta na vyžádání
  - Autentizace digitálními certifikáty (klíči)

TLS/SSL Handshake Protocol

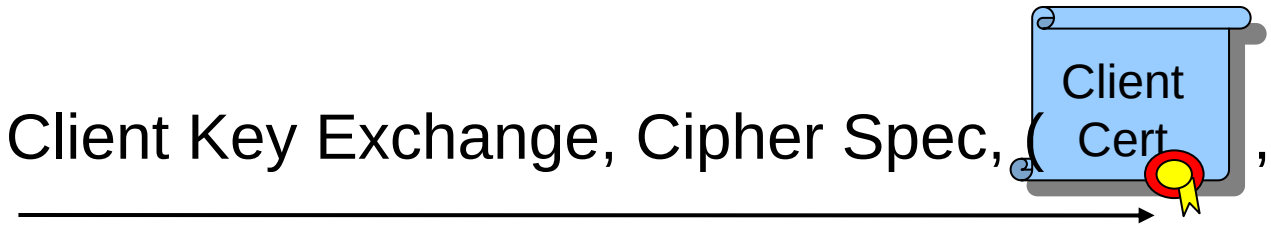
Server



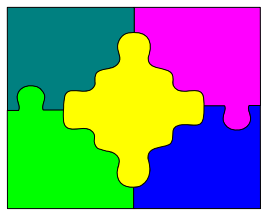
Client Hello



Server Hello, (Server Cert , Client Cert Request,…)



Client Key Exchange, Cipher Spec, (Client Cert , ...)



Application Data

S E C U R E

Protokoly, o kterých můžete slyšet

- IPSec – zajištění bezp. pro IPv4
- IPv6
  - Šifrování i ochrana integrity přímo v možnostech IP
- SET (Secure Electronic Transactions)
  - Dnes zajímavý příklad: bezpečnost vs. přidaná hodnosta
    - Bezpečnost velmi vysoká
    - Použitelnost z hlediska zákazníka a obchodníka komplikovaná
    - Náročnost vedla k zániku (původní verze)

Autentizace pro internetbanking

- Heslo – putuje nešifrovaný haš (slovníkový útok)
- TLS/SSL kanál – ochrana hesla
- Klientský certifikát (Trojský kůň!)
- Jednorázová hesla
  - Fyzický generátor (lze i závislost na čase ap.)
  - Předem vygenerovaná posloupnost na papíru
- Homebanking, speciální aplikace/plugin

Firewally

- Název odpovídá koncepci – jedná se o umělou překážku mezi chráněnou zónou a potenciálně nebezpečným okolím
- Chrání proti útokům zvenčí (proti těm, které přes něj vedou! ☺) na data/služby uvnitř
- Možnosti řešení:
  1. *Povol*
  2. *Zakaž*
  3. *Přelož (Proxy)*
- Citlivá otázka útoků odmítnutím služby

Systémy detekce průniku (narušení)

- Intrusion Detection Systems
- Principy jako u antivirů
  - Detekce atypického chování
  - Detekce vzoru (průniku)
- Umístění (v systému)
  - Počítačové (host-based)
  - Síťové (network-based)
- Neochrání proti tzv. sociálnímu inženýrství ☺

Odmítnutí služby (Denial of service)

- Provozovatel serveru
  - Ochrana vlastního systému
  - Závislost na páteřních sítích, DNS, příp. službách CA
- Uživatel – primárně ochrana vlastního počítače, ale dále
  - Může k provozu potřebovat fungující lokální síť
  - Spoléhá na ISP
  - Spoléhá na provozovatele serveru
- Distribuovaná verze útoku, farmy připravených strojů aj.

Zajímavost – Eternity server

- Ross Anderson ’96 (Pragocrypt)
  - `http://www.cl.cam.ac.uk/~rja14/#Peer-to-Peer`
- „Věčné“ uložení informací
- Lze jen uložit, nalézt a vyzvednout
  - lze dále kombinovat, např. se šifrováním
- Mazat nemůže ani původce (násilné donucení!)
- Velké množství spolupracujích serverů
- Různé geografické a právní umístění