Praktické zavádzanie informačnej bezpečnosti

Peter Bíro

Ministerstvo financií
Slovenskej republiky

MF SR, BA, júl 2009

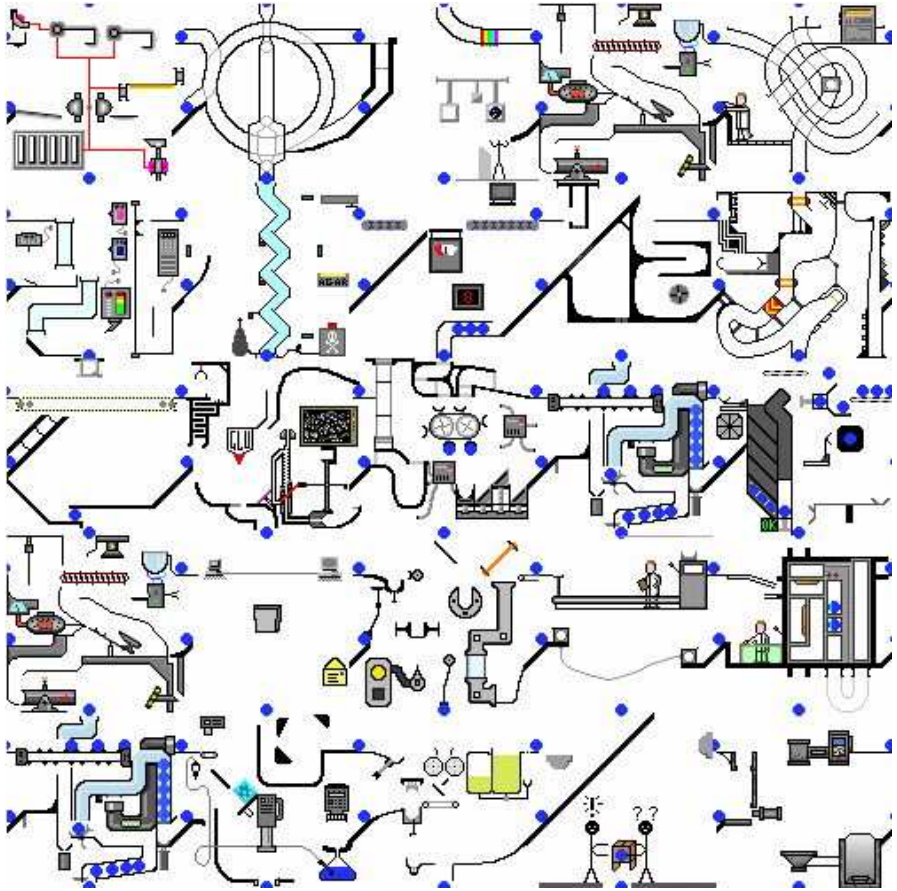
Trendy vývoja informačnej bezpečnosti

- Stále nové hrozby a spôsoby ochrany – napr. DNS cache poisoning -> DNSSEC, technológia RFID
- Útoky „nultého dňa", profesionalita kriminálnych živlov
- Významná kompromitácia osobných údajov v USA v roku 2008 – 17 mil. údajov (nárast o 69%)
- Väčšina (80%) manažérov (CIO) sa obáva najmä o kontinuitu činnosti (cca. 6% PC v Európe = 1,7 mil. incidentov)
- Na vzorke cca 1000 firiem sa manažéri v roku 2008 rozhodli navýšiť podiel bezpečnosti z rozpočtu IT na 12,6% (v roku 2007 to bolo 7,2%)
- Začína významnejšie zasahovať legislatíva a polícia:
  - uväznenie tvorcov trójskeho koňa v Japonsku, procesy so zneužívaním Wi-Fi v USA, Belgicku, v Pakistane je kybernetický terorizmus trestaný smrťou
- EÚ pripravuje povinnosť hlásiť incidenty
- Zvyšujúca sa snaha o spoluprácu bezpečnostných pracovníkov
- Informačná bezpečnosť stále významnejšia aj v SR – pribúdajúce el. služby, prepájanie registrov (možné ohrozenie z iného miesta)

Informačná bezpečnosť prakticky

Nutnosť dôslednej ochrany „okolo" celého systému

Informačná bezpečnosť prakticky



Ochranu je však nutné dobre navrhnúť – príliš komplikované riešenie môže byť kontraproduktívne

Desatoro funkčnej ochrany

1. Nutnosť poznať čo chránim, prečo to chránim a ako to chránim.
2. Úroveň bezpečnosti stanoviť na základe toho, čo chránim (tak, aby sa to útočníkovi „neoplatilo").
3. Ochrana musí byť systémová a popísaná, s jasnými zodpovednosťami.
4. Podpora vedenia je nevyhnutná.
5. Ochranná reťaz je len tak silná, ako jej najslabší článok.
6. Politiky je nutné založiť na spoločných znalostiach a požiadavkách používateľov a „technikov".
7. Riadenie prístupu na základe „potrebujem vedieť".
8. Prílišné (a neoverené) kombinácie ochranných prvkov sú vážnou hrozbou ich funkčnosti.
9. Technológia nie je všetko.
10. Spolupráca a komunikácia s ostatnými „dobrými".

Riadenie informačnej bezpečnosti prakticky

1. Znalosť prostredia – analýzy (systémy, procesy, organizácia, predpisy, štandardy/normy)
2. Prípravné činnosti – analýzy (aktíva, riziká)
3. Vytvorenie politík – všeobecné princípy
4. Vytvorenie opatrení – špecifické princípy, implementácia
5. Monitorovanie – analýzy vhodnosti opatrení a politík, overovanie praktického dodržiavania, monitorovanie aktuálnosti aktív a rizík
6. Návrhy úprav podľa zmien v 1 a 2 a výsledkov 5
7. Začiatok cyklu od 2, 3 alebo 4 (podľa potreby)

Niektoré odporúčané princípy pri zvažovaní riešení

- UTM – jednotná správa hrozieb (údržba samostatných operačných systémov a aplikácií, ktoré sú chránené jednotlivými prvkami ochrany, je komplikovaná, vyžaduje si kvalifikovaného administrátora, množstvo znalostí a času) - návrat k špecializovaným „krabiciam" – produkty na trhu však majú veľmi rôznu kvalita
- VPN
- Virtualizácia serverov
- Šifrovanie
- Vyššie úrovne identifikácie (jednorazové heslá, GRID, smart karty, biometrika atď.)

Praktické riešenie ochrany webových služieb a SOA

- validácia správ (napr. kontrola správnosti formátu (XML))
- riadenie prístupu k službe (najmä autentifikácia a autorizácia)
- používanie elektronického podpisu (preukázateľnosť pôvodu správy a integrita)
- používanie šifrovania na úrovni správy (end-to-end vs point-to-point)
- skrývanie (maskovanie) interných zdrojov a detailov implementácie (napr. potlačovanie http hlavičiek)
- vynucovanie pravidiel pre SLM (Service Level Management) (ovplyvňuje efektívne využívanie zdrojov, zabránenie zahlcovaniu)
- monitorovanie všetkých transakcií a prieskum podozrivých stavov (napr. atypicky dlhá správa, dlhý čas odozvy ~ SQL Injection)

Praktické riešenie zálohovania

- Pravidelná záloha sa zameriava na štyri oblasti:
  - Ochrana súborov na jednotlivých zariadeniach
  - Ochrana celkových kritických aplikácií organizácie bez nutnosti zastavenia ich činnosti (vrátane databáz)
  - Ochrana operačných systémov a obnova pre rozličné typy hardvéru
  - Ochrana zálohovaných údajov (napr. duplikáciou) a možnosť obnovy z iného miesta
- Existujú systémy schopné automatizovane rozoznávanie zmien (inkrementálne zálohy) – je potrebné nastaviť maximálny počet verzií jedného súboru (zálohy) a dobu uloženia
- Existujú aj vysokorýchlostné siete SAN (Storage Area Network) alebo NAS (Network Attached Storage) NAS je zálohovacie zariadenie pracujúce s dátovými súbormi, SAN je lokálna sieť viacerých zariadení, ktoré pracujú na úrovni diskových blokov.
- Minimalizácia prenášaného objemu údajov – napr. záloha dátových častí súborov (teda nie zálohu celého 100 MB súboru kvôli jednej zmene, ale iba danej časti)
- Rozoznávanie duplicitných súborov na základe obsahu (nezávisle od názvu alebo miesta uloženia)

Záver

Čo dodať záverom?

Pomaly, ale isto...

Ďakujem za pozornosť

Ing. Peter Bíro

Odbor legislatívy, metodiky, štandardov a bezpečnosti informačných systémov

Sekcia informatizácie spoločnosti

Ministerstvo financií SR

peter.biro@mfsr.sk / standard@mfsr.sk

+421/2/595 82 426