Informačná bezpečnosť
a
ochrana súkromia

(technický pohľad)

31. máj 2012

RSN

RSN činnosti

- Riadenie informačnej bezpečnosti (podľa ISO/IEC 27001) a IT procesov (ISO/IEC 20000-1)
- Projekty technické
- Projekty dokumentácie
- Konzultácie pre bezpečnost a procesy IT
- Audity

RSN

Kybernetický priestor

- Komplexné prostredie tvorené interakciou ľudí, softvéru a služieb na internete bez fyzickej formy a neexistujúcimi hranicami
- 3 druhy záujmových skupín (stakeholderi, užívatelia a provideri)
- 2 zásadné druhy útokov – zvnútra a zvonku

RSN

Ochrana kybernetického priestoru

- Pasívny monitoring (podklad pre detektívne činnosti) – IDS-sondy, agenti na serveroch, ACL – problém s virtuálnymi systémami
- Proaktívny monitoring – IPS-sondy, aktívny agenti na systémoch, proaktívny softvér ochrany
- Zvyšovanie povedomia užívateľov

RSN

Súkromie a jeho ochrana

- Informačná bezpečnosť neznamená ochranu súkromia
- Samotná legislatíva veľmi nepomôže, nezohľadňuje technickú stránku a typické vlastnosti a správanie ľudí
- Definovanie princípov súkromia

RSN

Štruktúra súkromia podľa ISO 29100

- Ciele pre štruktúru súkromia
- Požiadavky na súkromie
- Životný cyklus dátových procesov
- Kontrola dodržiavania súkromia

2 významné vplyvy prostredia:

- Právne a regulačné požiadavky
- Požiadavky podnikateľského prostredia

Požiadavky na súkromie

- PII model (Personally identifiable information)
- Lokálna alebo medzinárodná legislatíva
- Priemyselné normy
- Profesionálne normy
- Spoločenské pravidlá
- Organizačné politiky

RSN

Požiadavky na súkromie (2)

- Podnikateľské zámery a modely
- Prevádzkované aplikácie, typy dátových procesov, dátové prenosy
- Skúsenosti a porozumenie technológií
- Kontrola nad dátami vo všetkých procesoch
- Citlivosť obsahu

RSN

PII Model

- Jedinečné samostatné identifikátory ako národná identita – číslo pasu, zákaznícke číslo, biometrický identifikátor, č.kred.karty
- Ostatné PII ako meno, pohlavie, dátum narodenia, osobné tel.č.,e-mail adresa, IP adresa, zdravotný záznam, fotografia, profil správania, záznamy o návšteve web stránok, všetky informácie získané počas zdravotného ošetrenia, ...

RSN

Princípy ochrany súkromia

1. Obsah a výber
2. Špecifikácia účelu
3. Ohraničený zber
4. Obmedzenie používania, údržby a prezradenia
5. Minimalizácia dát
6. Správnosť, presnosť a kvalita
7. Otvorenosť a transparentnosť
8. Individuálna spoluúčasť a prístup
9. Zúčtovateľnosť
10. Bezpečnostné opatrenia
11. Zhoda s požiadavkami

RSN

Kľúčové faktory implementácie

- Zodpovednosť
- Politiky
- Katalogizácia a zoznamy
- Procedúry a opatrenia
- Governancia
- Zhoda s požiadavkami
- Dokumentovanie
- Školenia a povedomie

RSN

Znižovanie rizík súkromia a informačnej bezpečnosti

- Riadenie podľa rizík je hlavný faktor
- Zvyšovanie bezpečnostného povedomia a nepodceňovanie rizík (správanie na sociálnych sieťach, nákupy a platby, prenosné zariadenia, WiFi siete, cloud služby,...)
- Zavedenie technických opatrení
- Boj proti praktikám sociálneho inžinierstva

RSN

Opatrenia na redukciu rizík

- Pseudonymizácia a anonymizácia dát
- Aplikácia aspektov súkromia do životného cyklu dát (zber, spracovanie, prenos, skladovanie, archivácia, odstránenie)
- Definovanie zodpovedností a účtovateľností
- Zavedenie správy identít a prístupov
- Zavedenie štruktúr pre správu biometriky

RSN

Cloud Computing

- Služby IT ponúkané cez web – v kybernetickom priestore (dátové úložné priestory, softvérové produkty, výpočtové výkony,...)
- Kritické oblasti: technická realizácia, správa identít, dôvernosť údajov, správa a audity zdrojov, zmluvné dojednania medzi poskytovateľom a užívateľom.

RSN

Problémy prepojenia

- Technické normy vznikajú spoluprácou odborníkov na celom svete
- Legislatíva vzniká regionálne alebo lokálne a to politicky

RSN

Normy pre informačnú bezpečnosť a súkromie

Vydané normy:

ISO/IEC 27001 Riadenie informačnej bezpečnosti

ISO/IEC 27002 Implementácia informačnej bezpečnosti

ISO/IEC 27005 Riadenie rizík informačnej bezpečnosti

ISO/IEC 27031 Riadenie kontinuity

ISO/IEC 27035 Riadenie incidentov

ISO/IEC 29100 Definovanie súkromia

ISO/IEC 24760-1 Riadenie identít

RSN

Normy pre informačnú bezpečnosť a súkromie

Pripravované normy:

ISO/IEC 27014 Governancia IT

ISO/IEC 27032 Kybernetický priestor

ISO/IEC 27036 Outsourcing

ISO/IEC 29101 Štruktúra súkromia

ISO/IEC 24760-2 Riadenie identít

ISO/IEC 29745, Biometrické údaje

ISO/IEC 29146 Riadenie prístupov

ISO/IEC 27017 Cloud Computing

RSN

Ďakujem za pozornosť

Miloslav Ďurčík,CISA,CRISC mdurcik@rsn.sk