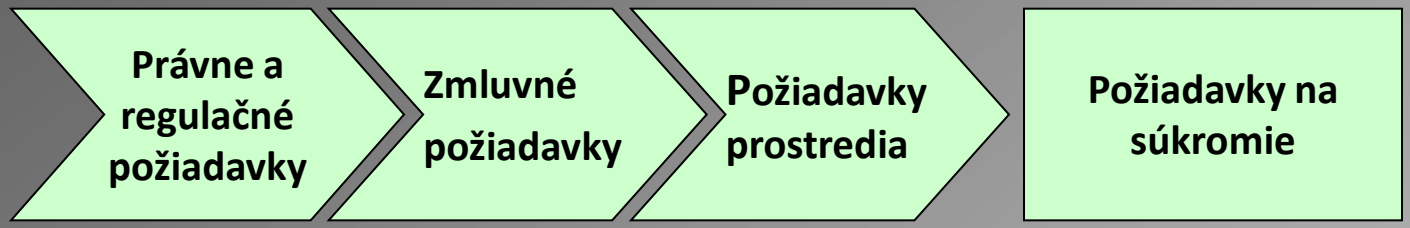
Ochrana osobných údajov v prostredí CC

SÚTN

21.februára 2013

Faktory ovplyvňujúce súkromie



- Medzinárodné právne požiadavky
- Národné zákony
- Ochrana spotrebiteľa
- ....

- Firemné politiky
- Priemyselné opatrenia
- Outsourcing
- Interný kontroling

- Podnikateľské prostredie
- Účel transakcií
- Klasifikácia obsahu
- Typy aplikácií

Právne a regulačné požiadavky

- 428/2002 Z.z. Ochrana osobných údajov
- Directive 95/46 EC Data protection
- Directive 2002/58 EC Privacy & Electronic Communication
- Regulation 45/2001 Legal Framework for processing personal data
- Foreign Intelligence Survillance Act (1978)
- Protect America Act (2007)

RSN

428 / 2002 Z.z.

Požiadavky:

- písomný súhlas na spracovanie
- bezpečnostný projekt
- určenie zodpovednej osoby
- registrácia na ÚOOÚ

Problematické oblasti zákona:

- nejednoznačné definície osobných údajov
- nešpecifikovanie technických rámcov ochrany

RSN

Požiadavky na ochranu súkromia

- Samotná legislatíva veľmi nepomôže, nezohľadňuje technickú stránku a typické vlastnosti a správanie ľudí
- Rozdiely pri tvorbe technických noriem a legislatívy
- Informačná bezpečnosť neznamená automaticky ochranu súkromia

RSN

Dôležité princípy ochrany súkromia podľa ISO/IEC 29100

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

PII Model

Definovanie entity „Actor“, ktorá môže mať tri základné úlohy (role):

PII Principal, PII Controller a

PII Procesor

Funkčné úlohy: PII provider a PII recipient

Definícia clasifikácie dát:

- Unique Information PII
- Sensitive Information PII (rôzne úrovne)
- Not identifiable PII Information

RSN

Implementácia princípov súkromia podľa ISO/IEC 29100

- Riadenie a redukcia rizík
- Definovanie zodpovedností PII controlleru
- Zvyšovanie bezpečnostného povedomia
- Otvorenosť a transparentnosť
- Minimalizácia dát

RSN

Znižovanie rizík súkromia

- Riadenie rizík
- Zavedenie technických opatrení a metód (Pseudonymizácia, Anonymizácia, Riadenie identít podľa ISO/IEC 24760, Riadenie prístupov podľa ISO/IEC 29146, Riadenie štruktúr pre správu biometriky, Riadenie rámcov viacfaktorovej autentizácie)
- Zvyšovanie bezpečnostného povedomia a nepodceňovania rizík (správanie na sociálnych sieťach, nákupy a platby cez internet, WiFi siete, cloud služby,..)
- Boj proti praktikám sociálneho inžinierstva
- Definovanie zodpovedností a účtovateľností

RSN

Kybernetický priestor a CC

• Definícia KP: Komplexné prostredie tvorené interakciou ľudí, softvéru a služieb v rozľahlých sieťach, bez fyzickej formy a bez hraníc

•Definícia CC: Služby ponúkané cez web v kybernetickom priestore

Problém:

Rozdielne ponímanie ochrany kybernetického priestoru, dát a služieb v USA, EU, Číne, Japonsku, Austrálii

RSN

Kritické oblasti CC

- Technické riešenie (ISO/IEC 27017)
- Ochrana súkromia (ISO/IEC 27018, ISO/IEC 29100, ISO/IEC 29101)
- Riadenie identít (ISO/IEC 24760)
- Riadenie prístupov (ISO/IEC 29146)
- Audit

RSN

CC aplikácie

- Poskytovanie dátových priestorov (Amazon)
- Sociálne siete (Facebook, Gmail,..)
- Aplikácie (Google Apps)
- Infraštruktúra (Rackscale)

RSN

Ďakujem za pozornosť

Miloslav Ďurčík,CISA,CRISC mdurcik@rsn.sk

RSN