Informačná bezpečnosť(3)

Všeobecné základy informačnej bezpečnosti

Obsah prednášky

- Špecifikácia problému: čo a prečo potrebujeme chrániť
- Čo je informačná bezpečnosť
- Kto za ňu zodpovedá
- Základné pojmy IB
-

CRITIS (kritická informačná infraštruktúra)

- IKT – zasahujú všetky sektory kritickej infraštruktúry
  - riadenie technologických systémov (SCADA)
  - Obchodovanie
  - Finančné transakcie
  - Doprava (riadenie letovej prevádzky) a spoje
  - Zdravotníctvo
  - Verejná správa
  - Armáda a bezpečnosť
- Sprostredkovane aj samé o sebe (komunikácia, informačné zdroje) IKT = kritická infraštruktúra
- Rozsiahle, rôznorodé, zložité, dôležité, obsluhujú ich často nedostatočne kvalifikovaní ľudia, pracujú s nimi laici – možnosť technickej poruchy, omylu alebo cieľavedomého útoku
- Globálny charakter – dominový efekt
-
-
  -
  -

Čo chrániť?

- Kľúčové sú informácie, bez nich IKT nemajú zmysel
- Technológie – lebo ich narušenie môže spôsobiť poškodenie alebo zneprístupnenie informácií
- Podpornú infraštruktúru – lebo jej narušenie môže vyradiť IKT
- Ľudí – lebo IKT nebude mať kto obsluhovať, resp. s nimi pracovať
- know-how – lebo nekvalifikovaní ľudia nebudú vedieť správne narábať s IKT
- A pod.
- Zdá sa, že všetko, čo súvisí so spracovaním informácií, ktoré si samé o sebe zasluhujú ochranu
- To je však veľmi vágne konštatovanie, aby sa z neho dalo vychádzať
- Preto sa konštituuje a rozvíja informačná bezpečnosť
-
-

Informačná bezpečnosť

- Trojaký význam
  - Ideálny stav IKT (systému)
  - Medziodborová disciplína, ktorá skúma hrozby voči IKT a hľadá riešenia, ako IKT chrániť
  - Činnosť smerujúca k dosiahnutiu ideálneho stavu IKT
- Potrebujeme rozvíja IB ako disciplínu, aby sme vedeli, čo, pred čím a ako chrániť; uplatňovať jej výsledky v praxi, aby sme dosiahli požadovaný stav
- 4 organizačné úrovne IB
  - Individuálny systém
  - Organizácia/inštitúcia
  - Štát
  - Globálny kybernetický/digitálny/virtuálny priestor

Odkiaľ začať?

- Kto by mal riešiť IB:
  - Jednotlivci
  - Organizácie/inštitúcie
  - Štát
  - Medzinárodné organizácie
- Podobá sa to síce organizačným úrovniam IB, ale neznamená to, že jednotlivci sa starajú len o individuálne systémy, organizácie výlučne o svoje atď.
- Budeme vychádzať z potreby zaistenia IB v organizácii (rozumný model a najprepracovanejší)
  - Čo, prečo a ako robiť
  - Zovšeobecnenie: čo by sa malo robiť na ostatných úrovniach
  - Čo je na to potrebné
  -
-
-
-

Terminológia IB

- Vyhnúť sa nedorozumeniu vyplývajúceho z terminologických nejasností (nedefinované pojmy, alebo lokálne definície v zákonoch: pre účely tohto zákona sa pod ... rozumie)
- Existuje výkladový slovník IB, ktorý nechalo vypracovať MF SR
- Terminológia je vo vývoji, nie všetko je poriadne a výstižne definované
- Nie všetko sa dá preložiť jednoznačne {fail, failure, fault, mistake, error}={chyba, omyl, zlyhanie, nedorozumenie, nepochopenie, nedostatok}
- A niečo už vôbec nie: Smurf attack, pink of death, tear drop attack
- Väčšina pojmov má pôvod v angličtine a niektoré výrazne iný kultúrny alebo spoločenský kontext
- Hoci terminológia vyzerá ako podružný problém, ukazuje sa potreba medzinárodnej unifikácie (základ angličtina?)

Najdôležitejšie pojmy IB (1)

- Len spomenieme, definície sú v krátkom slovníku
- Aktívum, delenie aktív, vlastník aktíva (systému), zodpovedná osoba a povinná osoba
- Informácia, údaje
- Spracovanie informácie (získavanie, prenos, vlastné spracovávanie, uchovávanie, archivácia, ničenie informácie)
- Hrozba, zraniteľnosť, nositeľ hrozby, dopad hrozby, typy hrozieb (vyššia moc, omyly, technické poruchy, organizačné nedostatky, právne sankcie, aktívne útoky)
- Útok, útočník, útočný potenciál
- Dopady hrozieb (spôsoby hodnotenia)
- Bezpečnostný incident
- riziká, odhad a vyhodnotenie rizika, kvantitatívny a kvalitatatívny prístup k vyhodnoteniu rizík, akceptovateľné riziko, zostatkové riziko.
- Správa/manažment rizík, analýza rizík.

Najdôležitejšie pojmy IB (2)

- Opatrenia (typy).
- Bezpečnostný projekt
- riadenie IB, personálna, fyzická, prevádzková, komunikačná bezpečnosť
- Bezpečnostná dokumentácia (bezpečnostný zámer, bezpečnostná politika, bezpečnostné smernice, bezpečnostné praktiky)
- Kontinuita činnosti (havarijné plány, plány obnovy činnosti)
- Monitoring
- Audit
- Funkcionálne bezpečnostné požiadavky/funkcie,
- Požiadavky na bezpečnostné záruky
- Certifikácia a akreditácia systémov
- Oprávnenia (povolané osoby/entity)
- Identifikácia, autentizácia
- Prístup (k údajom, do systému)
-
-
-

Čo je cieľom ochrany systému a/alebo organizácie?

- Všeobecný: aby príslušné IKT správne (= v súlade s bezpečnostnou politikou systému/organizácie) fungovali
- Konkrétnejšie: zaistenie dôvernosti, integrity a dostupnosti spracovávanej informácie (príp. služieb)
- ďalšie možné/časté požiadavky: autentickosť, súkromnosť, nepopretie prijatia, nepopretie pôvodu, anonymita, pseudonymita, zodpovednosť za činnosť v systéme
- IB sa definuje aj ako zaistenie dôvernosti, integrity a dostupnosti informácie

Dôvernosť (confidentiality)

- Informácia je zapísaná pomocou údajov (info=obsah, údaje=forma)
- Dôvernosť: zaistenie toho, aby sa k informácii obsiahnutej v údajoch nemohli dostať nepovolané osoby
- Ako:
  - Ochrana prístupu (bezpečné prenosové kanály, prístup do systému)
  - Šifrovanie
- Poznámka: dva významy pojmu: všeobecný a špeciálny (= 2. klasifikačný stupeň pre utajované skutočnosti)
-

Integrita (integrity)

- Ideálne celistvosť/neporušenosť údajov (použiteľné aj pre iné aktíva)
- Reálne nedosiahnuteľná požiadavka
- Realistickejšie: aby oprávnená osoba mohla zistiť/overiť, či údaje neboli zmenené
- ako:
  - ochrana prístupu k údajom,
  - Ochrana fyzických zariadení pred nepovolaným prístupom (fyzická)
  - Digitálne odtlačky (hašovacie funkcie – opäť kryptológia)
-

Dostupnosť

- Bez dostupnosti by informáciu nebolo treba chrániť, ale bola by nepoužiteľná
- Definícia: informácia musí byť k dispozícii kedykoľvek (do času t) o to oprávnená osoba požiada
- Použiteľné aj pre zariadenie, službu či iný zdroj systému
- Zaujímavý je čas t
  - Okamžite (t=0)
  - Prípustné je nejaké oneskorenie
- Aj štatistické chápanie dostupnosti: % času, kedy sú informácia alebo iný zdroj použiteľné pre oprávneného používateľa

Ďalšie bezpečnostné požiadavky (1)

- autentickosť (authenticity) – vzťahuje sa na nejaký dokument (nie surové údaje)
- Autentickosť (pôvodnosť): dokument je taký, ako ho autor vytvoril, t.j. dva aspekty: integrita a možnosť určiť autorstvo
- Riešenie: digitálne/elektronické podpisy
- Súkromnosť (privacy)
- Relevantná pre údaje, dokumenty obsahujúce informáciu vzťahujúcu sa na nejakú osobu
- Dotknutá osoba má možnosť určiť, ktoré údaje, komu a za akých okolností a komu (konkrétne osoby alebo okruh osôb) budú poskytnuté
- Príklad: osobné údaje zdravotná informácia
- Rozdiel medzi dôvernosťou a súkromnosťou

Ďalšie bezpečnostné požiadavky (2)

- Nepopretie autorstva/pôvodu (non repudiation of origin)
- Pri dokumentoch, ktoré majú právny význam
- Ale aj predpoklad pre presadenie zodpovednosti za činnosť v systéme
- Ako
  - Na dokumentoch elektronický/digitálny podpis
  - V systémoch identifikácia, silná autentizácia a záznamy o činnosti v systéme
- Nepopretie prijatia (non repudiation of receipt)
- Pri doručovaní právne relevantných dokumentov
- Podateľne, osobné schránky – potvrdenie o prijatí s časovou pečiatkou a podpisom
- Len technické riešenia nestačia
-
-

Ďalšie bezpečnostné požiadavky (3)

- Anonymita – nemožnosť určiť pôvodcu nejakej činnosti (napr. platby)
- Pseudonymita – namiesto identity pôvodcu sa používa pseudonym, ktorý pozná len dotknutá osoba a dôveryhodná tretia strana
- Zodpovednosť za činnosť v systéme (vystopovateľnosť, accountability) = možnosť určiť, kto a čo v systéme spravil;
- Čo na to treba: identifikáciu a autentizáciu
- Záznam auditu o činnostiach v systéme (log)
- Podobné ako v prípade *non repudiation of origin*, vzťahujúceho sa na činnosť v systéme
- Ešte: právna relevantnosť dôkazov
- Určite existujú aj ďalšie bezpečnostné požiadavky
-

Na čo sa vzťahuje IB ?

- Magický pojem: IB = ochrana kybernetického priestoru, cyberspace
- *Term originated by author William Gibson in his novel Neuromancer the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.*
- Súčasné chápanie – cyberspace je technické = elektronická informačná a komunikačná infraštruktúra organizácie, štátu alebo globálna
- Ale nemôže fungovať bez programového vybavenia
- Spracovávajú sa v nej údaje (bez nich nemá zmysel)
- Závisí od podpornej infraštruktúry
- Obsluhujú ju ľudia
- Riadi sa pravidlami (politika, normy, štandardy, legislatíva)
- A čo s papierovým svetom?
- Zlyhanie, chyba alebo úmyselné narušenie čohokoľvek z vyššie uvedeného môže viesť k narušeniu informácie
-

Čo potrebujeme chrániť?

- Už pri všeobecnom pohľade dva prístupy:
  - Lokálny (konkrétny IKT systém)
  - Globálny (celý digitálny priestor)
- Dopĺňajú sa
  - digitálny priestor tvoria konkrétne systémy a ich obsah
  - Bez ochrany lokálnych systémov sa nedá chrániť ani celok
  - Niektoré problémy sa nedajú riešiť na lokálnej úrovni
- Najprv sa sústredíme na globálny rámec
- V ďalších prednáškach rozoberieme konkrétne riešenia pre lokálne systémy, resp. špecifické otázky
-