Informačná bezpečnosť globálny pohľad

Prednáška č. 2

Obsah prednášky

- Globálny význam informačnej bezpečnosti
- Čo treba chrániť
- Kto má zaistiť informačnú bezpečnosť
- Ako
  - Koncepcie
  - Legislatíva
  - Organizačné zabezpečenie
  - Realizácia (oblasti)
  - Medzinárodná spolupráca
- Slovensko

Globálny význam informačnej bezpečnosti

- Prehlbujúca sa informatizácia spoločnosti
- Prienik IKT do kritickej infraštruktúry štátu
- Globálny charakter informačnej a komunikačnej infraštruktúry
- Narastajúce riziko zlyhania IKT
  - Zložitosť
  - Negatívne vplyvy okolia
  - Cielený útok (jednotlivci, štát, teroristi, kriminálne živly)
- Dopady nemusia mať lokálny charakter
- Informačná spoločnosť potrebuje správne fungujúce IKT
- Informačná bezpečnosť = vec národného záujmu

Čo treba chrániť ?

- Lokálny versus globálny pohľad (každý zodpovedá za svoje, resp. centrálne koordinovaná ochrana celej infraštruktúry)
- Pripomenieme The (US) National Strategy to Secure Cyberspace

  Everyone who relies on part of cyberspace is encouraged to help secure the part of cyberspace that they can influence or control. ... All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace.
- IKI (informačná a komunikačná infraštruktúra) – rozmanitá (technológie, vlastníctvo, účel, bezpečnostné požiadavky), ale tvoria ju navzájom prepojené systémy
- Nedostatočná ochrana jednej časti IKI ohrozuje ostatné (napr. bot-nets)
- Nechať jednu časť IKI bez dostatočnej ochrany by bolo možné len vtedy, ak by bola izolovaná od zvyšku
- Preto je predmetom ochrany celá IKI, jej obsah a jej bezpečnostné okolie
- Cyberspace (digitálny priestor)

Čo tvorí digitálny priestor ?

- Kľúčové aktívum je informácia
  - Údaje
  - Programové vybavenie
  - Dokumentácia
  - Know-how neinformatického charakteru
- Technické zariadenia na spracovanie informácie (IKT systémy)
- Komunikačné zariadenia a linky
- Podporná infraštruktúra (budovy, napájanie, klimatizácia, kúrenie,...)
- Kvalifikovaná obsluha IKT systémov (
- Používatelia
- Pravidlá hry (legislatíva, normy a štandardy, prevádzková dokumentácia)
- Prípadne iné veci, informácie, pravidlá ..., ktoré sú relevantné pre fungovanie IKT systémov a spracovanie informácie

Pred čím ochraňovať digitálny priestor a jeho aktíva?

- Spomínali sme (v základných pojmoch) hrozby a riziká z nich vyplývajúce
- Stručne – čo chceme dosiahnuť
  - Dôvernosť (confidentiality)
  - Integrita (integrity)
  - Dostupnosť (availability
  - Autentickosť (authenticity)
- Prípadne
  - Súkromnosť (privacy)
  - Nepopretie pôvodu (non repudiation of origin)
  - Nepopretie prijatia (non repudiation of receipt)
  - Zodpovednosť za činnosť v systéme (accountability)
  - Anonymita (anonymity) a i.

Bezpečnostné aspekty informácie

- Dôvernosť: k informácii obsiahnutej v údajoch majú prístup len oprávnené osoby
- Integrita : údaje nemožno zmeniť bez toho, aby si to oprávnená osoba všimla (napr. prenášaná správa)
- Dostupnosť – údaje sú k dispozícii oprávnenej osobe vždy, keď o to požiada

Ďalšie bezpečnostné požiadavky na IKT systémy, resp. na údaje, ktoré obsahujú

- Autentickosť = refers to the truthfulness of origins, attributions, commitments, sincerity, devotion, and intentions.
- Nepopretie prijatia – príjemca údajov nemôže poprieť, že ich prijal
- Nepopretie pôvodu – odosielateľ (tvorca dokumentu) nemôže poprieť, že dokument poslal/vytvoril
- Súkromnosť – osoba môže stanoviť, aké údaje o nej komu a za akých podmienok budú poskytnuté
- Anonymnosť – identita osoby vykonávajúcej nejakú činnosť ostáva utajená
- Zodpovednosť za činnosť v systéme – pre činnosti kritické z hľadiska bezpečnosti je možné stanoviť, kto, čo a kedy spravil

Ako zaistiť potrebnú úroveň bezpečnosti digitálneho priestoru?

- Bezpečnostné aspekty informácie a uvedené ďalšie bezpečnostné požiadavky sú len rámcové
- Treba ich konkretizovať
- Konkretizácia znamená zohľadniť potreby a možnosti jednotlivých IKT systémov
- Na úrovni konkrétnych IKT systémov to znamená
  - Popísať systém
  - Analyzovať hrozby voči aktívam systému
  - Analyzovať a vyhodnotiť riziká
  - Navrhnúť a implementovať opatrenia
- Podobne v prípade celého digitálneho priestoru
- Rozdiel – iný rozsah systémov, charakter hrozieb a iná miera podrobnosti, aj iné opatrenia

Kto zodpovedá za ochranu digitálneho priestoru ?

- Vzhľadom na globálny charakter – všetci
- Reálne – každý primerane svojej úlohe a možnostiam
- Kľúčoví hráči
  - Štát
  - Súkromné spoločnosti
  - Špeciálne IT firmy
  - Školstvo (akademická sféra)
  - Používatelia
- Potreba koordinácie
- Koordinátor - štát