Nemzetközi és hazai fejlemények az információ és hálózatbiztonság terén

Dr. Suba Ferenc
Testületi elnök
PTA CERT-Hungary
Igazgatótanácsi alelnök
ENISA

dr. Angyal Zoltán
Puskás Tivadar Közalapítvány
CERT-Hungary
hálózatbiztonsági igazgató

Kritikus infrastruktúra

27/2004. (X.6.) IHM rendelet

az informatikai és elektronikus hírkölési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről

2.§ 11.
Kritikus infrastruktúra mindazon létesítmények, szolgáltatások – beleértve az elektronikus hírközlési és informatikai rendszereket – amelyek működésképtelenné válása vagy megsemmisülése egyenként és együttesen jelentősen befolyásolhatja a nemzet biztonságát, az állampolgárok élet- és vagyonbiztonságát, a nemzetgazdaság és a közszolgáltatók működését.

PTA CERT HUNGARY

Kritikus infrastruktúra védelem

- **Kritikus Infrastruktúra Védelemhez kapcsolódó fogalmak:**
  - Sebezhetőség: a működés valamely (külső vagy belső) veszély általi megzavarásának, manipulálásának vagy megsemmisítésének lehetősége
  - Veszély: minden olyan jel, körülmény vagy esemény, amely potenciálisan megzavarhatja vagy megsemmisítheti a kritikus infrastruktúrát, illetve annak bármely részét
  - Kockázat: veszély, veszteség, kár vagy sérülés lehetősége, tekintettel az eszköznek tulajdonított értékre és az eszköz megsemmisülése vagy megváltozása által okozott hatás

NIIF CERT HUNGARY

Kritikus infrastruktúra védelem

- **Zöld Könyv – A kritikus infrastruktúrák védelmére vonatkozó nemzeti programról (2007)**
- 2112/2004 (V.7.) Korm. határozat – Szektorok meghatározása
- 2046/2007 (III.19.) Korm. határozat 1. sz. melléklet 2.3.1. - Keretrendszer, ágazatközi összehangolásról szóló előterjesztés
- 1/2007 (III.29.) Kormányzati Koordinációs Bizottság határozat 5.b) – KIV nemzeti program kidolgozásának megkezdése, hazai koordinációról és feladatokról szóló kormány előterjesztés előkészítése

Kritikus infrastruktúra védelem

- **Kritikus Infrastruktúra Védelem:**
  - a kormány, az infrastruktúra tulajdonosok és üzemeltetők által alkalmazott programok és tevékenységek
  - a rendszerek működőképességének és az elemek biztonságának garantálására, kockázatok csökkentésére irányul
  - informatikai, fizikai, személyi és eljárás jellegű elemzési, tervezési, végrehajtási és ellenőrzési védelmi intézkedés

PTA CERT HUNGARY

Kritikus információs infrastruktúra védelem

- **Kritikus Információs Infrastruktúra:**
  - teljes mértékben összekapcsolt informatikai eszközök, hálózat és kritikus információ továbbítását megvalósító folyamat
  - része a globális vagy nemzeti információs infrastruktúrának
  - elengedhetetlenül fontos a kritikus infrastruktúrák folyamatos üzemeléséhez.
  - Pl. telekommunikáció, informatikai eszköz, szoftver, Internet,

PTA CERT HUNGARY

Kritikus információs infrastruktúra védelem

- része a Kritikus Infrastruktúra Védelemnek
- olyan rendszerek, eszközök és erőforrások védelme, amelyek kritikus információs infrastruktúraként kerültek azonosításra
- a kritikus információs infrastruktúra elemek biztonságának garantálására, kockázatok csökkentésére irányuló informatikai, fizikai, személyi és eljárás jellegű elemzések

PTA CERT HUNGARY

Kritikus információs infrastruktúra védelem

- Kölcsönös függőség – Interdependencia:
  - két irányú kapcsolat két infrastruktúra között
  - milyen mértékben befolyásolják egymás működését
  - működésük milyen mértékben függ a másik működésétől
  - létezhet komponensek, funkciók és erőforrások között
  - karakterisztika és fokozat
- Pl.: Energia szektor <-> IT

PTA CERT HUNGARY

Kritikus információs infrastruktúra védelem

- A Kritikus Információs Infrastruktúra Védelem feladata:
  - A kritikus informatikai infrastruktúrák azonosítása
  - A kritikus informatikai infrastruktúrák védelmi megoldásainak biztosítása
  - A fenyegetésekre a reagálási kapacitás kialakítása
  - A védelem szereplői közötti együttműködés kialakítása
  - A nemzetközi együttműködés kialakítása (globális fenyegetésre globális a válasz!)

PTA CERT HUNGARY

Informatikai és hálózati biztonság

Kihívás és lehetőség:
- Üzleti szektor (elsősorban pénzintézetek, közlekedés)
- Közszolgáltatók
- Kormányzat
- Felhasználók

Jövő: KIIV
- Kritikus
- Információs Infrastruktúrák
- Védelme

PTA CERT HUNGARY

Üzleti szektor

Kihívás:
- Hogyan győzzük meg az ügyfeleket? („gondvezérelt” gondolkodás)
- Hogyan becsüljük meg a költségeket és hasznokat? (egymással vetélkedő kockázatkezelési módszertanok)
- Hogyan kerüljük el a túlszabályozást? (a bürokrácia „autopoézise”)

Lehetőség:
- Az IT elterjedésével és az incidensekkel párhuzamosan növekedő kereslet
- Soha véget nem értő történet (a biztonság csupán egy állapot☺)
- Új gazdasági gondolkodás (minden be nem következett veszteség nyereség + új biztosítási üzletág)

PTA CERT HUNGARY

Kormányzat

Kihívás:
- Hogyan válaszoljunk globálisan? (globális probléma)
- Hogyan reagáljunk hatákonyan? (túl lassú hivatalos eljárás)
- Hogyan tartsuk meg a munkaerőt? (szakemberek rotációja)

Lehetőség:
- Nemzetközi és nemzetek feletti együttműködés **ENISA -** Európai Hálózati és Információ Biztonsági Ügynökség
FIRST – Forum of Incident Response Team
EGC- európai kormányzati CERT-ek közössége

- Új, rugalmas szervezeti formák + kiszervezés (kormányzati CERT)

- De minimális szabályozás

PTA CERT HUNGARY

Felhasználók

Kihívás:
- Hogyan védjük meg őket? (leggyengébb láncszem)
- Hogyan oktassuk őket? (rossz tanulók)
- Hogyan tegyük őket felelőssé? (pl. internetbank)

Lehetőség:
- IT biztonság, mint az alaptanterv része
- Felhasználók „helyzetbe hozása” („kihelyezett munkaállomás”)
- Tudatosítás (felhasználóbarát módon☺)
- Felelősségek arányos elosztása szereplők között (arányos egyensúly a külső védelem és az öngondoskodás között)

PTA CERT HUNGARY

KIIV

Az informatikai és hálózatbiztonság jövője, mert:
- Létfontosságú
- Mindenütt érezhetően ott van
- Könnyű megérteni
- Nem csak műszakiaknak! (+jog, közigazgatás, oktatás, diplomácia, média)

Jelszó: EGYÜTTMŰKÖDÉS
- Ágazatokon belül és között (pénzvilág, energia, közlekedés)
- Társadalmi csoportok között (üzlet, kormányzat, oktatás kutatás, felhasználók)
- Államok között (globális kihívás)

Nemzetközi fejlemények

Nagy szervezetek nyitása:
- ITU – International Telecommunication Union **(ENSZ): Cybersecurity Action Plan**
- ICAAN (regisztráció)**: Draft Strategy 2007**
- FIRST: Future of First Task Force – világméretű információ megosztás
KIIV át- és kialakulás:
- EU – több program (2008-13 keretprogram), Zöld Könyv, CIP Action Plan, FP7 Joint Call, Initiative 2008
- ENISA: 2011-től nagyobb egység része
- UK: NISCC-ből CPNI (több CERT)
- USA: ISAC (információ megosztó szervezetek)
Nemzetközi együttműködés szakosodása:
- Meridian (kormányok közötti együttműködés): **SCADA munkacsoport** (távfelügyelet - folyamatirányítás)

Hazai példa: PTA CERT-Hungary

Funkciók:
- hálózatbiztonság, kritikus infrastruktúra védelem: technikai védelem, felvilágosító munka, szabályozási javaslatok, nemzetközi képviselet, hazai koordináció

Keret:
- Puskás Tivadar Közalapítvány

Felügyelet:
- Miniszterelnöki Hivatal Elektronikus Kormányzat Központ

Nemzetköz akkreditációk:
- FIRST, TF-CSIRT, EGC

Nemzetközi KIIV:
- Meridian (szabályozás, törvényhozás),
- IWWN - International Watch and Warning (szűkkörű operatív együttműködés)

Hazai KIIV:
- OIHF, CERT-Hungary
- Pénzügyi szektor, Energia szektor - folyamatban

Együttműködés a bankszektorral

2005 óta
- bizalmon és közös érdekeken alapul
- fő partnerek: Bankszövetség, PSZÁF
- fő „lökés”: phising támadáshullám 2006 nov – dec. között
- Incidenskezelési Munkacsoport (Bankszövetség, NNYI, PSZÁF, PTA CHK)
- gyakorlatok (kommunikációs, szimulált DDos), incidenskezelési címjegyzék
- PSZÁF együttműködés (munkacsoport, felvilágosítás, ajánlás)
- jövő: formalizált értesítési és letiltási eljárás,

Köszönöm megtisztelő figyelmüket!

PTA CERT-Hungary
www.cert-hungary.hu
Puskás Tivadar Közalapítvány