Ipari hálózatok biztonságának speciális szempontjai és szabványai

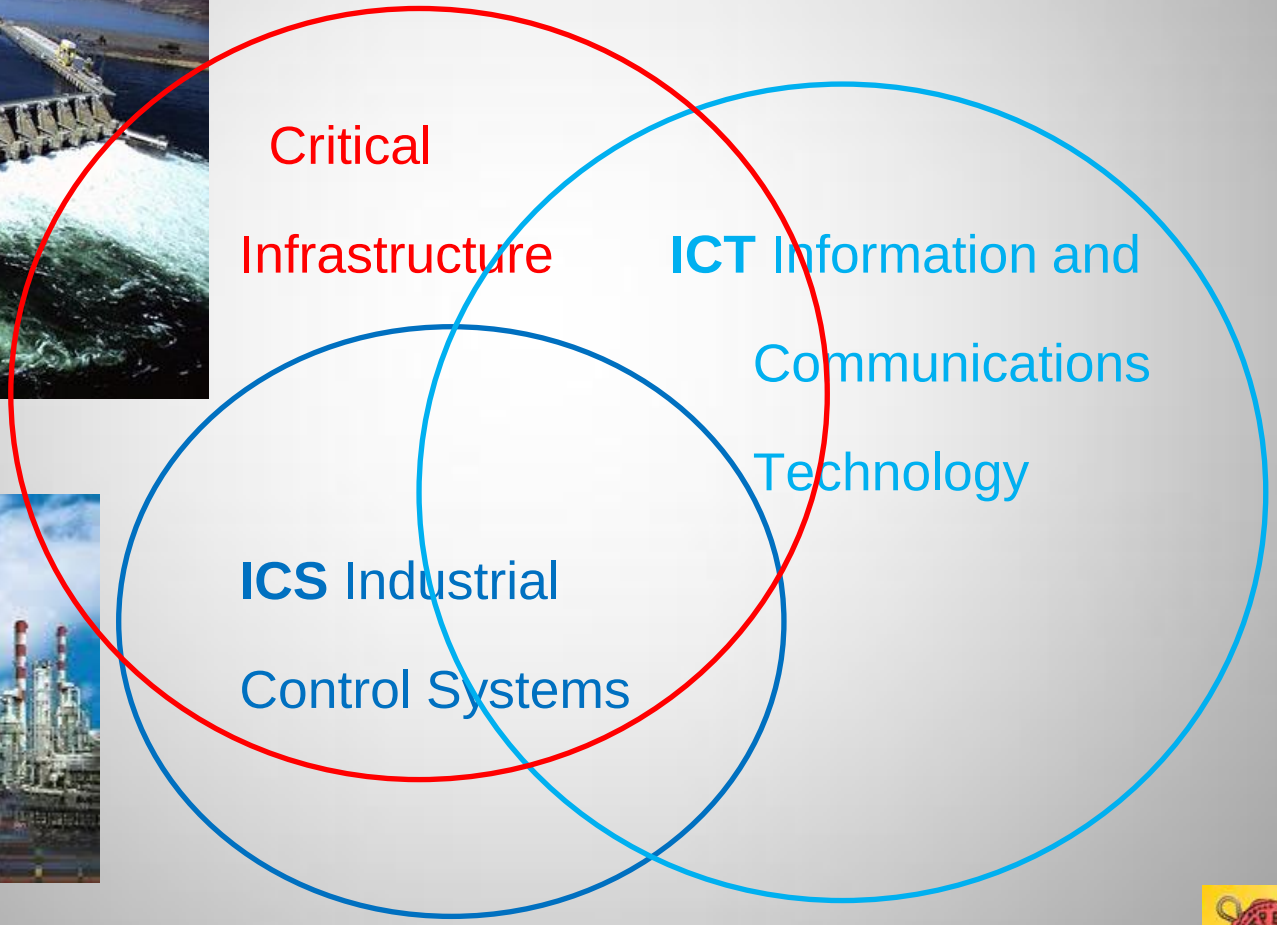
Borbély Sándor CISA, CISM, CRISC
Információvédelmi projekt vezető
sandor.borbely@noreg.hu

NOREG
Információvédelmi Kft.
SZIGORÚAN BIZALMAS

Tartalom

- Az ipari hálózatnál mennyiben, és miért más az elvárás, mint az általános informatikai hálózat esetén?
- Bizalmasság, Integritás, Rendelkezésre állás speciális követelményei ipari hálózatoknál.
- Az ipari hálózatok biztonsági struktúrája, szegmentálása.
- Okozhat-e kockázatot elterjedt biztonsági megoldások telepítése az ipari hálózatba?
- Ipari hálózatok, SCADA rendszerek speciális biztonsági szabványai.

Kritikus infrastruktúra, ICS, ICT



Miért más az ICS elvárás, mint az ICT

ICS Industrial Control Systems

- Rendszerhibából életet veszélyeztető esemény lehet
- Korábban céleszközökből álló sziget rendszerben működtek
- A kommunikációs eljárások egyediek voltak
- Alapelvárás volt: megbízható működés és ELVÁLASZTÁS

ICT Information And Communications Technology

- Biztonsága közvetlenül nem veszélyeztet emberi életet
- Egységesített elemekből áll, világhálóra kapcsolva
- Bevezetésre kerültek biztonsági megoldások és eljárások

Változások az ICS rendszereknél

Változások az utóbbi években

- Az egyedi eszközök helyett tipizált elemekből épülnek
- Az ICT elemek mind gyakrabban kerülnek felhasználásra
- Megjelentek a sziget rendszereket is fertőzni tudó kártevők
  (Pl. Stuxnet, mely más, mint a korábbiak)
- A sziget rendszerek kapcsolatba kerülnek az ICT-vel
  (Üzleti igény, néha „látszólagos” biztonsággal)
- Értetlenség az ICS és az ICT szakemberek között
  (A biztonsági területen szinte ellentét)
- Kritikus Infrastruktúra Védelem Program

Szabályozási környezet változások

Magyarország

A 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

Parlament előtt (2012.03.21.) a törvény javaslat a „létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről” (kritikus infrastruktúra).

Európai Unió

COM(2005) 576 final ZÖLD KÖNYV
(A KRITIKUS INFRASTRUKTÚRA VÉDELEM EURÓPAI PROGRAMJÁRÓL)

COUNCIL DIRECTIVE 2008/114/EC (2008.12.08)
(on the identification and designation of European critical infrastructures and…)

ENISA (2011.12.09) Protecting Industrial Control Systems
Recommendations for Europe and Member States

Biztonsági elvárások ICS esetén

Változott és részben más jellegű, mint ICT esetén

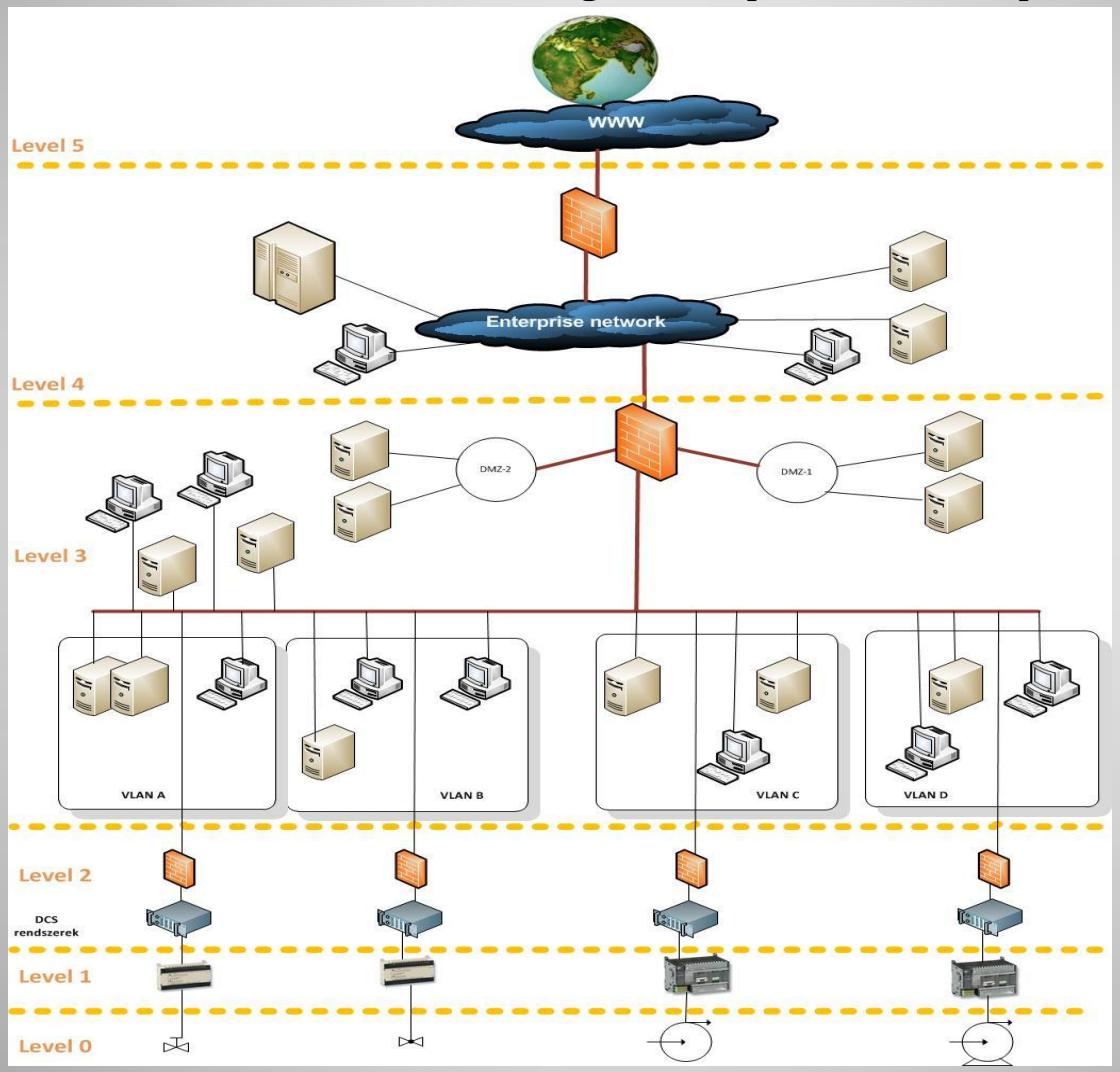
- Bizalmasság sérülése
  - Receptúrák, technológiai titkok
  - Gyártási mennyiségek, ütemezés

    (Night Dragon kémprogram)
- Hitelesség, sértetlenség sérülése
  - Receptúrák, technológiai előírások, gyártási mennyiségek módosítása. Támadás, szabotázs, katasztrófa okozás. Zsarolás.
- Rendelkezésre állás elvesztése
  - Ez eddig is kiemelt szempont volt, műszaki probléma tartalékolással kezelhető, a támadások nem.

Az ICS rendszerek struktúrája (minta)

Level 5 WWW	Világháló	ICT
Level 4 Enterprise Network	Szervezet irányítás	
Level 3 Manufacturing Control	Folyamat irányítás	ICS
Level 2 Production Control	SCADA	
Level 1 Automation Device	PLC	
Level 0 Production Process	Equipment	

ICS rendszer helye (minta)



Biztonsági megoldás okozhat-e rést?

Biztonsági megoldások/eljárások mit okozhatnak?

Minden, ami bekerül a védett környezetbe az hordozhat veszélyes tartalmat. Példák:

- Változások végrehajtása a rendszerben
  - Vezérlést érintő módosítás csak a szállító közreműködésével
  - A szállító változás követése a konfigurációra is kiterjed
- OS, alkalmazás biztonsági patchek
  - Okozhatnak leállást, vagy más abnormális viselkedést
  - Károkozók, kémprogramok juthatnak be a patch-el együtt
  - A felhasználónál általában nincs teljes teszt környezet

Biztonsági megoldás okozhat-e rést?

Biztonsági megoldások/eljárások mit okozhatnak?

- Vírusvédelem
  - Frissítéskor biztonsági résen más is bejuthat a védett környezetbe.
- IDS / IPS (Intrusion Detection/Protection System)
  - Külső management behatolásra ad lehetőséget
- Bejelentkezés/management kívülről
  - Adminisztrátor bejelentkezési lehetősége otthoni gépről
  - A szállító bejelentkezési lehetősége

Biztonsági rések kezelésére figyelni kell!

ICS IT biztonsági szabványok

- ISO
  - MSZ ISO/IEC 27000 szabványok (*információbiztonság irányítás*)
  - MSZ ISO/IEC 15408 szabványok (*értékelés*)

- ANSI/ISA
  - ISA International Society of Automation
  - ANSI/ISA-99 szabvány sorozat (*Security for Industrial Automation and Control Systems*)
  - Több kötetből áll:
  - 99.00.01-2007 Part 1. Terminology, Concepts, and Models 99.02.01-2009 Establishing an Industrial Automation and Control Systems Security Program (hivatkozás az ISO 27000-re)
  - TR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems

ICS IT biztonsági ajánlások

- ENISA

  - Protecting Industrial Control Systems Security: Recommendations for Europe & Member States Dec 2011, mellékletekkel együtt nagyon sok hasznos információt tartalmaz

- NIST

  - SP 800-82 Guide to Industrial Control Systems (ICS) Security *Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)* June 2011, 155 oldal.

  - SP 800-53 Rev3 Recommended Security Controls for Federal Information Systems and Organizations *August 2009, 237 oldal.*

ICS IT biztonsági ajánlások

- IEC International Electrotechnical Comission

  - IEC/TS 62351Power systems management and associated information exchange - Data and communications security *TECHNICAL SPECIFICATION 8 részből áll*
  - IEC/TR 62210 Power systems management and associated communications - Data and communications security *TECHNICAL REPORT,*
  - IECTS 62443 Industrial communication networks - Network and system security *TECHNICAL SPECIFICATION, több részből áll, egyes részek még draft verzióban.*

- IEEE (Institute of Electrical and Electronics Engineers)

  - IEEE 1686 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
  - IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security

ICS IT biztonsági iparági ajánlások

- AGA
  - AGA Report No.12.. Cryptographic Protection of SCADA Communications. *TECHNICAL SPECIFICATION 4 részből áll*
- API
  - API 1164, Pipeline SCADA Security *Guideline*
  - Security Guidelines for the Petroleum Industry *Guideline*
- DHS Department of Homeland Security
  - Common Cybersecurity Vulnerabilities in ICS *Report May 2011*
  - Recommended Practice for Patch Management of ICS

Ipari hálózat IT biztonsági kérdéseinek összefoglalója

Az ICS IT biztonság kialakításánál fontosak:

- Várhatóan jogszabályi kötelezettség alapján kell kialakítani.
- A kockázatfelmérés alapján tud az üzleti vezetés dönteni a biztonságra fordított összegekről, a felvállalt kockázatokról.
- A szakemberek felelőssége is, ha az üzleti vezetés nem ismeri a speciális ICS IT biztonsági hiány következményeit.
- A belső munkatársak alkalmi érdeke félrevezető lehet.
- A külső szakértők szakmai tudása biztonság növelést és költség csökkentést tud biztosítani.
- A nem kellő tapasztalattal összeállított megoldás hamis biztonságtudatot kelthet.

Kérdések

Köszönöm a figyelmet!

sandor.borbely@noreg.hu

NOREG
Információvédelmi Kft.
SZIGORÚAN BIZALMAS