Információbiztonság az energiaszolgáltató iparágban ISO/IEC 27019

Móricz Pál – ügyvezető igazgató
Szenzor Gazdaságmérnöki Kft.

Szenzor
GAZDASÁGMÉRNÖKI KFT.

Energiaszolgáltatási iparág sajátosságai

- gyakran kritikus infrastruktúrához kapcsolódnak, jogszabályi előírások
- magas biztonsági, megbízhatósági, illetve rendelkezésre állási, integritási követelmények
- nagy területen (alállomások, szabályozó/mérő eszközök), korlátok fizikai védelemre, folyamatos felügyelet nélküli automaták
- sok szereplős, komplex rendszerek, ICT szerepe nő, fenyegetések, sebezhetőségek is
- 20 vagy több éves életciklus(nem támogatott sw/hw hitelesítés, titkosítási funkció nélküli elemekkel, stb.)
- változáskezelés nehézségek (személyes jelenlét kellhet), patch, update nehézségek, előzetes teszt

Szabványok

Jelenleg érvényes (1. kiadás)

- **ISO/IEC TR 27019:2013**

Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

még ISO/IEC 27002:2005 alapján

Szabványtervezet (2. kiadás)

- **ISO/IEC FDIS 27019**

Information technology – Security techniques – Information security control for the energy utility industry

státusz: szavazás 2017.06.05-től (8 hét)

Alkalmazási terület, változások

- 27002-n alapuló útmutató (guidance) kontrollokra
  - energiaszolgáltató iparág által használt folyamatirányító rendszereknél
    - áram, gáz, olaj *(ez új terület)* és hő termelés, előállítás, átvitel, tárolás és elosztás szabályozás (controling) és monitoring, valamint
    - kapcsolódó támogató folyamatok szabályozás (control)
  - nukleáris terület kivételével (IEC 62645)

Alkalmazási terület példák 1/2

- központi és elosztott folyamat szabályozás, monitoring és automata technológiák, működésükhöz információs rendszerek, programozható, paraméterezhető egységek
- digitális szabályozók, automata komponensek, kontroll egységek vagy PLC-k, közte szenzorok és működtető/szabályozó rendszer elemek
- minden támogató információs rendszer, melyet a terület használ, pl. adat megjelenítéshez, vagy kontrolling, monitoring, archiválási, naplózási, jelentési, dokumentálási céllal
- használt kommunikációs technológiák, pl. hálózat, távközlési rendszer, szabályozó alkalmazások, távirányítási technológiák
- AMI komponensek (pl. smart meters)
- mérő egységek (pl. emisszió értéket mérő)

Alkalmazási terület példák 2/2

- digitális biztonsági és védelmi rendszerek, pl. PLC-k védő és biztonsági relék, vészhelyzeti irányító mechanizmus
- energiamenedzsment rendszerek, pl. elosztott energiaforrásokra, elektromos terheléskezelő infrastruktúrák háztartásokban, lakóépületekben vagy ipari vevők által telepítve
- hálózati környezet elosztott komponensei, pl. háztartásokban, lakóépületekben vagy ipari vevők által telepítve
- szoftverek, firmware-k, alkalmazások a fenti rendszerekhez, pl. elosztás irányítási (DMS) vagy kiesés menedzsment (OMS) alkalmazások
- helyiségek a fenti berendezésekre, rendszerekre
- távoli karbantartó rendszerek

Tartalomjegyzék

Felépítés

- ISO 27001-hez kapcsolódó követelmény (4. fejezet)
  - 4-10 fejezet változatlanul alkalmazandó
  - energiaszektor specifikus követelményekre is ki kell térni
    - kontrollok teljessége értékelésekor,
    - Alkalmazhatósági nyilatkozatban
- Kontrollok (5. fejezet)
  - 27002 kontroll alkalmazandó vagy
  - kiegészítő
    bevezetési útmutató, és/vagy
    egyéb információ
  - új kontroll esetén: kontroll, bevezetési útmutató, egyéb információ, van új szabályozási cél is

27002-n túli kontrollok (1/2)

- Belső szervezet (6.1)
  - Külső felekhez kapcsolódó kockázatok,
    Biztonság a vevő kapcsolatokban
- Területek védelme (11.1)
  - Biztonság a felügyeleti központban,
    Biztonság a berendezések helyiségeiben,
    Biztonság a „perifériákon”
- Biztonság külső felek épületeiben (11.3)
  - Berendezések energia szolgáltatóknál,
    Berendezések a vevőknél,
    Összekapcsolt szabályozó és kommunikációs rendszerek

27002-n túli kontrollok (2/2)

- Az üzemelés biztonsága (12)
  - Öröklött rendszerek (12.8)
  - Biztonsági rendszerek sértetlensége, rendelkezésre állása (12.9)
- A hálózati biztonság menedzsmentje (13.1)
  - Folyamatirányítási adatok kommunikációjának biztonsága
  - Logikai kapcsolat külső folyamatirányítási rendszerekhez
- Biztonság a fejlesztési és támogató folyamatokban (14.2)
  - Minimális funkcionalitás
- Redundanciák (17.2)
  - Vészhelyzeti kommunikáció

Specifikus szempontok (1/2)

- Példák kontroll szempontokra
  - szerepek, hatóságok (CERT, Katasztrófa védelem), mobil eszközök, távmunka (hozzáférés, MFA, funkciók, kommunikáció, elkülönítés, patch, hozzáférés felügyelet, távirányítási rendszer validáció), vagyonleltár (info, sw, fizikai elem, szolgáltatások), osztályozás, berendezés elhelyezés, naplózandók, hálózat elkülönítés,
    jogi követelményekre (biztonság, őrzés, megbízhatóság, piaci szétválasztás, kritikus infrastruktúra, adatvédelem, jogszabály, előre látható változások), stb.
- Kulcs szereplők
  - szigorú kiválasztás, megállapodások

Specifikus szempontok (2/2)

- Szempontok hozzáférési elvekre
  - közte kritikus eszköz mozgatás, kivonás, ha nincs egyedi azonosítás, biztonsági funkció (pl. egyedi azonosítás, jelszó módosítás, zárolás, időkorlát)
- További útmutatók
  - működés közmű kiesés esetén, kábelszakadás kezelés
  - dokumentált eljárás vészhelyzetekre
  - malware védelem (benne hálózat elválasztás, interfész védelem is)
  - idő szinkronizálás
  - sw telepítésre szempontok
  - vegyes (rádiós, vezetékes, vezetéknélküli) hálózatok
  - incidense esetén kommunikáció érintettekkel, lehet bejelentés köteles
  - sérülékenység vizsgálat

Elérhetőség

Móricz Pál **Mobil: 20-931-0584**

p.moricz@szenzor-gm.hu

Szenzor Gazdaságmérnöki Kft.

1087 Budapest, Könyves Kálmán körút 76.

Telefon: (+36)-1-331-5523

Fax: (+36)-1-311-9636

E-mail: szenzor@szenzor-gm.hu

Honlap: www.szenzor-gm.hu

„Változással a sikerért”