

Legacy (*elavult?*) rendszerek a kritikus infrastruktúrában

Kocsis Tamás · ICS/OT Cybersecurity Expert

CYBERSEC

Az OT nem használ elavult rendszereket, így a kritikus infrastruktúrák sem használnak!

Köszönöm a figyelmet!

CYBERSEC



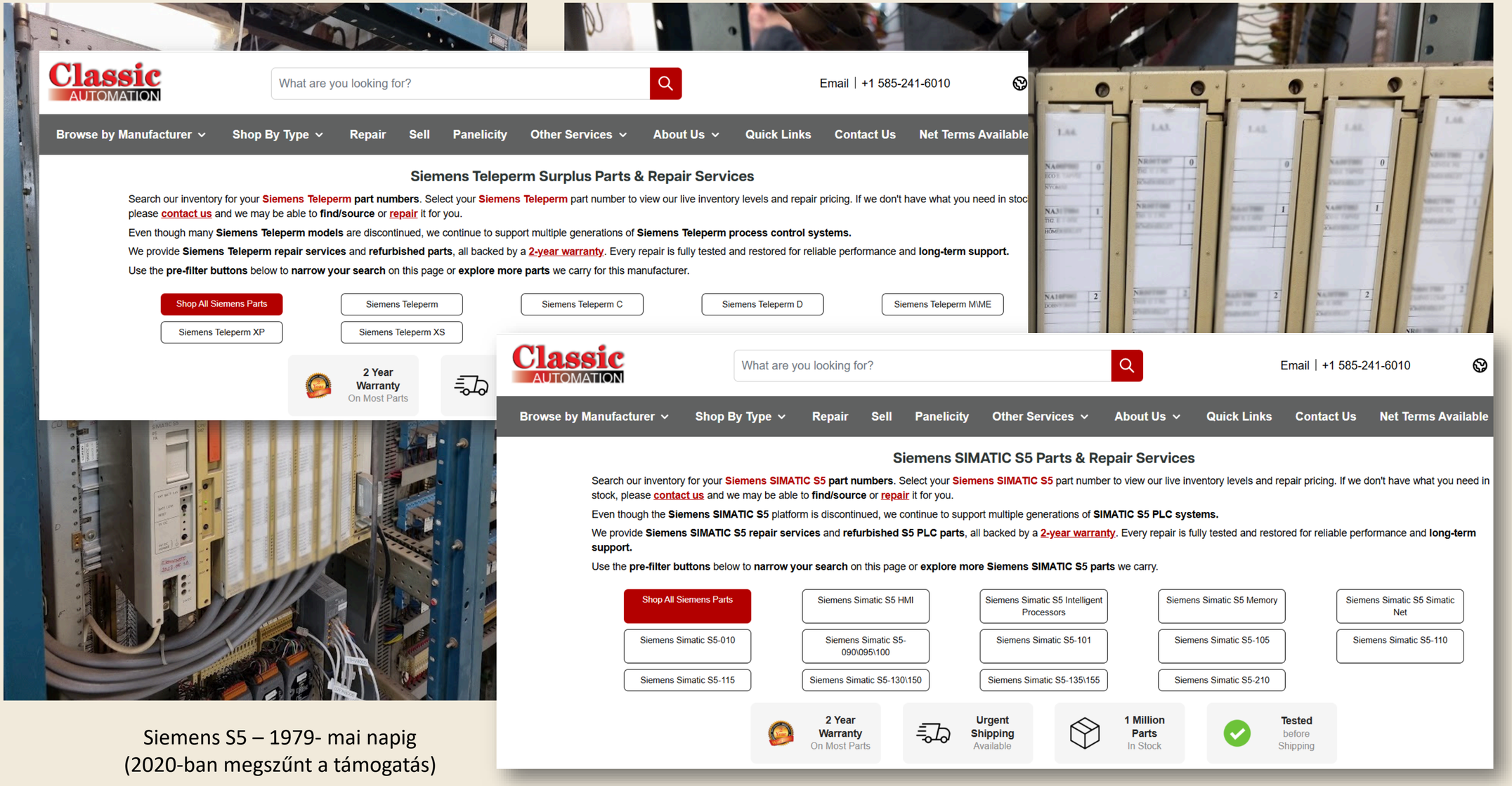
„Az OT-ban az az elavult rendszer, aminek ha tápot adsz, nem kapcsol be”

Cs. Péter, 32 éves (ex) karbantartó, a második éjszakai műszak előtt

Terminológia

- **A „legacy” – mint elavult rendszer**
  - Nem képes teljesíteni a funkcionális elvárásokat
  - Nem képes teljesíteni a termelési elvárásokat
  - A működése már nem üzembiztos és nem megbízható
- Az ilyen berendezések kiváltásra kerülnek

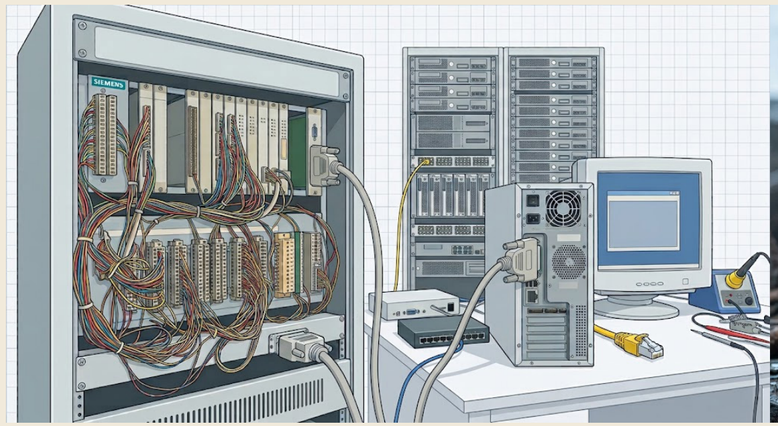
- **Kiberbiztonsági szempontból legacy rendszer**
  - ~~Elérte az életciklusa végét~~
  - Nem képes a modern kiberbiztonsági funkciók megvalósítására
  - Nem érkezik már hozzá (biztonsági) javítás
  - (kiber) fenyegetést jelent a többi eszközre, rendszerre, zónára
- Az ilyen berendezések NEM kerülnek kiváltásra, csak ha VALÓBAN elavult



Siemens S5 – 1979- mai napig
(2020-ban megszűnt a támogatás)

Ettől a probléma még adott

- **Nincs végzet, csak ha bevégzed!** *(de jobbára az OT-ban akkor sem ☺)*
  - Kiberbiztonsági fenyegetést jelenthetnek a többi rendszerre
  - De hogyan? Hiszen sokszor nincs is hálózati kapcsolat…





  - Az elérés igénye miatt a régi eszközök valahogyan kiforgatásra kerülnek a hálózatra
  - Pl. valamilyen busz kapcsolat egy 95/XP/W7-re, ami viszont már a hálózaton van
  - NT/95/XP/W7 is kiberbiztonsági szempontból legacy….

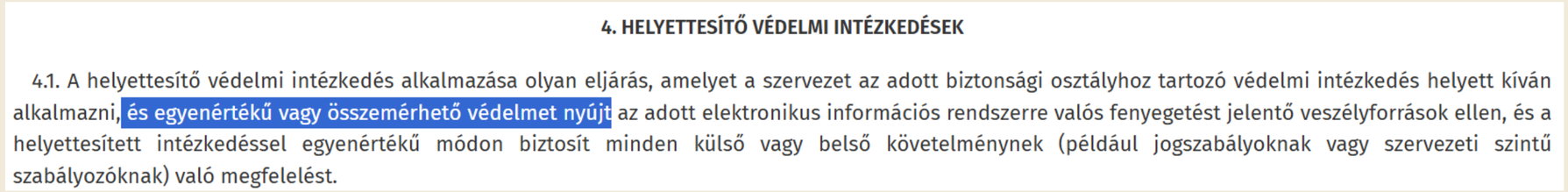
Ettől a probléma még adott

- **Mit nem kezdhetünk ezekkel az eszközökkel?**
  - Nem cserélhetjük le őket (ez nem az IT világa)
    - Egy eszköz és a futtatott logika nagyon szorosan összetartozik
    - Egy új eszköz miatt mindent is újra kellene írni – vagy fizikailag építeni
    - Folyamatos termelés
  - Nem patchelhetjük őket (akkor sem ha még van patch)
    - Egy eszköz és a futtatott logika nagyon szorosan összetartozik
    - Nem biztos hogy működni fog minden (üzembiztonság, megbízhatóság)
    - Szállítói, integrátori felelősségvállalás, garancia – integritáshoz kötött

  A kiberkockázatot azonban csökkenteni kell…

Ettől a probléma még adott

- **Mit kezdhetünk ezekkel az eszközökkel?**
  - Nem helyettesítő, hanem ***KOMPENZATÍV*** kontroll



4. HELYETTESÍTŐ VÉDELMI INTÉZKEDÉSEK

4.1. A helyettesítő védelmi intézkedés alkalmazása olyan eljárás, amelyet a szervezet az adott biztonsági osztályhoz tartozó védelmi intézkedés helyett kíván alkalmazni, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például jogszabályoknak vagy szervezeti szintű szabályozóknak) való megfelelést.

  - A 7/2024 ~~hülyeséget beszél~~ megfogalmazása gyakran az IT esetében sem reális
  - Az OT esetében egyáltalán nem kell, nem is mindig lehet egyenértékűségről beszélni
  - A célunk VALAMILYEN mértékű kockázatcsillapítás
  - Más kontrollcsaládok, más hatékonyság, alacsonyabb csillapítóerő

  - A kompenzatív kontroll az IT-ban ideiglenes, az OT-ban „A” kontroll

Ettől a probléma még adott

- **A kompenzatív kontroll**

Cél	Kontroll	Kontroll család
Jogosulatlan hozzáférés megakadályozása	Felhasználó név, jelszó	Megelőző
Jogosulatlan hozzáférés megakadályozása	Képernyőzár	Megelőző
Kártékony kód fertőzés megakadályozása	Végpontvédelem	Megelőző
Behatolás megakadályozása	IPS	Megelőző
Sérülékenység kihasználása	Patchelés	Korrekciós
Integritássértés megakadályozása	Kriptográfia	Megelőző

IT kontrollok és kontroll családok

OT kontrollok és kontroll családok

Cél	Kontroll	Kontroll család
Jogosulatlan hozzáférés megakadályozása	Kamerás megfigyelés	Észlelő
Jogosulatlan hozzáférés megakadályozása	Fizikai őrzés	Megelőző
Kártékony kód fertőzés megakadályozása	USB, internet tiltás	Megelőző
Behatolás megakadályozása	IDS	Észlelő
Sérülékenység kihasználása	Szegmentáció	Megelőző
Integritássértés megakadályozása	Szegmentáció	Megelőző

Szabályozás

- **Az IBSZ adaptálás nélkül nem erőltethető rá az OT-ra**
  - Az IT másképpen kezeli a „legacy” problémát
  - Az adaptálás nélkül OT-ra erőltetett szabályzat az üzembiztonságot fenyegetheti
  - A „legacy” probléma kezelése az OT-ban egyedi szabályozást igényel („OTBSZ”)

- OT Asset Inventory – eszköznyilvántartás
  - Ennek fontos eleme a kiberbiztonsági szempontból legacy eszközök nyilvántartása
  - Ha nem tudjuk hol van ilyen, milyen folyamatban vesz részt, hogy akarjuk megvédeni?
  - Kiberbiztonsági szempontból „legacy” állapot definiálása
  - Ha van inventory, van esély kompenzatív kontrollok alkalmazására
  - Ha nincs inventory, ismeretlen kockázatokat hordunk túl

Műszaki lehetőségek

- **Alapvető kompenzatív intézkedések**
  - *Szegmentáció* – hálózati hozzáféréskontroll, Pudue modell, zone-conduit modell
  - *Mikroszegmentáció* – egy eszköz fizikai vagy logikai leválasztása a saját zónájából
  - *Passzív IDS/monitoring* – forgalomtükrözés-alapú OT kiberbiztonsági platformok
  - *Egyirányú forgalmazás* – adatdióda (de jó lenne!!!!!!)
  - *Protokoll és parancsszűrés* – ipari protokollok funkcióinak korlátozása
  - *Protokollkonverterek* – sebezhető protokollról biztonságos protokollra fordítás
  - *USB kontroll* – fizikai, logikai
  - *Végpontvédelem* – speciális, OT számára fejlesztett végpontvédelmek
  - *Mentés, mentés, mentés* – reziliencia, helyreállás
  - *Virtualizáció* – alkalmazás, illetve régi OS bevirtualizálása (problémás buszkapcsolatok)

A legfontosabb...

- **Eszköz és fenyegetésvizibilitás**
  - Ha nem ismertek a kiberbiztonsági szempontból legacy eszközök, azok sebezhetőségei, gyengeségei és az általuk jelentett kockázat,
  - Ha nem ismert, milyen folyamatban és hogyan vesznek részt,
  - Ha nem ismert, milyen függőségek érintik ezeket az eszközöket, akkor

Egyáltalán nem lehet védelmi intézkedéseket tervezni, bevezetni és fenntartani!

Köszönöm a figyelmet!

SAFETY FIRST!