



27. Cestársky deň

Technické podmienky (TP) 93 – Centrálny riadiaci systém (CRS)
„Kybenetická bezpečnosť OT Systémov CRS“

Ing. Juraj Koreň
Sprecher Automation s.r.o.

© Sprecher Automation 2019



sprecher
automation

Agenda

- Prečo?** ... Incidenty, vírusy
... Legislatíva
- O čom?** ... IT/OT
... Industry / kritická infraštruktúra
- O kom?** ... Obstarávateľ, projektant, dodávateľ, prevádzkovateľ, správca
- Ako?** ... štandardy a koncepcie
... TP93, zmeny a doplnenia, kap. 4.10. KB technické požiadavky OT,

„Mýty a povery“



Kybernetická bezpečnosť OT Systémov CRS

Prečo? ... Incidenty, vírusy

2010: „STUXNET“ 1. malware, Irán, jadrové zariadenia
špecializovaný pre konkrétneho výrobcu PCS7!

2016: „Industroyer“
špecializovaný pre OT (RTU/PLC, IED ochrany), nezávislý od výrobcu!

2017: „WannaCry“
útoky na Deutsche Bahn, FedEx, Telefónica, ...

2019: „Lockergoga“
Norsk Hydro (škody >75 mio. USD / 3 mes.)

... To be continued



Kybernetická bezpečnosť OT Systémov CRS

Prečo? ... Legislatíva (TP93)

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016

zákon č. 69/2018 Zb. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov;

vyhláška NBÚ č. 362/2018 Zb. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení;

Odporúčania **NBÚ SK-CERT 2020**

zákon č. 45/2011 Zb. o kritickej infraštruktúre;



O čom? ... IT

V súčasnosti si už prakticky každý z nás nevie predstaviť život bez technických vymožeností ako sú osobné počítače, mobily, internet a iné zariadenia využívajúce moderné **IT technológie**. V súvislosti s týmito zariadeniami vnímame kybernetickú bezpečnosť ako ich neoddeliteľnú súčasť. Funkcie KB ako firewall, antivírus, šifrovanie, prihlasovacie „meno-heslo“ sú dnes samozrejmosťou.

Hlavnou funkciou IT systémov je **spracovávanie, prenášanie a prezentácia informácií**. Zariadenia, ktorých sa kybernetická bezpečnosť týka (tzv. komponenty) sú dobre známe servery, osobné počítače, notebooky, mobilné telefóny a pod. Kybernetickým útokom na IT systém sú ohrozené predovšetkým dáta a informácie.



O čom? ... OT

Hlavnou funkciou OT systémov je **signalizácia, monitorovanie, riadenie a chránenie technologických zariadení** v rôznych oblastiach a sektoroch priemyslu (energetika, doprava, voda, plyn, chémia,...).

Komponenty OT systémov predstavujú rôzne prístroje so špecifickými funkciami ako sú:

- **PLC** (Programmable Logic Computer) programovateľné logické automaty
- **RTU** (Remote Terminal Unit) terminály diaľkového ovládania
- **IED** (Intelligent Electronic Device) inteligentný riadiaci alebo ochranný terminál (energetika)
- **DCS** (Distributed Control Systems) distribuované riadiace systémy
- **SCADA** (Supervisory Control And Data Acquisition) dispečerské riadiace systémy

Kybernetický útok na OT systém nepredstavuje len hrozbu poškodenia samotného komponentu ale predovšetkým hrozbu **škody podstatne väčšieho rozsahu** na samotnom technologickom zariadení s možným dopadom na zdravie a životy ľudí ako aj možné ohrozenie životného prostredia.

O čom? ... OT

Kybernetická bezpečnosť systémov IT a OT je v základných rysoch podobná téma. Napriek tomu majú OT systémy svoje **vlastné špecifiká**, vid' tabuľka:

IT systémy:

Hlavné procesy:	spracovávanie informácií
Charakteristika:	Dynamické systémy
Životný cyklus:	4-6 rokov
Patch management:	2-3 x rok
Dostupnosť:	výpadky akceptované
Aktuálne zabezpečenie:	dobré
Komunikačné protokoly	TCP/IP
Koncové zariadenia:	server, PC/NB, LAN

OT systémy (ICS/IACS):

riadenie technologických procesov
Deterministické systémy
15-20 rokov
1 x rok(1 x 2roky)
7/24
nízke / žiadne
IEC80750-5-xxx, IEC61850, Profibus, Modbus
RTU, SCADA, PLC, DCS, EMS, ...

O čom? ... OT

Členenie OT systémov:

- **nekritická infraštruktúra** „industry“, riadiace a informačné systémy výrobných technológií
požiadavky KB: žiadne až stredné
- **kritická infraštruktúra** „utility“, riadiace a informačné systémy energetika, voda, plyn, **doprava**,
požiadavky KB: **stredné až vysoké**



- „ostatné“, riadiace a informačné systémy budov, public, IoT Internet vecí, ...
požiadavky na KB: žiadne až nízke

O kom?

Požiadavky KB sú záväzné a musia byť uplatnené počas všetkých fáz životného cyklu zariadenia, t.j.:

- **akvizícia** (obchodno-technická dokumentácia, výber zhotoviteľa, obchodná dodávateľská zmluva)
-> *zodpovednosť obstarávateľa,*
- **projektová príprava** (realizačná dokumentácia, dokumentácia skutočného vyhotovenia, ...)
-> *zodpovednosť projektanta,*
- **realizácia** (HW / SW, implementácia, skúšky, ...)
-> *zodpovednosť zhotoviteľa,*
- **prevádzka** (manipulačný a prevádzkový poriadok, návody na obsluhy, návody na školenie)
-> *zodpovednosť prevádzkovateľa,*
- **údržba** (návody na servis a údržbu, servisná zmluva)
-> *zodpovednosť správcu,*

Ako? ... štandardy a koncepcie (TP93)

IEC 62443 Cyber security standards for control systems

Medzinárodný štandard kybernetickej bezpečnosti pre riadiace systémy

BDEW White paper Whitepaper Requirements for Secure Control and Telecommunication Systems

Smernica bezpečnostných požiadaviek pre riadiace a telekomunikačné systémy

ISO/ISA 27001 Information Security Management System

Medzinárodný štandard systému riadenia informačnej bezpečnosti

Ako? ... TP93 zmeny a doplnenia 07/2020

kapitola 4.10 Kybernetická bezpečnosť - minimálne technické požiadavky

Minimálne technické požiadavky na kybernetickú bezpečnosť sa týkajú **každého jednotlivého prístroja CRS** obsahujúceho prvky IT (ako sú mikroprocesorová jednotka, komunikačné rozhrania a pod.) ako **aj celého systému**, ktorý je podľa kritérií kategorizácie sietí a informačných systémov klasifikovaný do **kategórie II alebo III**.

Minimálne technické požiadavky na funkcie a parametre aktívneho a účinného kybernetického zabezpečenia prístrojov CRS sú:

- funkcia generovania bezpečnostných Logov (napr. **Syslog** a iné typy aplikačných logov),
- zabezpečená komunikácia z monitorovania a analyzovania udalostí v sieťach a informačných systémoch (SIEM) protokolom **Radius** (Remote Authentication Dial-In User Service)
- funkcia manažmentu sietí **SNMP v1,2,3** (Simple Network Management Protocol),
- funkcia **Firewall** layer 2,3,4,7,
- funkcia **Router**, segmentácia sietí **VLAN** (Virtual LAN),

Ako? ... TP93 zmeny a doplnenia 07/2020

Minimálne technické požiadavky na funkcie a parametre aktívneho a účinného kybernetického zabezpečenia prístrojov CRS sú: (pokračovanie)

- funkcia zabezpečeného prístupu do systému a riadenia oprávnení **RBAC** (Role-based Access Control) a mechanizmu **AAA** (Authentication-Authorization-Accounting), **MAC** (Mandatory Access Control),
- funkcia zabezpečeného vzdialeného prístupu **SSL** (Secure Sockets Layer)/**TLS** (Transport Layer Security), **TLS** 1.2 (minimálne), **TLS** 1.3. preferované,
- funkcia šifrovania komunikácie **IPSec**, **OpenVPN**,
- funkcia šifrovania prostredníctvom **HW Crypto-chip**,
- všetky dáta ukladané na pamäťové médiá musia byť zabezpečené šifrovaním a chránené certifikátmi,
- systém antivírovej ochrany, **IPS** (Intrusion Prevention System), aktívna ochrana
- systém monitorovania a detekcie kybernetických incidentov **IDS** (Intrusion Detection System), pasívna ochrana
- zaistenie **upgrade a podpory** (Patch-management) zo strany výrobcu počas celej životnosti systému (**min 15-20 rokov**),

Mýty a povery

„doteraz sme to nepotrebovali a nič sa nestalo“ ... dopĺňame „áno, ale iba zatiaľ“.

Nástupom nových technológií priemyselných riadiacich systémov založených na mikroprocesorových riešeniach a vznikom nových špecializovaných škodlivých kódov (vírusov) vzniká nevyhnutná potreba riešenia kybernetickej bezpečnosti.

„máme samostatnú technologickú LAN sieť ktorá je zabezpečená firewall-om“

oddelenie LAN sietí prostredníctvom samostatného firewallu je v súčasnosti už nepostačujúce, keďže štatistika dokazuje, že cca 80% kybernetických útokov je „z vnútra“, to znamená že škodlivý kód je zanesený priamym pripojením sa do vnútornej LAN siete alebo dokonca priamym pripojením sa na komponent OT zariadenia.

„výrobcovia OT systémov nám tvrdia, že to majú vyriešené“ alebo „papier znesie všetko“

Pravda je taká, že čelíme tlaku dezinformácií, polo-právd a zmanipulovaných informácií. Stretávame sa aj s prípadmi, kedy výrobca xy predloží certifikát o kybernetickej bezpečnosti, ktorý si vystavil sám sebe!

Odporúčanie: Presvedčiť sa o skutočnej úrovni implementácie funkcií kybernetickej bezpečnosti v súlade s overenými koncepciami (napr. Defence-in-depth) vykonaním fyzického odskúšania vlastnou alebo nezávislou odbornou autoritou!

