Betamont®

Railway signaling systems

SHIELD TECH

Kybernetická bezpečnosť – Mýty a povery

Betamont®

SHIELD TECH

Juraj Koreň

architekt kybernetickej bezpečnosti OT systémov

+421 905 221162
koren@hep.sk
juraj.koren@shieldtech.sk
juraj.koren@ndsas.sk

SVŠT SjF, ASRTP, r. 1986, Ing., CUB, management r. 2002, certifikát MBA

30 rokov – zástupca výrobcov a dodávateľov automatizačnej techniky pre segmenty: energetika, doprava, plyn, voda, ropa/chémia, priemysel,… (SAT, Siemens, Sprecher)

5 rokov - konzultant, architekt kybernetickej bezpečnosti OT systémov (Transpetrol, NDS, ZSD, Shieldtech, projektanti, …)

4 roky – školiteľ kybernetickej bezpečnosti OT systémov (projektanti, prevádzkovatelia, zhotovitelia, Sekurkon CZ, …)

Obsah prezentácie

Náš spoločný cieľ:

Bezpečná a spoľahlivá prevádzka systémov EE a OZT ŽSR

Pracovné stretnutia 2021:

- O čom? (terminológia, IT, OT, IoT,)
- Prečo? (história, hrozby, incidenty, legislatíva, dokumentácia, ISO)
- O kom, pre koho? (výrobca/projektant/dodávateľ/prevádzkovateľ)
- Ako na to? (koncepcie, štandardy, best practice, desatoro KB)

Obsah prezentácie:

- Ako sme na tom? (výsledky auditov, IT vs. OT)
- Nové hrozby (Industroyer 2,... viď ESET, Ukrajina, ...)
- Mýty a Povery

Betamont®

Ako sme na tom?

SHIELD TECH

Výsledky zrealizovaných auditov priniesli aj **zaujímavú štatistiku** :
(zdroj ISACA Slovakia Chapter)

Verejná správa a inštitúcie - priemer:	**súlad 9%**, maximálny súlad 90%, minimálny súlad 5%	nesúlad 85%,	čiastočný súlad 6%,
Súkromný sektor - priemer:	**súlad 79%,** maximálny súlad 93%, minimálny súlad 9%	nesúlad 3%,	čiastočný súlad 16%

Okrem rozdielov medzi inštitúciami verejnej správy a súkromným sektorom, poukázali zistenia audítorov aj na **veľký rozdiel úrovne implementácie KB v systémoch IT a OT**.
Kým pri systémoch IT je problematika KB riešená už dlhodobo, v OT je implementácia KB na veľmi nízkej až žiadnej úrovni.

Betamont

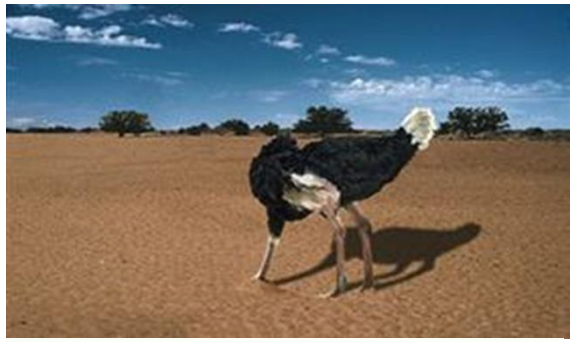
SHIELD TECH

Ako sme na tom?

Zistenia z auditov KB v spoločnostiach „prevádzkovateľ základnej služby“ (zdroj ISACA Slovakia Chapter).

Najčastejšie nálezy a zistenia audítorov sú:

- nedefinovaná stratégia KB, chýbajúca bezpečnostná dokumentácia,
- nepochopenie a nepodpora z pozícia najvyššieho manažmentu,
- neexistencia pozície manažéra KB,
- nesprávne prepojenie pozície manažéra bezpečnosti s operatívnym riadením IT a OT
- absencia vzdelávania v oblasti informačnej bezpečnosti,
- chýbajúce mechanizmy riadenia aktív, hrozieb a rizík,
- chýbajúci monitoring sietí a logovanie udalostí KB,
- neexistencia procesov riešenia incidentov a kontinuity činností,
- zastarané technológie nepodporujúce KB (predovšetkým v časti OT systémov),
- závislosť prevádzkovateľov na dodávateľoch (vendor-lock-in)
- a ďalšie



Legislatívna povinnosť ŽSR

NBÚ SK-CERT Národná jednotka kybernetickej bezpečnosti NBÚ, (Rady a návody)
(KCCKB kompetenčné a certifikačné centrum kybernetickej bezpečnosti)

zákon č. 69/2018 Zb. o kybernetickej bezpečnosti
zákon č. 95/2019 Zb. o informačných technológiách vo verejnej správe
ŽSR je prevádzkovateľom základnej služby!
zákon č. 45/2011 Zb. o kritickej infraštruktúre,
ŽSR je zaradený do kritickej infraštruktúry štátu!

Vyhláška NBÚ č. 164/2018 ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
Vyhláška NBÚ č. 165/2018 ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
Vyhláška NBÚ č. 362/2018 ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Vyhláška NBÚ č. 436/2018 o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
Vyhláška Úradu podpreds. vlády SR č. 179/2020 o štandardoch pre informačné technológie verejnej správy

Ako sme na tom?

Dobrá správa:

- Vedenie ŽSR si uvedomuje nevyhnutnosť okamžitého riešenia kybernetickej bezpečnosti!
- Overené riešenia účinnej kybernetickej bezpečnosti sú k dispozícii (netreba vymýšľať „teplú vodu“)
- „Začať treba dnes, ... zajtra môže byť neskoro!“

Druhá správa: nasledujúci audit KB už o 18 mesiacov !!!

Betamont®

Nové závažné hrozby

SHIELD TECH

Kybernetické útoky na OT systémy súvisia so **vznikom nových špecializovaných škodlivých kódov –vírusov**.

Tieto špecializované vírusy prinášajú nové závažné zraniteľnosti a ohrozenia, ktoré búrajú doteraz zaužívané mýty o kybernetickej bezpečnosti OT systémov.

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

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

https://www.mojandroid.sk/eset-analyzoval-priemyselnu-hrozbu/

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

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

2022: **„Industroyer2“ , „CaddyWiper“, „Orcshred“ , „Soloshred“, „Awfulshred“, …**

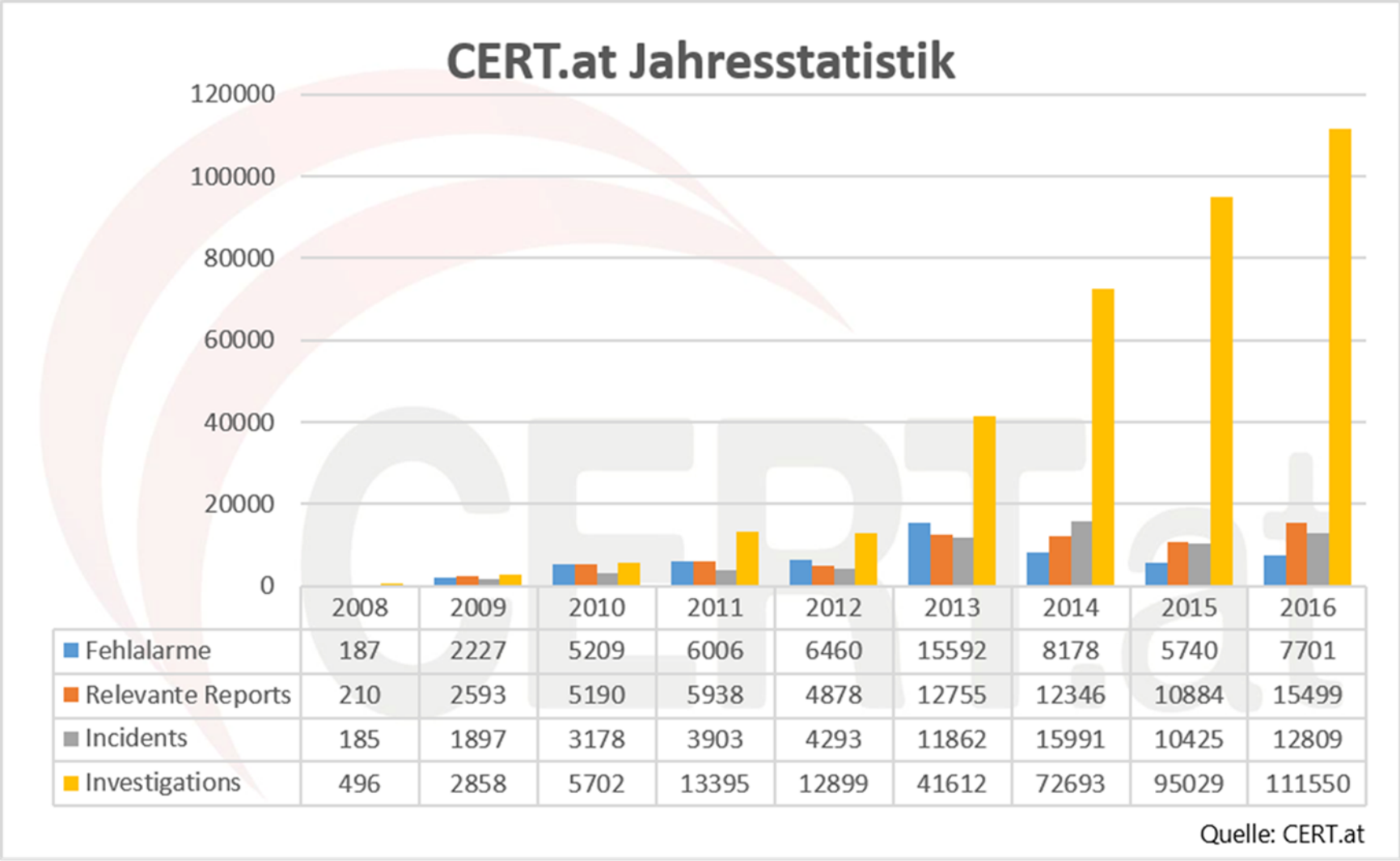
(zdroj ESET https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/)

… To be continued

Betamont®

Geometrický nárast

SHIELD TECH

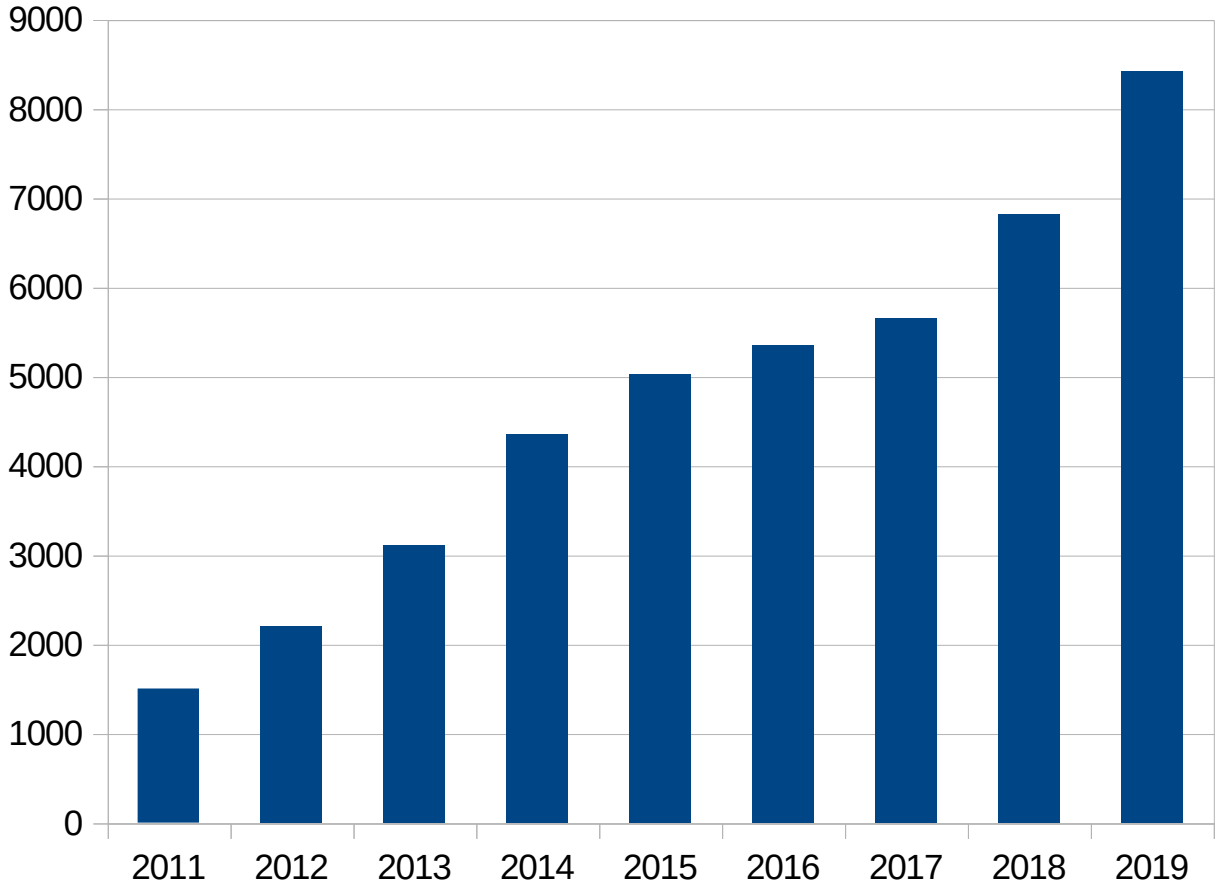


	2008	2009	2010	2011	2012	2013	2014	2015	2016
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550

Quelle: CERT.at

Kybernetická kriminalita

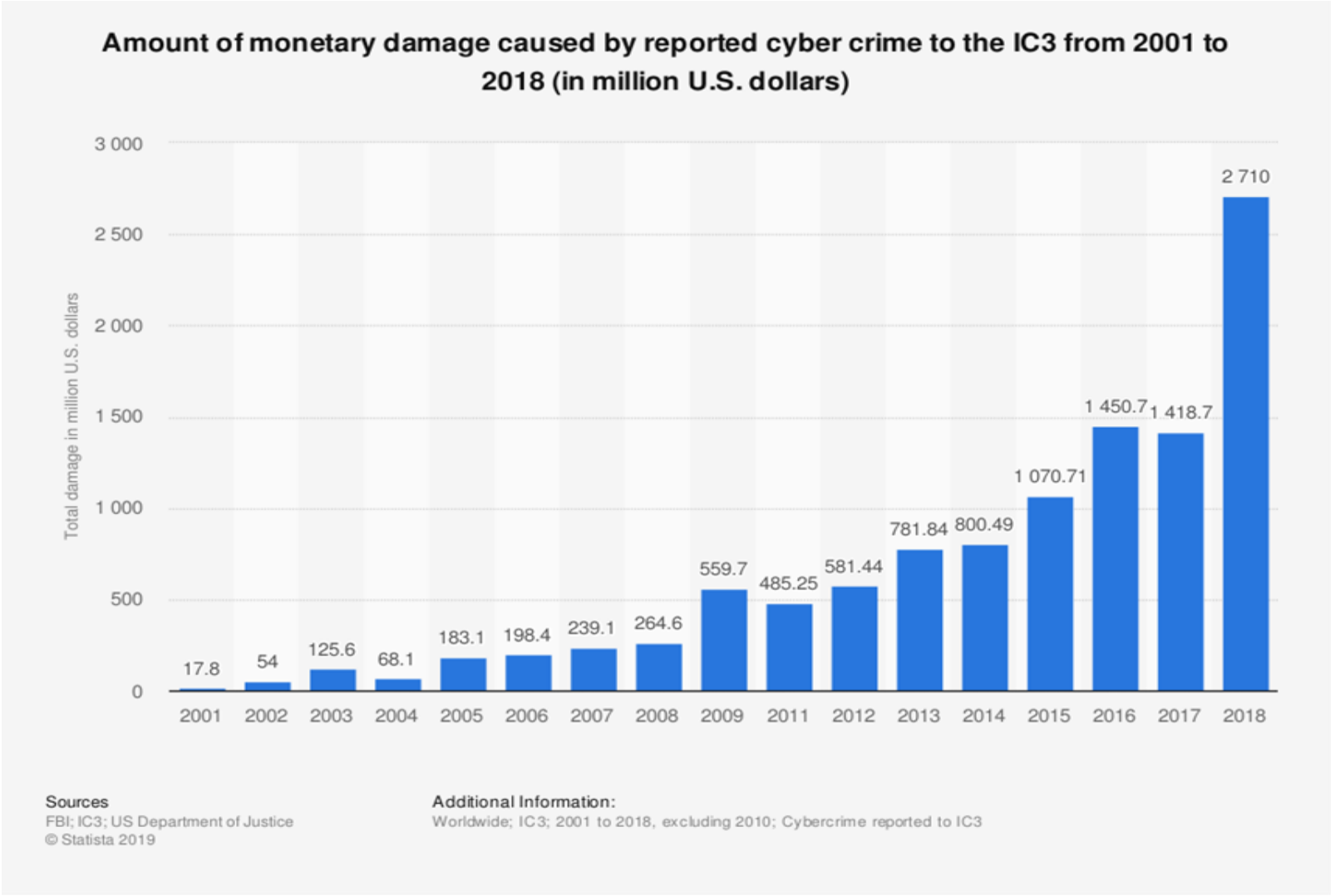
Počet trestných činov z oblasti kyber-kriminality v rokoch 2011 až 2019
(zdroj: Policie ČR)



Betamont®

Materiálne škody

SHIELD TECH



Betamont®

Zistenia ...

SHIELD TECH

Štatistika slovenského **CSIRT** tímu za rok evidovala **1 613 156 bezpečnostných incidentov,** iba ohlásených!!!

Aktuálne štatistiky úradu CSIRT ukazujú, že **okrem geometrického nárastu** počtu incidentov sa mení aj tzv. **„vektor útokov“,** tj. spôsob ako dôjde k prieniku škodlivého kódu do systému.

V minulosti bolo nevyhnutné chrániť systémy **voči prienikom z vonkajšieho prostredia** (internet, WAN, ...). Ochrana spočívala v oddeľovaní systémov a nasadzovaní bezpečnostných Firewall-ov na rozhraní systémov, tzv. **perimetri,** resp. postačovalo monitorovanie komunikačných sietí.

Tieto formy ochrany už v súčasnosti neposkytujú dostatočnú úroveň zabezpečenia. Okrem doteraz používaných nástrojov je **v súčasnosti nevyhnutná potreba** aktívnej a autonómnej ochrany nevyhnutnej **na úrovni každého prvku IT/OT systému**, t.j. **„z vnútra“** na úrovni tzv. „koncových zariadení“ ako sú PC, NB, Server, PLC, SCADA, ...

Tento jav sa v súčasnosti označuje ako 80/20

t.j. **80% útokov je z „vnútra“ systémov a len 20% útokov „zvonku“**

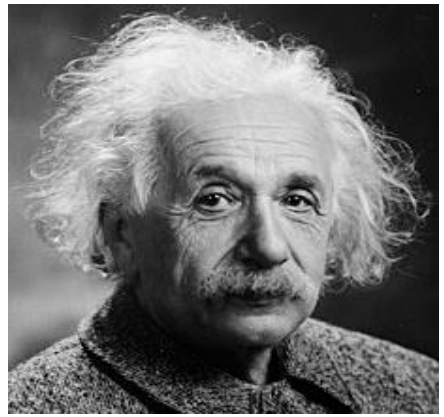
Betamont®

Riziko

SHIELD TECH

E = mc2

Energia = hmotnosť krát rýchlosť svetla na druhú



Riziko = Zraniteľnosť * Ohrozenie * Dopad

Zraniteľnosť: OS Windows XP/7/10 (v OT), nevhodná architektúra systému, proprietárne systémy, EOL, aktualizácie, ...
Najväčšia zraniteľnosť sa nachádza medzi klávesnicou a stoličkou!!!
Ohrozenie: škodlivý kód / vírus, požiar, zatopenie, elektromagnetická odolnosť, ...
Dopad: poškodenie / zničenie zariadenia (nie OT), výpadok služby, poškodenie životného prostredia, zdravia, životov, ...

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 oddelenú technologickú LAN sieť ktorá je zabezpečená firewall-om“

Oddelenie LAN sietí prostredníctvom samostatného firewallu je v súčasnosti pre OT 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. „Pseudoodborníci“ (aj z radov zavedených a známych dodávateľov) budú presviedčať o svojich riešeniach (viď brána v poli).

Stretávame sa aj s prípadmi, kedy výrobca xy predloží certifikát o kybernetickej bezpečnosti, ktorý si vystavil sám sebe!

Mýty a povery

„proprietárne riešenia sú bezpečné“

Mýtus, opak je pravdou! Proprietárne riešenia a proprietárne komunikačné protokoly predstavujú najvyššiu zraniteľnosť, t.j. Riziko

„sériová komunikácia je bezpečná“

Technológie sériových komunikácií boli vyvinuté v období kedy ešte nebola potreba riešiť KB a preto neobsahujú (ani nebudú obsahovať) funkcie a parametre KB, t.j. technológia EOL.

„KB je drahé, my si to nemôžeme dovoliť“

Mýtus! Aplikáciou koncepčných a overených riešení, t.j. Architektúra systému + použité prvky s funkciami a parametrami KB nepredstavujú žiadne náklady naviac. Dodatočné dopĺňanie čiastočných a nesystémových riešení predstavuje náklady naviac.

O cene za likvidáciu škôd a dopadov ani nehovorím!

Štandardy, odporúčania

Odporúčanie:

- Definovať minimálne požiadavky KB na architektúru systémov a výber prvkov na základe funkcií a parametrov KB.
- Implementácie funkcií kybernetickej bezpečnosti v súlade s overenými koncepciami (napr. Defence-in-depth)
- vykonať fyzické odskúšanie účinnosti technických riešení vlastnou alebo nezávislou odbornou autoritou!

Štandardy:

IEC 62443 Cyber security standards for control systems
Medzinárodný štandard kybernetickej bezpečnosti pre riadiace systém

BDEW White paper Whitepaper Requirements for Secure Control and Telecommunication Systems
Smernica bezpečnostných požiadaviek pre riadiace a telekomunikačné systémy

NBÚ SK-CERT Národná jednotka kybernetickej bezpečnosti NBÚ, Rady a návody
https://www.sk-cert.sk/sk/rady-a-navody/bezpecnost-priemyselnych-ot-systemov/index.html
(KCCKB kompetenčné a certifikačné centrum kybernetickej bezpečnosti)

ISO 27001 Information Security Management System
Medzinárodný štandard overovania systému riadenia informačnej bezpečnosti

Rekapitulácia

- Ako sme na tom? (výsledky auditov, porovnanie IT vs. OT, legislatíva)
- Nové hrozby (Industroyer 2,... viď ESET, zistenia a trendy, riziká, ...)
- Mýty a Povery (odporúčania, štandardy, koncepcie)

Dá sa povedať, že o Kybernetickej bezpečnosti už toho vieme dosť.

Čo nám ešte chýba aby sme mohli dosiahnuť náš cieľ?

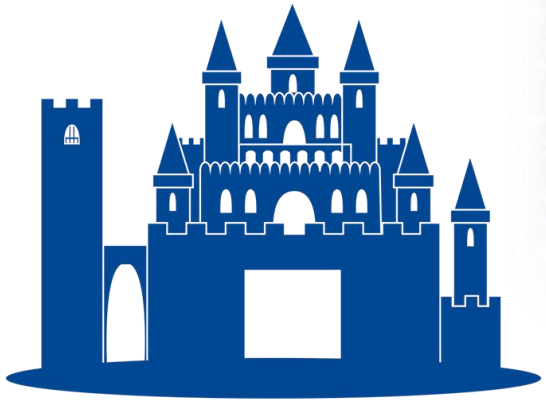
Bezpečná a spoľahlivá prevádzka systémov EE a OZT ŽSR

SPRÁVNE ROZHODNUTIE

SPRÁVNE ROZHODNUTIE

ROZHODNUTIE „A“

ROZHODNUTIE „B“



Betamont®

Ďakujem Vám za pozornosť

SHIELD TECH

Juraj Koreň, architekt kybernetickej bezpečnosti OT systémov
+421 905 221162
koren@hep.sk juraj.koren@shieldtech.sk