NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA (Technical Assessment Methodology)

Roman Kočnar, dipl.ing.el.

NEK Nuklearna Elektrarna Krško

- Westinghouse je počeo gradnju elektrane 1974.
- Tip elektrane je PWR (jedan reaktor)
- Proizvodnja struje od 1981.
- 700 MW
- baseload elektrana (18 mjeseci 24/7)
- nakon 40 godina rada dozvola za sljedećih 20 godina

Zakonski kontekst

NEK podliježe kibernetičkoj sigurnosti po dva slovenska zakona:

- Pravilnik o čimbenicima nuklearne i radiološke sigurnosti, izdan 2016., uključuje i dijelove koji se odnose na kibernetičku sigurnost, a nastali su na temelju američkog zakona 10CFR73.54 Protection of digital computer and communication systems and networks.
- Zakon o informacijskoj sigurnosti (ZinfV), izdan 2018. na temelju zahtjeva EU NIS direktive iz 2016.

NEK krovni dokumenti

Za područje kibernetičke sigurnosti u NEK su napisana dva programa:

- Program IS-1 Informacijska sigurnost definira kibernetičku sigurnost na području informacijske tehnologije (IT) u NEK u, dok
- Program SP-3 Cyber Security definira način provođenja kibernetičke sigurnosti na operativno tehnološkom (OT) području i definira uvjete za određivanje sustava koje ćemo štititi sukladno važećim zakonima.

Program SP-3 Cyber Security

- Za sustave koji su određeni kao ključni prema Zakonu o informacijskoj sigurnosti (ZinfV), provodimo ocjenu rizika prema standardima serije ISO 27000.
- Za sustave koji su određeni kao kritični prema Pravilniku o čimbenicima nuklearne i radiološke sigurnosti, provodimo analizu po EPRI TAM (Technical Assessment Methodology) metodi (u skladu s slovenskim regulatorom URSJV).
- Obje liste sustava tretiramo kao poslovnu tajnu
- Za sustav koji je prepoznat i kao ključni i kao kritični pripremamo dvije različite analize.

EPRI TAM

Electric Power Research Institute (EPRI)

- godišnji promet > $650M, 2100 zaposlenih,
- priprema primjenjive dokumente.

EPRI TAM metoda je sistematski pristup analizi sustava u kontekstu kibernetičke sigurnosti . TAM zahtjeva da korisnik:

- razumije rad njihovih sustava i komponenti,
- analizira stvarne ranjivosti i kako sustav može biti napadnut,
- smanji te ranjivosti na prihvatljivu razinu rizika,
- implementacijom učinkovitih sigurnosnih mjera.

EPRI TAM koraci

- utvrđivanje kritičnih sustava koje posebno branimo
- određivanje kritičnih digitalnih komponenti (CDA – Critical Digital Asset) unutar kritičnih sustava koje posebno štitimo
- identifikacija poznatih ranjivosti i vektora napada za svaki CDA
- ocjenjivanje mogućih prijetnji za svaku ranjivost
- odabir minimalnog broja potrebnih sigurnosnih mjera za zaštitu, detekciju i odgovor u slučaju kibernetičkog napada za svaku moguću prijetnju
- objektivnu ocjenu jesu li odabrane sigurnosne mjere dovoljne. Ako jesu, analiza se smatra završenom.

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- Na temelju EPRI TAM metode, u NEK u je napisana izvedbena procedura ESP 2.921 koja osigurava dosljedno provođenje analize sustava. Analiza sustava po proceduri ESP-2.921 ponavlja se:
  - svakih 18 mjeseci,
  - prije ugradnje nove komponente,
  - prije zamjene postojeće komponente,
  - prije promjene konfiguracije ugrađene komponente,
  - u slučaju nove ranjivosti neke komponente unutar sustava.

NEK kritični sistemi

- Od 134 računalna sustava u NEK, 40 je određenih kao kritični prema programu SP-3. To znači da je potrebno 40 analiza prema EPRI TAM metodi. Unutar tih 40 kritičnih sustava prepoznato je 1663 digitalnih komponenti (DA - Digital Asset).

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- Za svaku analizu rezultat je dokument koji se sastoji od četiri dijela. Cijeli dokument se klasificira kao poslovna tajna jer pruža detaljan uvid u sustav i njegove komponente, njihove ranjivosti te izabrane sigurnosne mjere koje se moraju implementirati.
- Prvi dio dokumenta opisuje sustav i objašnjava zašto je sustav kritičan u pogledu kibernetičke sigurnosti.

NEK KIBERNETIČKA SIGURNOST
EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- Prvi dio analize opisuje rad sustava i objašnjava zašto je sustav prepoznan kao kritičan u pogledu kibernetičke sigurnosti.

			ESP-2.921, App. 6.1
CDA ANALYSIS:		REVISION:	Page 1 of 1
CDA ANALYSIS NAME:			
CDA ANALYSIS STATUS:	☐InWork ☐Finished ☐Retired		
SYSTEM:			
CDA ASSET ID:			
CDA ASSET Description:			
Analysis Additional CDA:	☐ YES ☐ NO		
Comments:			
CDA Analysis Assessment Results			
All Attaack patways are mitigated: ☐YES ☐NO			
CDA Analysis Next Periodic Assessment:	Date:		
Responsible Engineer:	Signature:	Date:	
ING.PI Superintendent:	Signature:	Date:	

Security Controls Implementation status		
Security Controls Implemented:	Date:	
Security Controls Implementation Next Periodic Check:	Date:	
Responsible Engineer:	Signature:	Date:
ING.PI Superintendent:	Signature:	Date:

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- Drugi dio dokumenta je detaljni opis digitalnih komponenti (DA Digital Asset). Za svaku digitalnu komponentu sustava navode se niz podataka potrebnih za analizu: firmware, operativni sustav, instalirane programe, komunikacijske portove na samoj komponenti, ugrađene čitače različitih medija, HMI (Human Machine Interface) na samoj komponenti, komunikacijske protokole, posebne datoteke, usluge, aktivno skeniranje komponente (ako je provedeno), funkcije digitalne komponente koje je moguće onemogućiti ili u potpunosti ukloniti (u slučaju fizičkog modula), mogućnost instalacije dodatnih programa, izmjenu konfiguracije, održavanje komponente, zapisivanje podataka koje komponenta može generirati, pripremu sigurnosnih kopija podataka.

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

Appendix 6.2: Asset Characterization

5.3 Purpose of the system

5.3.1.1 Firmware Description and Version

Firmware name & version:
Update Method:
BIOS/UEFI Password Protection:
Requires Mobile Code? [ ] Describe:

5.3.1.2 Operating System and Version

OS name & version:
Update Method:

Requires Mobile Code? [ ] Describe:
Collaborative Computing? [ ] Describe:

5.3.1.3 Installed Application Software & Version

Application software name & version:

Update method:

Supports Access Control Accounts? [ ] Describe:

Requires Mobile Code? [ ] Describe:
Collaborative Computing? [ ] Describe:

5.3.1.4 Physical Communication Ports and Terminals

1.
2.
3.

5.3.1.5 Removable Media and Portable Devices

1.

Appendix 6.2: Asset Characterization

2.
3.

5.3.1.6 HMI Capabilities

1.
2.
3.

5.3.1.7 Available Data Communication Protocol(s):

1.
2.
3.

5.3.1.8 Data Files, Software Objects, Services, and Logical Communication Ports

1.
2.
3.
4.
5.

5.3.1.9 Active Scanning Used to Discover Asset Characteristics

Scan Tools Used:

Types of Scans Performed:

Summary of Scan Results: Scan Results Attached? [ ]

5.3.1.10 Installed Features/Options that can be Disabled or Removed that Affect any Attack Pathways:

Can be disabled:
1.
2.
3.

Can be removed:
1.
2.

Appendix 6.2: Asset Characterization

3.

5.3.1.11 Capability for Installation of Third Party Software

Description:

5.3.1.12 Configuration & Maintenance Method

1.
2.
3.

5.3.1.13 Event/Alert/Audit Log - Event Monitoring:

a) Events logged:
b) Event Record Content:
c) Time Stamp Synchronization Capability:
d) Log Storage Capacity and Behavior:
e) Response to Event Log Processing Failures:
f) Log Aggregation, Correlation, and Forensic Capability:
g) Log Protection Mechanisms:
h) Configuration Capability:

5.3.1.14 Asset Backup & Restore Capability:

5.3.1.15 Engineered Features and Functions Available for Cyber Security Use:

a) Windows Domain:
b) Logical User Configuration:

Static permissions associated with anonymous passwords or PINs [ ]

Static accounts and permissions [ ]
End-user defined accounts and permissions [ ]
Describe:

c) Authentication Mechanism Protections:
d) Hardware Access Control Features:
e) Centralized SIEM Event Log Capability:

Appendix 6.2: Asset Characterization

f) IDPS Capability:
g) Network Communications Protection:
h) Defensive Boundary Protection:
i) Cryptography Capabilities:
j) Other:

5.3.1.16 Vendor/Manufacturer Security Advisory & Patch Program:

5.3.1.17 Manufacturer Product/Company Security Certifications:

5.3.1.18 Other Model Numbers with the Same Asset Characteristics

5.3.1.19 List of Manuals & Documentation:

1.
2.
3.

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- Treći dio analize je spisak svih digitalnih komponenti u sustavu

MECL:	MECL Description:	Item number	Rebuildable Number	DA		CDA		CDA Assess. Finished
				NO	YES	NO	YES	
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐
				☐	☐	☐	☐	☐

Procedura ESP 2.921 Cyber security Assessment of critical digital assets (CDA) in NEK

- četvrti dio dokumenta je analiza CDA.
- za svaki CDA (kritičnu digitalnu komponentu) izvodi se pojedinačna analiza. Analiza se nalazi u dokumentu veličine jedne stranice A3 (Microsoft Excel), što znači da koliko ima CDA u sustavu, toliko imamo analiza.
- ako se u sustavu nalazi dvije ili više identičnih komponenti koje obavljaju istu funkciju, možemo pripremiti jednu analizu i koristiti je za više istih komponenti.
- može se pripremiti zajedničku analizu za dvije ili više različitih komponenti (za grupu CDA). Bez obzira na to za koje komponente je analiza pripremljena, važno je da se obrade sve prepoznate CDA u sustavu. Ne smije se zaboraviti niti na jednu digitalnu komponentu.

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

Attack Patways					
Number	Attack Pathways Physical Interface (1)	Attack Pathways communicatio n Protocol (2)	Attack Pathways Description (3)	Asset ID (MECL):	Asset Description:
A1					
A2					
A3					
A4					
A5					
A6					
A7					
A8					
A9					
A10					

SECURITY CONTROL METHODS		
Engineered Security Control Methods		
Method number	Security Control Methods (7)	Description (8)
M1		
M2		
M3		
M4		
M5		
M6		
M7		
M8		
M9		
M10		
Inherited Site Security Control Methods		
Method number	Security Control Methods (9)	Description (10)
I1		
I2		
I3		
I4		
I5		
I6		
I7		
I8		
I9		
I10		
Directly Implemented Inherited Site Security Control Methods		
Method number	Security Control Methods (11)	Description (12)
D1		
D2		
D3		
D4		
D5		
D6		
D7		
D8		
D9		
D10		

Attack Pathways and Associated Exploit Mechanisms						Allocation of Security Control Methods			
Technical Vulnerability Class			Applies? (4)	Applicable Attack Pathway(s) (5)	Mechanism to Exploit Vulnerability Class and Notes (6)	Protect (13)	Detect (14)	Respond & Recover (15)	Basis - Description (16)
Vulnerability Classes Associated with Direct Action Against the Component									Direct Action
Component Enable/Disablement-Immediate			NO						
Component Disablement- Delayed			NO						
Denial of Service (DOS)			NO						
Malware			NO						
Vulnerability Classes Associated with the 6 Critical Data Types									Critical Data Types
Operational Process Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
OEM Defined Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
User Defined Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
Security Operational Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
OEM Defined Security Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
User Defined Security Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						

Prepared by: _____ Date: _____

Approved by: _____ Date: _____

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

- Za svaki CDA potrebno je opisati sva fizička sučelja. Za svako sučelje potrebno je navesti ime, komunikacijski protokol i opisati kako se može zlorabiti. Pod sučeljem se smatraju fizički portovi (Ethernet, USB, Wi Fi, GSM, ...) kao i različite tipke i prekidači na samoj digitalnoj komponenti. Svako sučelje dobiva oznaku A1, A2, A3... Oznake poput A1, A2, A3... koristit će se u slijedećim koracima.
- Ako ocijenimo da kroz određeno sučelje nije moguć kibernetički napad, tada oznaku toga sučelja (A1, A2, A3...) nećemo koristiti u sljedećim koracima.

Attack Patways			
Number	Attack Pathways Physical Interface (1)	Attack Pathways Communication Protocol (2)	Attack Pathways Description (3)
A1			
A2			
A3			
A4			
A5			
A6			
A7			
A8			
A9			
A10			

Asset ID (MECL):	Asset Description:

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

- U prvom dijelu navode se sigurnosne mjere koje se konfiguriraju u samoj komponenti.
- U drugom dijelu navode se sigurnosne mjere koje se definiraju na razini tvrtke i ne implementiraju se izravno na samoj komponenti.
- U trećem dijelu navode se sigurnosne mjere koje su zahtijevane na razini tvrtke i implementiraju se izravno na samoj komponenti.

SECURITY CONTROL METHODS		
Engineered Security Control Methods		
Method number	Security Control Methods (7)	Description (8)
M1		
M2		
M3		
M4		
M5		
M6		
M7		
M8		
M9		
M10		
Inherited Site Security Control Methods		
Method number	Security Control Methods (9)	Description (10)
I1		
I2		
I3		
I4		
I5		
I6		
I7		
I8		
I9		
I10		
Directly Implemented Inherited Site Security Control Methods		
Method number	Security Control Methods (11)	Description (12)
D1		
D2		
D3		
D4		
D5		
D6		
D7		
D8		
D9		
D10		

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

- Sljedeća tablica povezuje predložene sigurnosne mjere (desna tablica) s iskorištavanjem ranjivosti. Za svaki red u lijevoj tablici (koji ukazuje na moguće iskorištavanje ranjivosti), potrebno je u desnoj tablici predložiti sigurnosne mjere.
- Predložene sigurnosne mjere dijele se na tri područja: zaštitu digitalne komponente, prepoznavanje iskorištavanja ranjivosti te odgovor i vraćanje komponente u sigurno stanje. Idealno bi bilo predložiti sigurnosne mjere za sva tri područja.
- Koliko je potrebno sigurnosnih mjera? Toliko koliko ocijenimo da je potrebno. Potrebna je objektivnost!
- Koje sigurnosne mjere se predlažu? Tražimo one mjere koje su učinkovite, a istovremeno su najjeftinije u smislu cijene, vremena i ljudskih resursa potrebnih za njihovu implementaciju.

NEK KIBERNETIČKA SIGURNOST EPRI TAM METODA

Roman Kočnar, dipl.ing.el.

CIRED HRVATSKI OGRANAK

HRVATSKA KOMORA INŽENJERA ELEKTROTEHNIKE

Attack Pathways and Associated Exploit Mechanisms						Allocation of Security Control Methods			
Technical Vulnerability Class			Applies? (4)	Applicable Attack Pathway(s) (5)	Mechanism to Exploit Vulnerabiity Class and Notes (6)	Protect (13)	Detect (14)	Respond & Recover (15)	Basis - Description (16)
Vulnerability Classes Associated with Direct Action Against the Component						Direct Action			
Component Enable/Disablement-Immediate			NO						
Component Disablement- Delayed			NO						
Denial of Service (DOS)			NO						
Malware			NO						
Vulnerability Classes Associated with the 6 Critical Data Types						Critical Data Types			
Operational Process Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
OEM Defined Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
User Defined Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
Security Operational Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
OEM Defined Security Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						
		At Rest	NO						
User Defined Security Program/ Configuration Data	Theft	In Transit	NO						
		At Rest	NO						
	Alteration	In Transit	NO						

ZAKLJUČAK

- Metoda ne pokriva sve moguće rizike, kao što su standard ISO 27000 ili Cybersecurity framework NIST.
- EPRI TAM metoda je pragmatična i izvediva.
- U analizi je potreban što objektivniji pogled na ranjivosti naše opreme, kao i na predlagane sigurnosne mjere.
- Najkasnije do kolovoza 2024. izlazi novi zakon ZinfV na osnovu direktive NIS 2. Da li će imati i kakav uticaj na našu implementaciju EPRI TAM metode još ne znamo.