SYNERIQ

Praktická témata z provozu kritické komunikační infrastruktury

Anotace: *Přednáška se zaměřuje na praktické aspekty návrhu, nasazení a provozu kritické komunikační infrastruktury (KKI). Představuje konkrétní scénáře z praxe, včetně reakce na incidenty, obnovy po haváriích a bezpečnostních strategií. Důraz je kladen na realistické požadavky, typová řešení, integraci do širších bezpečnostních rámců a udržitelnost systémů.*

Ing. Petr Kolouch, SYNERIQ, a.s.

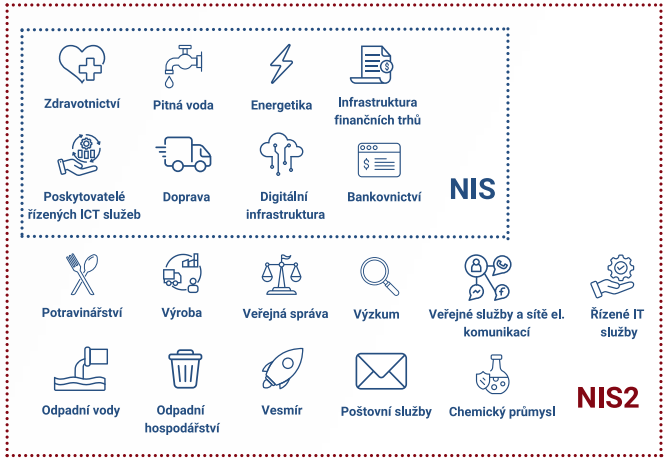
Konference Kybernetická bezpečnost – KB XIII
24. 09. 2025
Policejní akademie ČR v Praze, Praha 4, Aula od 9.00 hod

Belden | HIRSCHMANN A BELDEN BRAND | NET MODULE A BELDEN BRAND

Vstupuje nám v život nový předpis (hurá).

Ale hlavně nová logika…

- Zákon 264/2025, Sb. (vydán 4.8.2025, účinnost od 1.11.2025), národní implementace EU směrnice NIS2 (ekonomická směrnice!).
- 5 vyhlášek:
  - regulované služby,
  - vyšší povinnosti (VV),
  - nižší povinnosti (VN),
  - portál NUKIB,
  - neopominutelné funkce stanoveného rozsahu.
- Logika systému NZKB – služba jako primární aktivum,
  - podpůrná aktiva,
  - technická aktiva v průmyslu (§28 VV).
- A další novinky v logice
  - jedna organizace -> jeden režim,
  - společný systém – musíte se dohodnout, jinak máte problém všichni.
- Poměrně velká synchronizace (konečně) s logickou rodiny norem ISO27000.



Organizační opatření	Režim vyšších povinností	Režim nižších povinností
Systém řízení bezpečnosti informací	✓	
Zajišťování minimální úrovně kybernetické bezpečnosti		✓
Povinnosti vrcholového vedení	✓	✓
Bezpečnostní role	✓	✓
Řízení bezpečnostní politiky a bezpečnostní dokumentace	✓	✓
Řízení aktiv	✓	✓
Řízení rizik	✓	
Řízení dodavatelů	✓	✓
Bezpečnost lidských zdrojů	✓	✓
Řízení změn	✓	
Akvizice, vývoj a údržba	✓	
Řízení změn, akvizice, vývoje a údržby		✓
Řízení přístupu	✓	✓
Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	✓	✓
Řízení kontinuity činností	✓	✓
Audit kybernetické bezpečnosti	✓	

SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Základní parametry a vazby – KKI.

- Co vlastně má infrastruktura zajišťovat – papír a tužka.
  - Realistické požadavky - §14 NZKB, §28 VV, VV, VN.
  - Služby systému infrastruktury.
  - Redundance, konvergenční časy, strategie – §28 VV, VN.
  - Integrace do bezpečnostních požadavků nadřazených celků - §27 NZKB, VV.
  - Je projekt v regulaci KKI nebo v rámci BDŘ? – poskytovatel regulované služby.
- První design – technické aktivum s přihlédnutím k §28 VV.
  - Komunikační prostředky (pasivní části – optika, metalika) - §18 VV + fyzická bezpečnost.
  - Napájení a stabilita okolních systémů.
  - Požadavky na prostředí (rušení, teploty, voda ...) – fyzická bezpečnost, odolnost.

Základní parametry k rozmyšlení - bezpečnost.

- Bezpečnostní návrh systému.
  - Spadám do regulované KKI? – §6 NZKB
  - Mám bezpečnostní strategii? – §7 VV
  - Vnitřní znalosti věci a bezpečnosti? – §11 VV, §6 VN
  - Může moji bezpečnost vlastně řešit někdo mimo? – BDŘ a jeho rizika.

  - Typové řešení - §19 VV, §12 VN.
  - Bezpečnostní proces - §27 VV – zajištění dostupnosti služby.
  - Incident response, disaster recovery – co všechno držím v ruce - §27 VV, §7 VN.
  - Mám „bezpečnostní“ protikus v projektu? - §11 VV, §6 VN – řízení lidských zdrojů.

Volba celkové logiky nasazení a komponent.

- Když už vím, co mám dělat a čemu vyhovět, dokážu začít volit komponenty.
- Nedává smysl na začátku řešit krabičky a netušit, co mám vlastně dělat.
- Čím dál více se ukazuje, že nadhled, znalosti a komunikace mezi stranami jsou důležitější, než cenovka a podobné věci.
- Snaha o standardizaci komponent a typová řešení.
- Bezpečnost, obnovitelnost.
- Incident response v rozumném čase a rozumnými prostředky.
- Disaster recovery v rozumném rozsahu.
- Údržba a provoz systému jako celku.
- Bezpečnostní a životní cyklus systému.
- A na konci tedy volba komponent…

Vyhláška č. 131/2024 Sb. Vyhláška o dokumentaci staveb

- Vyhláška byla vydána na základě Stavebního zákona č. 283/2021 Sb. VPP. Je její princip je aplikovatelný i pro část dokumentace KKI?
- Komunikační infrastruktura je řešena často až ve stupni prováděcí dokumentace (Příloha č. 8 vyhlášky), která je s výkazem výměr častým podkladem pro výběr zhotovitele.
- Je komunikační infrastruktura zpracovávána dle časti D.1.2.6 TPS (technika prostředí staveb) - elektronické komunikace nebo D.2 TZS (technologická zařízení staveb)?
- Projektant – Dodavatel regulované služby? Důvěrnost.

Provozovaní kritické infrastruktury

- Model IT: Infrastruktura je dynamická a průběžně se mění. Správci se věnují výhradně infrastruktuře. Některé její části mají vlastní specializované týmy správců (např. firewally, Wi-Fi, úložiště, virtualizace).

- Model OT: Infrastruktura byla vytvořena s ohledem na technologii, která ji využívá, a změny lze předpokládat až při jejím technickém nebo morálním zastarání (obvykle po 10–15 letech). Údržba a profylaxe se zpravidla provádějí podle plánů odstávek.

Disaster Recovery Plan – plán obnovy po havárii

1. Scénáře obnovy:

- **Technická selhání HW/SW:**
  - Porucha kritického HW řídicího systému (např. PLC, server, dílčí komponenta)
  - Selhání napájení včetně záložních zdrojů (UPS, dieselgenerátory)
  - Ztráta nebo poškození konfiguračních dat / firmware
  - Výpadek síťové infrastruktury systému
  - Chyba obsluhy (neoprávněná nebo nesprávná změna)
- **Kybernetické incidenty:**
  - Infekce malwarem / ransomwarem
  - Útok na síťovou infrastrukturu (např. DoS)
  - Zneužití přístupových oprávnění (interní i externí)
  - Kompromitace zálohovacího / aktualizačního systému
- **Vnější vlivy:**
  - Ztráta konektivity s nadřazenými systémy
  - Nedostupnost dodavatele či klíčových komponent

Pozn.: Každý scénář by měl obsahovat popis, dopad na provoz, kroky obnovy, potřebné zdroje, reálnou dobu obnovy a návrh prevence.

Disaster Recovery Plan – plán obnovy po havárii

2. Časové cíle a reálné doby obnovy

- Stanovení cílových hodnot
  - **RTO (Recovery Time Objective) - „Za jak dlouho musíme být zpět v provozu?“**
  - **RPO (Recovery Point Objective) - „Kolik dat si můžeme dovolit ztratit?“**
- **Reálně dosažitelná doba obnovy** v podmínkách konkrétního scénáře s ohledem na:
  - dostupnost techniky a personálu,
  - logistické faktory a servisní lhůty,
  - případně možnost záložních řešení.

3. Seznam kritických komponent

- Kompletní seznam hardwaru, softwaru, síťových prvků a jejich konfigurací.
- Identifikace komponent se zásadním vlivem na provoz a jejich vzájemné závislosti.

4. Náhradní díly a skladové zásoby

- Doporučení k udržování skladových zásob kritických komponent.
- Minimální množství, odhadovaná dodací lhůta, doporučení k obnově zásob.

5. Role a odpovědnosti

- Rozpis zapojených osob/týmů v jednotlivých fázích obnovy.
- Eskalační schéma, kontaktní osoby a zajištění dostupnosti.

6. Ověřování a testování plánu

- Návrh plánu testování DRP (včetně simulací scénářů).
- Frekvence testů, záznam výsledků, návrh revizního cyklu dokumentu.

2. ZÁMĚR 2

3. VYBAVENÍ SW A HW 2

4. HARDWAROVÉ SELHÁNÍ 3

4.1. VÝMĚNA ZAŘÍZENÍ ZA IDENTICKÝ MODEL 3

4.1.1. Pomocí ACA modulu 3

4.1.2. Pomocí záložní konfigurace 4

4.2. NAHRÁNÍ FIRMWARE 4

4.2.1. pomocí ACA modulu 4

4.2.2. Pomocí WEBového GUI 5

4.3. OBNOVENÍ KONFIGURACE Z EXTERNÍ ZÁLOHY 5

5. SOFTWAROVÉ SELHÁNÍ 6

5.1. RESET DO TOVÁRNÍHO NASTAVENÍ 6

5.1.1. Pomocí WEBového GUI 6

5.1.2. Pomocí Seriové konsole nebo SSH 6

5.1.3. Pomocí SysMon1 a sériové konsole – ztráta admin hesla 6

5.2. NÁVRAT K PŘEDCHOZÍ VERZI FIRMWARE 7

5.2.1. Pomocí WEBového GUI 7

5.2.2. Pomocí SysMon1 a sériové konsole – ztráta GUI a CLI 7

5.3. ZÍSKÁNÍ LOKÁLNÍHO PŘÍSTUPU DO PRVKU 8

5.3.1. VLAN pro přístup k managementu 8

5.3.2. Vypnutý port 9

5.3.3. Vypnutí nastavení bezpečnost na portech 9

5.3.4. Vypnutí bezpečnost na vyvolený rozsah management adres 9

5.3.5. Zapnutí management přístupu SSH, HTTPS, HTTP, Telnet, SNMP 10

6. BEZPEČNOSTNÍ INCIDENT 11

6.1. IZOLACE ZAŘÍZENÍ 11

6.2. REINSTALACE FIRMWARE Z DŮVĚRYHODNÉHO ZDROJE 12

6.3. OBNOVA KONFIGURACE S REVIZÍ BEZPEČNOSTNÍCH NASTAVENÍ 13

SYNERIQ

Ukázka z obnovovací DRP procedury pro zařízení HIRSCHMANN s HiOS

5.3.2 Vypnutý port

Při situaci, kdy jsou všechny porty na prvku zakázány.

Vybereme vhodný port prvku pro připojení pracovní stanice dle kapitory 3.

Připojíme se konzolovým kabelem, přihlásíme se do prvku a postupujeme v konzolové řádce:

CLI [

```
>show port all                    // výpis aktuálního nastavení portů
----- povolení portu
>enable                           // vstup do administrace zařízení
#configure                        // mód pro provádění změn v nastavení
(Config)#interface 1/11           // zvolený byl na modulu 1 port 11
((Interface)1/11)#no shutdown     // zapnutí vybraného portu
((Interface)1/11)#exit
(Config)#exit
#exit
```