AŽD Praha s.r.o.

Cybersecurity versus Safety

Ing. Radek Prokopec

Hlavní inženýr výzkumu a vývoje, AŽD Praha s.r.o.

Obsah přednášky

- Legislativa a normy
- Obecné bezpečnostní definice
- Vztah safety a cybersecurity
- Posouzení kybernetické bezpečnosti
- Bezpečnostní opatření
- Požadavky na provoz a údržbu

Cíl: Smysluplný a efektivní celek tvořený: lidé, procesy, technologie

Legislativa a normy (zkrácené názvy)

- **Bezpečnost (Safety) drážních zařízení**
  - ČSN EN 50126-1 ed. 2 – Generický proces RAMS (etapy životního cyklu)
  - ČSN EN 50128 ed. 2 – Software pro drážní řídicí a ochranné systémy
  - ČSN EN 50129 ed. 2 – Elektronické zabezpečovací systémy (hardware)
- **Kybernetická bezpečnost (Cybersecurity)**
  - NIS Directive (EU) 2016/1148 – Network and Information Security (NIS2 2023)
  - Zákon č. 181/2014 Sb. – O kybernetické bezpečnosti (nový Z. během 2024)
  - Vyhláška č. 82/2018 Sb. – O kybernetické bezpečnosti (nové V. během 2024)
  - ČSN EN ISO/IEC 27001 – Systémy řízení bezpečnosti informací
  - ČSN EN IEC 62443-x – Bezpečnost pro systémy průmyslové automatizace a řízení
  - IEC 63452 – Railway applications – Cybersecurity (návrh)
  - CLC/FprTS 50701 – Railway applications – Cybersecurity (dle 50126-1)

Obecné bezpečnostní definice

- **Bezpečnost (Safety) drážních zařízení**
  - **RAMS** – reliability, availability, maintainability, safety
    – bezporuchovost (spolehlivost), pohotovost, udržovatelnost, bezpečnost
  - **SIL** 1 - 4 – safety integrity level – úroveň integrity bezpečnosti (safety)
  - Eliminace neúmyslných a náhodných hazardů, které by ohrozily uživatele.
- **Kybernetická bezpečnost (Cybersecurity)**
  - **CIA** – confidentiality, integrity, availability
    – důvěrnost, integrita (správnost), dostupnost
  - **SL** 0 - 4 – security level – úroveň bezpečnosti (security)
  - Eliminace škodlivých hrozeb, které by ohrozily zařízení a následně uživatele.
  - Zabývá se ochranou aktiv (primární a podpůrná).

Vztah safety a cybersecurity (TS 50701 příloha D)

- Bezpečnost (safety) usiluje především o ochranu lidí nebo okolního prostředí před poruchami automatizačních systémů, zatímco kybernetická bezpečnost (security) si klade za cíl chránit technické systémy před útoky z okolního prostředí.
- **Zásada 1:** Bezpečnost (safety) a kybernetická bezpečnost (security) jsou odlišné a podle toho by se k nim mělo přistupovat.
- **Zásada 2:** Bezpečnostní (security) prostředí by mělo chránit základní funkce, včetně bezpečnosti (safety).
- **Zásada 3:** Hodnocení rizik a hrozeb kybernetické bezpečnosti (cybersecurity) je hlavním rozhraním k hodnocení bezpečnosti (safety).

Vztah safety a cybersecurity

- **Zásada 4:** Posouzení kybernetické bezpečnosti (security) a bezpečnosti (safety) je nutné oddělit, jak jen to je možné, ale současně je nutné je efektivně koordinovat.
- **Zásada 5:** Kybernetická bezpečnost (security) by měla být hodnocena na základě mezinárodních standardů, např. IEC 62443.
- **Zásada 6:** Nelze provést pravděpodobnostní vyhodnocení rizik kybernetické bezpečnosti.
- **Zásada 7:** Opatření zaměřená na bezpečnost (safety) a kybernetickou bezpečnost (security) by se neměla spojovat.
- **Zásada 8:** Kybernetická bezpečnost (security) vyžaduje neustálé úsilí a spolupráci.

Posouzení kybernetické bezpečnosti

- Bezpečnostní opatření – Organizační opatření
  – Technická opatření
- Klasifikace aktiv (asset)
- Hodnocení rizik (risk assessment)
- Hodnocení hrozeb (threat assessment)
- Skenování zranitelnosti (vulnerability scanning)
- Penetrační testování (penetration testing)
- Stanovení úrovně bezpečnosti (security level) SL
- Důkaz kybernetické bezpečnosti (cybersecurity case)
- Verifikace, Validace, Přijetí a předání systému

Bezpečnostní opatření (Zákon č. 181/2014 Sb. § 5)

Odst. 2) **Organizační opatření**

a) systém řízení bezpečnosti informací (např. dle ISO 27001),

b) řízení rizik (riziko = dopad x hrozba x zranitelnost),

c) bezpečnostní politika,

d) organizační bezpečnost
(výbor pro řízení kybernetické bezpečnosti),

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv (garant aktiva),

g) bezpečnost lidských zdrojů,

Bezpečnostní opatření

h) řízení provozu a komunikací (řízení změn - významná změna),

i) řízení přístupu osob,

j) akvizice, vývoj a údržba,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit.

Vyhláška č. 82/2018 Sb., část druhá, § 3 až § 16

Odst. 3) **Technická opatření**

a) fyzická bezpečnost (perimetr),

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů (požadavky na hesla),

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jejich uživatelů a administrátorů,

Bezpečnostní opatření

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

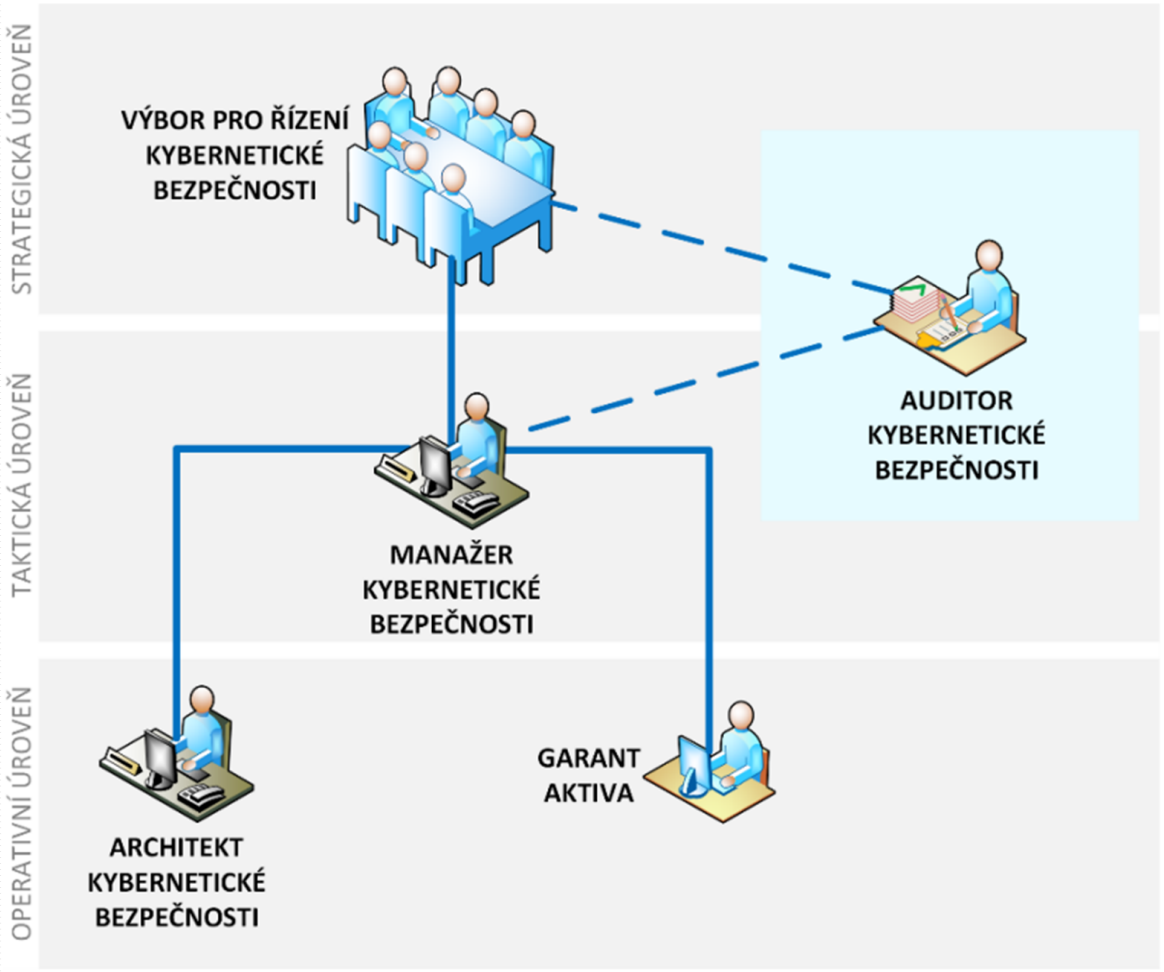
i) aplikační bezpečnost (penetrační testování),

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací a

l) bezpečnost průmyslových a řídicích systémů.

Vyhláška č. 82/2018 Sb., část druhá, § 17 až § 28



Obrázek č. 4 Osoby podílející se na zajišťování kybernetické bezpečnosti Zdroj: govcert.cz

Skenování zranitelnosti

- Skenování zranitelnosti má odhalit obecně známá zranitelná místa.
- Provádí se automatizovaně (SW nástroje).
- Provádí se zpravidla 1x za týden.
- Cíl: Chybějící záplaty a konfigurační nedostatky

Penetrační testování

- Penetrační testeři napodobují reálné útoky s cílem identifikovat možné obcházení bezpečnostních prvků systému.
- Provádí se manuálně a nezávisle na vývojovém týmu.
- Provádí se před uvedením do provozu, při významné změně systému, ke které dochází u PC systému přibližně 1x za rok.
- Metodiky: Open Source Security Testing Methodology Manual (OSSTMM v3)
  Penetration Testing Execution Standard (PTES)
- Klasifikace: Common Vulnerability Scoring System (CVSS)
- Cíl: Využití zranitelnosti pro reálnou kompromitaci systému

Úrovně bezpečnosti SL (security levels, TS 50701)

- **SL 0** - ochrana bezpečnosti není nutná.
- **SL 1** - ochrana proti náhodnému nebo neúmyslnému narušení bezpečnosti.
- **SL 2** - ochrana proti úmyslnému narušení s použitím jednoduchých prostředků s malými zdroji; znalosti útočníka jsou obecné a jeho motivace nízká.
- **SL 3** - ochrana proti úmyslnému narušení s použitím sofistikovaných prostředků s průměrnými zdroji; znalosti útočníka jsou specifické pro systém průmyslové automatizace a jeho motivace střední.
- **SL 4** - ochrana proti úmyslnému narušení s použitím sofistikovaných prostředků s rozšířenými zdroji; znalosti útočníka jsou specifické pro systém průmyslové automatizace a jeho motivace vysoká.

Důkaz kybernetické bezpečnosti (TS 50701 př. G)

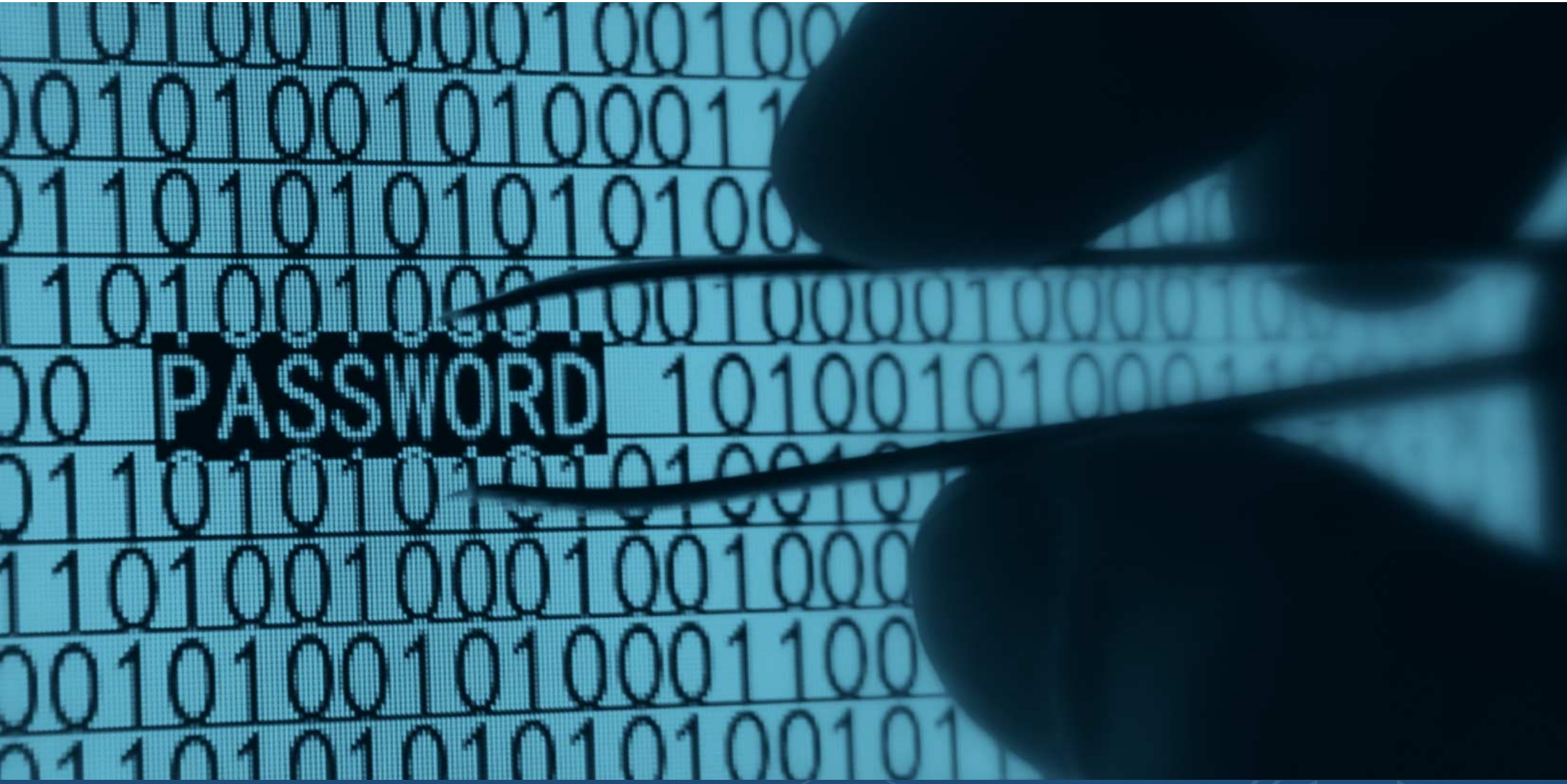
- **Úvod:** definice systému, hodnocení rizik a hrozeb
- **Specifikace požadavků na kybernetickou bezpečnost:** úroveň SL
- **Management kybernetické bezpečnosti:** politika KB, plán KB, proces KB; posouzení a management zranitelnosti
- **Splnění kybernetické bezpečnosti:**
  - Provedená opatření pro kybernetickou bezpečnost
  - Doklad o uplatnění procesu kybernetické bezpečnosti
  - Výsledky verifikace (ověření) a validace (potvrzení platnosti)
    - Bezpečnostní posouzení (např. Zpráva z penetračního testování)
    - Sledování požadavků na kybernetickou bezpečnost
- **Podmínky použití související s bezpečností:** instalace, provoz, údržba
- **Závěr:** prohlášení o kybernetické bezpečnosti, stav zbytkových rizik

Přijetí a předání systému (TS 50701)

- Nezávislé posouzení důkazu kybernetické bezpečnosti zpracovaného dodavatelem od provozovatele a správce systému - aktiva, jehož výsledkem je zpráva o přijetí (acceptance report), která učiní závěr o způsobilosti systému k provozu.
- Předání systému je založeno na platném důkazu kybernetické bezpečnosti vytvořeném a zdokumentovaném v předchozích fázích návrhu a v etapách životního cyklu železniční aplikace.
- V oblasti bezpečnosti (safety) je vhodné vyvarovat se častých změn kvůli nákladům na prokazování bezpečnosti. V kybernetické bezpečnosti (security) by aktualizace měla být snadná, aby bylo možné systém včas záplatovat. Změna v kybernetické bezpečnosti (security) by neměla ovlivňovat bezpečnost (safety).

Požadavky na provoz a údržbu

- Zajistit, aby kybernetická bezpečnost byla dodržována po celou dobu provozu, údržby a také při likvidaci systému.
- Doba, kdy „fyzický perimetr“ znamenal skutečné oddělení interního prostředí od okolního světa, je nenávratně pryč.
- Pamatujte, že technologie samy o sobě bezpečnost nezajistí.
- **Management zranitelnosti** - aktivně odhalovat, klasifikovat a napravovat zranitelná místa.
- **Management bezpečnostních záplat** (security patch)
- **Servisní smlouva** mezi dodavatelem, provozovatelem a správcem


PASSWORD

Děkuji za pozornost

Ing. Radek Prokopec

prokopec.radek@azd.cz

Žirovnická 3146/2, Záběhlice, 106 00 Praha 10