SCADA SECURITY 2026

Policejní akademie ČR v Praze, 25. března 2026

závěrečná zpráva

Konference **SCADA Security 2026** se zaměřila na progresivní transformaci průmyslové bezpečnosti v éře konvergence IT a OT systémů a na nové hrozby, kterým čelí kritická infrastruktura. Hlavními tématy byly **automatizovaná obrana**, **legislativní změny v ČR** a role **umělé inteligence** v kybernetických konfliktech. Konference se rovněž věnovala problematice **krizového řízení a krizové připravenosti**.

Stručné shrnutí klíčových bodů konference:

1. Aktuální stav hrozeb a geopolitický kontext

- **Rychlost útoků:** V roce 2026 se „luxus času" na obranu vytrácí; AI akcelerace umožňuje útočníkům přejít od průniku k exfiltraci dat během pouhých **72 minut**, což je rychleji, než dokáže reagovat lidský analytik.
- **Průmyslová špionáž a sabotáže:** V roce 2025 byl zaznamenán **50% nárůst ransomwarových incidentů** v OT sektoru. Mezi významné případy patřilo ovládnutí norských přehrad proruskými hackery či útok na Jaguar Land Rover, který způsobil škody v řádu miliard liber.
- **Fragmentace ekosystému:** Kyberbezpečnost se stává geopolitickým nástrojem, což dokládá například zákaz západního bezpečnostního softwaru v Číně. Organizovaná kyberkriminalita se stala třetí největší ekonomikou světa po USA a Číně.

2. Strategická a legislativní opatření v ČR

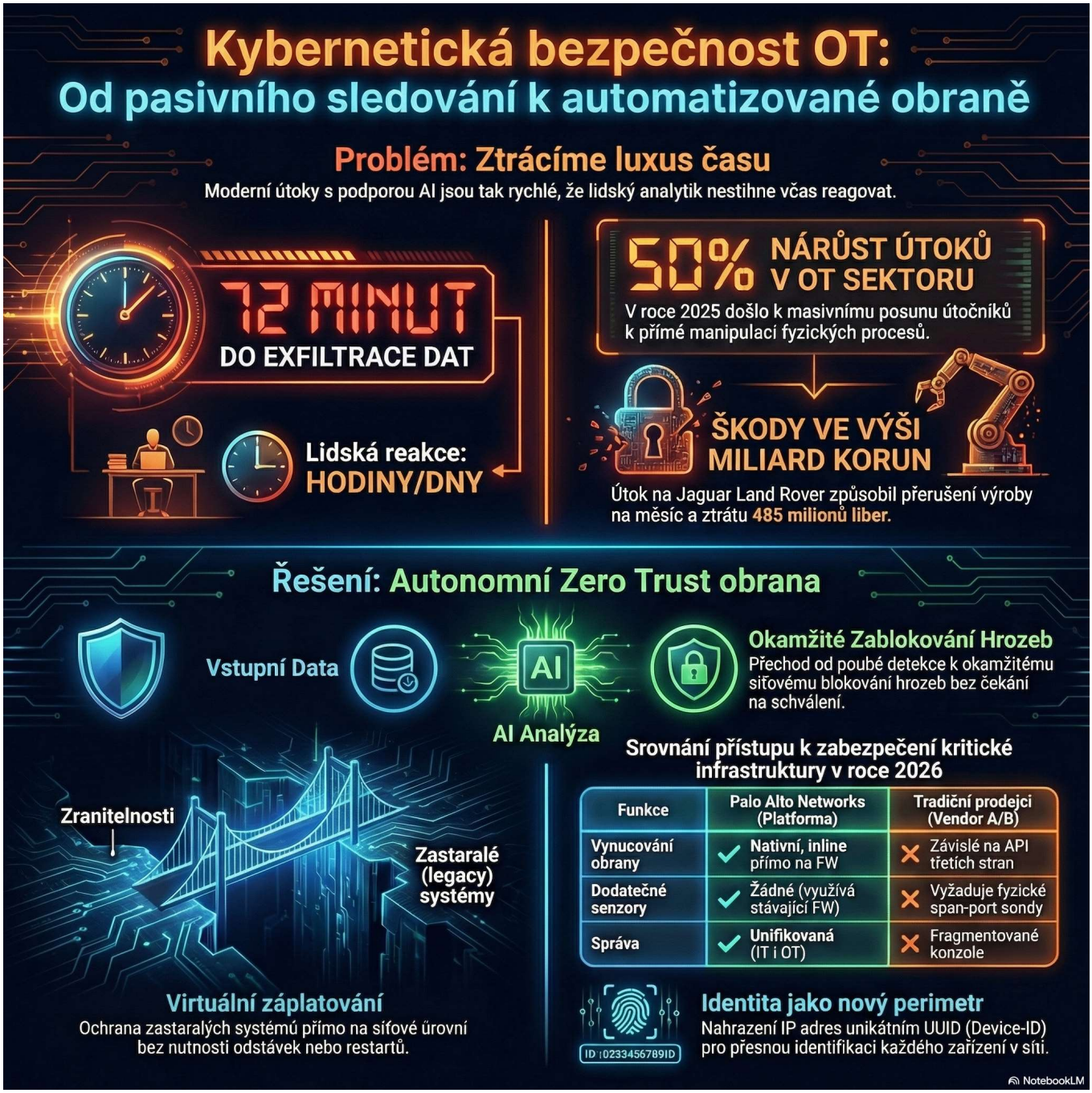
- **Nový zákon o odolnosti:** Ministerstvo průmyslu a obchodu (MPO) představilo **zákon č. 266/2025 Sb.**, o odolnosti subjektů kritické infrastruktury.
- **Nové metodiky:** Připravují se prováděcí předpisy pro hlášení incidentů a zabezpečení technických aktiv, včetně využití matice **MITRE ATT&CK pro ICS** k modelování hrozeb.
- **Odpovědnost managementu:** Stále více manažerů a CISO přebírá přímou odpovědnost za kybernetickou bezpečnost OT, která je nyní vnímána jako prioritní.

3. Technologické trendy v obraně

- **Zero Trust pro IoT/ICS:** Prosazuje se architektura nulové důvěry, kde identita zařízení (např. Advanced Device-ID) slouží jako nový perimetr.
- **Virtuální záplatování (Virtual Patching):** Tato metoda umožňuje chránit zastaralé (legacy) systémy přímo na síťové úrovni bez nutnosti jejich odstávek nebo restartů.
- **Platformní přístup:** Experti doporučují sjednocení bezpečnosti IT a OT pod jednu platformu, což eliminuje „analytický šum" a umožňuje nativní blokování hrozeb v reálném čase.
- **Monitorování fyzické vrstvy:** Až **59 % problémů v síti** souvisí s fyzickou infrastrukturou. Řešení jako „inteliPhy" umožňují on-line monitoring 100 % datové linky a vytváření **digitálních dvojčat** datových center pro efektivní správu.

4. Role AI a lidský faktor

- **AI jako multiplikátor:** Zatímco útočníci využívají AI k automatizaci skenování a hledání zranitelností, obránci ji nasazují k eliminaci šumu a identifikaci reálných hrozeb (např. model Claude Opus 4.6 pomohl najít stovky závažných chyb v open-source knihovnách).
- **Trvalá zranitelnost:** Přes technologický pokrok začíná až **68 % incidentů lidskou chybou**, přičemž phishing a sociální inženýrství zůstávají kriticky úspěšnými metodami průniku.



5. Krizové řízení a krizová připravenost

K této problematice se věnovalo několik prezentací, zejména prezentace Martina Koňaříka, MV ČR a zejména diskusní panel moderovaný Jaroslavem Pejčochem.

- **Zákon o odolnosti:** Klíčovým pilířem připravenosti je nový **zákon č. 266/2025 Sb.**, o odolnosti subjektů kritické infrastruktury. Tento zákon zavádí komplexní rámec pro zajištění kontinuity služeb nezbytných pro chod státu.
- **Plány odolnosti a hodnocení rizik:** V rámci prováděcích předpisů se připravuje vyhláška MV, která definuje povinnost zpracovávat **plány odolnosti** a provádět pravidelná **posouzení rizik**. Tato opatření mají zajistit stabilitu subjektů kritické infrastruktury před krizovými stavy.
- **Portál kritické infrastruktury:** Připravenost je podpořena vznikem vyhlášky o **Portálu kritické infrastruktury**, který bude sloužit jako centrální nástroj pro hlášení incidentů a koordinaci při krizových situacích.
- **Metodika pro technická aktiva:** Ministerstvo průmyslu a obchodu (MPO) ve spolupráci s NÚKIB připravuje návodnou metodiku pro implementaci zabezpečení průmyslových a řídicích systémů (dle § 27 nového zákona).
- **Modelování hrozeb pomocí MITRE:** Strategická příprava zahrnuje rozšíření analýz o matici **MITRE ATT&CK pro ICS**, což umožňuje vypracování cílených modelů hrozeb specifických pro operační technologie (OT) v ČR.
- **Odpovědnost managementu:** Program zdůrazňuje, že odpovědnost za kybernetickou bezpečnost a krizovou připravenost OT systémů se přesouvá přímo na **vrcholové manažery (CIO/CISO)**.
- **Role AI v krizích:** Program reflektuje realitu, kde AI zrychluje kybernetické útoky i obranu, což vyžaduje **automatizovanou reakci v reálném čase**, protože tradiční reakční doba lidského analytika je v krizových scénářích roku 2026 nedostatečná.