Ministerstvo
průmyslu a obchodu

Strategické pohledy na KB v kontextu ochrany kritické infrastruktury

Připravenost ČR na nové bezpečnostní a regulatorní výzvy

Tomáš Poledno

Proč MPO

- Podpora podnikání
- Energetické agendy
- Regulace v oblastech výroby a obchodu vojenských materiálů a zboží dvojího použití
- Zvýšení odolnosti subjektů kritické infrastruktury

Co děláme mimo KB úřadu

- Účast v pracovních skupinách zaměřených na ochranu energetické infrastruktury
- Spolupráce na tvorbě legislativy

Kybernetické útoky na průmyslové subjekty

- Během roku 2025 byl zaznamenán téměř padesátiprocentní nárůst ransomwarových incidentů v OT sektoru
- Posun v taktice útočníků směrem k přímé manipulaci fyzických procesů a mapování kontrolních mechanismů
- Tři klíčové hrozby:
  - AZURITE cílí na inženýrské stanice
  - PYROXENE využívá dodavatelské řetězce
  - SYLVANITE zneužívá zranitelnosti hraničních prvků

Kybernetické útoky na průmyslové subjekty

- **Přehrada v Norsku** - duben 2025
- Vzdálené ovládnutí řídících systémů přehrady
- Doba trvání: Po 4 hodiny byly plně otevřeny výpustě přehrady, což vedlo k významnému ovlivnění průtoku vody
- Kdo: Ze sabotáže je důvodně podezřelá proruská hackerská skupina
- Cíl: Vyvolat strach a paniku

Kybernetické útoky na průmyslové subjekty

- **Rumunský národní operátor ropovodů Conpet** - 5. 2. 2026
- Prolomení podnikové IT infrastrukturu a oficiální webové stránky společnosti
- Odcizení téměř 1 TB citlivých dokumentů včetně finančních údajů a citlivých osobních údajů včetně skenů pasů
- Incident zasáhl administrativní systémy, provozní technologie SCADA a samotný transport ropy a derivátů nebyly narušeny
- Kdo: K útoku se přihlásila ransomwarová skupina Qilin
- Cíl: Extrakce citlivých dokumentů

Kybernetické útoky na průmyslové subjekty

- **Jaguar Land Rover** (JLR) - 31. 8. 2025
- Útok způsobil masivní narušení výroby a logistiky v Británii, v Číně, Indii, Brazílii a také na Slovensku
- Doba trvání: Výroba byla přerušena na více než měsíc, přičemž úplné obnovení bylo hlášeno až v říjnu 2025
- Způsob: Prostřednictvím ukradených přihlašovacích údajů k systému Jira
- Kdo: Ransomware útok přisuzovaný hackerským skupinám HELLCAT, nebo Scattered Lapsus$ Hunter
- Ztráty: JLR vykázala za toto období těžkou ztrátu 485 milionů liber, přičemž náklady spojené s kybernetickým útokem dosáhly 196 milionů liber
- Celkové dopady: V rámci dodavatelského řetězce se dopady útoku přenesly na cca 5000 organizací v UK. Celkový dopad na britskou ekonomiku 1,9 miliardy liber (53 miliard Kč)

Zákon o kritické infrastruktuře

- Zákon č. 266/2025 Sb. o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů
- Prováděcí právní předpisy:
  - Nařízení vlády o základních službách a kritériích významnosti (ve stadiu vypořádání/předložení LRV/vládě)
  - Vyhláška MV o plánu odolnosti, posouzení rizik, opatřeních k zajištění odolnosti subjektů kritické infrastruktury a o hlášení incidentu (ve stadiu vypořádání)
  - Vyhláška MV o Portálu kritické infrastruktury (ve stadiu tvorby)
- Nahlášení subjektů

Co připravujeme

MPO ve spolupráci s NÚKIB a dalšími subjekty plánuje

Metodika

Vytvoření návodné metodiky pro implementaci § 27 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

MITRE pro OT

Rozšíření CTI analýza za využití matice MITRE ATT&CK® pro ICS a vypracování cíleného modelu hrozeb pro OT

Zvyšování povědomí

Organizování konference k tématice bezpečnosti kritické infrastruktury a OT systémů obecně, moderace odborných diskuzí reagující na aktuální vývoj v oblasti bezpečnosti

Ministerstvo
průmyslu a obchodu

Děkuji
za pozornost

Tomáš Poledno

tomas.poledno@mpo.gov.cz