

Kybernetická bezpečnost SŽ



Petr Soukup

náměstek pro kybernetickou bezpečnost

Kybernetická bezpečnost na SŽ v roce 2026

navýšení počtu zaměstnanců

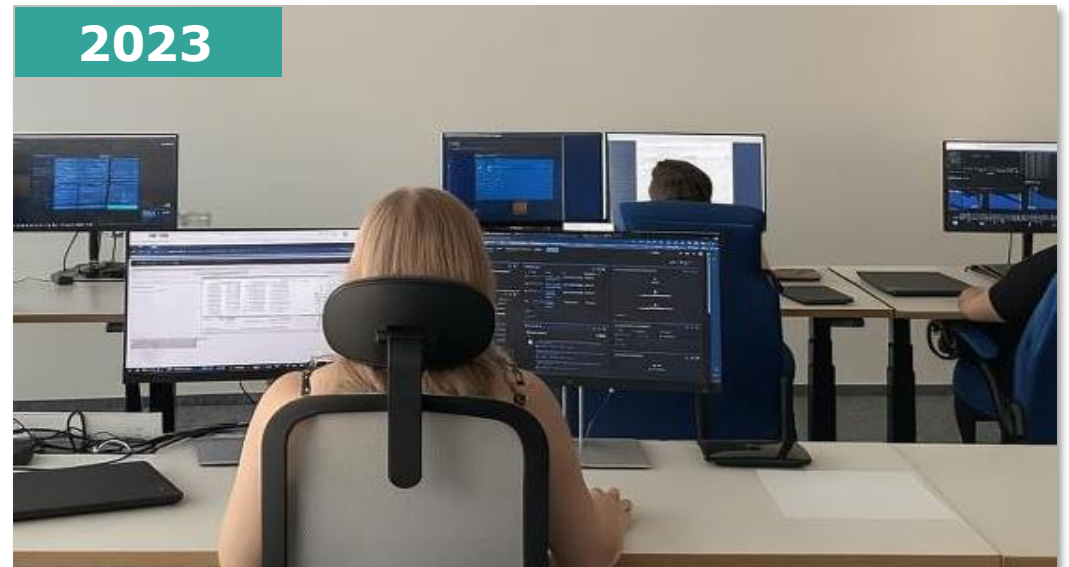
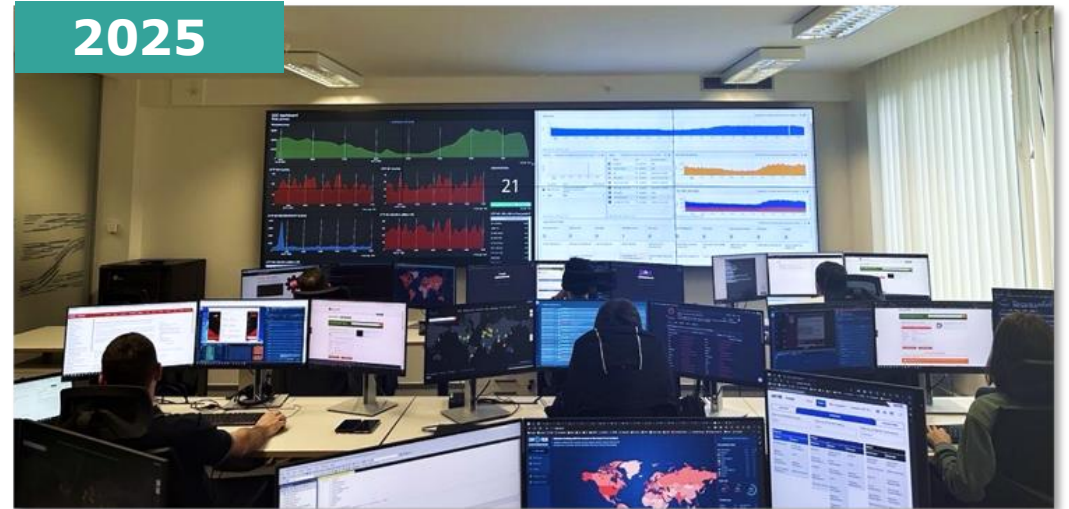
- nárůst na **cca 25**

specializace

- specializace s **možností zastupování**
- **SOC** (OT, malware, penetrační testování)
- **metodický odbor** (vzdělávání, hodnocení rizik)
- **odbor architektury** (MS, non MS, OT)

vnímání ve společnosti

- již nám neříkají:
„Co jste to vymysleli za nesmysl!“
- lepší zpětná vazba



Hlavní činnosti: Zákon o kybernetické bezpečnosti 264/2025 Sb.



- ✓ **účinnost zákona od 1. 11. 2025**
 - *13.1 Provozování železniční dopravní cesty*
 - *13.2 Provoz celostátní dráhy*
- ✓ **stanovení rozsahu řízení** kybernetické bezpečnosti
- ✓ definování **požadavků na dodavatele** na základě hodnocení rizik – ZoP, Norma IEC 62443
- ✓ zavedení **bezpečnostních opatření** podle příslušné vyhlášky



Zákon o kybernetické bezpečnosti 264/2025 Sb.

Co je pro nás důležité?



- ✓ **poskytovatelé regulované služby**
- ✓ **změna způsobu identifikace povinných osob – § 12 Stanovení rozsahu**
 - 2014 – kritické systémy
 - 2025 – poskytované služby
- ✓ **hlášení KBI**
 - do 24 hodin prvotní hlášení
 - úřad sdělí významnost incidentu
 - do 72 hodin aktualizace hlášení včetně dopadů
 - do 30 dnů závěrečná zpráva

- ✓ **odpovědnost managementu**
 - vrcholové vedení nese přímou odpovědnost za kybernetickou bezpečnost
- ✓ **bezpečnost dodavatelského řetězce**
Strategicky významná služba
 - s vynaložením přiměřeného úsilí zjišťujeme a evidujeme informace o dodavatelích
 - hlásíme NÚKIB – pokračuje v prověřování
 - NÚKIB může vydat opatření obecné povahy -> zákaz využití plnění dodavatele
- ✓ **pokuty**
 - 250 milionů Kč za neplnění povinností
 - 250 mil neprovede registraci
 - 100 mil nenahlásí kontaktní údaje

Vize kybernetické bezpečnosti



OT systémy jako hlavní prvek businessu



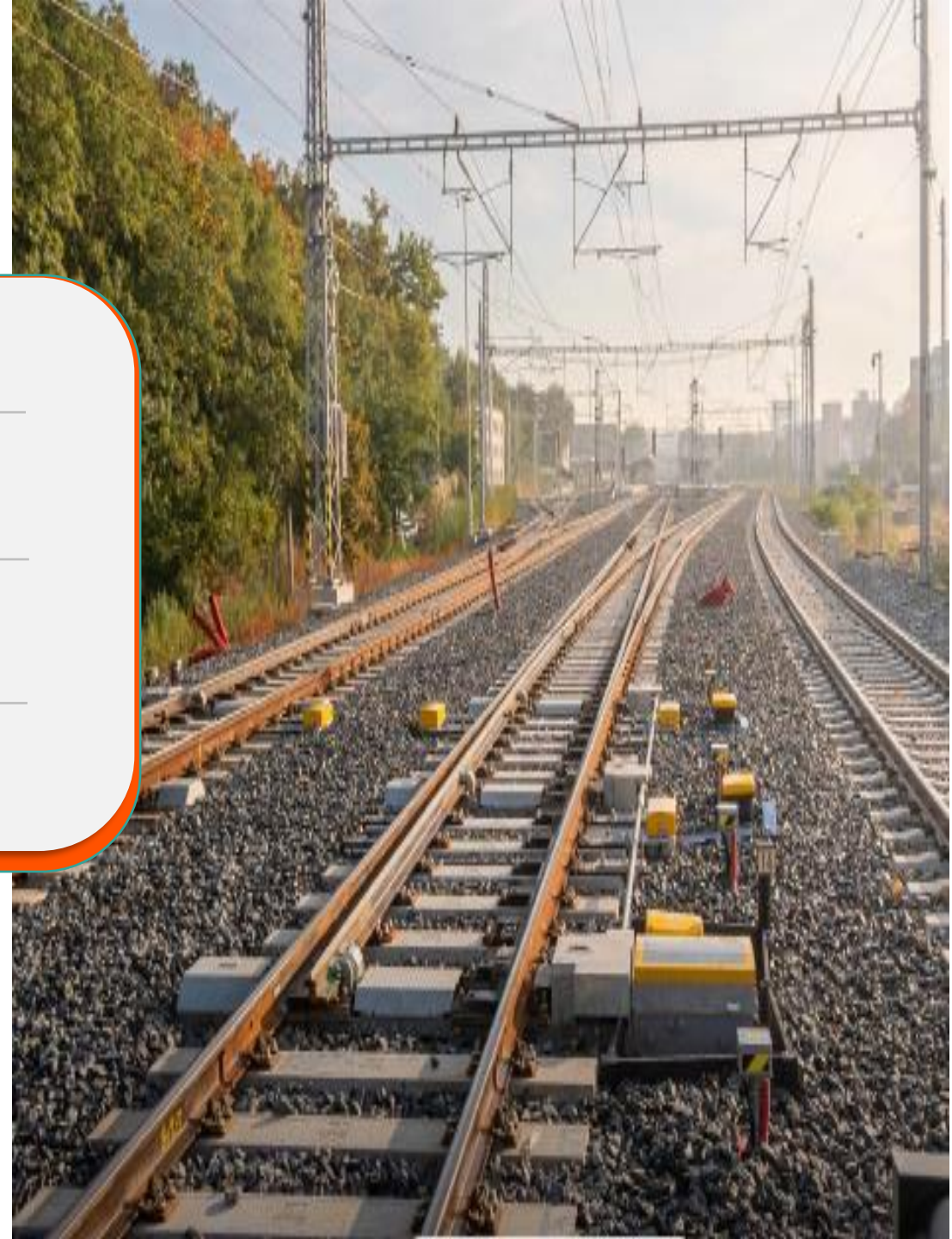
zvýšit povědomí uživatelů o kybernetické bezpečnosti s přesahem do osobního života



kybernetická bezpečnost jako **součást firemní kultury**

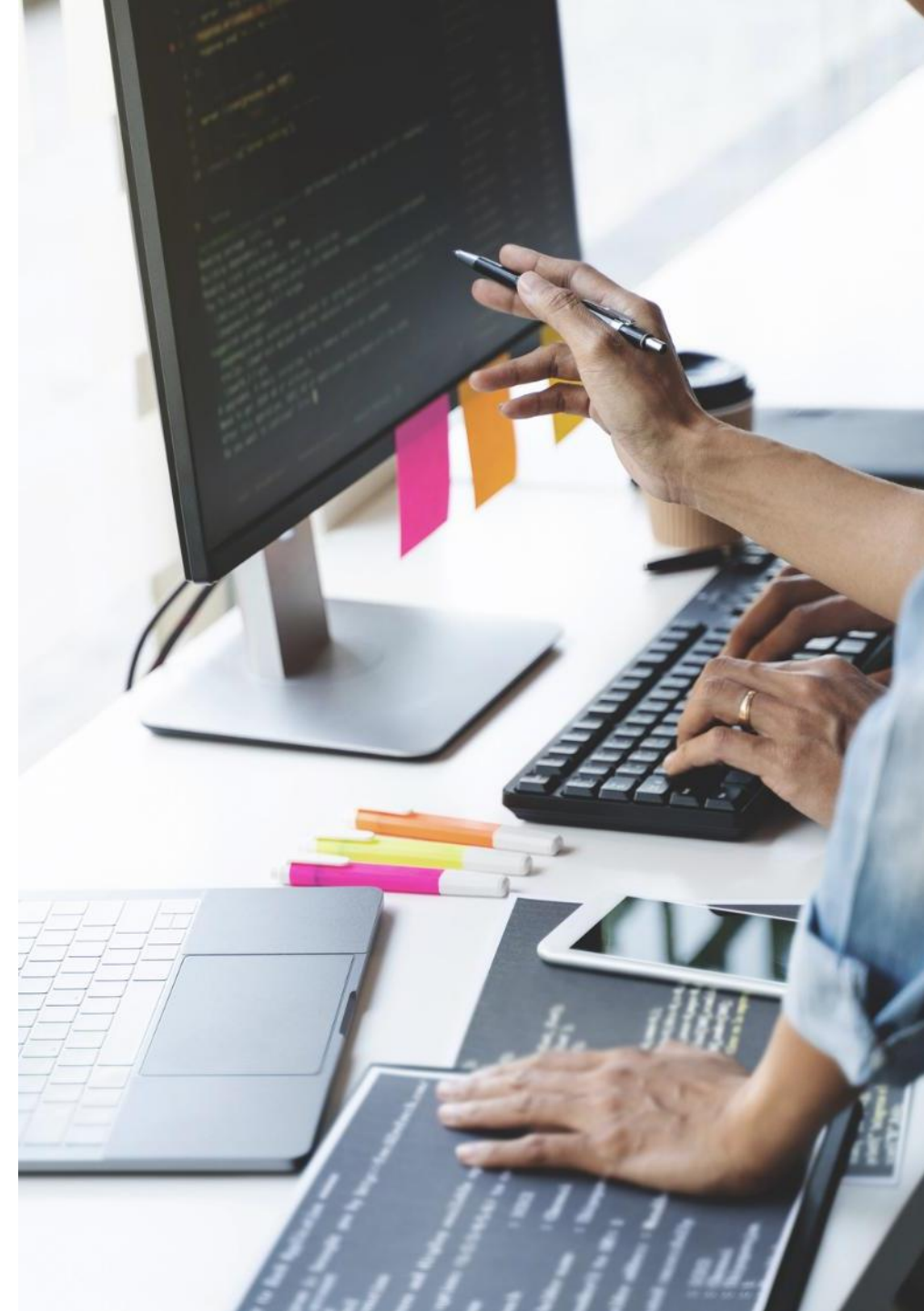


nastavit užší spolupráci v rámci zajištění fyzické bezpečnosti



OT a IT - rozdíly

IT	OT
ochrana dat, zachování důvěrnosti, integrity a dostupnosti (CIA)	ochrana fyzických procesů, bezpečnost lidí, stabilita provozu, dostupnost
dostupnost důležitá, ale často více tolerovatelné výpadky	velmi vysoká dostupnost, nízká latence, bezpečnost nesmí výrazně narušit provoz
relativně kratší – časté upgrady, patchování	často mnoho let (10+), obtížnější změny
standardní IT infrastruktura, kanceláře, datacentra	procesní prostředí – průmyslové sítě, řídicí systémy, SCADA/DCS, fyzická zařízení





Specifická rizika pro OT



- ✓ existence systémů, které **nebyly navrženy** s ohledem **na zajištění kybernetické bezpečnosti**
- ✓ propojení OT a IT sítí (digitalizace, IIoT) zvyšuje možnosti útoků
- ✓ nároky na dostupnost, bezpečnost a funkčnost **v reálném čase**
- ✓ **kybernetický útok může přímo ovlivnit provoz SŽ** s ohrožením bezpečnosti osob
- ✓ **složitost schválení změn** – v OT prostředí jsou změny často pomalejší, musí být rozsáhle testovány

Způsob zajištění OT

- ✓ **fyzická bezpečnost** (kontrola vstupu, ochrana zařízení)
- ✓ důraz na **vícevrstvé zabezpečení OT systémů**, tj. žádné jediné opatření není kritické pro udržení bezpečnosti a provozní stability
- ✓ jasné **oddělení mezi IT a OT sítěmi**, např. využití jednosměrných datových diod, oddělení účtů pro údržbu a administraci
- ✓ **ochrana koncových zařízení** (zákaz portů, služeb, revize oprávnění, MFA)
- ✓ v OT prostředí musí být zabezpečení vyváženo s potřebami provozu – **nasazení bezpečnostních opatření by nemělo ohrozit funkčnost nebo bezpečnost procesu**

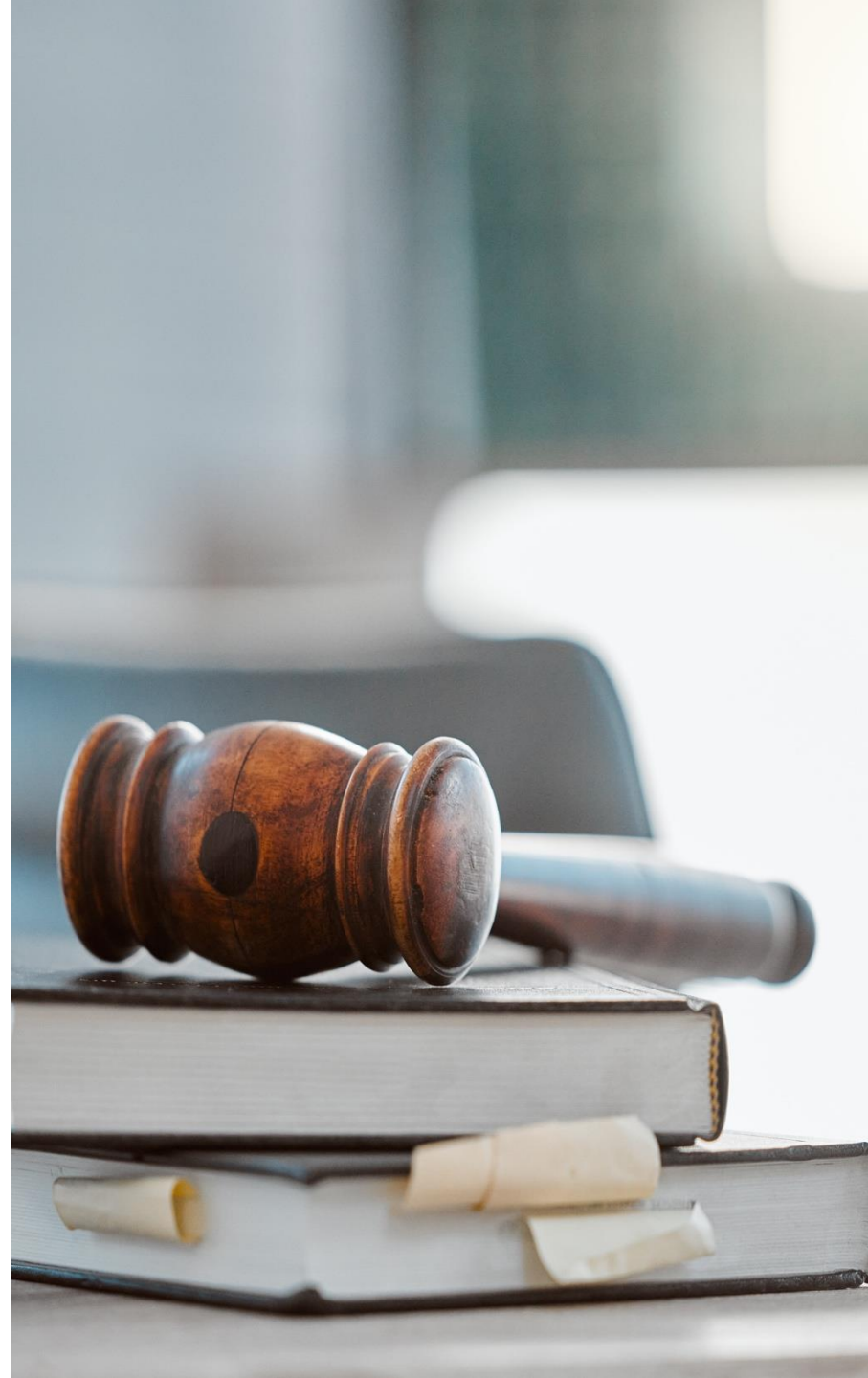


Zvláštní obchodní podmínky



Podstata změn

- **zavedení kategorií dodavatelů** (běžný, významný a SVS)
- **integrace logů do SIEM** (VD)
- **povinné použití MFA a PAM** pro administrátorské přístupy (VD)
- **skenování zranitelností a penetrační testy**
- **pravidelné reporty o incidentech**
- **hlášení kybernetických incidentů** do 3 hodin



Řada norem IEC 62443 pro kybernetickou bezpečnost průmyslových řídicích systémů



- ✓ **specificky zaměřená na OT prostředí**
- ✓ komplexní rámec pro zabezpečení průmyslových systémů během celého jejich životního cyklu (návrh, implementace, provoz a rizika)
- ✓ **rozdělení systému do bezpečnostních zón** – komunikace mezi nimi je řízená
- ✓ definuje úroveň ochrany proti různým typům útočníků (SL 1 až 4)
- ✓ **ochrana ve více vrstvách**
 - fyzická bezpečnost (kontrola vstupu, kamerové systémy)
 - síťová bezpečnost (FW, segmentace, oddělení IT a OT)
 - bezpečnost endpointů (patch mngmt, hardening)
 - aplikační bezpečnost (řízení přístupů)
 - monitorování a detekce

Děkuji za pozornost

SoukupP@spravazeleznic.cz

