

Kybernetické hrozby pro liniové dopravní stavby

01

Proč je to téma
důležité právě pro vás

Tohle není teoretická hrozba

EU · 2024–2025

#2

nejčastěji cílený sektor

Doprava je druhý nejcílenější sektor v EU po veřejné správě.

ENISA Threat Landscape 2025

ČESKO · 2024

268

kybernetických incidentů

Rekordní počet nahlášený NÚKIB.
43 % DDoS, 27 % ransomware.

Zpráva o stavu KB ČR 2024

GRU · ATRIBUCE 2025

10 000+

kamer pod dohledem GRU

Jednotka 26165 monitorovala uzly
dopravní infrastruktury napříč NATO.

Společné upozornění NÚKIB, BIS, VZ, FBI, NSA · 05/2025

Nejsou to jen čísla, mluví o tom naše úřady



CO ŘÍKAJÍ AUTORITY

Lukáš Kintr, ředitel NÚKIB

„Nejvýrazněji se projeví kyberútoky skupin pod ruskými zpravodajskými službami.“

Úvodní slovo, Zpráva o stavu KB ČR 2024

Michal Koudelka, ředitel BIS

„Narůstající snahy aktérů především z Ruska a Číny napadat kritickou infrastrukturu.“

Veřejná výroční zpráva BIS 2024

Martin Kupka, ministr dopravy

„Ruské skupiny opakovaně zaútočily na České dráhy.“

Seznam Zprávy · 12/2024

CO SE S TÍM DĚLÁ

3 formální atribuce státních aktérů

Poprvé v historii ČR.

APT28 (05/2024) · GRU 26165 (05/2025) · APT31 (05/2025)

Nový ZoKB 264/2025 účinný od 11/2025

Z ~400 na 6 000–9 000 regulovaných subjektů.

Sankce až 250 mil. Kč. Hlášení incidentů do 24 h.

SOC centra v klíčových subjektech dopravy

Správa železnic

Letiště Praha

02

Kdo útočí, jak útočí, a
kde to bolí

Čtyři typy útočníků a jejich motivace

KYBERZLOČINEC

Ransomware, vydírání

Motivace: peníze

Cíl: zašifrovat účetnictví, data, zakázky. Dopad: výkupné + výpadek + reputace.

HACKTIVISTA

DDoS, defacement, leak

Motivace: ideologie, pozornost

Cíl: viditelná disrupce. Dopad: ztrapnění, mediální skandál.

STÁTNÍ AKTÉR

Dlouhodobá persistence v OT

Motivace: geopolitika, sabotáž

Cíl: řízení infrastruktury. Dopad: provozní selhání v krizi.

INSIDER / DODAVATEL

Legitimní přístup zneužitý

Motivace: pomsta, výhoda, omyl

Cíl: cokoliv, kam má přístup. Dopad: únik IntProp, sabotáž projektu.

IT vs. OT: proč to není totéž

IT ÚTOK

CO SE STANE

Zašifrují data
Zablokují přístup k systémům
Ukradnou citlivé informace

ŠKODA

Peníze. Reputace. Čas.
Obnovitelné ze záloh.

Chráníte: **DŮVĚRNOST DAT**

OT ÚTOK

CO SE STANE

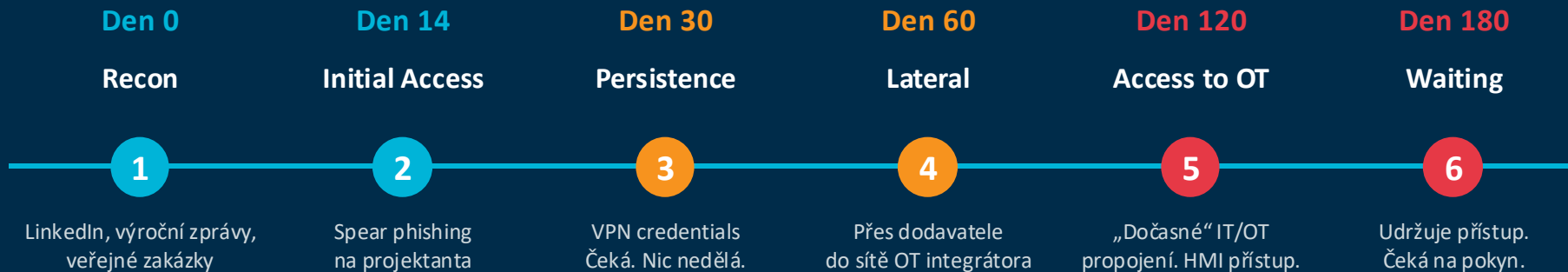
Vypnou osvětlení v tunelu
Zablokují SOS volání, hlášení
Přepnou ventilaci, manipulují signalizaci

ŠKODA

Lidé. Zranění. Životy.
Neobnovitelné.

Chráníte: **ABY NĚKDO NEZEMŘEL**

Kill chain: jak útok reálně probíhá



Útočník nespěchá. Vy ano.

Carmel Tunnel, Izrael 2013

2013

před 13 lety

2

DNY UZAVŘENÍ

Silniční tunel Carmel v Haifě.
Kybernetický útok na řídicí systém.

3

NEJVĚTŠÍ MĚSTO IZRAELE

Masivní dopravní kolaps.
Provozovatel mluvil o „komunikačním výpadku“.

0

NATION-STATE SOFISTIKACE

Haktivistická úroveň typu Anonymous.
Amatéři. Přesto dva dny paralýzy.

Představte si, co dnes zvládnou profesionálové s AI nástroji.

Posledních 24 měsíců

BŘEZEN 2026

LA Metro

Ababil of Minab (Írán)

Publikované screenshoty z real-time rail yard management systému.

Reálné pozice vlaků, obsazení kolejí, out-of-service stavy.

Útočníci tvrdí: smazáno 500 TB dat.

2022–2025

EU železnice

Pro-ruské skupiny

Dokumentované útoky:
Lotyšsko · Litva · Rumunsko · Estonsko

Cíle: signalizace, prodej jízdenek, informační systémy.

Zdroj: ENISA, CrowdStrike.

2024–2025

OT hacktivisté

Z-Pentest, Sector 16, NoName057, CARR

+51%

nárůst hacktivistických incidentů 2024→2025.

1,06 milionu globálně v roce 2025 (Cyble).

Polsko: železnice v první linii hybridní války

SRPEN 2023

RADIO-STOP ÚTOK

\$30

za rádiové vybavení

Zneužití nešifrovaného analogového signálu na 150 MHz.

18 zastavených vlaků. Koridor Białystok.

LISTOPAD 2025

VÝBUŠNINA C-4 NA
KOLEJÍCH

C-4

Warszawa—Lublin—Rzeszów

Linka pro vojenskou pomoc Ukrajině.

Tusk: „státní terorismus“.

CO SE DĚJE ZA SCÉNOU

ATRIBUCE

Ruské zpravodajské služby GRU a FSB.
Rekrutace přes Telegram, platba v kryptu.

ROZSAH

775 neautorizovaných zásahů (2024).
55 osob zadržených od ledna 2024.

OPERACE HORYZONT

10 000

vojáků nasazených
na ochranu kritické
infrastruktury.

Tunel, který dnes navrhujete,
bude v provozu i v roce 2076.



Kolik geopolitických krizí do té doby proběhne?

03

APEL

Proč je potřeba na bezpečnost myslet už dnes



Byli jste na seznamu dřív, než padl zákon

2013



Carmel Tunnel
První veřejný útok
na dopravní tunel

12 LET

zpoždění legislativy za realitou

2024



NIS2 vstupuje
v platnost v ČR

CO POTŘEBUJE ÚTOČNÍK

Jedno neaktualizované HMI. Jednu zapomenutou VPN. Jeden kompromitovaný účet dodavatele.

Riziko patří do zadání, ne do auditu

TOHLE UŽ DĚLÁTE

- **Geotechnické riziko**
Řešíte v projekční fázi.
Ne až při kolaudaci.
- **Požární bezpečnost**
Je součástí zadání.
Ne dodatku po průšvihů.
- **Statika konstrukce**
Návrhový parametr.
Ne compliance kontrola.

Víte, že některá rizika musí být vyřešena už v návrhu.

TOHLE ZATÍM NE

- **Threat model**
Patří do studie proveditelnosti.
Ne do auditní zprávy.
- **Segmentace IT/OT**
Součást architektury.
Ne dodatku po incidentu.
- **Bezpečnostní požadavky**
V zadávací dokumentaci.
Ne po kolaudaci.

**Kyber je další kategorie rizik.
Stejná logika. Stejný okamžik.**

Stavíte infrastruktury,
na kterou se těší útočník,
kterého ještě neznáte.

Co si o tom myslí projekt, který právě zadáváte?