Problematika stárnutí z perspektivy kybernetické bezpečnosti

Hrozby a dopady

Ing. Jana Rozehnalová, M.Sc.

Další tvář stárnutí zařízení

- Stárnutí = nejen materiál, ale i **HW a SW prvky řídicích systémů**.
- Přechod k **digitalizaci výroby** (Industry 4.0 / Industry 5.0) → nové zdroje rizik.
- Kybernetické slabiny – nový zdroj hrozeb a vznik rizik havárie

Příklady havárií způsobené kybernetickým útokem

Stuxnet (2010) – sabotáž íránských centrifug. Cílem byly PLC systémy v íránských jaderných zařízeních, narušil řídicí procesy centrifug pro obohacování uranu a způsobil jejich fyzické poškození. Tento incident je považován za první známý kybernetický útok s destruktivním reálným dopadem.

Německá ocelárna (2014) – destrukce vysoké pece z důvodů zamezení řádného vypnutí.

Kyjev (2016) – výpadek proudu – cílený útok na přenosovou síť.

Malware TRITON (2017) – narušení ochranných systémů

Skupina XENOTIME - cílení na bezpečnostní systémy

Nedávné případy kybernetických incidentů

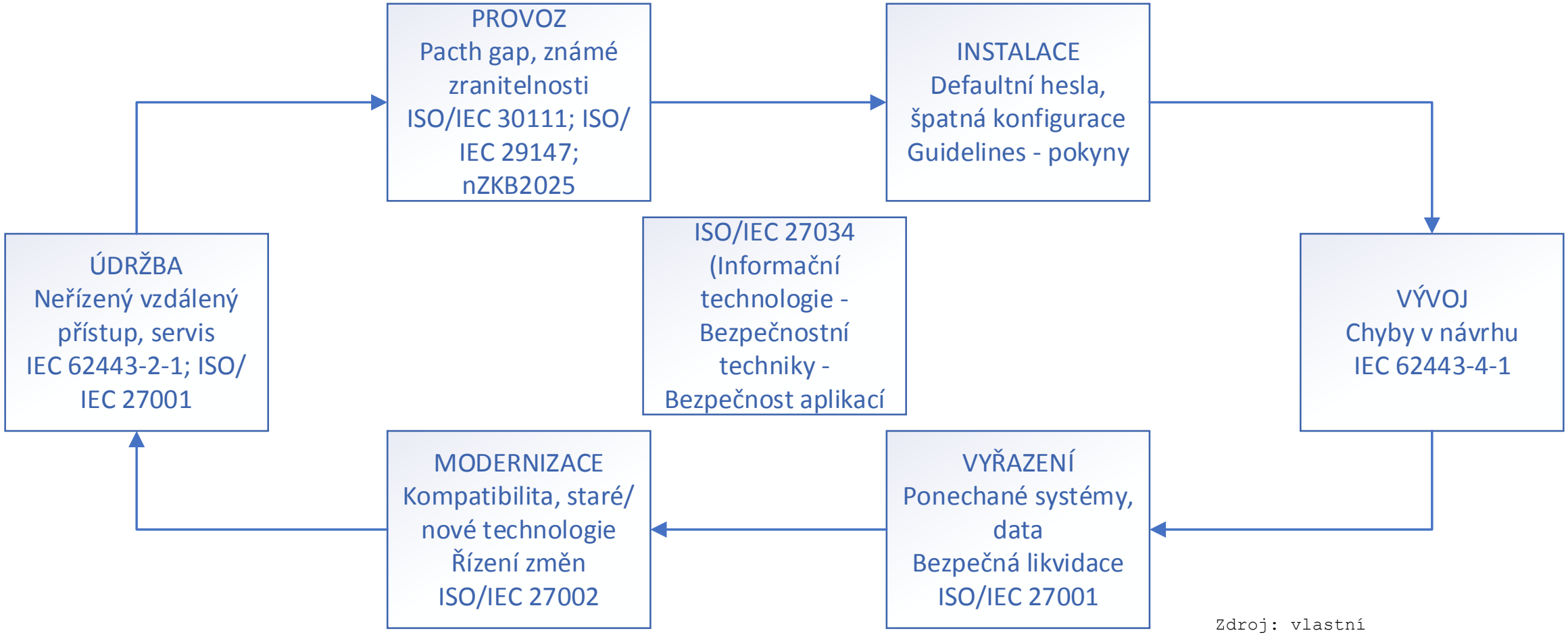
Případ	**Současnost**	**Typ dopadu**
Sabotáž přehrady v Norsku (Bremanger)	Duben 2025	Fyzický útok na řízení vodní infrastruktury
FrostyGoop – přerušení tepla (Lvov)	Zima 2024	Vypnutí vytápění jako fyzický dopad
Odborná zpráva: stovky útoků s fyzickým dopadem	2023	Výrazné ohrožení bezpečnosti a životního prostředí
Jaguar Land Rover – zastavení výroby	2025	Provozní dopady, narušení výroby
Rockwell Automation – zranitelnosti OT	2025	Hrozba pro provozní technologie a kontrolu strojů

Životní cyklus zařízení a kybernetic ká rizika

Rizika v každé fázi životního cyklu

Největší slabiny: patch gap, zastaralý HW, nekompatibilita

Modernizace = i SW a řídicí jednotky



Zdroj: vlastní zpracování

LCA cyklus a kybernetické hrozby

Stárnutí HW

Slabší výkon → nemožnost moderního zabezpečení

Zastaralé porty a protokoly (RS-232)

Vyšší poruchovost = nižší dostupnost

Stárnutí SW

Staré OS bez podpory (XP, staré Linuxy)

Známe zranitelnosti = snadno zneužitelné

Legacy protokoly (SMBv1, Telnet, RDP bez šifrování)

CIA triáda

DŮVĚRNOST:
SLABÉ/ŽÁDNÉ ŠIFROVÁNÍ

INTEGRITA: NEMOŽNOST
OVĚŘIT SPRÁVNOST DAT

DOSTUPNOST: ČASTÉ
VÝPADKY A PORUCHY

Vulnerability a Patch management

Patch gap = doba mezi zranitelností a opravou

V praxi u starých systémů ∞

Kompenzace: segmentace, whitelisting, monitoring

Problém dlouhodobých aktualizací OS

Výrobní stroje mají životnost klidně **20–30 let**, zatímco:

- **OS od velkých výrobců** (Microsoft, Apple, Linux distribuce) má podporu typicky cca 5–10 let (Windows 10: do 2025, Ubuntu LTS: 5 let).

- **Proprietární OS výrobce stroje** může být podporován ještě kratší dobu – nebo se přestane vyvíjet hned po ukončení modelu.

Vzniká **časové okno (patch gap)**, kdy stroj je stále provozován, ale už nemá k dispozici bezpečnostní opravy.

Preventivní opatření

- Inventarizace HW/SW
- Plán životního cyklu
- Segmentace sítí
- Řízení vzdálených přístupů (VPN + MFA)
- Monitoring a detekce anomálií
- Školení personálu

Shrnutí

Stárnutí = technické + procesní + kybernetické riziko

Industry 5.0 vyžaduje bezpečnou spolupráci člověk–stroj

Prevence havárií musí zahrnovat i kybernetickou dimenzi

Děkuji za pozornost

V Brně dne 11.9.2025