IT bezpečnost ve výrobě

PŘEDSTAVENÍ

Erik Zapletal

IT Business analytik IT bezpečnosti
ve Škoda Auto a.s.
ShopFloor IT
erik.zapletal@skoda-auto.cz

AGENDA

Výrobní sítě a zařízení v nich
- Výrobní sítě dříve
- Výrobní sítě dnes
- Je útok na výrobní sítě fikce?
- Reálné incidenty ve výrobě
- Snižování rizik

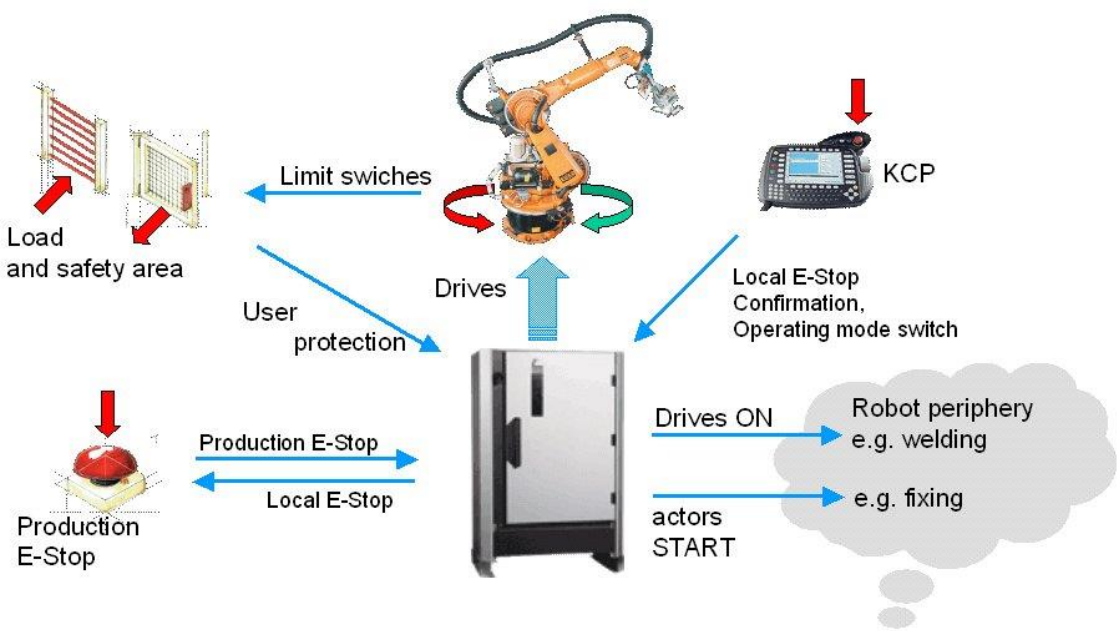
Aplikace pro výrobu
- Bezpečnost při vývoji aplikací
- Zajištění dostupnosti

Výrobní sítě a zařízení v nich

4/2023 | IT bezpečnost ve výrobě | Škoda Auto a.s. | Erik Zapletal

VÝROBNÍ SÍTĚ DŘÍVE

- Malé a nezávislé celky technologií
- Z pohledu sítí fyzicky oddělené od dalších celků
- Předávání informací např. přes štítky

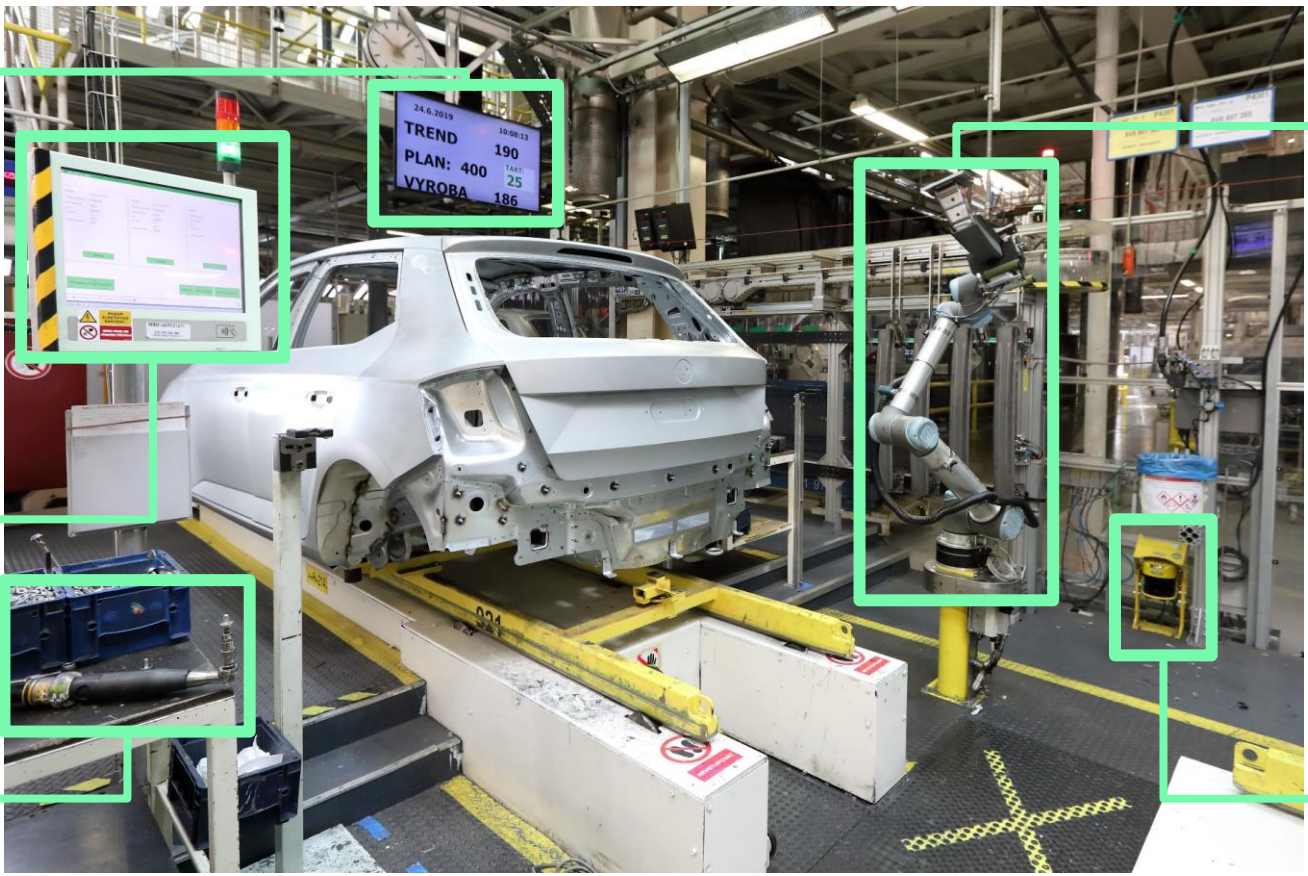


VÝROBNÍ SÍTĚ DNES

Pracoviště na svařovně

VÝROBNÍ SÍTĚ DNES

Pracoviště na svařovně



VÝROBNÍ SÍTĚ DNES

A další …

JSOU ÚTOKY NA VÝROBNÍ SÍTĚ FIKCE?

- S aktuálními trendy jako je Průmysl 4.0, Umělá inteligence, Rozšířená realita a Machine Learning roste počet zařízení a hlavně i jejich pestrost
- Roste potřeba sdílení dat mezi stroji a zároveň data posílat do IT systémů pro vyhodnocení (optimalizace, prediktivní údržba…)
- Frekvence aktualizací u výrobních zařízení je prováděna v delších intervalech
- Zařízení jsou často používána déle, než byla jejich plánovaná životnost (20 let)
- Zhoršující se politická situace.
- Škoda Auto se podílí na HDP ČR ve výši 5%.
- Často je možné se ve výrobě setkat s reakcemi typu:
  - Nám se to nemůže stát.
  - Pravděpodobnost je menší, než zásah meteoritem.
  - Proč by na nás chtěl někdo útočit?
  - OT svět není tak zlý jako IT svět.

REÁLNÉ INCIDENTY VE VÝROBĚ

ASCO Industries (Belgie)

- Jeden z největších výrobců leteckých komponent s napojením na armádní sektor

- Červen 2019, ransomware napadl zařízení ve výrobní síti

- 3 týdny bez plného výrobního programu
- 1 000 zaměstnanců na nuceném volnu
- Odškodnění pro Spirit Aerosystems ve výši 150 000 000 $

REÁLNÉ INCIDENTY VE VÝROBĚ

Oldsmar Water Plant (USA)

- Úpravna vody, zásobující pitnou vodou 15.000 obyvatel floridského městečka Oldsmar.

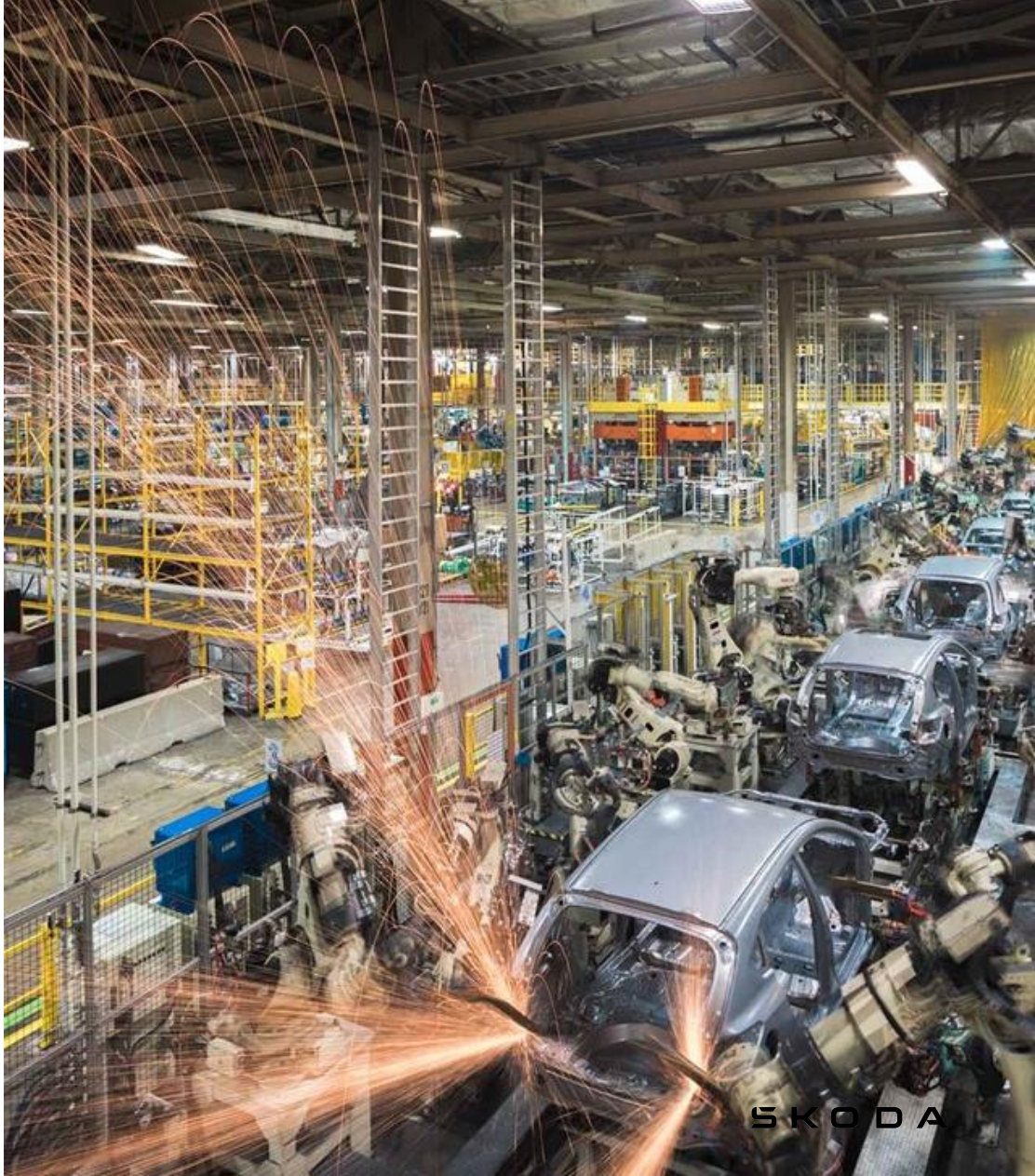
- únor 2021, došlo k neautorizovanému přihlášení do systému pro řízení úpravy vody a ke stonásobnému zvýšení dávky Hydroxidu Draselného (žíravina).

- Počítač byl provozován na již nepodporovaném systému Windows 7, byl vystaven přímo do Internetu a měl sdílené heslo.

REÁLNÉ INCIDENTY VE VÝROBĚ

Subaru (USA)

- Automobilka s roční produkcí cca 1 000 000 aut
- červenec 2018, chyba programátora způsobila vadné sváry na B sloupku
- Necelé tři stovky aut muselo být sešrotováno



REÁLNÉ INCIDENTY VE VÝROBĚ

OKD (CZ)

- Česká těžební společnost s ročním obratem 24 mld. Kč a 10000 zaměstnanci
- V rámci dodavatelského řetězce důležitý partner pro další společnosti

- prosinec 2019 – došlo k napadení ransomwarem

- Těžba musela být zastavena na 4 dny a během Vánoc vytvořena nová oddělená síť.

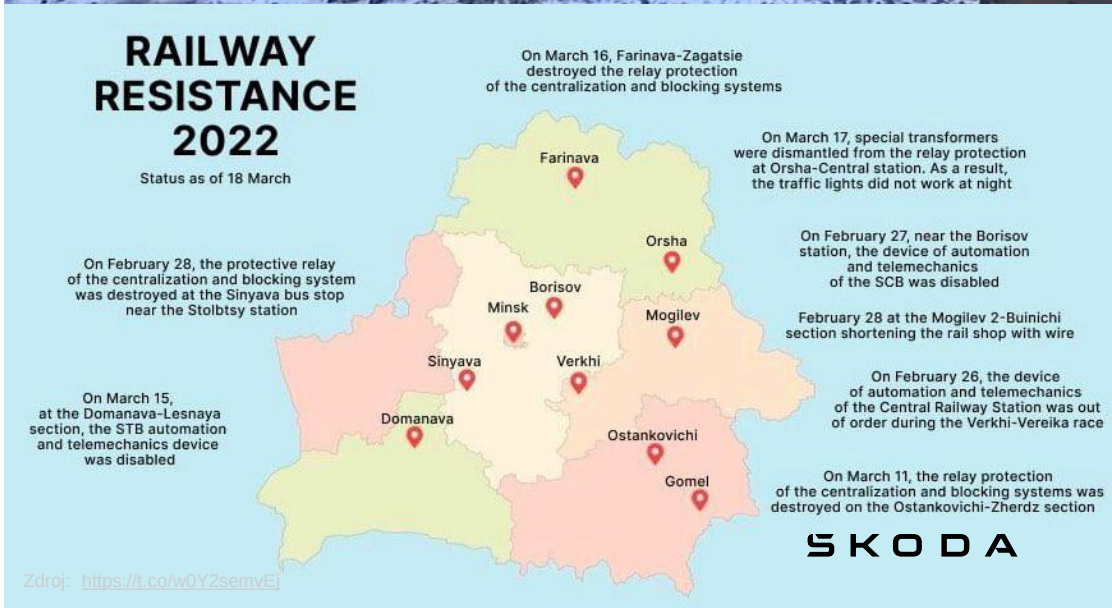
Zdroj: INFORMAČNÍ MĚSÍČNÍK SPOLEČNOSTI OKD, a.s.

REÁLNÉ INCIDENTY

Belarusian Railway (BY)

- Národní správce železničních drah
- Má ve správě kompletní běloruské železniční trasy, v součtu 5 512 km

- Q1 2022 - Sabotážní akce částečně zaměřené také na drážní automatizaci zpomalují přesuny vojenské techniky na území Ukrajiny



Zdroj: https://t.co/w0Y2semvEj

SNIŽOVÁNÍ RIZIK

1. Segmentace sítí
2. Nastavení pravidel
3. Audit a monitoring
4. Evidence a kontakty

SNIŽOVÁNÍ RIZIK

Segmentace sítí

SNIŽOVÁNÍ RIZIK

Segmentace sítí

- Rozdělit síť na menší celky, např.:
  - Dle typu zařízení
  - Dle provozu
  - Dle účelu

- VLANy napojené na Firewall

- Network Access Control pro autorizaci zařízení

- Přístup do Internetu s využitím proxy serveru

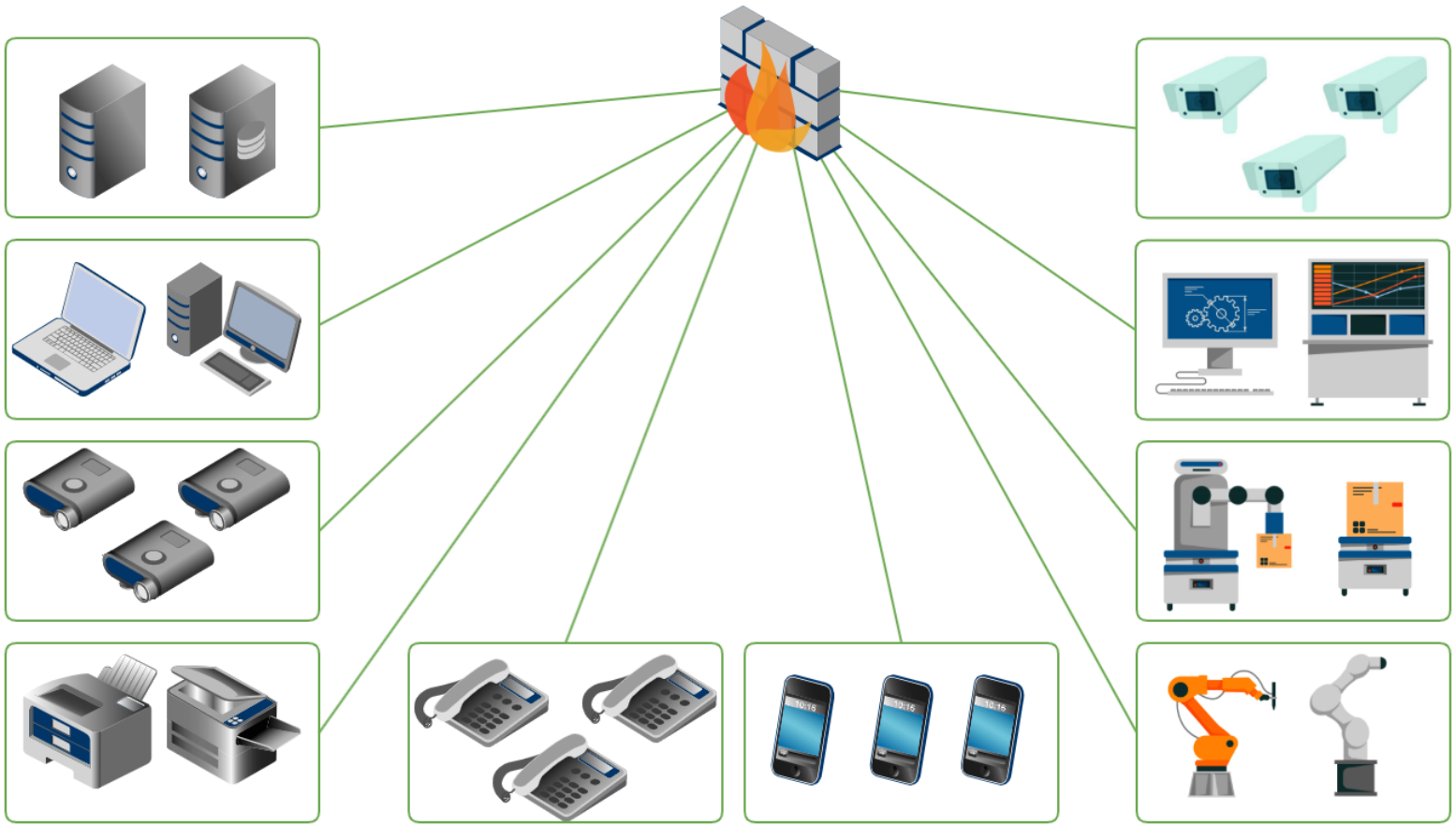
- Vzdálená správa přes terminálové servery

- Přístupy na interní weby přes reverzní proxy

- Evidujte a pravidelně prověřujte povolené porty

SNIŽOVÁNÍ RIZIK

Segmentace sítí



SNIŽOVÁNÍ RIZIK

Nastavení pravidel

Stanovení pravidel pro pořízení nového HW nebo SW:

- Dokumentace dodávek
- Povinnost řešení dodávek s IT Partnerem
- Technické požadavky na provoz v síti(NAC, DHCP…)
- Požadavky na bezpečnostní konfiguraci
- Základní architektonické standardy (PSB, 3 vrstvá architektura…)
- Zajištění servisu, dostupnosti a SLA

Tam, kde to lze prosazovat již existující HW s interní správou.

SNIŽOVÁNÍ RIZIK

Audit a monitoring

1. Pravidelné audity na základě ISO 27001
2. Monitoring komunikací a událostí (SIEM, IDS/IPS)
3. Security Operation Center - vyhodnocuje a prověřuje podezřelé komunikace na síti
4. Skenování zranitelností
5. SCADA / ProfiNet Security sondy

SNIŽOVÁNÍ RIZIK

Evidence a kontakty

1. Určení hlavních partnerů odpovědných za IT v každém provozu
   - Zná svůj provoz
   - Dokáže pomoci s identifikací pro nás neznámých zařízení
   - Schvaluje registrace zařízení do jemu konkrétně zpřístupněných sítí
   - Kontaktní osoba pro SOC v případě nutnosti prověření bezpečnostní události
   - Řídí implementace nových bezpečnostních opatření

2. Vedení evidence
   - Zařízení, sítě, aplikace, FW pravidla…
   - Umožňuje nám samotnou orientaci v síti
   - Rychlejší reakce na případné bezpečnostní události

Aplikace pro výrobu

4/2023 | IT bezpečnost ve výrobě | Škoda Auto a.s. | Erik Zapletal

ŠKODA

APLIKACE PRO VÝROBU

Bezpečnost při vývoji aplikací

- Konsolidace aplikací (prověření požadavku, udržitelnost)

- Systémová specifikace
  - Klasifikace důvěrnosti, integrity, nepopiratelnosti a dostupnosti
  - Konkrétní opatření dle klasifikací výše
  - Architektura

- Code review

- Analýza pro stanovení kritičnosti

- Penetrační testování

APLIKACE PRO VÝROBU

Zajištění dostupnosti

- Vlastnictví zdrojového kódu
- Ustanovení servisní smlouvy s dodavatelem (SLA)
- Monitoring
- Eskalační příručky
- Náhradní postupy v případě výpadku aplikace

Dotazy?