VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Kyberbezpečnost OT sítí – Segmentace OT sítí a nasazení průmyslových IPS a Firewall

Miroslav Knapovský
KNA0047

Referát do Kybernetická bezpečnost
C/01, 9:00

Obsah

1 Úvod

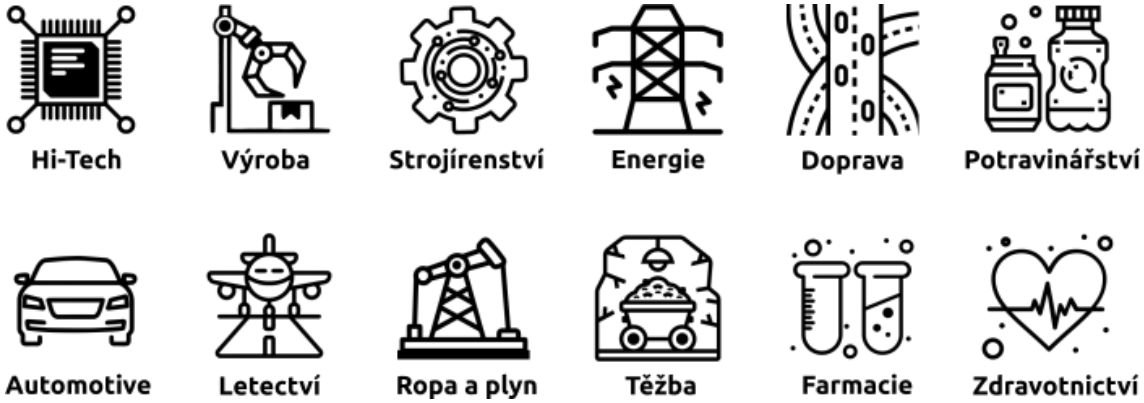
Průmyslová automatizace a integrace operačních technologií (OT) s informačními technologiemi (IT) je tu s námi už dlouho, ale v posledních letech získává na významu. Důvodem jsou „nedávné“ útoky na kritickou infrastrukturu, na které navázala regulace ze strany Evropské unie, což činí ochranu proti kybernetickým útokům vcelku aktuální téma.

Segmentace OT sítí představuje zásadní opatření k oddělení různých částí sítě. Tím se minimalizuje možnost šíření hrozeb a zároveň zlepšuje správa a ochrana těchto systémů. Segmentace na IT a OT sítě se ideálně provádí pomocí datové diody. Firewally se využívají pro segmentaci OT sítí na středně velké celky, zatímco na nejnižší úrovni se uplatňují IPS (Intrusion Prevention Systems), které se instalují přímo před kritická zařízení nebo na klíčové body v síti. Tyto systémy nejen detekují a blokují známé hrozby, ale také umožňují reagovat na neobvyklé chování v síti.

Cílem tohoto referátu je seznámit spolužáky se specifiky kyberbezpečnosti operačních technologií, přiblížit základní vrstvy segmentace OT sítí, popsat průmyslové IPS, Firewally a rozdíly mezi nimi.

1.1 Co to jsou OT (Operational Technology) sítě?

OT sítě představují technologie používané k řízení a monitorování fyzických procesů, zařízení a infrastruktury. Na rozdíl od IT (Information Technology) sítí, které se zaměřují na zpracování dat a komunikaci, se OT sítě zaměřují na řízení a kontrolu reálných procesů v průmyslu, energetice, dopravě nebo zdravotnictví. [1]



Obrázek 1.1 Ilustrace nejčastějších prostředích využívajících OT sítě [2]

1.1.1 Charakteristika OT sítí

Účel:

- Monitorování, řízení a automatizace fyzických procesů, jako jsou výroba, distribuce energie, řízení dopravy nebo provoz průmyslových zařízení.
- OT systémy často interagují s fyzickým světem (např. spuštění ventilátorů, uzavírání ventilů, ovládání robotů).

Provozní prostředí:

- OT sítě zahrnují kritické infrastruktury, které vyžadují nepřetržitý provoz a nejsou tolerantní k výpadkům.
- Pro firmy je **dostupnost a spolehlivost** na prvním místě.
- Vytížení sítě je často dobře předvídatelné.

1.1.2 Systémy řízení a monitorování [1] [3]

SCADA (Supervisory Control and Data Acquisition):

- Systém pro vzdálené řízení procesů, který propojuje více lokací, sbírá data ze senzorů a umožňuje řízení a sledování v reálném čase.

DCS (Distributed Control Systems):

- Používá se v průmyslu k řízení komplexních procesů (např. chemická výroba, rafinerie).
- Na rozdíl od SCADA je zaměřen na řízení procesů v rámci jednoho závodu nebo zařízení.

HMI (Human Machine Interface):

- Rozhraní, které umožňuje operátorům komunikovat s OT systémy.
- Ovládací panely PLC a různých dalších přístrojů (na OS Linux, Windows nebo proprietálních systémech) mohou být nebezpečné, protože často nedostávají bezpečnostní aktualizace.

1.1.3 Řídicí jednotky [3]

PLC (Programmable Logic Controllers):

- Programovatelné zařízení pro automatizaci a řízení strojů nebo procesů.

RTU (Remote Terminal Units):

- Zařízení pro sběr dat a vzdálené ovládání fyzických zařízení, jako jsou ventily nebo čerpadla.

1.1.4 Senzory a akční členy

Senzory:

- Zařízení, která měří fyzikální vlastnosti (teplotu, tlak, hladinu kapaliny) a odesílají data do řídicích systémů.

Akční členy (Actuators):

- Zařízení, která převádějí elektronické signály na fyzickou akci (otevření ventilu, spuštění motoru).

1.1.5 Komunikační protokoly v průmyslu [4]

Klíčové vlastnosti průmyslových protokolů:

- **Deterministická komunikace:** Protokoly zajišťují přesné časování a pořadí zpráv, což je klíčové pro řízení strojů a procesů. Lze garantovat právo přístupu k médiu
- **Nízká latence:** Jsou optimalizovány pro rychlou odezvu.
- **Odolnost proti rušení:** Navrženy tak, aby fungovaly spolehlivě i v prostředí s elektromagnetickým rušením.
- **Kompatibilita:** Podporují integraci zařízení od různých výrobců.

Základní průmyslové protokoly:

- **Modbus:**
  - Jednoduchý a široce používaný protokol pro komunikaci mezi zařízeními, jako jsou PLC.
  - **Modbus RTU**: Sériová komunikace (RS-232,RS-485) a **Modbus TCP**: Ethernetová verze.
  - Protokol sám o sobě nevyžaduje žádné šifrování nebo autentizace.
- **S7Comm a S7Comm+:** Protokol vyvinutý firmou Siemens. **S7Comm+** je modernější a šifrovaný.
- **CIP (Common Industrial Protocol):** Všeobecný protokol pro výměnu dat mezi průmyslovými zařízeními. Ze kterého vycházejí zabezpečenější protokoly jako EtherNet/IP a ControlNet.
- **OPC UA (Open Platform Communications Unified Architecture):** Univerzální protokol pro propojení průmyslových zařízení a IT systémů.

2 Motivace zaměření se na kyberbezpečnost OT

Motivace vychází z kombinace: **Reálné riziko** + **umělý postih regulátorem**.

Relativně nedávno si legislativa i pojišťovny začaly všímat zvýšeného ohrožení OT systémů, což je důsledek kybernetických útoků. Existuje reálné riziko útoků, které bylo v minulosti opakovaně potvrzeno. Zatímco v IT sítích jsou hlavní hrozbou **ekonomické ztráty**, v OT sítích mohou kybernetické útoky vést k okamžitým fyzickým důsledkům, včetně **ohrožení lidských životů.**

2.1 Nedostatečné zabezpečení historických zařízení.

V OT prostředí je běžné, že mnoho zařízení **nedostává pravidelné bezpečnostní aktualizace**, na rozdíl od IT systémů. Pokud se porouchá zařízení s **více než 10 let starým řídicím systémem**, obvyklým řešením je jeho oprava výměnou za **identické zařízení**, které často obsahuje **stejný archaický operační systém**. Takový systém je dnes již **plný známých bezpečnostních zranitelností**.

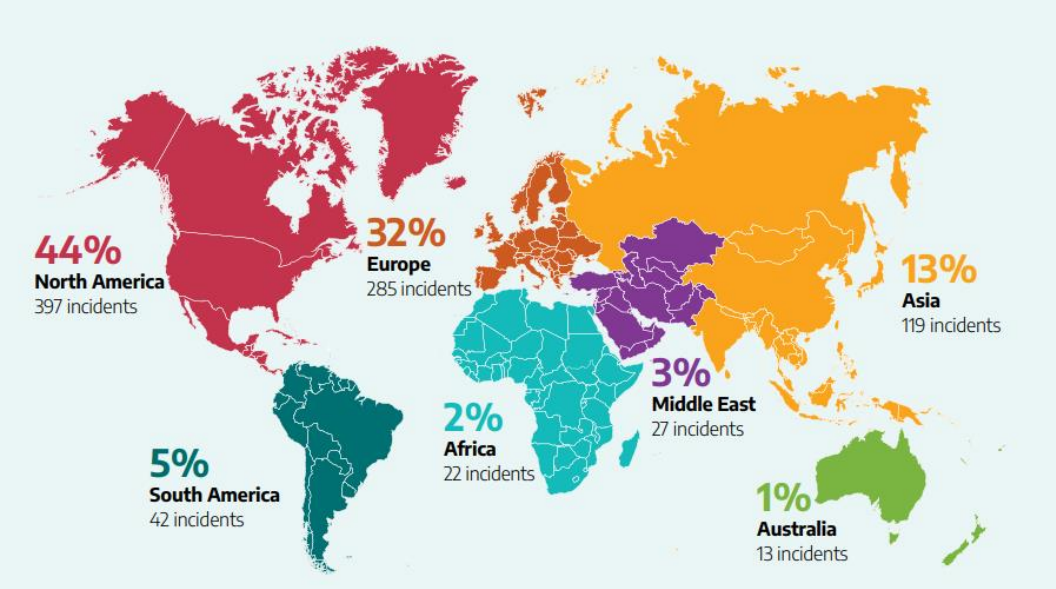
I když samotný zařízení může mít novější verzi, hlavní prioritou pro firmy stále zůstává **dostupnost a spolehlivost systému**, zatímco bezpečnost je často upozaděna. [5][6]

2.2 Ohrožení firem a kritické infrastruktury

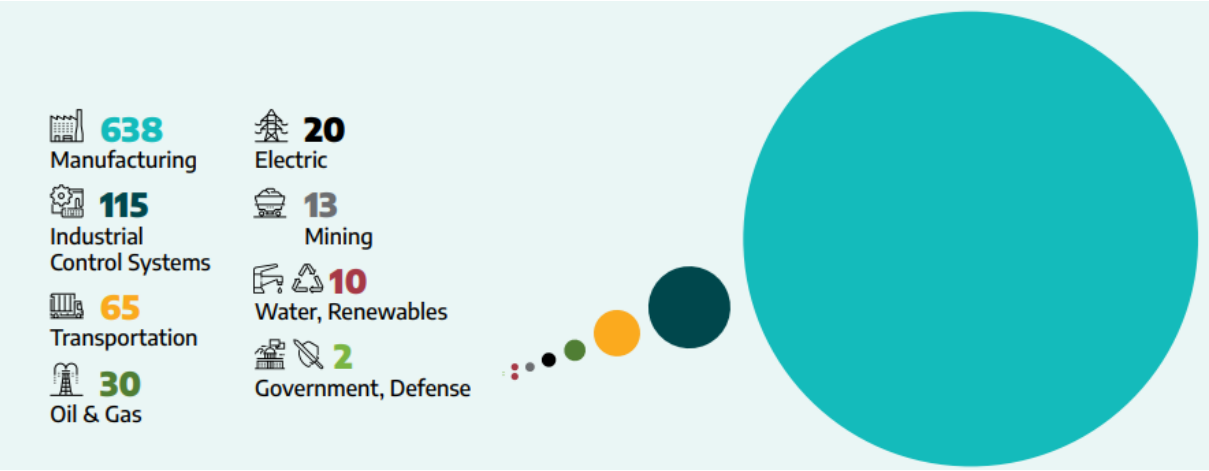
Hlavní potenciální útočník je jiný stát (samozřejmě ne přímo, ale prostřednictvím státem podporovaných „hackerských“ skupin). Nedávné události ukázaly, že hrozby pro OT systémy se již neomezují jen na státní aktéry.

Kybernetický útok typu **ransomware**, který původně cílil hlavně na **IT systémy za účelem finančního zisku**, se ukázal být stejně efektivní – nebo dokonce efektivnější – v OT prostředí. Tento typ útoku může narušit nebo zcela zastavit provoz kritických systémů.

Společnosti věnující se analýze kybernetické bezpečnosti dnes znají více než **12 hackerských skupin** věnujících se přímo útokům na OT. Tyto skupiny nejen provádějí útoky, ale také vyvíjejí sofistikované automatizované nástroje, které jim usnadňují průnik a kontrolu nad OT prostředími. [7]



Obrázek 2.1 Geografické rozložení útoku pomocí ransomware na firmy kde se to týkalo i OT sítí v roce 2023 [7]



Obrázek 2.2 Počet ransomware útoků na jednotlivé odvětví za rok 2023 [7]

2.3 Příklady incidentů

2.3.1 Útok na vodárenský systém v Oldsmaru na Floridě [8]

V únoru 2021 byl pokusem o narušení kritické infrastruktury, která by mohla ohrozit veřejné zdraví.

Přístup k systému přes TeamViewer:

- Útočník získal neoprávněný přístup k systému SCADA, který se používá k řízení a monitorování vodárenských zařízení.
- Přístup byl zajištěn prostřednictvím softwaru TeamViewer, který umožňuje vzdálené ovládání systémů. Tento nástroj používali zaměstnanci pro práci na dálku.

Změna hladiny hydroxidu sodného (louhu):

- Během útoku útočník upravil nastavení hladiny hydroxidu sodného v systému.
- Hydroxid sodný se běžně používá k úpravě pH vody, ale ve vysokých koncentracích je toxický.
- Útočník zvýšil hladinu hydroxidu sodného z 100 částic na milion (ppm) na nebezpečných 11100 ppm, což by mohlo způsobit vážnou otravu vody.

Rychlá reakce operátora:

- Operátor vodárenského zařízení si všiml změn v nastavení téměř okamžitě, protože systém byl v reálném čase monitorován.
- Do několika minut operátor změny zvrátil a obnovil normální hodnoty, čímž zabránil, aby se kontaminovaná voda dostala ke spotřebitelům.

Šetření a důsledky:

- Po incidentu bylo zjištěno, že vodárna měla **slabé bezpečnostní mechanismy**, včetně **sdílených hesel** pro vzdálený přístup a nedostatečného zabezpečení síťových systémů.

Následná opatření:

- Po útoku byla provedena revize kybernetické bezpečnosti v Oldsmaru a dalších podobných zařízeních.
- Úřady včetně FBI a tajných služeb zahájily vyšetřování. **Útočník nebyl identifikován**, ale útok se stal varováním pro ostatní organizace spravující kritickou infrastrukturu.

2.3.2 Kybernetické útoky na ukrajinskou energetickou síť [9]

Útok v roce 2015:

- Útočníci použili phishingové e-maily obsahující infikované přílohy (např. dokumenty Microsoft Office), které obsahovaly malware BlackEnergy.
- Zaměstnanci energetických společností otevřeli tyto přílohy, což útočníkům umožnilo získat přístup k jejich systémům.

Průzkum a příprava:

- Útočníci strávili několik měsíců průzkumem vnitřních sítí a sbíráním informací o průmyslových řídicích systémech, které spravovaly přenosovou soustavu.

Útok:

- V prosinci 2015 byly najednou napadeny tři regionální energetické společnosti.
- Útočníci použili vzdálený přístup k systémům SCADA (Supervisory Control and Data Acquisition) a manuálně odpojili více než 30 rozvodných stanic, což vedlo k výpadku elektřiny pro přibližně 230 000 lidí.
- Současně nasadili malware KillDisk, který smazal kritická data, aby znemožnil rychlé obnovení systému.

Rušení telefonních linek:

- Útočníci navíc zahájili útoky na call centra energetických společností, čímž blokovali komunikaci mezi operátory a zákazníky.

Obnova:

- Výpadek trval několik hodin, než byl elektrický proud manuálně obnoven.
- Škody způsobené malwarovým útokem trvalo opravit delší dobu.

Útok v roce 2016:

Použití malwaru Industroyer:

- V roce 2016 byl útok sofistikovanější a útočníci použili malware známý jako **Industroyer** nebo **CrashOverride**.
- Industroyer byl navržen specificky k narušení průmyslových řídicích systémů a komunikoval přímo s protokoly používanými v elektrických rozvodných sítích (IEC 101, IEC 104).

Cíl:

- Útok byl zaměřen na kyjevskou rozvodnou síť a způsobil výpadek elektřiny na přibližně hodinu.

Průběh:

- Útočníci automatizovali útok pomocí Industroyeru, který přepínal vypínače a odpojoval elektrické stanice.
- Malware zároveň vyřazoval komunikaci mezi SCADA systémy a fyzickými zařízeními.

Obrana a následky:

- Ukrajinské energetické společnosti dokázaly rychleji reagovat díky zkušenostem z předchozího roku.

Útoky na české nemocnice 2020, (včetně Fakultní nemocnice Brno), cílily na IT infrastrukturu. Ta však byla úzce propojena s OT systémy, což vedlo k narušení jejich funkčnosti a ovlivnilo provoz nemocnic. [10]

2.4 Regulace evropské unie

Evropská unie v posledních letech jako reakci na útoky z minulých let přijala několik klíčových směrni které se průběžně implementují v ČR. Firmy nedodržující tyto směrnice mohou být pokutovány až ve stovkách tisíc euro. [11]

2.4.1 Směrnice NIS2 (2022/2555) [12]

Platí výslovně pro firmy z kritických odvětví, kde jsou operační technologie klíčové (energetika, vodohospodářství, doprava, výroba léčiv a zdravotnictví). Pro tyto organizace stanovuje přísnější povinnosti než pro běžné firmy.

Minimální požadavky:

- Zavedení **systému řízení rizik kybernetické bezpečnosti** (např. pravidelné hodnocení rizik, implementace bezpečnostních politik, řízení přístupu, ochrana dat).
- **Oznamování kybernetických incidentů** relevantním orgánům do 24 hodin od jejich zjištění.
- **Zavedení školení a postupů** pro zajištění povědomí zaměstnanců o kybernetické bezpečnosti.
- Dodržování **bezpečnostních standardů** a certifikací stanovených na evropské úrovni.

Prakticky pro to bezpečnost znamená:

- Omezení fyzického přístupu
- Omezení oprávnění
- Segmentace sítě
- Omezení vzdáleného přístupu a správy
- Zálohování a obnova aktivit

Kterých firem se týká:

- **Střední a velké podniky** v klíčových sektorech, jako je energetika, doprava, zdravotnictví, vodohospodářství, finanční služby, veřejná správa a digitální infrastruktura.
- **Minimální hranice:** Firmy s více než **50 zaměstnanci** nebo ročním obratem přesahujícím **10 milionů eur**.

Česká implementace:

- Nový zákon o kybernetické bezpečnosti: Národní úřad pro kybernetickou a informační bezpečnost (**NÚKIB**) splnující požadavky směrnice NIS2. První verze návrhu byla zveřejněna počátkem roku 2023 a následně prošla mezirezortním připomínkovým řízením.
- **Rozšíření působnosti:** Odhaduje se, že se v ČR dotkne více než 6 000 soukromých i státních subjektů, což je výrazný nárůst oproti předchozímu stavu.

2.4.1 Akt o kybernetické bezpečnosti (2019/881) [13]

Produkty s **digitálními prvky**, které se používají v OT prostředí (např. průmyslové řídicí systémy nebo SCADA), musí splňovat požadavky na:

- **Bezpečný návrh a vývoj**: Produkty musí být zabezpečené proti kybernetickým hrozbám již od jejich návrhu.
- **Aktualizace a patchování**: Výrobci musí zajistit, že tyto systémy budou průběžně aktualizovány, aby byly chráněny před známými zranitelnostmi.

Výjimku tvoří malé a mikro firmy, pokud nejsou považovány za kritické (neplní klíčovou roli v daném sektoru).

Minimální požadavky:

- Certifikace kybernetické bezpečnosti OT produktů a služeb podle evropského rámce.
- Produkty a služby musí splňovat **úrovně zabezpečení** po **celou dobu životního cyklu**.

3 Segmentace sítě

Segmentace OT sítí spočívá v rozdělení sítě na menší, izolované části, aby se omezil pohyb kybernetických hrozeb a zvýšila kontrola nad provozem v síti. Tento přístup zajišťuje, že každá část sítě je oddělena od ostatních na základě svých funkcí, kritičnosti a bezpečnostních požadavků. [5]

3.1 Ostrovní systémy OT sítí

Hlavní největší oddělení je od veřejné a IT sítě, pak následují dělení podle funkcí. Ostrovně izolované systémy znamenají **úplnou absenci digitální komunikace mezi OT sítí a okolním světem**. Toto řešení se používá pouze u **nejrizikovějších systémů**, jako jsou například **jaderná elektrárna Temelín**, **výroba mikroprocesorů TSMC na Tchaj-wanu** nebo **Mezinárodní vesmírná stanice (ISS)**.

I přes **fyzickou izolaci** mohou být tyto systémy kompromitovány, například prostřednictvím **infikovaných USB disků** nebo **lidských chyb**. Proto je nutné i u nich implementovat **dodatečné bezpečnostní prvky**.

Ačkoli jde o velmi efektivní způsob, jak chránit OT sítě před kybernetickými hrozbami, firmy od tohoto řešení ustupují. Důvodem je **potřeba vzdáleného přístupu při selhání**, **nutnost rychlé reakce na bezpečnostní incidenty**, **regulační požadavky** na propojení OT s IT nebo cloudem a rostoucí **nároky na sdílení dat v reálném čase**. [5]

3.1.1 Použití datových diod

Rozšířenou možností ostrovního systému je datová dioda které umožní jen komunikaci z OT sítě do IT ale ne naopak. Tento mechanismus je zajištěn hardwarově (např. laserové nebo optické propojení), což znemožňuje jakékoli obcházení softwarovými prostředky. Vyžaduje síťovou konfiguraci na podporovaných protokolech (UDP, Syslog, OPC UA, Modbus). Nelze použít protokoly vyžadující zpětné potvrzení (TCP). Pokročilejší datové diody můžou simulovat zpětné potvrzení tudíž můžou využívat i například TCP/IP protokol.

Datová dioda umožňuje propojení těchto dvou prostředí bez rizika, že by útočník mohl proniknout z méně zabezpečené IT sítě do OT prostředí. [14]

Obrázek 3.1 Dva typy datových diod, přičemž pravá varianta umožňuje podporu protokolů vyžadujících zpětnou odezvu.

Tabulka 3.1 Rozdíl mezi datovou diodou a firewallem pro oddělení OT od IT: [14]

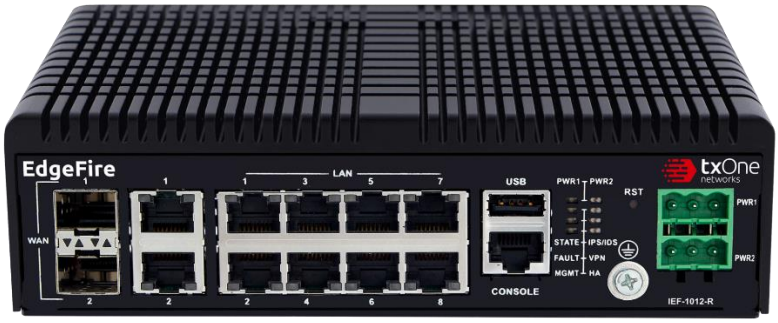
Faktor	Datová dioda	Firewall (OT-IT)
Směr přenosu dat	Jednosměrný	Obousměrný, kontrolovaný pravidly
Bezpečnost	Fyzicky zabezpečené řešení	Závisí na správné konfiguraci softwaru
Komplexita nastavení	Využití podporovaných protokolů	Vyžaduje detailní nastavení pravidel

3.2 Průmyslové Firewally

Průmyslové firewally jsou klíčovým prvkem zabezpečení OT sítí a musí být **přizpůsobeny specifickým potřebám průmyslových prostředí**. Jsou ideální pro **středně velké segmenty** obsahující více řídicích systémů, což umožňuje vytvoření **jednoduše spravovatelných zón**. OT firewally podporují **průmyslové protokoly**, jako jsou **Modbus**, **OPC UA**, **BACnet** nebo **Profinet**, což jim umožňuje zajistit, že povolené komunikace odpovídají očekávaným vzorcům. Dále umožňují **bezpečné vzdálené připojení** prostřednictvím **VPN**, což technikům poskytuje možnost diagnostiky a údržby. Vzhledem k náročným provozním podmínkám v průmyslových prostředích musí být tyto firewally odolné vůči **kolísání teplot**, **prašnosti** a **mechanickým nárazům**, na rozdíl od zařízení umístěných v serverovnách. Pro zajištění vysoké dostupnosti lze využít i **redundantní napájení**. [15]

Kromě těchto základních vlastností by měli průmyslové firewally nabízet i **pokročilé bezpečnostní funkce**:

- **Virtuální záplatování (Virtual Patching)**, které čerpá z výzkumů zranitelností programu **Zero Day Initiative (ZDI)**, umožňuje chránit zařízení i bez fyzické aktualizace softwaru, což je ideální pro **zastaralá zařízení bez dostupných aktualizací**.
- **Granulární řízení přístupu (Granular Access Control)** zajišťuje jemnou kontrolu nad OT protokoly a příkazy, blokuje neoprávněné operace a povoluje pouze **legitimní komunikaci**.
- **Uzamčení IP a dalších protokolů (IP and Protocol Lockdown)** omezuje komunikaci na předem definované **protokoly**, například může být do části sítě povolena pouze komunikace jedním protokolem. [15]



Obrázek 3.2: Průmyslový firewall EdgeFire od společnosti TXOne Networks. [15]

3.3 Průmyslové IPS (Intrusion Prevention System)

Průmyslové systémy IPS jsou klíčovým nástrojem pro **aktivní ochranu OT sítí** před kybernetickými hrozbami a **Microsegmentaci sítě**. Lze je nasadit přímo před kritická zařízení nebo na klíčové body v síti.

Na rozdíl od firewallů, které fungují jako prevence a filtr, IPS systémy **aktivně monitorují provoz a mohou provést zásah do provozu.**

To zahrnuje:

1. **Detekci a blokování útoků:** IPS používá metody, jako je **podpisová analýza** (signature-based detection), která porovnává provoz se známými hrozbami v databázi, a **behaviorální analýza** (behavior-based detection), která identifikuje odchylky od běžného chování. Pokud detekuje problém, automaticky zablokuje podezřelý provoz.

2. **Kontrola hloubky dat (Deep Packet Inspection):** IPS zkoumá nejen hlavičky síťových paketů, ale i obsah komunikace (vrstvy L2–L7). Díky tomu dokáže zjistit například pokusy o injekci škodlivého kódu, neobvyklé příkazy nebo manipulaci s daty.
3. **Reakce v reálném čase:** IPS okamžitě reaguje na detekované hrozby – blokuje konkrétní provoz, izoluje napadené segmenty I bez zásahu administrátora.
4. **Virtuální záplatování (Virtual Patching):** Chrání systémy s nezáplatovanými zranitelnostmi tím, že blokuje pokusy o jejich zneužití, aniž by bylo třeba aktualizace.

Stejně jako Firewally jsou IPS přizpůsobeny podmínkách průmyslových prostředích ale navíc často umožnují funkci **Hardware bypass (Fail Open)**, což je fyzická funkce IPS zařízení, která umožňuje síťovému provozu procházet přímo mezi vstupními a výstupními porty zařízení bez zpracování dat IPS modulem. Toto se může hodit při **výpadku napájení** IPS, aktualizaci firmware. [16]

3.3.1 Nasazení a základní nastavení IPS

IPS musí být strategicky umístěno v síti, například mezi **kritickými zařízeními a zbytkem sítě** nebo **před specifickými OT segmenty.**

Výběr režimu provozu:

- **Monitorovací režim (IDS)**: IPS pouze sleduje provoz a hlásí podezřelé aktivity bez zásahů. Tento režim se obvykle používá při počáteční konfiguraci, aby se minimalizovala rizika špatného nastavení.
- **Preventivní režim (Prevention)**: IPS aktivně blokuje podezřelé provozy podle stanovených pravidel.

Založení bezpečnostních politik:

- Povolení komunikace mezi klíčovými zařízeními (např. PLC, HMI nebo SCADA systémy).
- Omezení komunikace pouze na důvěryhodné IP adresy, porty a protokoly.

Vytváření pravidel na základě analýzy provozu:

- IPS může využít **AI-driven auto-learning** (například v EdgeIPS 102), který analyzuje síťový provoz a generuje baseline pravidla.
- Tato pravidla lze dále ručně upravovat, aby odpovídala specifickým požadavkům dané infrastruktury. [17]

Obrázek 3.3: Průmyslový IPS společnosti TXOne Networks a OPSWAT. [16] [18]

3.4 Software pro centralizovanou správu průmyslových Firewall a IPS

Software pro centralizovanou správu průmyslových firewallů a IPS představuje klíčový nástroj pro řízení a monitorování OT sítí. Tyto platformy umožňují správcům **spravovat, konfigurovat a monitorovat více zařízení z jednoho centralizovaného rozhraní**, čímž výrazně zjednodušují údržbu a provoz.

Klíčové vlastnosti:

- **Centralizovaná správa**: Umožňuje jednotné řízení zařízení, jako jsou OT IPS a Firewall, včetně jejich bezpečnostních politik a aktualizací.
- **Komplexní viditelnost**: Poskytuje přehled o stavu OT sítí, včetně stínové infrastruktury, a nabízí přizpůsobitelný dashboard.
- **Efektivní údržba**: Automatizace aktualizací firmwaru, pravidel a podpisů hrozeb snižuje administrativní zátěž.
- **Flexibilní nasazení**:
    - **On-premises verze**: Správa více linek v jedné továrně.
    - **Cloudová verze**: Možnost centralizované správy více lokalit prostřednictvím jednotného rozhraní, včetně zrychlené implementace a podpory více produkčních míst.

Výhody:

- **Škálovatelnost**: Podpora tisíců zařízení v různých lokalitách.
- **Proaktivní prevence**: Identifikace a eliminace rizik ještě před jejich dopadem na provoz.
- **Snížení nákladů**: Intuitivní rozhraní a automatizace snižují nároky na administrativní údržbu.
- **Integrace třetích stran**: Interoperabilita se SIEM a SOC prostřednictvím API zajišťuje jednotnou správu zabezpečení. [19]

3.5 Hráči na poli OT bezpečnosti

TXOne Networks

- Firewally: EdgeFire – robustní OT firewall s podporou průmyslových protokolů.
- IPS: EdgeIPS – zařízení s funkcemi IPS, včetně virtuálního záplatování a CPSDR.
- Software: EdgeOne – platforma pro správu EdgeIPS a EdgeFire, monitorování hrozeb a aktualizace.

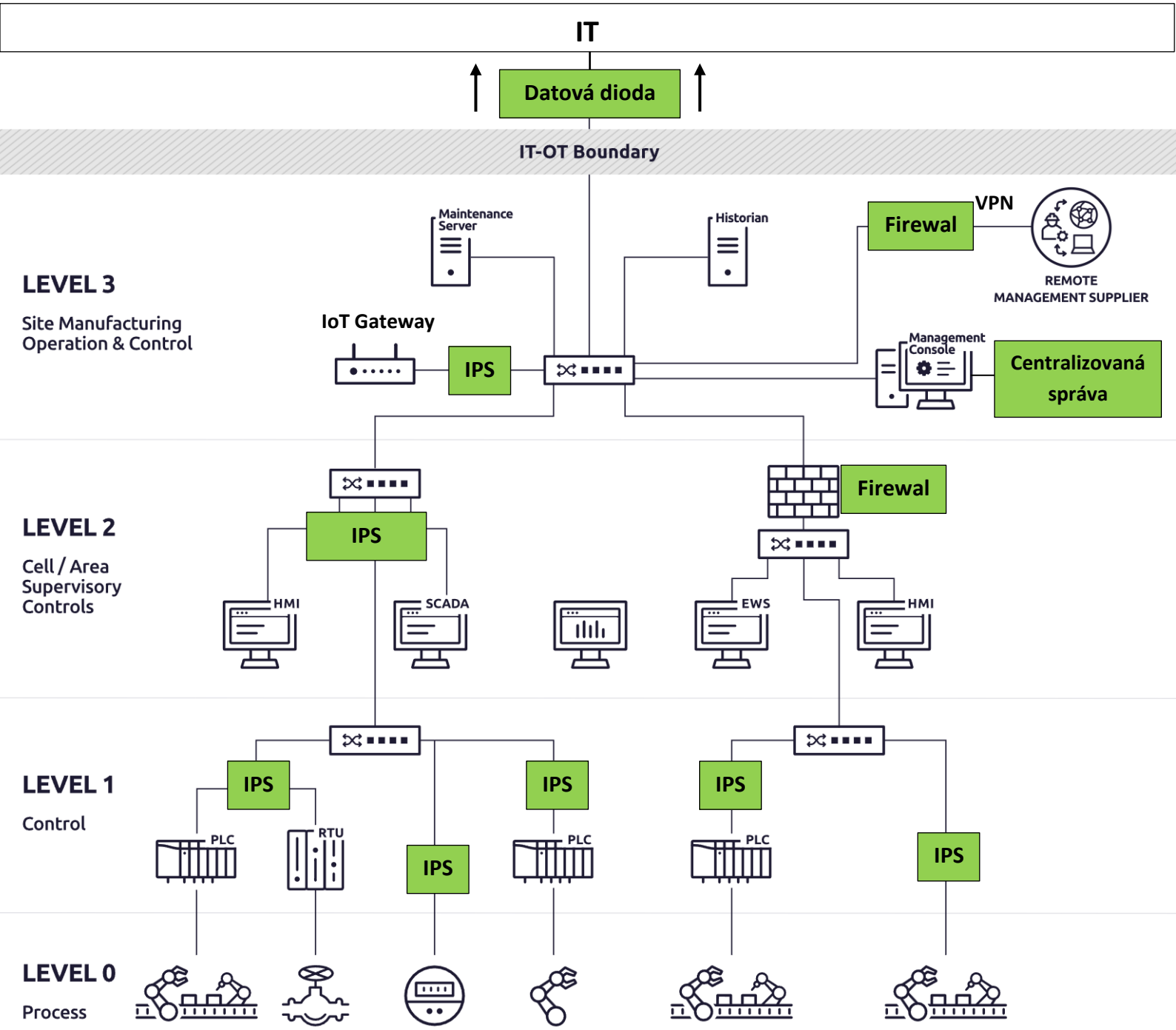
Cisco

- Firewally: Cisco Secure Firewall – přizpůsobené OT prostředí, pokročilá analýza.
- IPS: Firepower Threat Defense – IPS integrovaný do Cisco firewallů.
- Software: Cisco SecureX a DNA Center – centrální správa a analýza bezpečnostních událostí.

Palo Alto Networks

- Firewally: PA-220R a další modely pro průmyslové prostředí.
- IPS: Součást Next-Generation Firewalls (NGFW) s podporou OT protokolů.
- Software: Panorama – nástroj pro centrální správu a monitoring.

4 Příklad nasazení v síti [20]



5 Vlastní pohled na téma a závěr

Z pohledu praktického využití jsou přínosy jasné: segmentace minimalizuje šíření kybernetických hrozeb a umožňuje precizní kontrolu nad různými částmi sítě. IPS a firewally nabízejí jak aktivní, tak pasivní ochranu proti útokům a podporují bezpečné fungování i starších zařízení, což je v průmyslovém prostředí velmi časté. Díky přibývajícím regulacím jsou firmy nuceny do této oblasti více investovat, což pro většinu firem asi znamená pouhou snahu splnit minimální požadavky, aby nedostaly pokutu. To však nutně zvyšuje zabezpečení OT sítí.

Hrozba je podle mě reálná, a v období, kdy dle statistik počet kyberútoků roste a formují se skupiny hackerů, které se na tuto oblast zaměřují, se riziko zvyšuje. Firmy jako Txone přicházejí s komplexním řešením od skenu sítě po nasazení hardwarových zařízení, která umožňují i firmám bez lidského kapitálu v oblasti kyberbezpečnosti ochránit svou infrastrukturu a výrobní zařízení.

Nacházíme se v paralýze, kdy je svět až příliš komplexní a lidé jsou často specializovaní na úzký profil své práce. Tudíž bezpečák nerozumí procesům v OT a průmysloví technici zase nerozumí kyberbezpečnosti, což vede k tomu, že zabezpečení OT sítí často trpí.

Do budoucna si myslím, že spojený tlak regulátorů a útoků ze strany hackerů nakonec zlepší zabezpečení OT sítí.

6 Použitá literatura

[1] What is operational technology (OT)? Online. Dostupné z: https://www.tenable.com/principles/operational-technology-principles. [cit. 2024-11-26].

[2] OTSEC. *Bezpečnost OT/ICS*. Online. Dostupné z: https://otsec.cz/bezpecnost-ot-ics/. [cit. 2024-11-26].

[3] MOTOROLA, INC. *SCADA Systems: A Comparision of RTUs and PLCs*. Online. Dostupné z: https://www.motorolasolutions.com/content/dam/msi/Products/scada-systems/SCADA_Sys_Wht_Ppr-2a_New.pdf. [cit. 2024-11-26].

[4] ŠNAJDR, Václav. *Generátor datového provozu pro průmyslové protokoly*. Online. Bakalářská práce. Brno: Vysoké učení technické v Brně. 2019. Dostupné z: https://theses.cz/id/0d7bgp/.

[5] OTSEC. *Proč se bezpečnosti Operačních technologií věnovat*. Online. Dostupné z: https://otsec.cz/dozvedet-se-vice-proc-je-bezpecnost-ot-vyzvou/. [cit. 2024-11-26].

[6] TXONE. *The 2023 Industrial Cybersecurity Tech, Solutions & Services Buyer's Guide*. Online. 2023. Dostupné z: https://media.txone.com/prod/uploads/2023/06/Industrial-Cybersecurity-Buyer-Guide-2023.pdf. [cit. 2024-11-26].

[7] DRAGOS. *OT CYBERSECURITY THE 2023 YEAR IN REVIEW*. Online. 2023. Dostupné z: https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en. [cit. 2024-11-26].

[8] TECHTARGET. *Florida city's water nearly poisoned in TeamViewer attack*. Online. 9 Feb 2021. Dostupné z: https://www.techtarget.com/searchsecurity/news/252496102/Florida-citys-water-nearly-poisoned-in-TeamViewer-attack#:~:text=An%20unknown%20threat%20actor%20used,before%20it%20could%20be%20completed.. [cit. 2024-11-26].

[9] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *Cyber-Attack Against Ukrainian Critical Infrastructure*. Online. 2021. Dostupné z: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [cit. 2024-11-26].

[10] NÚKIB. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020*. Online. 2020. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf. [cit. 2024-11-26].

[11] *EU se rozhodla posílit kybernetickou bezpečnost a odolnost v celé Unii: Rada přijala nový právní předpis*. Online. 28 listopadu 2022. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/. [cit. 2024-11-26].

[12] ÚŘEDNÍ VĚSTNÍK EVROPSKÉ UNIE. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555*. Online. 2022. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555. [cit. 2024-11-26].

[13] NÚKIB. *Akt o kybernetické bezpečnosti*. Online. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=2713. [cit. 2024-11-26].

[14] OWL CYBER DEFENSE. *What's the Difference Between Firewalls & Data Diodes?* Online. Dostupné z: https://owlcyberdefense.com/wp-content/uploads/2019/05/24-OWL-V4-DataDiodes-Firewalls.pdf. [cit. 2024-11-26].

[15] TXONE. *EdgeFire datasheet*. Online. Dostupné z: https://media.txone.com/prod/uploads/2023/09/TXOne-EdgeFire-Datasheet-202309.pdf. [cit. 2024-11-26].

[16] TXONE. *EdgeIPS*. Online. Dostupné z: https://www.txone.com/products/network-defense/edgeips/#datasheet. [cit. 2024-11-26].

[17] EC-COUNCIL. *IDS and IPS: Understanding Similarities and Differences*. Online. Dostupné z: https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/#:~:text=Response%3A%20IDS%20tools%20send%20alerts,to%20prevent%20or%20mitigate%20threats.. [cit. 2024-11-26].

[18] OPSWAT. *MetaDefender Industrial Firewall™*. Online. Dostupné z: https://www.opswat.com/products/metadefender/industrial-firewall. [cit. 2024-11-26].

[19] TXONE. *EdgeOne*. Online. Dostupné z: https://media.txone.com/prod/uploads/2024/10/EdgeOne-Datasheet-20240928.pdf. [cit. 2024-11-26].

[20] TXONE. *Deployment Model*. Online. Dostupné z: https://www.txone.com/products/. [cit. 2024-11-26].