ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra počítačů

Bezpečnost průmyslových sítí

Industrial Network Security

Bakalářská práce

Studijní program: Softwarové inženýrství a technologie

Vedoucí práce: doc. Ing. Leoš Boháč, Ph.D.

Michal Koreš

Praha 2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Koreš** Jméno: **Michal** Osobní číslo: **469838**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra počítačů**

Studijní program: **Softwarové inženýrství a technologie**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Bezpečnost průmyslových sítí

Název bakalářské práce anglicky:

Industrial Network Security

Pokyny pro vypracování:

Analyzujte datový provoz vybrané části průmyslové řídicí sítě ve firmě Škoda auto a.s. a zmapujte typy použitých technologií a jejich napojení do IT infrastruktury podniku. Na základě této analýzy vytvořte metodiku pro zajištění kybernetické bezpečnosti této sítě. Navrhněte vhodné SW prostředky pro zajištění síťové kybernetické bezpečnosti tohoto provozu. Využijte k tomu již existující SW (primárně open-source), tak případně i vlastní programové vybavení. Dle možné součinnosti se Škoda auto a.s. ověřte navrženou metodiku v praxi.

Seznam doporučené literatury:

[1] KNAPP, Eric D. a Joel Thomas LANGILL. Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other indistrial control systems. Second edition. Waltham, MA: Syngress, 2015. ISBN 0124201148.
[2] ACKERMAN, Pascal. Industrial cybersecurity: efficiently secure critical infrastructure systems. Birmingham: Packt Publishing, 2017. ISBN 1788395158.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

doc. Ing. Leoš Boháč, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2020** Termín odevzdání bakalářské práce: **14.08.2020**

Platnost zadání bakalářské práce: **30.09.2021**

doc. Ing. Leoš Boháč, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

Datum převzetí zadání	Podpis studenta

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 13. 08. 2020

…….

Michal Koreš

Poděkování

Rád bych poděkoval mému vedoucímu bakalářské práce doc. Ing. Leoši Boháčovi, Ph.D. za cenné rady, připomínky a čas, který mi věnoval při řešení této problematiky. Dále bych chtěl poděkovat firmě Škoda Auto a.s., především Bc. Janu Šedovi, který byl vedoucím mé stáže.

Abstrakt

Bakalářská práce se skládá z teoretické a praktické části. Teoretická část práce se zabývá standardem průmyslových sítí Profinet a principy komunikace. Pozornost je také věnována adresaci a identifikaci zařízení. Dále jsou zde popisovány základní typy útoků na tyto sítě.

V praktické části bakalářské práce je analyzován provoz ve vybraném provozu Škoda Auto a.s. z bezpečnostního hlediska, rozboru zabezpečení a ochrany sítě, útoky na ní a protiopatření. Závěr této části je věnován praktickým nasazením a použitím navrhovaných bezpečnostních nástrojů.

Klíčová slova

profinet, průmyslové sítě, bezpečnost, komunikace, riziko, hrozby, ochrana, detekce

Abstract

The bachelor thesis consists of a theoretical and practical part. The theoretical part deals with the standard of industrial networks Profinet and the principles of communication. Attention is also paid to addressing and identifying devices. The basic types of attacks on these networks are also described here.

The practical part of the bachelor's thesis analyzes the operation in the selected operation of Škoda Auto a.s. from a security point of view, analysis of network security and protection, attacks on it and countermeasures. The conclusion of this part is devoted to the practical deployment and use of the proposed security tools.

Keywords

profinet, industrial networks, security, communication, risk, threats, protection, detection

Obsah

Seznam tabulek

Seznam obrázků

Seznam zkratek

ISO	Mezinárodní organizace pro normalizaci
OSI	Open Systems Interconnection
LAN	Local Area Network
MAC	Media Access Control
PCP	Peripherals Communication Protocol
TCP	Peripherals Communication Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
NRT	Non Real Time
RT	Real Time
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
VLAN	Virtuální Local Area Network
IRT	Isochronous Real-Time
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
PTP	Precision Time Protocol
PC	Personal Computer
TDMA	Time Division Multiple Access
PLC	Programovatelný Logický Automat
HMI	Human Machine Interface
I/O	Input/Output
DCP	Discovery and Configuration Protocol
SNMP	Simple Network Management Protocol
CR	Komunikační relace
AP	Aplikační relace
RPC	Remote Procedure Call
CBA	Component Based Automation
VPN	Virtual Private Network

DCE-RCP	Distributed Computing Environment – Remote Procedure Calls
MITM	Man-in-the-middle
ARP	Address Resolution Protocol
DoS	Denial of Service
IT	Information Technology
USB	Universal Serial Bus
NSE	Nmap Scripting Engine
CIA	Confidentiality-Integrity-Availability
STP	Spanning Tree Protocol
CAM	Content Addressable Memory
RFID	Radio Frequency Identification
CVE	Common Vulnerabilities and Exposures
NVD	National Vulnerability Database
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
CLI	Command Line Interface
GUI	Graphical User Interface
SPAN	Switched Port Analyzer
BPF	Berkeley Packet Filter
DPI	Deep Packet Inspection
JSON	JavaScript Object Notation
YAML	YAML Ain't Markup Language
MIB	Management Information Base
OID	Object Identifiers
CSV	Comma Separated Values
HTML	Hypertext Markup Language
ICMP	Internet Control Message Protocol

1. Úvod

S nastupujícím trendem Průmyslu 4.0 jsou otázky zajištění bezpečnosti a optimalizace systému průmyslových sítí jednou z těch nejpalčivějších. V současné době se zvětšuje důraz (i politicky) na intenzivní digitalizaci a automatizaci výroby. Troufám si tvrdit, že nasazení nových technologií, jako je strojové učení, autokonfigurace, autodiagnostika do průmyslu, bude mít za následek revoluci na pracovním trhu. Nové systémy průmyslu a celkový koncept bude postupně nahrazovat pracovníky s nižší kvalifikací a naopak budou vznikat nová pracovní místa vyžadující vyšší kvalifikaci zaměstnanců.

Na základě dosavadních výzkumů a diskusí, se bezpečnostní experti shodují na tom, že existuje šest hlavních hrozeb, které ovlivňují interní síť:

- neoprávněný přístup,
- nezabezpečený přenos dat,
- nezašifrovaná klíčová data,
- neúplné logy událostí,
- nedostatečný monitoring zabezpečení,
- lidský faktor při konfiguraci.

Aby nedocházelo k ohrožení sítí externími a interními hrozbami, je zásadní, aby síťoví pracovníci měli vyšší kvalifikaci, hrozbám, které nejen v Průmyslu 4.0 jsou, rozuměli a dokázali vymyslet a implementovat řešení, díky kterým budou sítě bezpečné. Nejdůležitější je, aby síťoví technici dokázali nasadit zařízení, která budou integrovat takové bezpečnostní prvky, aby sítě byly v bezpečí před externími i interními hrozbami.

Z výše popsaných důvodů se moje bakalářská práce zabývá problematikou Profinet sítě, která je jedním z hlavních komunikačních sběrnic určená pro řídicí systémy v oblasti průmyslové automatizace. Profinet standard je vystaven na základech průmyslového Ethernetu. Tato technologie je podporována řadou výrobců a využívána v řadě průmyslových odvětví, jako je např. automobilový průmysl, strojírenství nebo potravinářský průmysl.

Bakalářská práce je rozdělena do dvou hlavních částí. První kapitola se zabývá Profinetem a je teoretickou částí bakalářské práce. Tato část si klade za cíl vytvořit stručný úvod do průmyslové technologie Profinet a seznámit čtenáře s jejími základními principy funkce.

Druhá praktická část bakalářské práce se zabývá konkrétní analýzou a vyhodnocením provozu ve vybraném provozu Škoda Auto.

V první kapitole druhé části se věnuji analýze provozu průmyslové sítě, jejím specifikám, posouzením rizik, modelům hrozeb a analýze zranitelností v konkrétním provozu Škoda Auto.

V další kapitole se zabývám zabezpečením a ochranou sítě, kterou klasifikuji do třech částí podle ISO/OSI modelu. Dále v této kapitole uvádím konkrétní typy útoků, kterými jsou průmyslové sítě často ohroženy a navrhuji konkrétní protiopatření, které lze proti nim využít.

V poslední kapitole tyto útoky provádím na laboratorní síti, která je modelem konkrétního provozu Škoda Auto, a ověřuji, zda jsou navržené nástroje a postupy z výše uvedené kategorie účinné.

Praktická část si klade za cíl analyzovat možné hrozby, které se mohou v průmyslové síti Škoda Auto (a nejenom zde) vyskytnout. Účelem bakalářské práce je také tyto hrozby

specifickým způsobem klasifikovat a navrhnout protiopatření nasazením specializovaných softwarových nástrojů. Doporučené nástroje jsou také v síti ověřeny.

2. Popis standardu Profinet

Profinet je komunikační protokol, který umožňuje výměnu dat mezi jednotlivými stanicemi. Tyto sítě vznikly na základě průmyslového ethernetu (IEEE 802.3). Jeho specifikace je popsána v otevřeném standardu IEC 61158. V současné době je nainstalováno po celém světě více než 26 miliónů zařízení Profinet [20]. Jednotlivá stanice je jednoznačně identifikována pomocí Media Access Control (MAC) adresy, která je vždy přiřazena k síťové kartě. Síť může pro výměnu dat mezi jednotlivými stanicemi používat následující přenosová média:

- metalická,
- optická,
- bezdrátová.

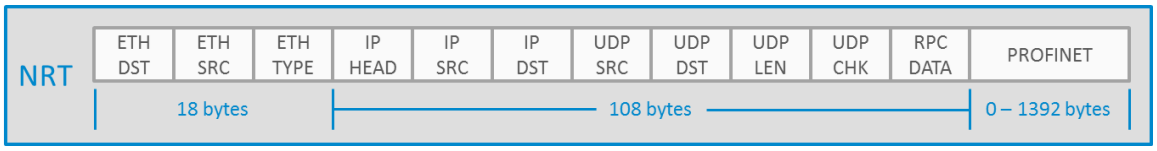
Základní aktivní prvky této sítě jsou, stejně jako u klasického Ethernetu, síťové přepínače (tzn. switche), které předávají zprávy ze vstupního portu na výstupní port. Dělí celou síť na logicky samostatné části (Virtuální LAN – IEEE 802.1Q). Toto rozdělení je výhodné, protože jednotlivé části jsou snadněji spravovány, dochází ke zvýšení výkonu a větší bezpečnosti. Síťové přepínače navíc prioritizují provoz na základě PCP tříbitové hodnoty priority datového rámce. Komunikace průmyslové sítě Profinet se dělí na následující typy:

- datové přenosy přes TCP/IP, UDP/IP;
- komunikace pro reálný čas (Automation);
- komunikace pro izochronní reálný čas (Motion control).[6][1]

2.1 Datové přenosy přes TCP/IP, UDP/IP

Datové přenosy přes TCP/IP jsou označovány také jako Non Real Time (NRT) a využívají všechny vrstvy referenčního ISO/OSI modelu. Použití všech síťových vrstev ISO/OSI modelu přidává určité množství zpoždění a časové nejistoty (jitteru), a proto je tento kanál nejpomalejší (u velkých sítí může dosahovat zpoždění 10ms – 100ms).

Tyto datové přenosy se většinou používají pro komunikaci konfiguračního, parametrického, případně diagnostického charakteru. Jelikož se pro přenos dat používá IP protokol, je nutné, aby zařízení mělo přiřazené unikátní IP adresy. Jelikož mnoho zařízení v sobě integruje webové servery, je umožněna interakce s uživatelem pomocí webového prohlížeče. [14]

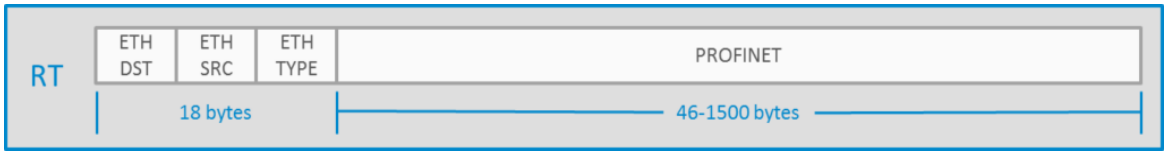


Obrázek 1 - Příklad NRT paketu

2.2 Komunikace pro reálný čas

Komunikace pro reálný čas bývá také označována jako Real Time komunikace (RT) a je určena pro časově kritická procesní data, např. událostmi řízená přerušení nebo cyklická uživatelská data. Tento druh komunikace vyžaduje (na rozdíl od Non real time komunikace) co nejmenší zpoždění a jitter – tím je docíleno přeskočením zapouzdření v síťové, transportní a relační vrstvě, přičemž linková a fyzická vrstva zůstávají v nezměněné podobě – viz obrázek 2. To znamená, že v Real Time komunikaci nejsou používány IP adresy, ale pouze MAC adresy. Z toho vyplývá, že rámce v této podobě nemohou být směrováni mezi LAN sítěmi. Pro RT komunikaci mezi sítěmi je nutné využít tzv. UDP-RT nadstavbu, někdy také označovanou jako RT over UDP/IP. Šestnáctibitová hodnota EtherType v ethernetovém rámci, na rozdíl od NRT komunikace, která má klasickou IPv4/IPv6, je nastavena na kód 0x8892, který označuje použití PROFINET protokolu. [8] [51]

Tato síť poskytuje časovou odezvu jednotky až desítku milisekund a je výkonově rovnocenná s jinými průmyslovými sběrnicemi (např. Profibus). Taktéž zde lze používat standardní síťové komponenty, protože tato komunikace má výrazně snížené požadavky na výkon procesoru. Díky optimalizovanému softwarovému zásobníku může RT komunikace probíhat paralelně s Non Real Time komunikací. Pro splnění požadavků v reálném čase používá RT komunikace v záhlaví VLAN nejvyšší dostupnou prioritní úroveň 6, čímž se zajistí, že rámce komunikace pro reálný čas jsou přepínány přednostně.[14]

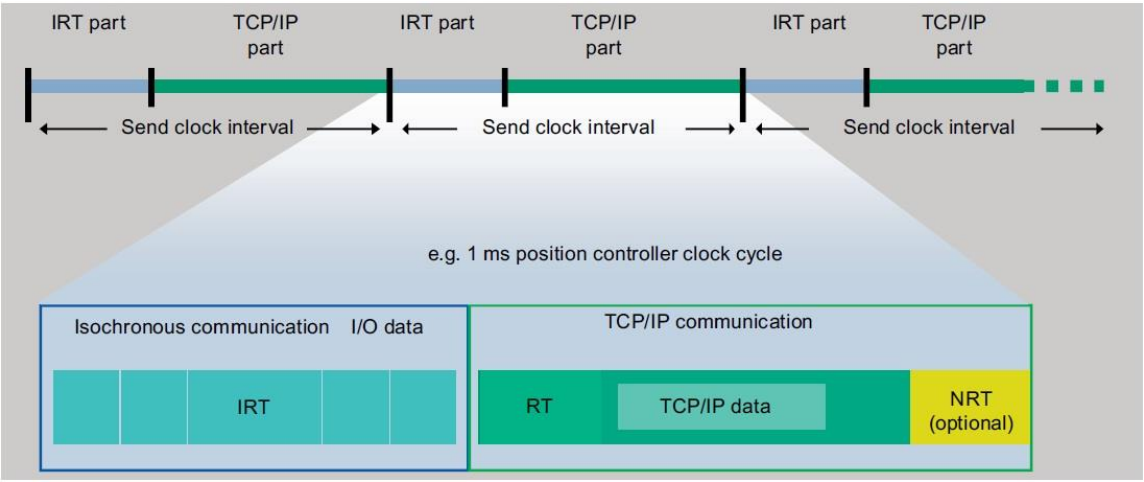


Obrázek 2 - RT paket bez VLAN tagy

2.3 Komunikace pro izochronní reálný čas

Pro komunikaci pro izochronní reálný čas, případně synchronní taktování v reálném čase, se používá zkratka IRT. Tento druh komunikace je schopen dosáhnout odezvy pod 1ms a jitterem do 1 µs. Je určená pro konkrétní, specifické aplikace, které vyžadují přesné taktování a rychlou odezvu (např. řízení pohybu). Pro dosažení výše uvedených vlastností se komunikační cyklus rozdělí na uzavřenou a otevřenou část. V otevřené části je možné posílat RT a TCP/IP data, naopak zavřená (tzv. deterministická) část je vyhrazena pouze pro IRT přenosy. Oba typy přenosů dat mohou existovat vedle sebe tak, že nevzniknou žádné kolize (na rozdíl od klasického Ethernetu s CSMA/CD protokolem zavádí tzv. TDMA[1] síť), jak je vidět na obrázku 3. Komunikace je dopředu plánovaná, tudíž je možné, si předem spočítat, jak dlouho bude trvat doručení každé zprávy s mikrosekundovou přesností. [8] [14] [21] [51] [52]

1 Time Division Multiple Access – každému účastníkovi je přiřazen specifický a ohraničený časový slot pro přenos dat. Díky této vlastnosti je možné sdílet jedno přenosové médium pro více uživatelů.



Obrázek 3 - Princip komunikace v reálném čase

Tato metoda časových slotů vyžaduje, aby každý přepínač přesně věděl, kdy uzavřená a otevřená část pásma začíná. Před každou IRT komunikací probíhá obvykle synchronizace všech účastníků datového přenosu pomocí Precision Time Protocolu (PTP). Na začátku každého cyklu PTP-master vyšle broadcast packet, který synchronizuje hodiny účastníků. [50] [59] [52]

2.4 Zařízení v síti Profinet

Profinet sítě a jejich zařízení nejsou na rozdíl od technologie Profibus koncipována jako "master-slave" (tedy "nadřízená-podřízená"). Všechny komponenty jsou na Ethernetu rovnocenná – díky použitím přepínačů funguje bezkolizní komunikace, a tedy není nutné přístup k síti řídit. Přístup z Profibusu se přenesl na model „provider-consumer" (tedy „poskytovatel-spotřebitel"). Spotřebitel má za úkol data zpracovat a poskytovatel vysílá bez čekání na výzvu. [8]

2.5 Typy zařízení Profinet I/O

Ve standardu Profinet jsou definovány tři role komponent, jak je vidět na obrázku 4. Tyto role jsou založeny na tom, jakým způsobem interagují s ostatními zařízeními na síti. Profinet rozděluje přenos dat na cyklickou (plánovaná, opakovaná komunikace) a acyklickou (neplánovanou komunikaci na vyžádání). Někdy se k těmto dvěma typům přidává ještě tzv. Lateral Data Traffic, což je synonymum pro multicastovou Ethernetovou komunikaci. [21]

2.5.1 Profinet I/O Device

Zařízení je samostatná jednotka, jehož účelem je předávání informací v reálném čase Controlleru. Tato jednotka nekomunikuje se stejnou Device jednotkou přímo, ale vždy přes Controller. Svá data hlásí cyklicky přímo do jednotky Controller. Jednotce Supervisor hlásí acyklicky poplašná, případně diagnostická data. I/O Device je poskytovatelem vstupních dat a spotřebitelem dat výstupních. [10] [13]

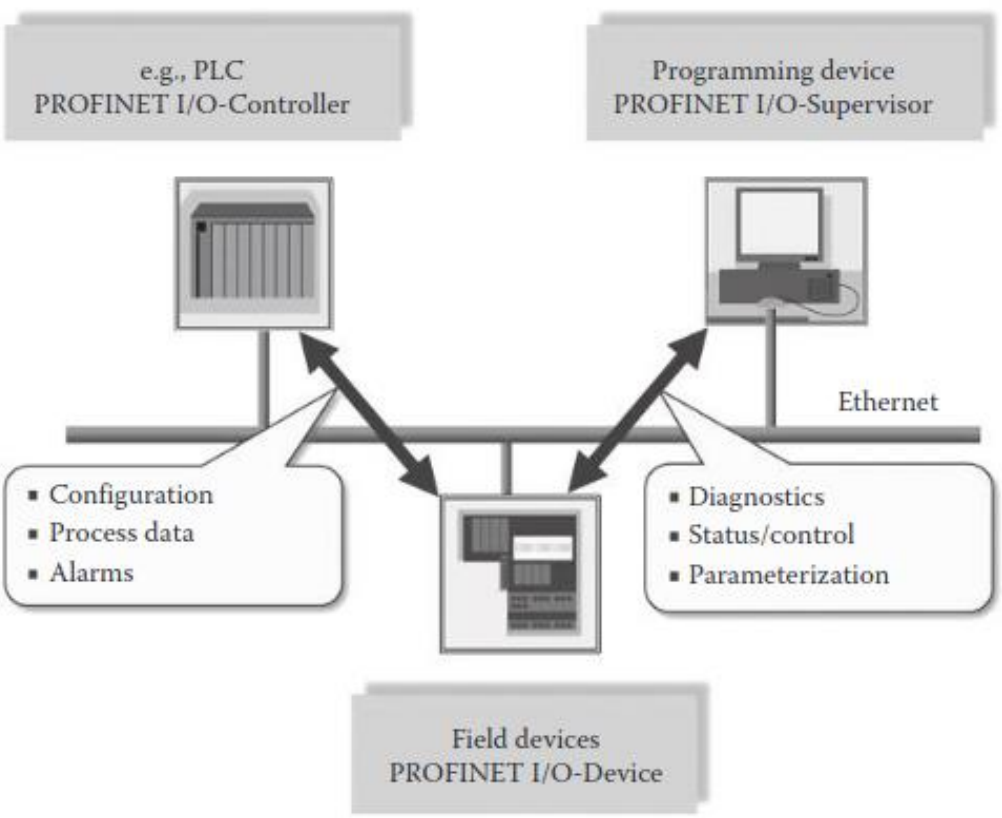
Profinet I/O Device se dají rozdělit do dvou typů – tzv. Compact field devices (jednotka je nerozšiřitelná) a Modular field devices (zařízení lze rozšířit v závislosti na oblasti použití). [17]

2.5.2 Profinet I/O Controller

Řadiče shromažďují cyklická data od jedné nebo více Device zařízení. Sledují nejen data v reálném čase, ale shromažďují také výstražné zprávy nebo informace o stavu údržby každého zařízení a tyto informace dále prezentují koncovému uživateli. Řadiči jsou obvykle softwarové aplikace pro PC, PLC nebo různé HMI panely. I/O Controller poskytuje výstupní data konfigurovaným I/O Device ve své roli poskytovatele a je spotřebitelem vstupních dat I/O Device. [8] [10]

2.5.3 Profinet I/O Supervisor

Zařízení Supervisor je podobné zařízení jako Controller, ale nemá přístup k cyklickým (realtime) datům. Koncoví uživatelé používají zařízení typu Supervisor ke čtení diagnostických informací z I/O Device, přiřazování DCP názvů stanic, analýzy sítě, odstraňování probémů sítě, přiřazování IP adres apod. [8] [10] [14]



Obrázek 4 - Komunikační cesty I/O zařízení

2.6 Conformance Class

Jednotlivé produkty pro Profinet sítě jsou označovány jako Conformance Class A, B, C. Do první třídy A jsou zařazovány produkty, které mají následující funkcionality:

- datové přenosy přes TCP/IP (UDP/IP) a RT,
- certifikované výměny zařízeních a řadičů,
- diagnostika a varování,
- cyklická a acyklická výměna dat,
- standardní komunikace prostřednictvím Ethernetu,
- standardní diagnostika sítě Ethernet.

Produkty třídy B jsou rozšířeny o následující vlastnosti:

- datové přenosy přes TCP/IP (UDP/IP) a RT,
- certifikované síťové prvky,
- použití SNMP,
- jednoduchá výměna zařízení.

Produkty nejvyšší třídy C mají navíc tyto vlastnosti:

- datové přenosy přes TCP/IP (UDP/IP), RT a IRT,
- certifikace síťových prvků a HW podpory. [8][9]

2.7 Komunikační relace

Pro výměnu cyklických i acyklických dat mezi I/O Controllerem a I/O Devicem je nutné nejdříve navázat komunikaci. Ta probíhá v rámci komunikační relace (CR), která je součástí aplikační relace (AR). Každá aplikační relace tedy obsahuje jednu nebo více komunikačních relací – těch je více druhů:

- alarm CR – slouží k výměně alarmů a je přenášen acyklicky,
- record data CR – přenosy parametrů s využitím protokolu RPC, rovněž acyklická výměna,
- I/O data CR – výměna cyklických dat.

Každá CR má svého poskytovatele dat (odesílatel) a konzumenta dat (příjemce). Jelikož je komunikační relace vždy jednosměrná, je nutné v rámci jedné aplikační relace vytvořit vždy minimálně dvě komunikační relace (směr tam a zpět). O tzv. multicastu v komunikační relaci hovoříme v případě, kdy je přenos dat od jednoho poskytovatele k více (nebo všem) spotřebitelům.

Acyklické výměny dat jsou explicitně potvrzovány. Cyklická výměna dat je nepotvrzována – není potřeba, protože při ztrátě dat jsou data nahrazena v dalším cyklu. [2][8]

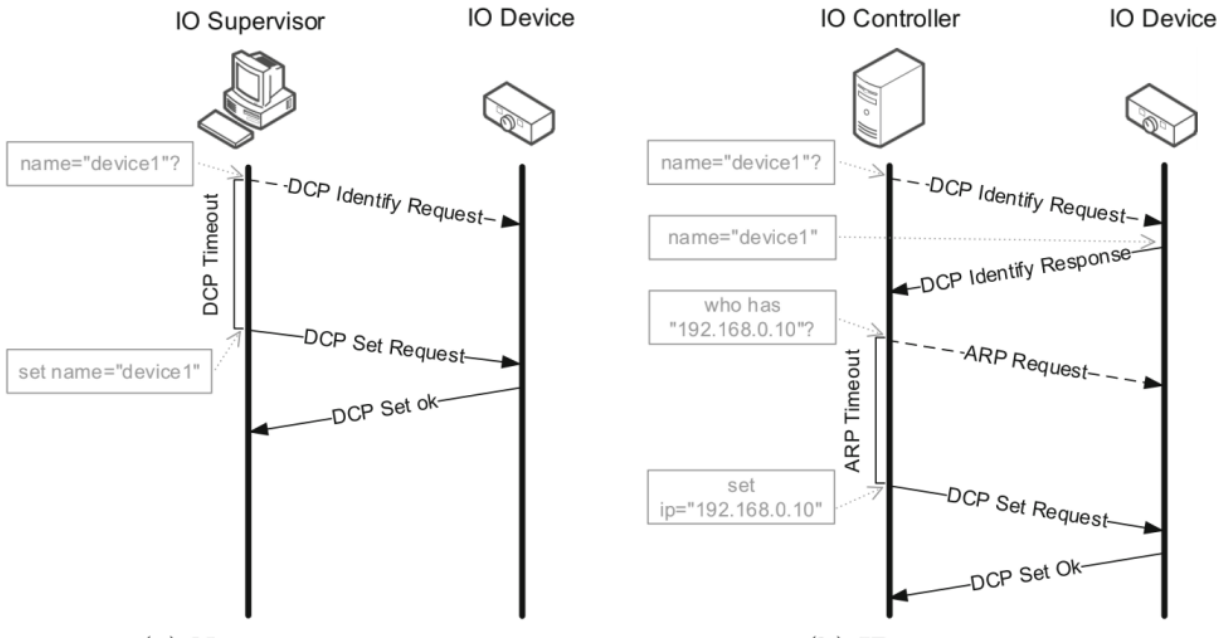
2.8 Adresace zařízení v síti

Pro jednoznačnou identifikaci zařízení se používá buď MAC adresa (pro real-time komunikaci), případně IP adresa (pro non real-time komunikaci). Profinet přináší další identifikaci zařízení, jedná se o tzv. Name of Station. Název stanic s sebou nese několik výhod:

- při výměně zařízení není nutné měnit konfiguraci sítě;
- pro uživatele je jméno zařízení snadněji zapamatovatelné, snadněji se určí umístění zařízení.

Tento název lze rozšířit o název systému IO, který je podobný konstrukci adresy URL pro internetové názvové konvence.

Profinet DCP je součást sady protokolů a znamená „Discovery and Configuration Protocol". Tento protokol se použije vždy při uvádění nového Profinet zařízení do provozu. Profinet I/O Supervisor, který přiděluje jména stanic dle MAC adresy, provede sekvenci zpráv pro identifikaci zařízení v sítě. [16][7][18]



Obrázek 5 - Sekvence zpráv pro identifikaci zařízení v síti (vlevo přiřazení Name of Device, vpravo přiřazení IP adresy)

Na obrázku 5 vidíme přiřazení jména zařízení "device1". I/O Supervisor odešle multicastem DCP Identify request, pokud již některé zařízení má tento název přiřazený, pošle okamžitě DCP Identify response. Pokud Supervisor neobdrží žádné DCP Identify response do DCP Timeoutu, Supervisor má za to, že žádné takové jméno nebylo přiřazeno. V tom případě Supervisor pošle DPC Set Request zařízení, které má obdržet jméno "device1". Pokud je proces úspěšný, je ukončen odpovědí DCP Set ok směřovanou od I/O Device na Supervisora.

Proces pro přiřazení IP adresy (obrázek 5 vpravo) je obdobný jako u přiřazení Name of Station. Jako první I/O Controller pošle multicastem DCP Identify request, kterým se dotáže všech zařízení, které z nich má jméno "device1". Takto pojmenované I/O Device na tento dotaz odpoví pomocí DCP Identify Response. V dalším kroku je broadcastem zaslán ARP Request, který má za úkol zjistit, zda je konkrétní IP adresa již k někomu přiřazená. Pokud se do požadovaného ARP timeoutu neobjeví žádný ARP Reply, má I/O Controller za to, že adresa je zatím nepoužívaná, je tedy volně dostupná a pomocí dotazu DCP Set Request nastaví příslušnému zařízení konkrétní IP adresu. Pokud je proces úspěšný, je taktéž ukončen odpovědí DCP Set OK směřovanou od I/O Device na Controllera. Další možností, jak nastavit zařízení IP adresu je přes DHCP server. [1][8]

2.9 Profinet CBA

Profinet CBA (Component Based Automation) definuje další pohled na automatizační zařízení. Základní úvahou CBA je, že závod lze v mnoha případech rozdělit na autonomní jednotky, tzv. Technologické moduly. Tyto technologické moduly mají funkčnost definovanou řídícím programem, psaným uživatelem a předávají předem definované signálu jinému I/O Controlleru. Komponenty Profinetu jsou vyráběny nezávisle na výrobci a jsou naprogramovány se vstupy a výstupy podle návrhu konkrétní autonomní jednotky. Profinet CBA podporuje deterministickou komunikaci s přenosovými cykly až 10 ms a je velmi vhodný pro komunikaci mezi jednotlivými I/O Controllery. [3]

2.10 Bezpečnost v síti Profinet

Automatizační systémy hrají v moderním průmyslu klíčovou roli, a proto jsou důležitou součástí naší ekonomiky. Nově používané technologie se snaží maximalizovat účinnost tak, že zjednodušují instalaci automatizačních systému a zlepšují poskytování dat na podnikové úrovni. V poslední letech je zřetelný průnik známých IT technologiích do oblastech, kde byly dříve používány specializované a nekompatibilní technologie.

Profinet, stejně jako řada ostatních automatizačních standardů, se většinou zabývá především otázkou spolehlivosti jednotlivých služeb, ale poskytují pouze omezené množství bezpečnostních mechanismů. V kombinaci s průnikem IT technologií to představuje reálné riziko kybernetických útoků. [11]

Některé z nejdůležitějších bezpečnostních problémů jsou:

- důvěrnost – důvěrná data může číst pouze oprávněná osoba;
- integrita – neautorizované subjekty nemohou měnit data bez detekce;
  dostupnost – funkční systém nebo jeho součást v okamžiku, kdy je vyžádáno jeho použití;
- autentizace – ověření pravosti entity, subjekt je opravdu tím, za koho se vydává.

Dostupnost je nejvíce proklamovaný problém, protože má největší dopad na provoz. [12] Avšak dostupnost a integrita z bezpečnostního hlediska v aplikačních sběrnicích (tzv. fieldbus) neexistují – průmyslové standardy s nimi v návrhu nepočítali. Tyto dva problémy se řeší z pohledu provozu, tzn. ochrana před náhodnými chybami, elektromagnetickými emisemi, nikoliv ochrana před úmyslně škodlivou manipulací s daty. [11]

Pro „obvodovou“ ochranu se dnes využívají nejmodernější IT prvky, jako jsou firewally, IDS a IPS systémy omezující příchozí a odchozí provoz do sítí. V rámci sítě chráněné stejnou obvodovou ochranou je komunikace založena na vzájemné důvěře a jednotlivé uzly sítě mohou mezi sebou komunikovat bez omezení. Pro komunikace mimo vlastní hranice sítě se doporučuje použití Virtual Private Network (VPN) technologie. [12]

Jak již bylo výše řečeno, Profinet využívá nativní TCP/IP protokoly pro cyklickou i acyklickou komunikaci. Profinet IO využívá tzv. Distributed Computing Environment-Remote Procedure Call (DCE-RCP) [60] a UDP/IP pro správu kontextu, např. pro inicializaci AR a CR. Pro RT data vytváří pak na vrstvě Ethernetu komunikační kanál bez

použití TCP/IP. Kvůli tomu, že Profinet IO nespoléhá na IP vrstvu pro komunikaci v RT a navíc používá pro komunikaci unicast i multicast, je obtížné využít stávající bezpečnostní protokoly, jako je např. IPSec. [12]

2.10.1 Man-in-the-middle-attack (MITM)

Jelikož Profinet sítě používají standardní Ethernet přepínače, lze provést dobře MITM útok známý především z klasických IT sítí (známy pod názvy „ARP Poison“, nebo „Port stealing“). Podstatou tohoto způsobu, který útočí na kryptografii, je snaha útočníka aktivně odposlouchávat komunikaci mezi dvěma účastníky tak, že se stane jejich prostředníkem, aniž by o tom jedna či druhá strana věděla. [12]

Identifikace I/O Device je prováděna především na základě Profinet jména, nikoliv IP adresy. Toto unikátní jméno je přiřazeno skrz DCP protokol a I/O Device ho uloží do své non-volatile paměti. Útok MITM využívá typicky třech problémů, které mohou nastat. [22]

2.10.1.1 Neunikátní IP adresa

Pokud je Profinet jméno zkontrolováno jako unikátní, přejde se ke kontrole IP adresy pomocí ARP požadavku. Standardní zásobník ARP nezpracovává dvojité odpovědi na ARP požadavek – pokud tato situace nastane, tabulka ARP je aktualizována na poslední přijatou odpověď. Typicky zde není žádná signalizace vyšším vrstvám, že se v síti vyskytují zařízení se stejnou IP adresou. AR se tedy založí nezávisle na jméně Profinet zařízení s tím, který je obsažen v ARP tabulce.[22]

2.10.1.2 Neunikátní Profinet jméno

DCP protokol provádí pojmenování zařízení. V úvodním multicastu všechna Profinet zařízení obdrží dotaz od I/O Controlleru ohledně zaslání svého jména. Tento seznam se zobrazí obsluze, která vybere samotné přiřazení. Při sestavování AR I/O Controller zjišťuje jména zařízení pomocí DCP-Identify pomocí broadcastu. Pokud dostane I/O Controller více odpovědi, zastaví svůj proces a uživatel obdrží chybovou hlášku.[22]

2.10.1.3 Podvrhnutí MAC adres

MAC adresa by měla být jedinečná po celém světě. Je ovšem pro útočníka velice jednoduché tuto adresu změnit/upravit tím způsobem, aby provedl úspěšný útok. Ethernetový přepínač využívá MAC adresy k tomu, aby určil výstupní port, na který má rámec poslat. Jelikož v IT světe lze jednoduše manipulovat se síťovými zařízeními, je nutné, aby přepínač neustále aktualizoval svou tabulku s přiřazenými porty a jejich MAC adresami. Pokud útočník chce provést MITM útok, pošle ethernetový rámec s cizí MAC adresou a všechny následující rámce bude přepínač posílat na MITM zařízení, místo toho, aby je posílal na vyhrazené zařízení. Protože každý rámec odeslaný I/O Devicem způsobí aktualizaci MAC tabulky přepínače, je nutné, aby útočník ihned odeslal další rámec s falešnou MAC adresou. Pokud jsou odesílána cyklická data od I/O Device

např. každých 5ms, je nutné, aby útočník svůj modifikovaný frame také odesílal každých 5ms tak, aby MAC tabulka přepínače stále obsahovala útočníkův záznam. Útok je poměrně lehce odhalitelný, neboť výše zmíněné generuje dvojnásobek zatížení oproti ostatním portům na přepínači. [22]

2.11 Denial-of-Service (DoS)

Existují kybernetické hrozby, které nelze pomocí kryptografických metod zmenšit. Těmito úkony jsou právě Denial of service, jejichž cílem je útok na dostupnost systému. Dopady těchto útoky jsou především v ekonomické rovině. Pokud je síť určitého systému tímto způsobem úspěšně napadena, není možné pokračovat ve výrobě. Na rozdíl od DoS útoků v klasickém IT světe, ve kterém jsou již poměrně propracovaná bezpečnostní opatření, je ve vestavěných průmyslových sítích obtížné zvládnout obranu před takovým to útokem. Navíc útočníci mají často k dispozici mnohem větší výkon, než je automatizovaných systémech, a proto je poměrně rychlé vyčerpání systémových prostředků. [12]

Přerušení propojení systému lze docílit pomocí dvou technik:

- Plýtváním sítí zdroje – útočník se snaží (např. zaplavením sítě nevyžádanými zprávami) „ukrást“ celou šířku pásma pro úplné přerušení komunikace mezi zařízeními v postiženém segmentu.
- Plýtváním systémových prostředků – útoky jsou vedeny na:
  - zařízení, které je důležité pro provoz sítě (důležité servery, brány firewall apod.);
  - zařízení, které jsou spojeny přímo s automatizací (I/O Device, I/O Controllers, pracovní stanice apod.);
  - propojovací zařízení, která mají za úkol propojit zařízení (směrovače, routery apod.).

Oběma útokům se dá částečně předejít pomocí jedné, případně druhé techniky obrany – DoS detekce a Opatření proti DoS útokům.[23]

2.11.1 DoS detekce

Jednou z možností, jak odhalit DoS útoky, je použití systému Detekce narušení (Intrusion Detection System – IDS). Cílem tohoto systému je vytvořit „normálové“ schéma provozu sítě a monitorovat neobvyklý síťový provoz nebo abnormální chování systému. Tento systém se skládá ze čtyř podsystémů

1) Sběrné složky zodpovědné na sběr dat pozorováním síťového provozu.
2) Část zabývající se zpracováním dat a rozhodnutí, zda se v síti vyskytuje podezřelé chování.
3) Komponenta pověřená shromažďováním výsledků a ukládáním pozorovaných dat.
4) „Výkonná“ část zodpovídající za zahájení určitých protiopatřeních a minimalizace následků útoku.[53]

3. Analýza provozu průmyslové sítě

Před samotnou analýzou je nutné si vyjasnit některé pojmy. Začnu s vymezením pojmů „safety“ a „security“. Prvním pojmem překládaným také jako bezpečnost se rozumí „funkční bezpečnost“, např.: ochrana před úrazem (bezpečnost práce), ochrana životního prostředí, požární ochrana apod. Zatímco já budu pracovat s pojmem bezpečnosti ve smyslu pojmu „security“, která se lépe do češtiny dá přeložit jako „kyberbezpečnost“, popř. „bezpečnost v IT“.

Komunikace na bázi Ethernetu hraje klíčovou roli v automatizačním prostředí. Výhoda nasazení Ethernetu v tomto prostředí je především jedna – umožnění nasazení otevřených, standardizovaných IT technologií, které umožňují implementaci integrovaných sítí. Tato výhoda však zvyšuje riziko narušení přístupu, které je nutné posoudit a následně implementovat vhodné bezpečnostní koncepty. Tyto útoky nemusí nutně souviset s hackerským narušením. Může se jednat o narušení způsobené servisním technikem. Ten může navázat spojení s řídící sítí a poté jednoduše, spuštěním několika aplikací, může tento servisní technik zahltit síť do té míry, že některá automatizační zařízení selžou a tím se spustí úplné přerušení provozu. V kontextu automatizačních systémů lze tedy za bezpečnostní problém považovat jakékoliv provozní narušení, ať již záměrně či omylem. Zabezpečení sítě není věcí, kterou lze umístit na jedno místo. Všichni, kteří se podílí na instalaci a správě musí být zahrnuti do tohoto konceptu. Může se jednat o oddělení IT, odborníky na PLC, bezpečnostní tým, dokonce i výrobce komponent je do tohoto procesu zahrnutý. [7]

Úspěšné útoky na komponenty průmyslových sítí mají obrovské dopady na celou řadu aspektů, dělící se na lokální dopad (dopad na provoz), regionální (okolní území) a globální (národní, nadnárodní):

- dopad na kvalitu výrobku,
- pověst společnosti,
- ztráta výroby,
- ztráta duševního vlastnictví,
- mikroekonomický dopad,
- dopad na životní prostředí,
- ztráty na životech,
- makroekonomický (hospodářský) dopad,
- obecná panika,
- Rozsáhlá katastrofa čítající mnoho ztrát na životech a obrovský dopad na životní prostředí.

Výsledky průzkumu zveřejněné společností Positive Technologies jasně říkají, že průmyslové sítě jsou z hlediska kyberbezpečnosti špatně chráněné, navzdory tomu, že jsou rozhodující pro provoz průmyslových zařízení (a tedy pro samotné průmyslové podniky). Podle zprávy má 73% testovaných podnikových informačních systémů a sítí nedostatečnou perimetrickou ochranu před vnějšími útoky. Penetrační testeři získali přístup k podnikové síti a využili tento přístup k průniku do průmyslové sítě obsahující zařízení v 82% testovaných sítí. V 67% úspěšných případů průniku byly vektory útoku ohodnoceny jako triviální nebo

malé. „Implementace těchto útočník vektorů by vyžadovala pouze využití stávajících konfiguračních nedostatků v zařízení a segmentaci sítě, jakož i zranitelnosti OS, pro které jsou exploitační nástroje dostupné i online.“ uvádí se ve zprávě. [24]

Bob Noel, ředitel strategických vztahů a marketingu společnosti Plixer řekl: *„Existuje dnes tolik útočných vektorů pro kyberzločince, že každá organizace, zejména kritická infrastruktura, musí předpokládat, že bude porušena. K posílení bezpečnostních strategií by měla být analýza síťového provozu implementována tak, aby hledala zneužití důvěryhodnosti, boční pohyby (tzv. lateral movement) a anomálie v protokolech a aplikacích. Jak bylo demonstrováno penetračními testery, jakmile kybernetičtí zločinci proniknou do sítě, jsou schopni obejít bránu mezi podnikovou sítí a sítí podporující průmyslové systémy“*. [43]

Ethernet je velice využíván v aplikacích průmyslové automatizace a v kancelářských prostředích průmyslových firem. Díky tomuto je mnoho lidí přesvědčeno, že postupy zabezpečení, které jsou využívány v kancelářských prostředí lze snadno aplikovat na průmyslové sítě. Bohužel to není pravda, protože existuje několik významných rozdílů mezi průmyslovými a kancelářskými ethernetovými sítěmi.

Cíl ochrany

Zatímco kancelářské sítě se zabývají především zabezpečením dat (obsahují totiž všechny druhy vysoce citlivých dat jako jsou mzdy, příjmy, seznam zákazníků, marže apod.), největším problémem pro průmyslové sítě obecně je provozuschopnost. Ve většině aplikací kancelářských sítí lze tolerovat přerušení služeb na několik minut, případně na několik hodin až dní (v případě svátků, víkendů apod.). Průmyslové sítě naopak nepřenáší data s touto úrovní citlivosti, avšak nepřetržitý provoz 24/7 je pro ně velice klíčový. [25]

Omezený přístup

Velké množství kancelářských systémů musí mít rozsáhlé propojení s okolním světem. Mzdové systémy jsou spojeny s bankovními systémy, prodavači na pobočkách musí mít přístup k informacím o zákazníkovi apod. Na rozdíl od průmyslových sítí, které mohou mít úzce regulovaný přístup, díky kterým lze realizovat určitá bezpečnostní opatření, která by v kancelářské síti nebyla praktická. Jedná se například o poskytnutí přístupu na základě požadavků určité osoby. [25]

Velikost a stabilita

Obecně jsou kancelářské sítě mnohem větší, do sítě se připojuje mnohem více počítačů, tabletů, chytrých telefonů a dalších zařízení. Oproti tomu k průmyslové síti je připojené omezené množství zařízení. Tyto zařízení jsou také mnohem statičtější – přidání dalšího stroje, jeho HMI nebo PLC, do výrobního systému obvykle není častým jevem (častější je spíše výměna za jiný) a je poměrně běžné, že síť průmyslové automatizace zůstává v podstatě stejná nebo hodně podobná celé roky.

Taktéž komunikace je mnohem statičtější u průmyslových automatizačních sítí, než je tomu u kancelářských sítí. Z tohoto důvodu lze snadněji detekovat jakékoliv odchylky od normálních vzorců, které by mohly naznačovat problém v síti nebo vniknutí útočníka. [25]

Hardware a Software

Kancelářské sítě propojují standardní hardware, jakou jsou počítače, tablety, tiskárny apod. Mnoho z těchto zařízení je vybaveno ethernetovými porty a komunikuje přes Ethernet IP a další standardní protokoly. Software, který běží na těchto zařízeních je taktéž vysoce standardizovaný (z hlediska síťové komunikace). Průmyslové sítě spojují rozhraní HMI, řadiče, motorové pohony a další proprietární a embedded zařízení. Většina těchto zařízení má ethernetový port, ostatní spolu komunikují jednoduššími metodami, jakou jako napěťové či proudové smyčky apod.[25]

Softwarové aktualizace

Obecně se kancelářské sítě a systémy neustále záplatují a inovují pomocí nejnovějších aktualizací softwaru díky čemuž mají poměrně dobrou reakci na různé nalezené hrozby a zranitelnosti. Průmyslové sítě jsou na rozdíl od kancelářských sítí těžkopádnější, protože se musí pečlivě otestovat každá změna softwaru tak, aby nedošlo k ovlivnění komunikace s ostatními zařízeními. Z tohoto důvodu mnoho správců sítě tyto aktualizace nenasazuje. Díky tomu jsou sice sítě průmyslové automatizace stabilnější, mají zvýšenou dobu provozu schopnosti než kancelářské sítě, ale pokud jde o samotné aktualizace software, tak jsou méně aktuální. Tento kompromis zapříčiní menší pružnost reakcí na nově nalezené hrozby a zranitelnosti.[25]

3.1 Posouzení rizik

Co je to riziko? Existuje celá řada definic, z nichž nejcitovanější a obecně neuznávanější je definice dle ISO, která definuje riziko jako „potenciál, který daná hrozba bude zneužívat zranitelnosti aktiva a tím poškodit organizaci“. [26] Z této definice vyplývá, že riziko se skládá ze tří modifikátorů:

- pravděpodobnost dané hrozby,
- potenciální zranitelnost aktiva,
- výsledné důsledky, které ovlivní provoz.

Základní koncept řízení rizik je takový, že můžeme snížit nebo zmírnit riziko zaměřením na jeden nebo na více výše zmíněných modifikátorů. Obecný názor říká, že nejjednodušší metoda snížení rizika je identifikace a eliminace zranitelných míst, která mohou být zneužita. Například zavedením systému správy patchů, které pravidelně aktualizuje software pro odstranění identifikovaných bezpečnostních nedostatků. Riziko lze také snížit omezením rozsahu škod. Tato metoda bývá často přehlížena, ačkoliv může být mnohem efektivnější a levnější ve srovnání s jinými metodami.

Pro identifikaci rizik v IT bylo vyvinuto několik metod. Tabulka 1 uvádí ty nejčastěji používané. Provedení analýzy rizik je obtížný úkol, protože je nutné, aby bylo homogenní při posuzování všech rizik a situací, které mohou nastat. Aby tento proces byl co možná nejpřesnější, je nutné, aby metoda bylo složena z poměrně jednoduchých kroků. Tyto kroky se stávají především z inventarizace systému a na základě tohoto seznamu lze provést vyhodnocení se správně definovaným měřítkem. Tyto seznamy mají také další funkci a to takovou, aby analytik nezapomněl opomenout důležité body zabezpečení.

V závislosti na těchto metodách lze popsat kategorie komponent, hrozeb, zranitelnosti, možných dopadů. Tyto metody lze využít na různých úrovních společnosti – od zkoumání organizačních procesů ve společnosti až po technickou úroveň. [4]

Jméno	Zakladatel	Odkaz
EBIOS	ANSSI, 1995, 2010, 2018	https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/
MEHARI	CUSIF, 1995	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html
OCTAVE	Carnegie Mellon, 1999	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html
CORAS	UiO/SINTEF, 2001	http://coras.sourceforge.net/
MEGARIT	Spanish Ministry for Public Administrations, 1997	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
SP800-30	NIST, 2002	https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
CRAMM	British CCTA, 1985	https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
TARA	MITRE, 2011	https://www.mitre.org/sites/default/files/pdf/11_4982.pdf

Tabulka 1 Hlavní metody analýzy rizik informační bezpečnosti

Hodnocení rizik je činnost, která probíhá jako součást procesu řízení rizik. Jde však o činnost, která je iniciována pouze v pravidelných intervalech, nikoliv kontinuálně. Hodnocení rizik obvykle slouží k identifikaci a analýze možných zranitelností a hrozeb daného systém. To se provádí za účelem odhadu rizik, kterým může provozovatel čelit. Výstup této fáze je základem pro všechny ostatní činnosti v rámci řízení rizik tím, že vyvolává nové požadavky na bezpečnost, vyhodnocuje současné bezpečnostní politiky, posuzuje stávající ochranné mechanismy, pomáhá při výběru protiopatření apod. [58]

Výsledkem posouzení rizik je kvalitativní a kvantitativní hodnocení možných rizik, kterým je síť vystavena s přihlédnutím k pravděpodobným hrozbám a kontextu. [58]

3.2 Událost ohrožení

Událost ohrožení se sestává z několika součástí, které mohou výrazně ovlivnit riziko, které jsou následující:

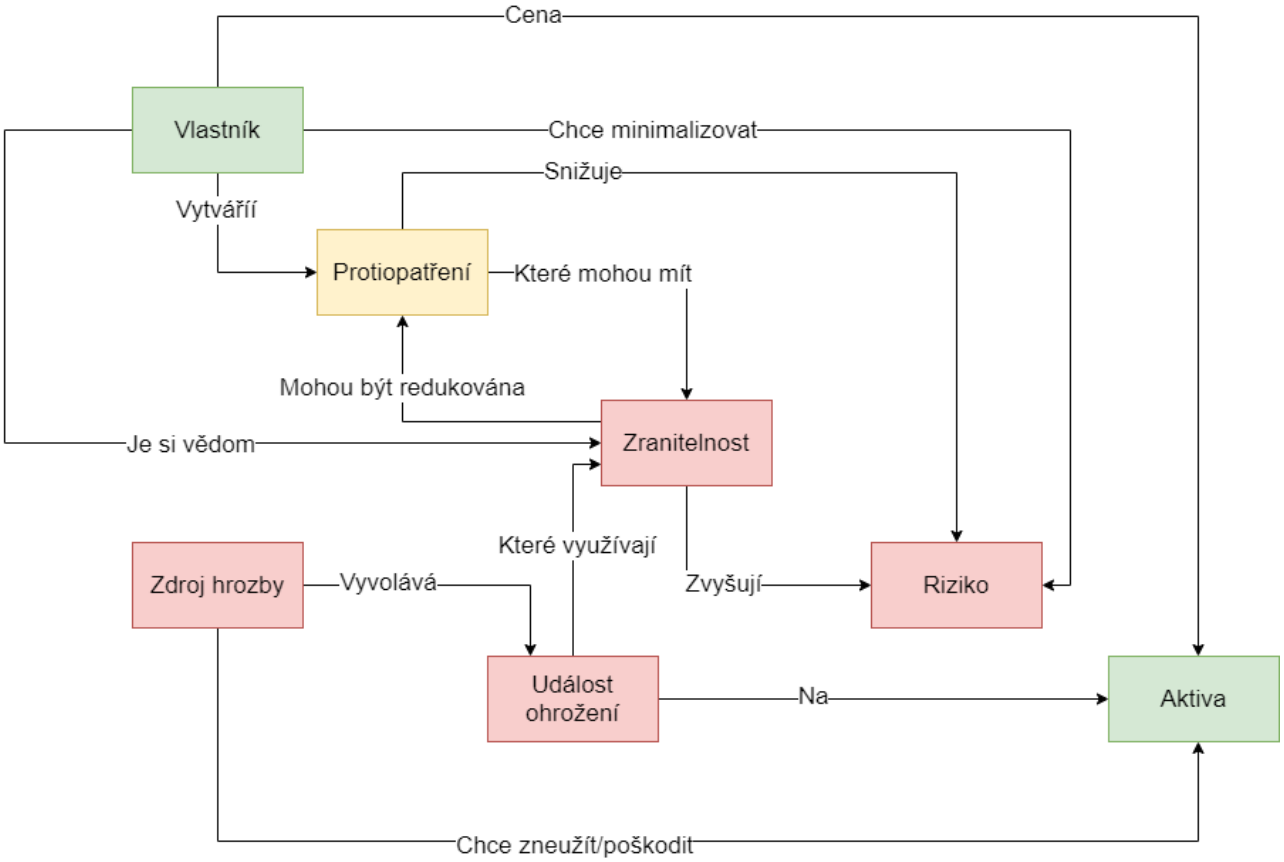
- zdroj hrozby,
- vektor hrozeb,
- cíl hrozby.

Řešení jednoho nebo více těchto součástí může taktéž ovlivnit riziko. Vektory útoku jsou například nechráněné USB porty, nesprávně nakonfigurovaný firewall apod. Termín „zmenšení útočné plochy“ označuje metodu, která může zcela vyloučit jeden z vektorů útoku (např. zcela zakázat řadič USB). [47]

Zdroj hrozby (neboli lidský útočník) provede kybernetický útok, pokud útočník má následující tři vlastnosti:

- znalost provedení útoku,
- záměr způsobit škodu,
- příležitost k zahájení útoku.

Existuje mnoho nástrojů (komerčních i s otevřeným zdrojovým kódem), které umožní provést kybernetický útok s poměrně malou znalostí problematiky. Pro organizace je velmi obtížné snížit riziko vnějšího zdroje útoku, protože to není v jejich přímé kontrolu. Pokud však útok vychází z vnitřního zdroje (případně vnější útočník získá oporu uvnitř), je hrozba zvládnutelnější. [49] Vztahy mezi jednotlivými objekty kybernetické bezpečnosti reprezentuje obrázek číslo 6.

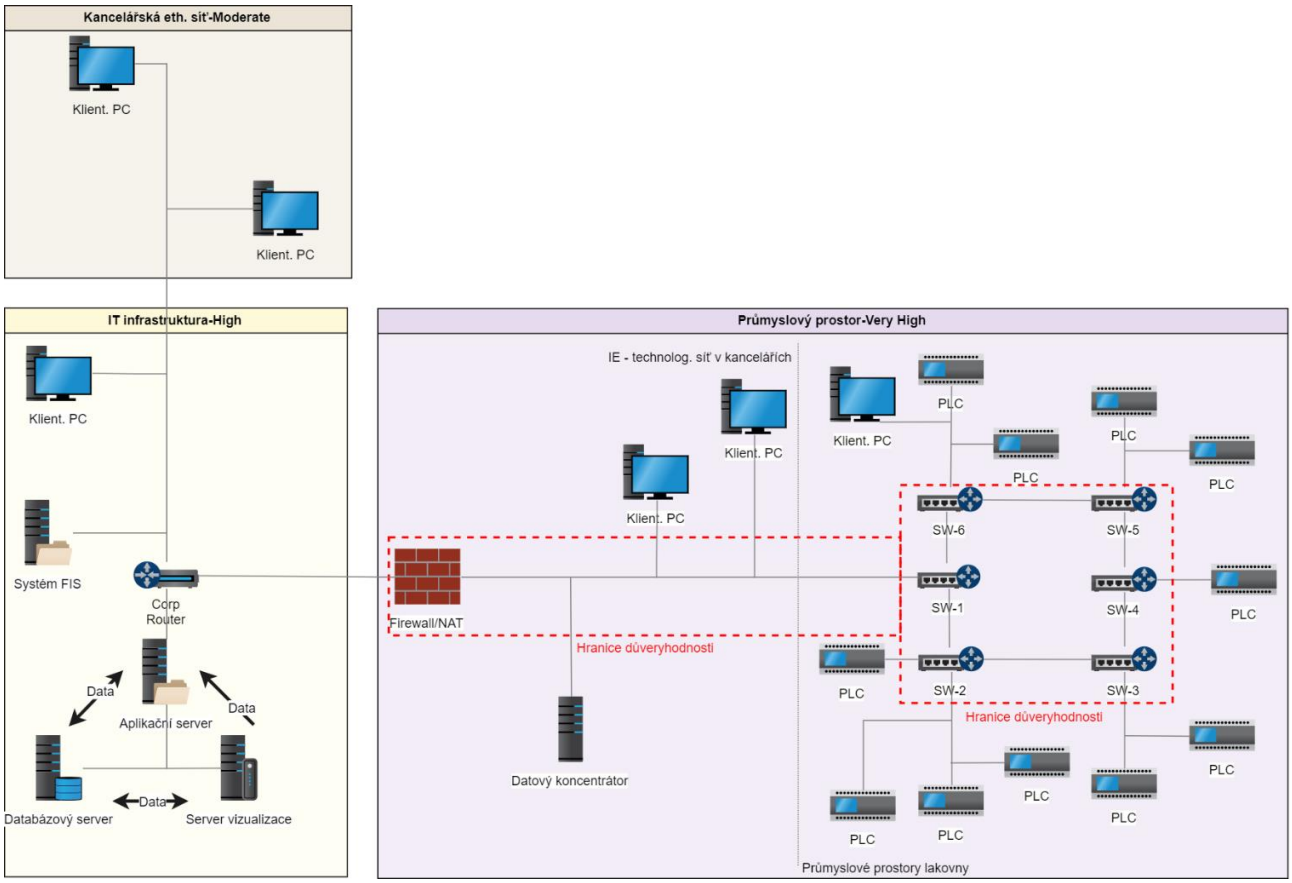


Obrázek 6 Vztahy mezi objekty bezpečnosti

3.3 Identifikace fyzických a logických aktiv

Identifikace aktiv a charakterizace systému se provádí pomocí konceptu zón. Tento přístup umožňuje podívat se na architekturu sítě a vytvořit zónu perimetru zvanou „hranice důvěryhodnosti“. [27] Obrázek 7 zobrazuje hranice důvěrnosti ve vybraném provozu Škoda Auto. Schéma obsahuje v zásadě pět typů aktiv – firewall, datový

koncentrátor, klientské PC, PLC a síťové přepínače. Tyto vstupní body mohou být použity jako útočné vektory od potenciálních útočníků. Je nutné také zjistit, zda aktivum nemá skrytý útočný vektor (např. vestavěné bezdrátové funkce 802.11, Bluetooth apod.). Tabulka 2 identifikuje fyzické vstupní body a jejich přidružená aktiva.



Obrázek 7 Hranice důvěrnosti ve vybraném provozu Škoda Auto

Název vstupního bodu	Popis vstupního bodu	Tok dat spojeným se vstupním bodem	Přidružená aktiva se vstupním bodem
Firewall	Interní Firewall mezi průmyslovou sítí a IT infrastrukturou	OPC Server	PLC
		Vizualizační server	PLC, Klientské PC
		AD ověření	Klientské PC
		Datový koncentrátor	PLC
		DHCP server	Klientské PC, PLC
Klávesnice	Klávesnice	Vstup z klávesnice	Klient. PC, Datový koncentrátor
CD/DVD mechanika	CD/DVD mechanika	Datové soubory	Klient. PC
		Software	
USB port	USB port	Datové soubory	Klient. PC, Datový koncentrátor
		Software	
Bezdrátová technologie	802.11/Bluetooth		Klient. PC
LAN	Konektor RJ-45		Switch, Klient. PC, Datový koncentrátor, PLC
Modbus	Modbus port na PLC zařízeních	Modbus TCP	PLC

Tabulka 2 Identifikace vstupních bodů – fyzický přístup

Jiný pohled na aktiva je z hlediska logického přístupu (tabulka 3). Většina bezpečnostních kontrol chrání především logická aktiva spíše než fyzická. Je například dobré zvážit instalaci antivirových programů, které zabrání neoprávněnému spuštění škodlivého kódu.

Fyzické aktivum	Logické aktivum	Hrozba logickému aktivu
Firewall	Konfigurace	Změna konfigurace vede ke změně chování Firewallu
	Logy	Úprava logů pro vyhnutí se auditu logů
	Firmware	Modifikace firmwaru vede ke změně chování Firewallu
	Správa portů	Modifikace firmware, modifikace konfigurace
	Komunikační rozhraní	Denial-Of-Service útok
	Autentizační služby	Zvýšení oprávnění útočníka (Elevation of privilege)
Switch	Konfigurace	Změna konfigurace vede ke změně chování Switche
	Porty	DoS, Zvýšení oprávnění útočníka, Vložení malwaru (malware injection)
PLC	Modbus rozhraní	DoS
	Ethernet rozhraní	DoS, Vložení malwaru (malware injection)
Klientské PC	Windows OS	DoS, Zvýšení oprávnění útočníka
	Uložené soubory	Kopie citlivých dat, Změna nebo odstranění dat
	Aplikace pro dohled a konfigurace	Změny uložených konfigurací, Posílání příkazů na PLC, Změna běžící konfigurace
	Ethernet rozhraní	DoS, Vložení malwaru (malware injection), Získání

Fyzické aktivum	Logické aktivum	Hrozba logickému aktivu
		vzdáleného přístupu
	Klávesnice	DoS, Zvýšení oprávnění útočníka, Změna všeho
	CD/DVD mechanika	Vložení malwaru (malware injection), Kopie citlivých dat
	USB porty	Vložení malwaru (malware injection), Kopie citlivých dat
	Bezdrátové technologie	DoS, Zvýšení oprávnění útočníka, Vložení malwaru (malware injection)
Datový koncentrátor	Linux OS	DoS, Zvýšení oprávnění útočníka
	Uložené soubory	Kopie citlivých dat, Změna nebo odstranění dat
	Ethernet rozhraní	DoS, Vložení malwaru (malware injection), Získání vzdáleného přístupu
	Log soubory	Úprava logů pro vyhnutí se auditu logů
	Konfigurace	Změna konfigurace vede ke změně chování Datového koncentrátoru

Tabulka 3 Identifikace vstupních bodů – logický přístup

3.4 Sběr dat

Dokumentace aktiv je ověřována pomocí různých metod sběru dat. U hodnoceného systému bude snazší identifikovat kritické fyzická a logická aktiva, která tvoří základ softwarového a hardwarového vybavení sítě. Metody sběru dat nejenom ověřují a aktualizují existující inventář aktiv, ale hlavně mohou odhalit skrytá a nezdokumentovaná zařízení a přístroje, které by mohly významně zvyšovat riziko útoku (resp. zvýšit počet útočných vektorů). Online sběr dat poskytuje schopnost přesně identifikovat všechny otevřené komunikační porty, spuštěné aplikace a služby na konkrétním přístroji. Tyto informace se později používají k vyhodnocení potenciálních útočných vektorů v systému. [2]

Existuje celá řada skenovacích komerčních i nástrojů s otevřeným zdrojovým kódem. Tyto nástroje však mohou mít kritické účinky na fungování sítě jako takové, takže by se neměly používat bez rozsáhlé přípravy „offline“ testování pro zjištění, jakým způsobem samotný sběr dat ovlivní síť jako takovou. V tomto ohledu jsou nejnebezpečnější nástroje ty, které provádí aktivní sběr dat dotazováním – měly by být používány pouze pokud je síť v offline režimu (např. při plánované odstávce výroby). [2]

Základní typy skenerů jsou určeny k identifikaci zařízení, identifikaci konkrétních aplikací a komunikaci určitých služeb dostupných na těchto zařízení. Jedním z nejoblíbenějších mapovačů je nmap, který je k dispozici pro většinu operačních systémů. Tento nástroj je s otevřeným zdrojovým kódem a zahrnuje detekce hostitelských služeb, detekce operačních systémů, spoofing, vyhledávání hostitelů apod. a má navíc schopnost spouštět vlastní scripty pomocí Nmap Scripting Engine (NSE). [28] Nástroj nmap provádí veškerý sběr dat prostřednictvím síťové externí injekce paketů a následné analýzy. Tento nástroj je realistickou reprezentací toho, jak útočník provádí skenování v síti, avšak není ideálním nástroje pro identifikaci systémových aktiv.

Pasivním a „přátelským“ (ve smyslu, že neohrožuje časově citlivou komunikaci mezi komponenty sítě) nástrojem je Network statistics neboli netstat. Užitečnost tohoto

nástroje vychází ve schopnosti zobrazit počet síťových funkcí založených na hostiteli včetně aktivních a naslouchajících síťových připojení, mapování aplikací a přidružených služeb, identifikaci aktivních relací vzdálených hostitelů a služeb, které tyto hostitelé používají (toto je obzvlášť důležitá informace při mapování toku dat v síti). [29]

3.5 Skenery zranitelnosti

Tyto skenery tvoří další typ běžně používaného vybavení pro zvýšení zabezpečení sítě. Existuje taktéž celá řada komerčních (Tenable Nessus, Core Impact) i nástrojů s otevřeným zdrojovým kódem (OpenVAS). Tyto nástroje se specializují na identifikaci zranitelných míst, které porovnávají vůči své databázi zranitelností. Je tedy možné, že schopnost detekovat zranitelnosti se může u jednotlivých nástrojů značně lišit. [44] Zranitelnost není jen přítomnost neopatchovaného softwaru, ale také použití zbytečných aplikací a služeb, které nelze zjistit pouhým skenováním, nesprávné ověření, špatné řízení přístupu, nekonzistentní dokumentace apod. Fáze hodnocení závisí do značné míry na automatizovaném skenování zranitelnosti softwaru – kontrola aplikace, hostitele, konfigurace sítě. [45]

Skener zranitelnosti ve vybraném provozu Škoda auto má za cíl identifikovat „backdoory“ a bezpečnostní „díry“, které existují v průmyslové síti. Zařízení, které má malé nebo žádné bezpečnostní prvky je náchylné na útok a mělo by být umístěné samostatně ve zvláštních bezpečnostních zónách. Tabulka 4 obsahuje seznam chyb zabezpečení, které může útočník zneužít ke svému dosažení cíle.

Kategorie	**Zranitelnost**
Síť	Špatná správa konfigurace
	Chyby konfigurace
	Špatná fyzické zabezpečení
	Nedostatečná bezpečnost portů
	Nepotřebná pravidla brány Firewall
	Žádná schopnost detekovat narušení
Konfigurace	Špatná správa účtů
	Špatné zásady pro hesla
	Žádný systém správy záplat
	Špatně nakonfigurovaný whitelist aplikací
Embedded zařízení	Špatná správa konfigurace
	Chyby konfigurace
	Špatné fyzické zabezpečení
	Použití zranitelných protokolů
Bezpečnostní politika	Nedostatečné bezpečnostní povědomí
	Nedostatečná kontrola přístupu
	Nedostatečná fyzická kontrola
	Citlivost na útoky sociálního inženýrství

Tabulka 4 Chyby zabezpečení

3.6 Skenery síťového provozu sítě

Dalším typem skeneru, který se běžně používá pro zvýšení zabezpečení sítě jsou skenery síťového provozu. Tyto nástroje jsou určeny pro sběr surových síťových paketů, aby mohly být poskytnuty pro následnou analýzu, která zahrnuje identifikaci hostitele a datových toků, mohou být také použity pro vytvoření sady pravidel pro firewall. Nejznámějším nástrojem pro sběr je tcpdump pro Unixové systémy a windump pro Windows. Výše zmíněné nástroje opravdu pouze zachycují pakety a pro analýzu se používají jiné – nejznámější je Wireshark, který obsahuje GUI a je na něm tudíž analýza mnohem pohodlnější. Wireshark využívá protokol „disektorů“, takže protokoly používané v různých vrstvách ISO/OSI modelu lze rozdělit a prezentovat samostatně, což umožňuje rozebrat konkrétní podrobnosti protokolu v každé vrstvě. [30]

3.7 Analýza toku dat

Síťový provoz dat se vyhodnocuje na základě společných charakteristik paketů. Za datový tok považujeme provoz, který sdílí určité společné vlastnosti a přesouvá se z jednoho hostitele na druhého. Tok, jako takový, se neukládá, ukládají se pouze metadata paketů. Analýza provozních toků (toků dat) je založena na skupině protokolů, které umožňují implementovat procesy generování, přenosu, ukládání a předzpracování metadat. Existují dva protokoly, které představují dva různé přístupy k implementaci analýzy toku provoz – NetFlow a sFlow.

3.8 Zdroje hrozeb

Mnoho vyvíjených metodik pro kybernetickou bezpečnost vychází z předpokladu, že největší zdroje hrozeb se nacházejí mimo organizaci. To vede společnosti k nasazení specifických bezpečnostních kontrol, které by měly zabránit těmto externím hrozbám. Dokumentované zprávy o bezpečnostních incidentech z několika zdrojů nicméně hovoří o tom, že většina incidentů měla původ v interním zdroji. Původ zdroje se rozlišuje na 4 různé typy: [31] [32]

- záměrný útočník z venku,
- náhodný útočník z venku,
- záměrný útočník zevnitř,
- náhodný útočník zevnitř.

3.9 Událost ohrožení

Neboli „threat event“ představuje podrobnosti o útoku, který provedl konkrétní zdroj hrozby. Níže tabulka číslo 5 ukazuje nejčastější události ohrožení ve vybraném průmyslovém provozu Škoda Auto.

Událost ohrožení
Provádění skenování/průzkumu sítě
Dodání škodlivého kódu do systému
Zaměstnanec s nekalými úmysly
Využití fyzického přístupu k zařízením organizace
Využití špatně nakonfigurované sítě
Využití známých chyb v zabezpečení

Využití nedávno objevených zranitelných míst
Prováděné útoky pomocí neautorizovaných portů, služeb a protokolů
Provedení DoS útoků
Provedení fyzických útoků na organizační zařízení
Provedení fyzických útoků na infrastrukturu
Útok na změnu síťového provozu
Útok typu man-in-the-middle
Útok s využitím sociálního inženýrství ve snaze získat informace
Získání neoprávněného přístupu
Útoky v dodavatelském řetězci
Způsobení zhoršení služeb
Způsobení ztráty integrity
Získání citlivých informací pomocí exfiltrace (vývoz dat)
VLAN hopping, MAC flooding, ARP spoofing
Koordinované útoky pomocí vnějších a vnitřních zdrojů hrozeb
Zavedení a využití zranitelností v SW produktech

Tabulka 5 Seznam událostí ohrožení

3.10 Modely hrozeb

Pro analýzu průmyslové sítě Škoda Auto jsem si vybral dva modely hrozeb, které se používají nejčastěji. Každý z nich na hrozby nahlíží svým způsobem a vzájemně se doplňují. Pro co nejbližší pochopení hrozeb je nutné používat tyto modely současně, protože složitost tohoto problému je značná a není možné na ní pohlížet pouze z jedné strany.

3.10.1 DREAD Model

DREAD model vyvinutý firmou Microsoft je nyní jedna z nejpopulárnějších technik, jak čelit stále rostoucím rizikům spojeným s bezpečnostními hrozbami. Tato technika by se dala definovat jako kvalitativní model rizik, který se skládá z pěti hodnocení:

- **Damage** (poškození) – toto hodnocení se zabývá otázkou „jak špatné?“, respektive „jak špatný by mohl útok být?“.
- **Reproducibility** (reprodukovatelnost) – ptá se „jak často se uvedená událost může vyskytnout?“ Případně „jak je tato hrozba všudypřítomná?“.
- **Exploitability** (využitelnost) – pokládá otázku „Kolik práce stojí zahájit útok?“ případně „Jak jsme zranitelní vůči tomuto útoku?“.
- **Affected Users** (postižení uživatelé) – otázka zní „Kolik lidí bude útokem ovlivněno?“, resp. „Kolik lidí se této událost dotkne?“.
- **Discoverability** (zjistitelnost) – ptá se „Jak snadné je odhalit hrozbu?“ Případně „jak snadné je odhalit zranitelnost?“. [46]

Bodová škála těchto hodnocení se pohybuje od 1 (Nízká) do 3 (Vysoká). Níže tabulka číslo 6 s jednotlivými hodnocení a jejich bodování pro analyzovanou průmyslovou síť.

Hrozba	**D**	**R**	**E**	**A**	**D**	**Skóre**
Sniffing	1	3	3	1	2	10
MITM	2	1	2	2	1	8
DoS	3	2	3	3	1	12
Exfiltrace DAT	1	2	2	1	1	7
Malware	2	1	1	2	1	7
Cryptojacking	2	3	2	1	1	9
Rootkity	2	1	1	2	3	9

Tabulka 6 Kvalitativní model hodnocení rizik DREAD

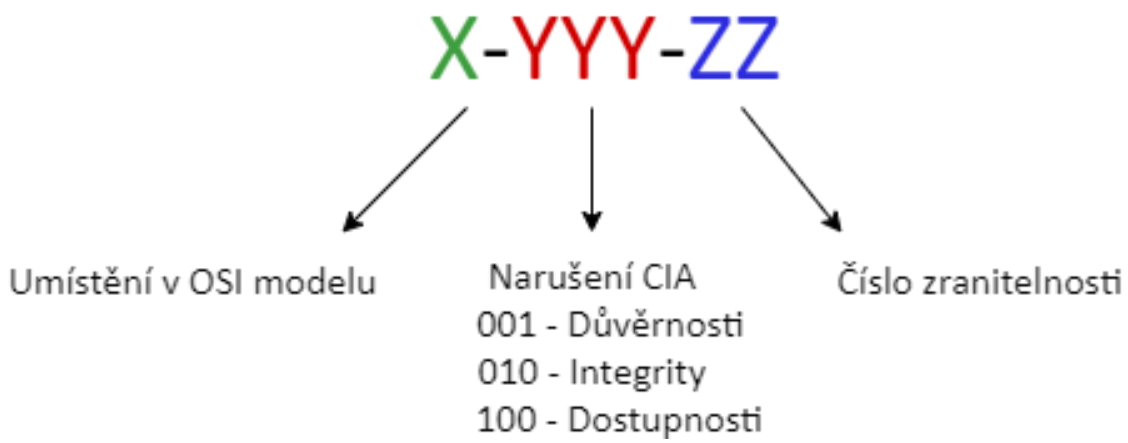
3.10.2 STRIDE Model

Jiný přístup využívá model hrozeb zvaný STRIDE model. Je to v podstatě odpověď na otázku „Co se může v tomto systému pokazit?“. Model je rozdělený do 6 hlavních typů hrozeb [33]. Vytvořená mind mapa (obrázek 8) zobrazuje STRIDE model pro vybranou průmyslovou síť Škoda Auto.

Obrázek 8 STRIDE analýza hrozeb

3.11 Analýza zranitelností dle OSI modelu

Vzhledem ke komplexitě a velkého množství zranitelností v infrastruktuře průmyslové sítě Škody Auto jsem zvolil rozdělení těchto zranitelností podle referenčního ISO modelu, který síť dělí do sedmi vrstev. Dále jsem vytvořil klasifikaci (viz obrázek 9), podle které jsou jednotlivé zranitelnosti zařazovány.



Obrázek 9 Klasifikace zranitelností

V následujících podkapitolách se podrobně věnuji jednotlivým zranitelnostem vyskytující se v konkrétním provozu Škoda Auto a klasifikuji je do tříd. Každá zranitelnost v následujících tabulkách má odkaz na konkrétní protiopatření, které zranitelnosti odstraňují, snižují riziko využití, případně upozorní na skutečnost, že se útočník snaží zranitelnost využít k útoku na průmyslovou síť.

3.11.1 Fyzická vrstva

Vrstva 1 se týká fyzického aspektu sítí – jinými slovy kabeláže a infrastruktury používané pro komunikaci sítí. V Tabulce 7 se zabývám nejčastějšími zranitelnostmi na fyzické vrstvě.

Třída	Název zranitelnosti	Popis zranitelnosti	Protiopatření
1-100-01	Fyzické útok na zařízení	Fyzické poškození nebo zničení HW.	4.1 Fyzická ochrana sítě
1-100-02	Fyzický útok na médium	Fyzické poškození nebo zničení média.	4.1 Fyzická ochrana sítě
1-100-03	Přerušení napájení	Přerušení napájení HW.	4.1 Fyzická ochrana sítě
1-001-04	Fyzická krádež dat	Krádež nosičů dat.	4.1 Fyzická ochrana sítě
1-101-05	Fyzická krádež HW	Krádež HW.	4.1 Fyzická ochrana sítě
1-100-06	Odpojení fyzických datových spojení	Rozpojení datového spojení.	4.1 Fyzická ochrana sítě
1-001-07	Nezjistitelné zachycování dat	Odposlechy média.	4.1 Fyzická ochrana sítě
1-001-08	Keystroke logger a jiné zachycování vstupu	Zachytávání vstupu z klávesnice, případně nahrávání obrazovky apod.	4.1 Fyzická ochrana sítě

Tabulka 7 Seznam zranitelností na 1. vrstvě OSI

3.11.2 Spojová vrstva

Spojová vrstva neboli vrstva datového spojení, zabývající se logickým přenosem mezi dvěma přímo připojenými uzly sítě. Tabulka číslo 8 obsahuje nejčastější zranitelnosti na linkové vrstvě. Jako protiopatření jsou zde uvedené odkazy na kapitolu 4. Zabezpečení a ochrana sítě, ve které popisuji konkrétní nasazení bezpečnostních politik a nástrojů.

Třída	Název zranitelnosti	Popis zranitelnosti	Protiopatření
2-001-09	ARP poisoning	Umožní útočníkovi vydávat se v síti za jiné zařízení.	4.2.1 Použití statických ARP a 4.2.2 Nasazení monitorovacího programu ARP watch
2-001-10	MAC spoofing	Umožní útočníkovi vydávat se v síti za jiné zařízení.	4.2.3 Použití protokolu 802.1X a 4.2.4 Port security
2-001-11	MAC flooding	Vynutí posílání citlivých informací do částí jiné části sítě.	4.2.3 Použití protokolu 802.1X a 4.2.4 Port security
2-001-12	STP útok	Spanning tree útok, umožní útočníkovi vložení dalšího switche do sítě.	4.2.4 Port security
2-001-13	Přetečení CAM tabulky	Donutí přepínače chovat se jako rozbočovač, dojde k úniku citlivých informací.	4.2.4 Port security
2-001-14	VLAN hopping – Switch spoofing	Útočník imituje trunkovací Switch, dostane se k více VLAN sítím.	4.2.5 Nastavení ostatních portů přepínače do přístupového módu
2-011-15	VLAN hopping – Double tagging	Útočník mění 802.1Q tagovací hlavičku.	4.2.6 Zamezení použití výchozí VLAN 1 sítě
2-001-16	Port stealing	Odcizení portu a únos komunikace.	4.2.4 Port security

Tabulka 8 Seznam zranitelností na 2. vrstvě OSI

3.11.3 Síťová vrstva

Síťová vrstva se stará primárně o směrování v síti a síťové adresování. Propojuje systémy a sítě, které spolu přímo nesousedí. Tabulka číslo 9 vyjmenovává tyto útoky a klasifikuje je do tříd.

Třída	Název zranitelnosti	Popis zranitelnosti	Protiopatření
3-111-17	IP adress spoofing	Vytvoření paketu s falešnou zdrojovou IP adresou.	4.2.3 Použití protokolu 802.1X
3-100-18	Ping flood	Zahlcení ICMP echo pakety.	4.3.1 Filtrování paketů
3-001-19	Network scanning	Pasivní útok mající za úkol získat informace o síti a zařízeních v něm.	4.3.1 Filtrování paketů a 4.3.2 Použití VPN tunelů
3-100-20	Smurf Attack	Zahlcení ICMP pakety.	4.3.1 Filtrování paketů
3-100-21	Teardrop Attack	Zahlcený fragmentovanými pakety.	4.3.1 Filtrování paketů
3-001-22	Packet Sniffing	Pasivní útok mající za úkol získat informace o síti a zařízeních v něm.	4.3.2Použití VPN tunelů
3-100-23	Ping of death	Zaslání velkého paketu.	4.3.1 Filtrování paketů

Tabulka 9 Seznam zranitelností na 3. vrstvě OSI

3.11.4 Transportní vrstva

Umožňuje adresovat data přímo mezi jednotlivými aplikacemi pomocí portu, které v kombinaci s IP adresou dopravují data k dané aplikaci. V tabulce 10 nalezneme jednotlivé zranitelnosti, jejich klasifikaci a odkaz na protiopatření.

Třída	Název zranitelnosti	Popis zranitelnosti	Protiopatření
4-100-24	SYN flooding	Útočník posílá posloupnost paketů SYN, ale pak už neodpovídá.	4.4.1 Zvýšení fronty nevyřízených požadavků a 4.4.2 Uzavření nejstaršího polootevřeného spojení
4-001-25	Port knocking	Útočník skenuje, jaké porty jsou otevřené.	4.3.1 Filtrování paketů
4-011-26	TCP Session Hijacking	Útočník získá kontrola nad relací.	4.3.2 Použití VPN tunelů
4-011-27	TCP sequence prediction	Útočník se snaží uhodnout sekvenční číslo, které má hostitel použít.	4.3.2 Použití VPN tunelů
4-110-28	TCP veto	Útočník odposlouchává a předpovídá velikost dalšího pakety, aby legitimní paket cíl označil jako duplikát	4.3.2 Použití VPN tunelů

Tabulka 10 Seznam zranitelností na 4. vrstvě OSI

3.11.5 Relační, Prezentační a aplikační vrstvy

Vzhledem k velkému množství používaných služeb na síti uvádím, že se v bakalářské práci zabývám pouze útoky na první, druhou, třetí a čtvrté vrstvě ISO modelu.

4. Zabezpečení a ochrana sítě

V následující kapitole se zabývám konkrétními opatřeními, které buď určitou zranitelnost, analyzovanou v předchozí kapitole, zcela vyloučí, případně zmenší riziko napadení či rozsah dopadů. Navrhuji využívání konkrétního softwaru, případně konkrétní úpravu konfigurace přepínače.

4.1 Fyzická ochrana sítě

V této podkapitole zkoumám způsoby, jakým způsobem bránit fyzickou vrstvu před napadením. Fyzická ochrana je nejdůležitějším bodem pro snížení rizika napadení sítě fyzických způsobem. Bezpečnostní kontroly, které snižují riziko napadení sítě na první úrovni ISO modelu zahrnují následující tři metody, které by měly být použity:

- Metody pro odrazení vetřelců mohou zahrnovat bezpečnostní osvětlení, výstražné cedule apod.
- Ke zpoždění vetřelců se používají různé fyzické překážky, jako jsou ploty, brány, zámky apod. Tyto překážky mohou mít také částečně odrazující účinek.
- Detekce útočníků – používají se typicky systému detekce narušení a poplachy.

Fyzická bezpečnost je vnímána odlišně od kontrol a zranitelností ve vyšších vrstvách OSI modelu. Fyzická bezpečnost se totiž především zaměřuje na vetřelce, vandaly a zloděje.

Taktéž jako v síťovém světě se i ve fyzickém světě nejlépe osvědčil tzv. model hloubkové ochrany (defense-in-depth model), na rozdíl od jedné silné obranné linie. Ten spočívá v tom, že obrana je stavěná na více redundantních obranných opatření, pokud tedy útočník prorazí jednou obranou (např. díky nějaké specifické zranitelnosti), je před něj kladen další obranný val. [49]

4.1.1 Ochrana perimetru

První ochrana je na hraně perimetru a zabraňuje tak neoprávněnému vstupu. Pro ochranu perimetru lze typicky použít následující opatření:

- přírodní překážky,
- ploty a zdi,
- vnější stěny budov.

Pro další zvýšení bezpečnosti mohou být použity následující mechanismy:

- systémy detekce vniknutí,
- bezpečnostní osvětlení,
- bezpečnostní stráže,
- výstražné značky a upozornění.

4.1.2 Ochrana závodu

Je nezbytné poskytovat pouze minimální množství požadovaného přístupu do oblastí a dbát na zákazy vstupu neoprávněných osob. Níže uvádím několik způsobů, které lze využít pro zvýšení fyzické ochrany vstupu do závodu:

- okna,
- dveře,
- zdi,
- řízení přístupu (přístupové kontroly),
- detekce narušení.

Řízení přístupu je mechanismus, kterým je jednotlivci udělen nebo odepřen přístup do konkrétní části budovy. Tento mechanismus mimo jiné zajišťují především zámky (ať již mechanické, či elektronické).

4.1.3 Vstupní body

Vstupní body jsou ty části budov, ze kterých se může útočník dostat dovnitř. Ty jsou typicky následující:

- dveře pro přístup personálu,
- průmyslové, bezpečnostní dveře,
- přístupy pro vozidla,
- okna,
- střešní okna.

4.1.4 Fyzické kontroly

Pro další zvýšení bezpečnosti můžeme využít fyzických kontrol, níže uvádím nejčastější příklady těchto fyzických kontrol:

- identifikační bezkontaktní čipové (RFID) karty,
- dohledový kamerový systém,
- pohybové a tepelné poplašné senzory,
- biometrické kontroly (otisky prstů, rozpoznávání obličeje apod.). [34]

4.2 Ochrana linkové vrstvy

Jedná o ochranu na úrovní rámců, které působí jako spojení mezi síťovou vrstvou (pakety s IP adresami) a fyzickou vrstvou (v našem případě elektrickými signály). Přepínače jsou nejdůležitějším zařízením pracující na této vrstvě, proto se bude následující doporučení především týkat konfigurace jejich rozhraní.

Dalším důležitým aspektem této vrstvy je správná konfigurace. VLAN sítě mají klíčovou roli v zabezpečení systémů, neboť přispívají k oddělení provozu a segmentaci sítě.

4.2.1 Použití statických ARP

Protokol ARP umožňuje definovat statický záznam ARP a může být nakonfigurován tak, aby ignoroval všechny pakety s automatickou odpovědí ARP. Nevýhodou této metody může být, že je obtížné ji udržovat ve velkých podnikových sítích, neboť mapování IP / MAC adres musí být dynamicky prováděno u všech zařízení v sítí. Pro účely nasazení do průmyslové sítě (která je v podstatě statická na rozdíl od sítě podnikové) toto řešení doporučuji.

4.2.2 Nasazení monitorovacího programu ARP watch

Pro detekci ARP poisoningu doporučuji nasazení nástroje ARP watch. Tento nástroj s otevřeným zdrojovým kódem umožňuje monitorovat aktivitu v Ethernetové síti a udržuje databázi párování MAC adres – IP adres. Tyto dvojice opatřuje časovým razítkem, které umožní lépe analyzovat aktivitu v průmyslové síti. [35]

4.2.3 Použití protokolu 802.1X

Používání tohoto protokolu je doporučováno samotnými výrobci používaných přepínačů v průmyslové síti Škoda Auto. Pokud se klient připojí do sítě, bude od něj vyžadována autentizace a do té doby, než se klient úspěšně neautentizuje, veškerá datová komunikace z jeho strany bude blokována přepínačem. Níže uvádím podkapitolu věnující se nutné podmínce pro úspěšné nasazení 802.1X.

4.2.3.1 AAA protokol – RADIUS

Protokol 802.1X vyžaduje pro svoje nasazení formu autentizace, a proto je nutné zajistit AAA protokol, který by autentizaci prováděl.

4.2.4 Port security

Pro zvýšení bezpečnosti v průmyslové síti Škoda Auto doporučuji zaměřit se mimo jiné na problematiku zabezpečení portů na samotných přepínačích. Síťové přepínače by měly mít povolený omezený počet MAC adresy, které lze zjistit na portech připojených ke koncových stanicích.

Tato metoda funguje tak, že síťový přepínač kontroluje MAC adresu na příchozích rámcích a pokud je zdrojová MAC adresa odlišná od povolené, přepínač buď tento rámec zahodí případně vypne port.

4.2.5 Nastavení ostatních portů přepínače do přístupového módu

Pro všechny porty, které jsou připojené ke koncovým zařízením doporučuji napevno nastavit port do přístupového módu (tzv. access mode). V tomto módu nebude možné pro útočníka imitovat „trunkový“ přepínač a tím se dostat ke komunikaci na více VLAN sítí.

4.2.6 Zamezení použití výchozí VLAN 1 sítě

Klíčový nástroj pro útok VLAN hopping – Double tagging je využití nativní sítě VLAN. Protože VLAN 1 je výchozí VLAN pro přístupové porty a výchozí nativní VLAN je „trunkovací“, je to pro útočníka snadný cíl. Protiopatření spočívá v tom, že se odeberou přístupové body z výchozí VLAN 1.

4.3 Ochrana síťové vrstvy

Tato vrstva pracuje s IP protokolem, který je zodpovědný za směrování paketů ze zdrojového hostitele do cílového hostitele přes jednu nebo více IP sítí. IP doručování paketů poskytuje nespolehlivou službu. Spolehlivost doručení zaručuje vyšší vrstva zvaná TCP.

Na této vrstvě budeme pracovat především s routery a L3 přepínači, které se používají v průmyslové síti Škoda Auto. Dalším významným bezpečnostním prvkem

pracující (mimo jiné) na této úrovni je Firewall, který bude také součást návrhu zabezpečení sítě.

4.3.1 Filtrování paketů

Filtrování paketů je technika brány firewall, která slouží k řízení přístupu k síti sledováním odchozích a příchozích paketů a umožňuje na základě zdrojové a cílové adres a portů internetového protokolu tyto pakety zastavovat nebo předávat dále.

4.3.2 Použití VPN tunelů

Mezi jednotlivými bezpečnostními zónami (viz kapitola 4.5.1 Návrh architektury sítě) je vhodné použít vyhrazené virtuální sítě VPN. Jedná se tedy o tunelové spojení dvou sítí (resp. dvou bezpečnostních zón).

4.4 Ochrana transportní vrstvy

Hlavním úkolem této vrstvy je zajišťování přenosu dat mezi koncovými uzly. Musí poskytovat takovou kvalitu přenosu, jakou požadují vyšší vrstvy OSI modelu. Vznikla řada odlišných transportních protokolů s rozdílnými vlastnostmi, protože různé aplikace vyšších vrstev mají na kvalitu přenosu různé požadavky. Ve vybrané průmyslové síti Škoda Auto jsou používány dva druhy nejznámějších typů transportních protokolů, pro které budu v následujících podkapitolách navrhovat zabezpečení.

4.4.1 Zvýšení fronty nevyřízených požadavků

Jedna z reakcí na velké objemy SYN paketů je zvýšit maximální počet možných pootevřených spojení, které operační systém umožní. Aby bylo toto možné provést, je nutné, aby OS vyhradil další paměťové prostředky, aby se zabývaly všemi novými požadavky. Nicméně tato fronta SYN paketů opět může narazit na strop, který nebude schopná vyřídit. V určitých případech je nicméně toto lepší, než aby OS službu rovnou odmítl.

4.4.2 Uzavření nejstaršího polootevřeného spojení

Lze definovat strategie, která uzavře nejstarší polootevřené spojení, tak, že díky tomu se uvolní prostředky a bude možné nastávající žádosti o spojení začít vyřizovat. Opět je toto řešení pouze částečné, protože pokud útočník zvětší objem útoku, problém zůstane stejný.

4.5 Obecná ochrana sítě

Následující doporučení, které mám pro průmyslovou síť Škody Auto není neřeší konkrétní zranitelnost, ale jsou to návrhy, které obecně zvýší zabezpečení této sítě.

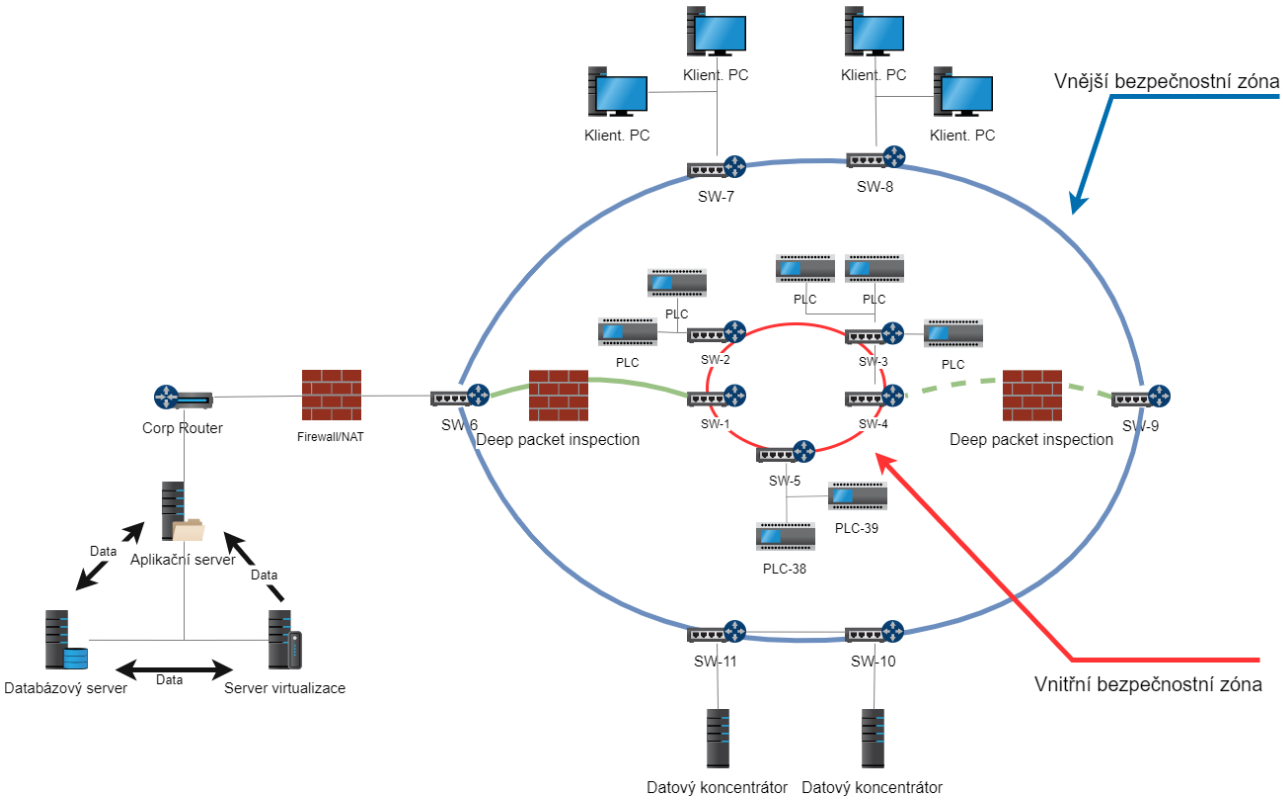
4.5.1 Návrh architektury sítě

Pro návrh architektury topologie sítě jsem využil koncept bezpečnostních zón, které mají velký vliv na bezpečnost průmyslové sítě. Logika tohoto konceptu je jednoduchá – izolováním aktiv do skupin a ovládáním veškerého komunikačního toku uvnitř a mezi skupiny se útočná plocha jakékoliv dané skupiny minimalizuje na tu svou skupinu. Bezpečnostní zóny se dají definovat z hlediska fyzického nebo logického. Fyzické zóny jsou definovány podle seskupení aktiv na základě jejich

fyzické polohy. Logické zóny jsou spíše virtuální v tom smyslu, že aktiva jsou seskupovány na základě konkrétní funkce nebo charakteristiky.

Pokud jsou tyto zóny správně implementovány, omezují digitální komunikaci tak, že každá zóny bude ze své podstaty bezpečnější. Poskytuje proto velmi stabilní základ, na kterém lze stavět a udržovat politiku kybernetické bezpečnosti a podporuje další známé zásady, jako je zásada nejmenšího oprávnění (ve které uživatelé mohou přistupovat pouze k systémům, ke kterým jsou oprávnění).

Následující topologie logických zón (obrázek číslo 10) je tedy mým návrhem pro vybranou průmyslovou síť Škoda Auto, která vychází ze současného stavu, která je vidět na Obrázek 7 Hranice důvěrnosti ve vybraném provozu Škoda Auto.



Obrázek 10 Návrh architektury sítě založené na bezpečnostních zónách

4.5.2 Patch management

Včasné nasazení aktualizací softwaru je zásadní pro udržení provozu nejen základních komponent jako jsou servery, pracovní stanice apod., ale také pro bezpečnostní technologie (aplikace, zařízení, firewall apod.), které jsou implementovány za účelem ochrany sítě. Správa oprav je tradičně definovaný do několika fázi jako je příprava, dodání, instalaci a validace.

Průmyslové sítě se sestávají z velkého počtu komponent včetně serverů, pracovních stanic, síťových zařízení, embedded zařízení, PLC a podobně. Každá z nich má CPU, která je schopná vykonávat kód, nějakou formu operačního systému a

místního úložiště. Z toho vyplývá, že každý z těchto zařízení má potenciál mít zranitelnosti, které musí být opraveny.

Lze síťovou infrastrukturu ohrozit prostřednictvím jedné zranitelnosti, a proto by měla být také síťová zařízení zahrnuta do správy oprav, stejně jaké servery, pracovní stanice apod.

Na rozdíl od klasických kancelářských sítí je na průmyslové sítě kladena vysoká úroveň dostupnosti (která je běžně 99,99 %, což znamená 15 minut nedostupnosti za rok), což znamená, že měsíční restarty vyžadovaný k aktivaci „hotfix“ oprav (jako známe z kancelářských sítí) jsou zde nepřijatelné. Ačkoliv dost často jsou průmyslové sítě vybaveny redundantními komponentami, celkový systém v tu dobu bude v neredundantní konfiguraci. V tento okamžik je také nutné brát do úvahy riziko výpadku výroby v důsledku známé hrozby (což v tomto případě představuje systém, pracující bez redundance) nebo neznámé hrozby (kybernetická událost vzniklá z neopatchovaného systému).

Je nutné dodržovat především komplexní testování před nasazením samotného patche, protože aktualizace mohou mít nepříznivý dotaz na opravovanou součást.

4.5.2.1 Common Vulnerabilities and Exposures (CVE)

Jsou otevřené, volně dostupné databáze, které poskytují zveřejněné zranitelnosti v oblasti kybernetické kriminality. Cílem těchto databází je usnadnit sdílení informací o zranitelnost, které by mohly být využity pro vedení útoku. Každý záznam musí obsahovat minimálně jeden odkaz na uvedenou zranitelnost. Pro Siemens řadu síťových přepínačů používaných ve vybraném provozu Škoda auto se od roku 2018 v této databázi (resp. v databázi NVD) objevilo celkem 24 případů zranitelnosti. Samotná firma Siemens k těmto zranitelnost vydává stanovisko, ve kterém blíže popisuje, klasifikuje riziko a dále provádí doporučení pro jeho mitigaci. Aktualizaci firmwaru, ve kterém reaguje na tyto zranitelnosti firma Siemens, vydává zhruba jednou ročně – od roku 2018 vydala novou verzi firmwaru celkem třikrát.

5. Detekce událostí a monitorování sítě

Monitorování sítě a následná analýza síťové provozu je kriticky nezbytná součást provozování sítě. Monitoringem sítě se zabývají systémy zvané „Intrusion Detection System“ (IDS), resp. „Intrusion Prevention System“ (IPS), které mají za úkol provoz analyzovat a pomocí statistických či deterministických metod odhalovat potenciální hrozby v síti. „Intrusion Prevention System“ se navíc snaží těmto útokům aktivně zabraňovat. V následující kapitole se zabývám analýzami a konkrétními nástroji pro detekci událostí, které mohou být použity ve vybrané části Škoda Auto.

5.1 Zachytávání a analýza paketů

Zachycení paketů je proces, při kterém se zachycená data (tj. data, která reálně prošla sledovacím médiem) lokálně nebo vzdáleně ukládají, často ve formátu PCAP. Uložená data se následně analyzují buď ručně nebo automatizovaně. Pokud data analyzujeme automatizovaně, může to být poměrně výpočetně náročné, zejména v těch případech, kdy k detekčnímu systému IDS napojíme modul „Deep Packet Inspection“, který zkoumá data na všech vrstvách ISO/OSI modelu a podrobuje je často i různým statistickým testům. V případě ruční analýzy lze využít i další nástroje, které nám výrazně usnadní tento typ práce. Tyto nástroje lze poté ovládat pomocí příkazové řádky (CLI) nebo prostřednictví grafického uživatelského rozhraní (GUI) [54][55]

Samotné zachycování všech paketů v síti se často provádí v režimu zrcadlení rozhraní (tzv. „port mirroring“). Zrcadlení portů kopíruje pakety vstupující nebo vystupující z určitého rozhraní na jiné, které následně odesílá tento datový provoz na server (případně do klientského PC), kde je následně ručně nebo automatizovaně analyzován. Kopie datového toku lze zasílat z více rozhraní – zde je nutné si dát pozor na to, abychom nepřesáhli kapacitu výstupního rozhraní, případně nenarazili na výkonnostní strop samotného síťové prvku. [36]

5.1.1 TCPdump

Pomocí knihovny libcap je možné analyzovat data buď aktuálně přicházející ze sítě, případně uložená v souborech PCAP. TCPdump tuto knihovnu využívá a staví nad ní další vrstvu pro filtrování, což lze využít např. pro filtrování paketů se specifickou zdrojovou nebo cílovou adresou, číslem portů, protokolů třetí a čtvrté vrstvy OSI/ISO modelu apod. Pomocí logických operátorů lze tato pravidla různě kombinovat. Technologie zvaná „Berkeley Packet Filter“ (BPF) umožňuje pakety filtrovat podle definovaných pravidel ještě dříve, než se uloží. Není tedy nutné ukládat veškerou komunikaci, ale pouze tu, která je pro nás důležitá – tímto způsobem lze ušetřit značné množství HW prostředků zařízení. [37]

5.1.2 Wireshark

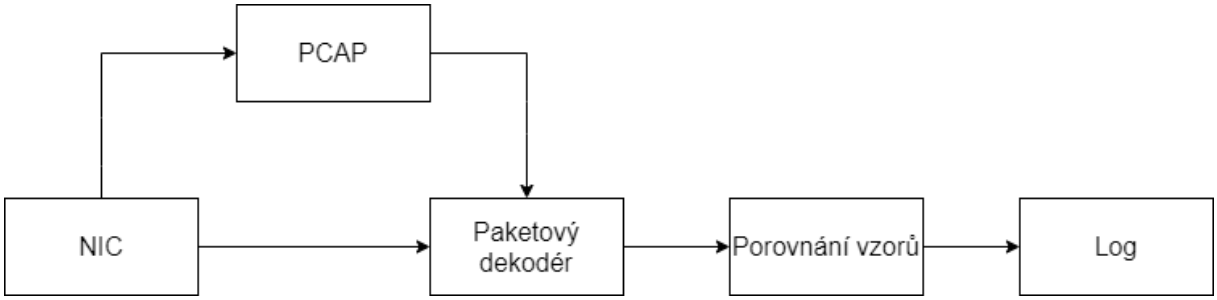
Tento grafický nástroj se příliš neliší od výše zmíněného TCPdumpu. Oba totiž dokážou využívat knihovnu „libcap“ pro zachycení „živého“ provozu nebo reprezentovat data uložená ve formátu PCAP. Hlavní rozdíl mezi těmito nástroji je v tom, že Wireshark se snaží poskytovat uživateli srozumitelnější a přehlednější reprezentaci dat na rozdíl od TCPdumpu, který vypisuje spíše strohá data paketů.

Data jsou ve Wiresharku zobrazována v nastavitelných oknech s barevně odlišenými pakety. Navíc, filtry, které lze použít pro zobrazení požadovaných dat, jsou pestřejší, takže s nimi lze dosáhnout lepšího zobrazení dat. Navíc poskytuje další možnosti statistické analýzy dat, tvorby grafů a vkládání volitelných pluginů a skriptů. [38]

5.1.3 Deep Packet Inspection (DPI)

„Deep Packet Inspection“ – neboli hloubková analýza paketů je pokročilá metoda umožňující vyhodnocení datové části a záhlaví jednotlivých paketů, které jsou přenášeny přes kontrolní bod hloubkové analýzy. Tato metoda je schopna na základě datového obsahu paketů lokalizovat, detekovat, kategorizovat, blokovat nebo přesměrovávat pakety na jiné místo určení. Existují typicky dva typy přístupu vytvoření filtrů, první je založená na porovnávání vzorů a druhá na analýze událostí. [23]

První typ analýzy je založen na porovnávání vzorů. To znamená, že DPI prochází celý síťový provoz a hledá známé sekvence bytů nebo shody regulárních výrazů. V rámci optimalizace může být hledání omezeno na konkrétní pakety nebo na její konkrétní části. Na obrázku číslo 11 je schematicky znázorněna metoda porovnávání vzorů. Tato metoda je poměrně populární, protože její výhodou je o něco jednodušší implementace. Tato výhoda se ovšem může změnit v nevýhodu, pokud chceme hledat vzory, které jsou obtížně popsatelné pomocí regulárních výrazů. [23] [57]

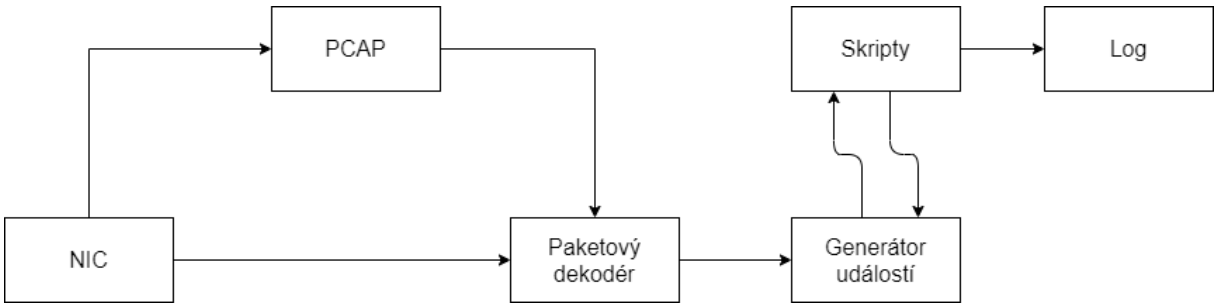


Obrázek 11 DPI – metoda porovnávání vzorů

Druhý typ analýzy je založen na analýze událostí. Ten částečně nahrazuje nedostatky první metody, protože pakety jsou zpracovávány do událostí (odchycený paket spustí generátor událostí), které jsou zase dále zpracovávány pomocí skriptů. Na obrázku 12 je zobrazeno schéma metody založené na analýze událostí.

Tyto skripty mohou být někdy velmi složité, čímž v podstatě přidávají novou vrstvu funkcionality do DPI systému. Algoritmy, které události zpracovávají mohou být dvojího typu – stavové a bezestavové. Stavové algoritmy jsou takové algoritmy, které využívají proměnných k uchování stavu objektu mezi jednotlivými událostmi.

Bezestavové algoritmy žádné proměnné nevyužívají, takže jejich reakce je pouze reakcí na určitou událost bez kontextu. [54] [57]



Obrázek 12 DPI – metoda analýza událostí

5.1.4 Suricata

Suricata je otevřený systém software určený pro detekci bezpečnostních hrozeb, který poskytuje možnosti monitorování zabezpečení sítě, a to včetně detekce narušení (IDS), prevence narušení (IPS) a „offline“ zpracování PCAP záchytů paketů. Tento program využívá hloubkovou analýzu paketů (DPI) porovnáním vzorů. Suricata je vícevláknová aplikace, což znamená, že může (na rozdíl od nejznámějšího nástroje Snort) zpracovávat více událostí současně, aniž by bylo nutné přerušovat další příchozí požadavky. Toto je velmi výhodné především pro analýzu komunikace probíhající v průmyslových sítích, kde je striktní požadavek, aby zpoždění bylo co nejmenší. Suricata je navíc kompatibilní s celou řadou nástrojů třetích stran. Používá standardní vstupní a výstupní formáty jako JSON a YAML, jenž umožňují snadnou následnou integraci s dalšími nástroji jako jsou Splunk, Kibana, ElasticSearch apod. [61]

5.1.5 Zeek

Zatímco výše zmínění nástroj Suricata je orientovaný na porovnávání vzorů, software Zeek je založen na analýze událostí. Poskytuje ucelené skriptovací prostředí, do něhož lze implementovat algoritmy a detekční pravidla. Architektonicky je Zeek rozdělen do dvou hlavních bloků. Prvním z nich je modul událostí, který redukuje příchozí tok paketů na řadu událostí vyšší úrovně. Druhou částí je potom intepreter skriptů, který provádí obsluhy událostí napsaných ve skriptovacím jazyce. Tyto skripty mohou představovat různé zásady zabezpečení, např. jakou akce je třeba provést, když monitor detekuje různé typy aktivit. Obecně řečeno mohou ze vstupního provozu odvodit celou rozmanitou škálu požadovaných vlastností a různé typy statistik. Skripty také mohou generovat výstrahy v reálném čase a mohou spouštět libovolné externí programy, např. ty určené pro vyvolání aktivní reakce na útok. [39] [54]

5.2 Simple Network Management Protocol (SNMP)

SNMP je široce používaný protokol aplikační vrstvy definovaný v RFC1157, který slouží pro výměnu informací určených pro správu síťových zařízení. Využívá jednoduchou architekturu založenou na modelu klient-server. Klientem je jakékoliv zařízení (většinou síťové), které má být na dálku spravované SNMP serverem (často nazývaným jako správce), jako je např klientské PC, ale také síťové přepínače, směrovače, tiskárny apod.

Data, které SNMP protokol využívá, jsou organizována do datového stromu. Datový strom se skládá z několika větví (resp. tabulek), které se nazývají „Management Information Base" (MIB). Tyto tabulky seskupují konkrétní typy zařízení, nebo jejich součásti. Cílem MIB je shromažďovat informace a organizovat je do hierchického datového formátu. Správce SNMP používá informace z MIB k překladu a interpretaci zpráv před jejich odesláním koncovému uzlu. Uvnitř těchto MIB tabulek se nachází datová reprezentace celé řady spravovaných objektů, které mohou mít odlišnou datovou reprezentaci – může se jednat o čítače, čísla, texty apod. Každý z těchto objektů se identifikuje pomocí identifikátoru objektu (object identifier – OID). Jedná se o posloupnost čísel, jež určují přesnou polohu datového objektu ve stromu MIB datové struktury.

5.3 RRD Tool

Pro účinné a systematické ukládání dat jsem vybral otevřený nástroj „RRD Tool", který umožňuje archivovat a analyzovat data ze všech druhů zdrojů dat. Tento nástroj umožňuje v sledovat v reálném čase průběh požadovaných veličin a následně je vykreslovat do grafu (např. průběh zatížení CPU v čase, nebo množství dat prošlých v daném směru přes dané rozhraní sítě apod.).

RRD nástroj využívá pro ukládání dat RRD soubory, které jsou v čase konstantní (jejich velikost je dána v okamžiku vytvoření). Pokud je databáze daty naplněná, začnou se nejstarší záznamy přepisovat novými, jedná se o metodu ukládání dat typu „circular-buffer".

5.4 Syslog

Syslog je standard pro zasílání logovacích zpráv, pomocí něhož může zařízení nebo aplikace odesílat logovací data o svém stavu, událostech, diagnostice apod. Komunikuje probíhá prostřednictvím UDP portů 514 a 601.

Zprávy syslogu mají vestavěnou úroveň závažnosti od 0, která je nejzávažnější (nouzový stav) až po úroveň 7, která je informativního (resp. debugového) charakteru. Pracuje podobně jako SNMP protokol s architekturou klient-server. Syslog server přijímá, ukládá a interpretuje zprávy Syslog.

Pro ukládání syslogových dat doporučuji MySQL server a pro samotnou interpretaci výše zmíněný otevřený nástroj „RRD Tool". Ten lze navíc rozšířit o plugin syslog, který poskytuje další úroveň zpracování a reprezentaci dat (různé grafy, export zpráv ve formátu CSV, HTML a textové alarmy, podpora Native MySQL 5.1 apod.).

6. Testování bezpečnosti sítě

Cílem této kapitoly popsat testování sítě pomocí otevřených nástrojů určených pro odhalování zranitelností v modelu vybrané sítě Škoda Auto. Na síť byly nasazeny některé nástroje, které jsem doporučil v kapitolách 4 a 5.

Vzhledem k této situaci není možné testovat fyzické zabezpečení sítě, a proto se omezím na L2 a L3 vrstvu ISO OSI modelu. Podle DREAD modelu hrozeb vytvořeného v kapitole 3, jsem se v laboratorním testování sítě zaměřil na dvě největší hrozby, které z tohoto modelu vznikly. Jedná se o hrozbu DoS útoku, který dosáhl nevyššího skóre a hrozbu Sniifing útoků, které dosáhly druhého nejvyššího ohodnocení.

Tyto dvě největší hrozby jsou simulovány pomocí nástrojů uvedených níže v kapitole. Dále se zabývám nástroji a technologiemi, které tyto hrozby buď zcela zastaví (případ nasazení Suricaty a následná definice pravidel), případně upozorní na podezřelou aktivitu (syslog, SNMP a RRD tool).

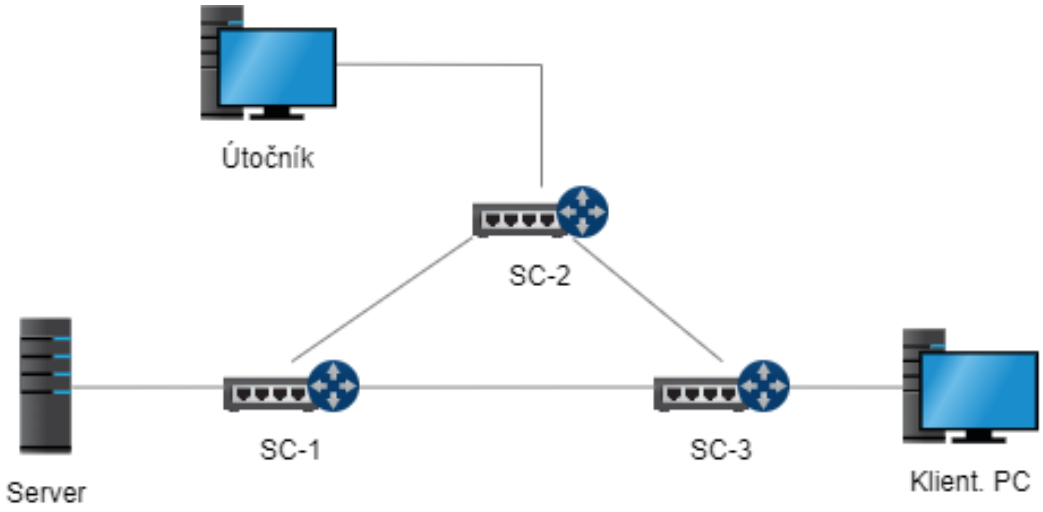
6.1 Popis a konfigurace testovacího prostředí

Vzhledem k nemožnosti testování zranitelností sítě v reálném provozu Škoda Auto jsem navrhl a nakonfiguroval experimentální síť vycházející z modelu vybrané sítě Škoda Auto, jejíž topologii mi firma poskytla.

Seznam všech síťových prvků a stanic je uvedeno společně s IP adresami v tabulce číslo 11. Samotná topologie sítě je zakreslena na obrázku 13.

Zařízení	Popis	Operační systém/Verze	IP adresa
SC-1	L3 Switch Siemens Scalance XC208G	04.01.00	192.168.1.10
SC-2	L3 Switch Siemens Scalance XC208G	04.01.00	192.168.1.20
SC-3	L3 Switch Siemens Scalance XC208G	04.01.00	192.168.1.30
Server	NTP, rsyslog, ARPWatch, Suricata, RRDTool + Cacti	Ubuntu 20.04	192.168.1.160
Útočník	Sbírka nástrojů pro různé útoky	Kali Linux 2020.02	192.168.1.100
Klient. PC	Pracovní stanice údržby	Windows 10	192.168.1.200

Tabulka 11 Seznam zařízení v testovací síti



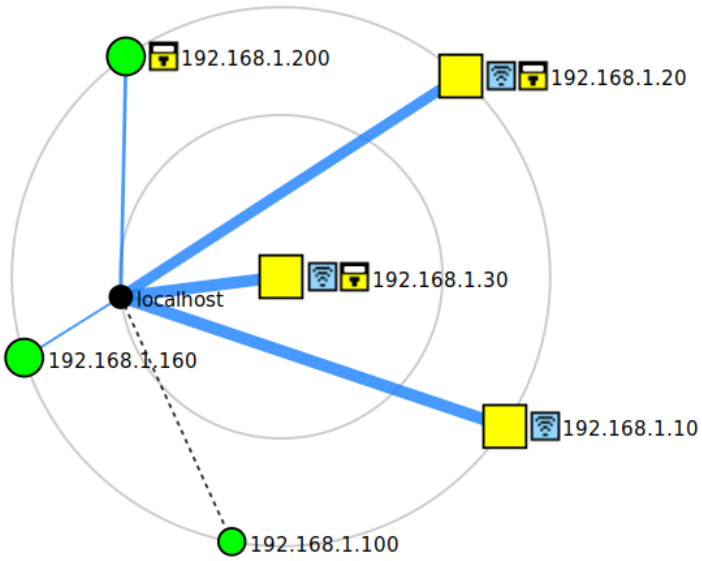
Obrázek 13 Topologie laboratorní sítě

6.2 Interní testování laboratorní sítě

Pro interní testování jsem vycházel z předpokladu, že útočník pronikne do sítě přes fyzické zabezpečení přepínačů a bude mít tedy fyzický přístup k ethernetovým rozhraním přepínačů. Pro tyto účely jsem využil následující nástroje.

Zenmap

Tato utilita je v podstatě grafickou nadstavbou pro nástroj zvaný nmap. Trvalo ji několik málo minut oskenovat kompletně celou modelovou síť včetně otevřených portů jednotlivých zařízení. Níže nakreslená topologie na obr. 14 je tou, kterou Zenmap vytvořil automaticky.



Obrázek 14 Zenmap topologie laboratorní sítě

Macchanger

Nástroj, který jsem použil umožňuje změnu MAC adres síťového rozhraní útočníka (v našem případě s IP adresou 192. 168. 1. 100). Dokáže MAC adresy měnit na konkrétní adresu, případně lze vygenerovat náhodnou. Tento nástroj využívám pro útok na zranitelnost v infrastruktuře definovanou v kapitole 4.

Hping3

Hping je generátor paketů, který na rozdíl od klasického pingu umožňuje útočníkovi generovat nejenom ICMP echo žádostí, ale také podporuje širokou řadu protokolů TCP, UDP, ICMP, a RAW-IP. Tento nástroj používám pro simulaci DoS útoků na sítě.

Ostinato Packet Generator

Ostinato je generátor síťového provozu s otevřeným zdrojovým kódem, který má také možnosti manipulace a analýzy paketů. V laboratorním prostředí nástroj používám pro vytvoření vstupních dat pro monitorovací software RRD Tool. Podporuje většinu běžných protokolů a Python API umožňuje provádět automatizované úlohy.

6.3 Suricata IDS

Instalace

Instalace pro Linuxovou distribuci Ubuntu, používanou pro experimentální síť, je poměrně jednoduchá, protože Suricata je k dispozici ve formě PPA balíčků. Stačí tedy pouze jediný příkaz *apt-get install suricata* a IDS systém se nainstaluje.

Konfigurace

Konfigurace se provádí pomocí několika konfiguračních souborů, z nichž nejdůležitější jsou následující

- **Suricata.yaml** – v tomto hlavním konfiguračním souboru lze (mimo jiné) specifikovat síť interní (tzv. HOME_NET) a externí (tzv. EXTERNAL_NET), nad kterou bude Suricata pracovat.

- **Adresář „rules“** – v tomto adresáři jsou umístěné pravidla, podle kterých bude Suricata odchytávat provoz a následně definovaným způsobem se zachyceným provozem pracovat, způsoby práce s odchytaným provozem jsou následující:
  - Pass – provoz nebude kontrolován, jedná se v podstatě o tzv. „whitelist“;
  - Drop – zahodí paket, odesílatel o této skutečnosti nebude informován;
  - Reject – zahodí paket, odesílatel o této skutečnosti bude informován pomocí ICMP protokolu
  - Alert – předá výstrahu do logu s definovanými metadaty

  V testovací síti, se kterou pracuji nechávám vše nastavené na Alert, abych demonstroval odchycený útok.

Detekce útoků

Dle nastavených pravidel Surikata může detekovat útoky na různá zařízení v síti. Jako příklad uvedu některé typy útoky jmenované v tabulce v kapitole 4. Tyto útoky budu směřovat na přepínače, případně na klientský PC.

DoS Smurf útok

Nástroj hping jsem využil k simulaci Smurf útoku – ten spočítá v tom, že se vydávám za jiné zařízení v síti. Zprávu Echo request pak má zdrojovou adresu oběti přepínače SC-1, na které pak všechna zařízení v síti odpovídají zprávou Echo reply. Tímto způsobem dojde k zahlcení přepínače a DoS útok je úspěšně vykonán. Na obrázku 15 je vidět provedení útoku na zařízení útočníka.

```
kali@kali:~$ sudo hping3 -1 --flood -a 192.168.1.10 192.168.1.100
HPING 192.168.1.100 (eth0 192.168.1.100): icmp mode set, 28 headers + 0 dat
a bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.100 hping statistic ---
722546 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
kali@kali:~$
```

Obrázek 15 Simulovaný Smurf útok

DoS Smurf zachycení

Na obrázku 16 je vidět zachycení DoS Smurf útoku Suricatou, který tuto událost vypisuje do logu, což je vhodné pro naše laboratorní účely. Suricata může především tyto odchycené pakety zahazovat, čímž úspěšně zabrání DoS útoku, který byl provedený výše.

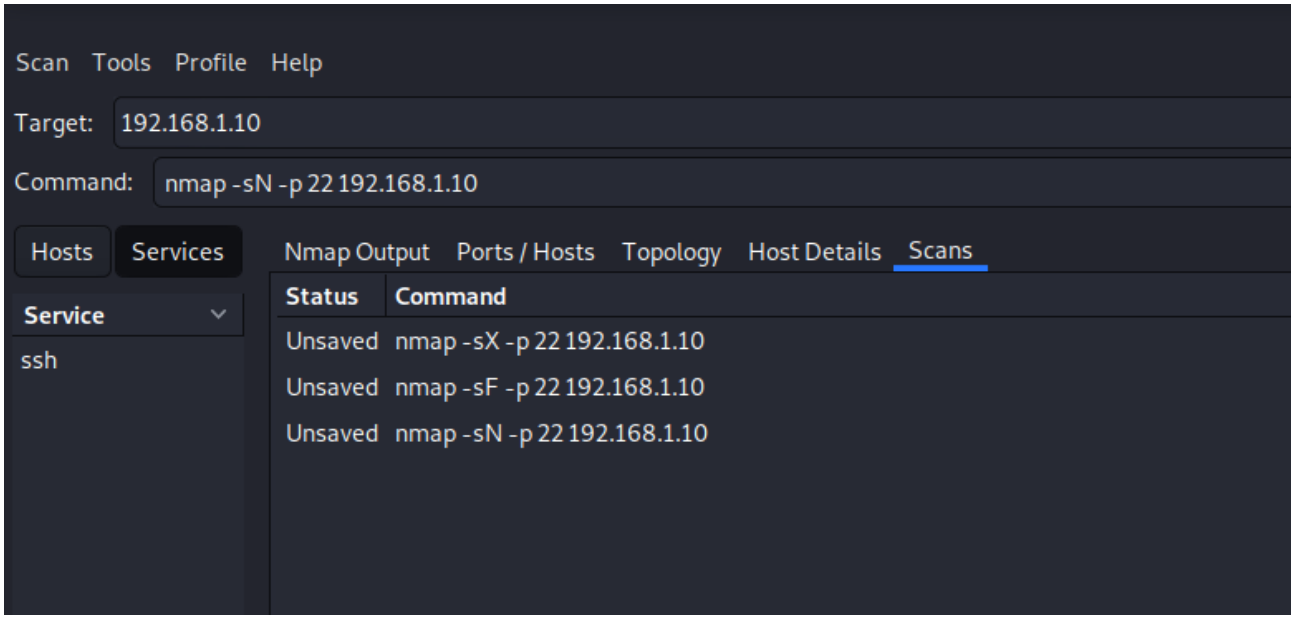
```
07/28/2020-09:15:36.866242  [**] [1:2100478:1] GPL SCAN Broadscan Smurf Scanner [**] [Classification
: (null)] [Priority: 3] {ICMP} 192.168.1.100:0 -> 192.168.1.10:0
07/28/2020-09:21:16.225847  [**] [1:2100478:1] GPL SCAN Broadscan Smurf Scanner [**] [Classification
: (null)] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.10:0
07/28/2020-09:26:49.540358  [**] [1:0:0] GPL SCAN Broadscan Smurf Scanner [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.1.100:8 -> 192.168.1.10:0
07/28/2020-09:27:01.830693  [**] [1:0:0] GPL SCAN Broadscan Smurf Scanner [**] [Classification: (nul
l)] [Priority: 3] {ICMP} 192.168.1.100:0 -> 192.168.1.10:0
```

Obrázek 16 Zachycení simulovaného Smurf útoku

Network scanning útok

Jak lze vidět na obrázku 17, pomocí nmap nástroje provádím 3 typy skenování sítě, jsou to tyto následující

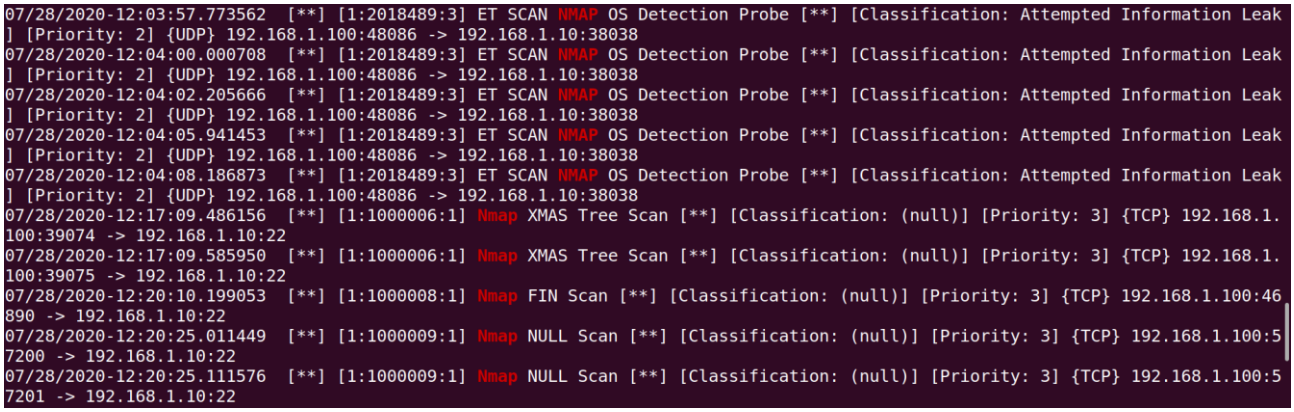
- nmap -sX – tento typ skenování je nazýván xmas tree scan, protože v záhlaví TCP nastavuje příznaky PSH, URG a FIN jako blikající žárovky na vánočním stromku. Každý operační systém na tyto „vánoční“ pakety reaguje odlišně – díky této vlastnosti lze odhalit informace o operačním systému cílové zařízení, stavech portů a další.
- nmap -sF – klasický TCP syn scan nechává na cílovém hostiteli mnoho otisků prstů, čímž odhaluje identitu útočníka, navíc často jsou IDS systémy nastaveny tak, aby sledovaly SYN pakety zaměřené na konkrétní porty. Z výše popsaných důvodů jsem využil FIN skenování, které inicializuje skenování pomocí paketu FIN. Protože mezi cílovým a zdrojovým hostitelem není žádná předchozí komunikace, cíl odpoví paketem RST a resetuje spojení. Tím však odhalí svou přítomnost.
- nmap -sN – tzv. null scan attack je řada TCP paketů, které obsahují pořadové číslo 0 nemají žádné nastavené příznaky. Jelikož v produkčním prostředí se nikdy neobjeví tento typ paketu, může proniknout firewallem, protože ty filtrují pakety s konkrétními příznaky. Pokud je port uzavřen, cíl pošle paket RST. Pokud je port otevřený, paket zahodí a nepošle žádnou odpověď zdrojovému hostiteli – tím však odhalí pro útočníka svůj stav.



Obrázek 17 Simulovaný Network scanning

Network scanning zachycení

Na obrázku 18 je vidět zachycení Suricatou všech výše zmíněných skenovaných útoků. Detekce mají popis Nmap XMAX Tree Scan, Nmap FIN Scan a Nmap NULL Scan – konkrétně se jedná o posledních 5 řádků výpisu. Suricata díky správnému nastavení pravidel tyto pokusy o sken zachytila a může o tom informovat bezpečnostního pracovníka, který následně bude zkoumat příčinu vzniku této události a další podrobnosti.



Obrázek 18 Zachycení simulovaného Network scanning

Pravidla, podle kterých Suricata analyzuje datový provoz se skládá ze tří částí

- Akce, která určuje, co se bude provádět, pokud vyhodnocení bude pozitivní.
- Hlavička pravidla definuje protokol, IP adresy, porty a směr zachytávání.
- Možnosti pravidel definují další specifika.

Na obrázku číslo 19 jsou vidět pravidla, které jsem vytvořil pro zachycení výše jmenovaných útoků. Například první pravidlo se skládá z následujících částí:

- *alert* – pokud se pravidlo shoduje s datovým provozem, Suricata vytvoří výstrahu;
- *imcp* – kterého protokolu se pravidlo týká;
- *any -> $HOME_NET* – zdroj a cíl provozu (v našem případě proměnná $HOME_NET je nastavena na síť 192.168.1.0/24);
- *any -> any* – zdrojový a cílový port;
- *msg: "GPL SCAN Broacscan Smurf Scanner"* – zpráva, která se zobrazí uživateli;

- *detection_filter: track_by_dst, count 100, second 2* – definuje hodnoty, které musí hostitel překročit, aby pravidlo spustilo událost. V našem případě je sledována zdrojová IP adresa (track_by_dst), povolený maximální počet shod s pravidly před překročením detekčního filtru (count 100) a počet sekund po které se počítá počet shod (second 2).

```
#Smurf Attack

alert icmp any any -> $HOME_NET any(msg: "GPL SCAN Broadscan Smurf Scanner";
                                    detection_filter:track by_dst,count 100,seconds 2;sid:2100478; rev:001;)

# Store all Windows executables
alert http any any -> any any (msg:"FILE magic -- windows"; flow:established,to_client;
                               filemagic:"executable for MS Windows"; filestore; sid:18; rev:1;)

#NMAP Scanning

alert tcp any any -> $HOME_NET any (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)

alert tcp any any -> $HOME_NET any (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1; )

alert udp any 10000: -> $HOME_NET 10000: (msg:"ET SCAN NMAP OS Detection Probe"; dsize:300; content:"CCCCCCCCCCCCCCCCCCCC";
                                        fast_pattern:only; content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC>
                                        depth:255; content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"; within:45;
                                        classtype:attempted-recon; sid:2018489;rev:1;)

alert tcp any any -> $HOME_NET any (msg:"Nmap NULL Scan"; flags:0; sid:1000009; rev:1; )

alert tcp any any -> any ![80,8080] (msg:"SURICATA HTTP but not tcp port 80, 8080";
                                flow:to_server; app-layer-protocol:http; sid:2271001; rev:1;)

alert tcp any any -> any 80 (msg:"SURICATA Port 80 but not HTTP"; flow:to_server; app-layer-protocol:!http; sid:2271002; rev:1;)

# Unually short file
alert http any any -> any any (msg:"FILEMAGIC short"; flow:established,to_server; filemagic:"very short file (no magic)";
```

Obrázek 19 Pravidla pro Suricata IDS

6.4 Další nástroje pro monitoring sítě

ARP Watch

Instalace je taktéž jednoduchá, neboť je taktéž k dispozici ve formě PPA balíčku, po zadání příkazu *apt-get arpwatch* se balíček stáhne a nainstaluje. Samotná databáze ethernetových/IP adres se pak nachází v souboru /var/arpwatch/arp.dat (cesta k souboru se může lišit v souvislosti s distribucí).

Arpwatch jakékoliv změny, případně neobvyklou aktivitu loguje do systémového log souboru. V našem případě se jedná o syslog standard. Na obrázku 20 můžeme sledovat změnu MAC adresy útočníka pomocí nástroje macchaner. Na dalším obrázku 21 vidíme, že každou změnu MAC adresy útočníka server zaznamenal do svého systémového log souboru. Ten je může být následně dále zpracováván (např. pomocí RRD toolu) a upozornit na potenciální bezpečnostní incident.

```
kali@kali:~$ sudo macchanger -r eth0
Current MAC:   3a:15:f9:4f:0e:19 (unknown)
Permanent MAC: c8:5b:76:25:95:04 (unknown)
New MAC:       d6:7e:07:58:0b:43 (unknown)
kali@kali:~$ sudo macchanger -r eth0
Current MAC:   d6:7e:07:58:0b:43 (unknown)
Permanent MAC: c8:5b:76:25:95:04 (unknown)
New MAC:       fe:e6:30:a1:99:6d (unknown)
kali@kali:~$ sudo macchanger -r eth0
Current MAC:   fe:e6:30:a1:99:6d (unknown)
Permanent MAC: c8:5b:76:25:95:04 (unknown)
New MAC:       32:27:a2:26:4f:c7 (unknown)
```

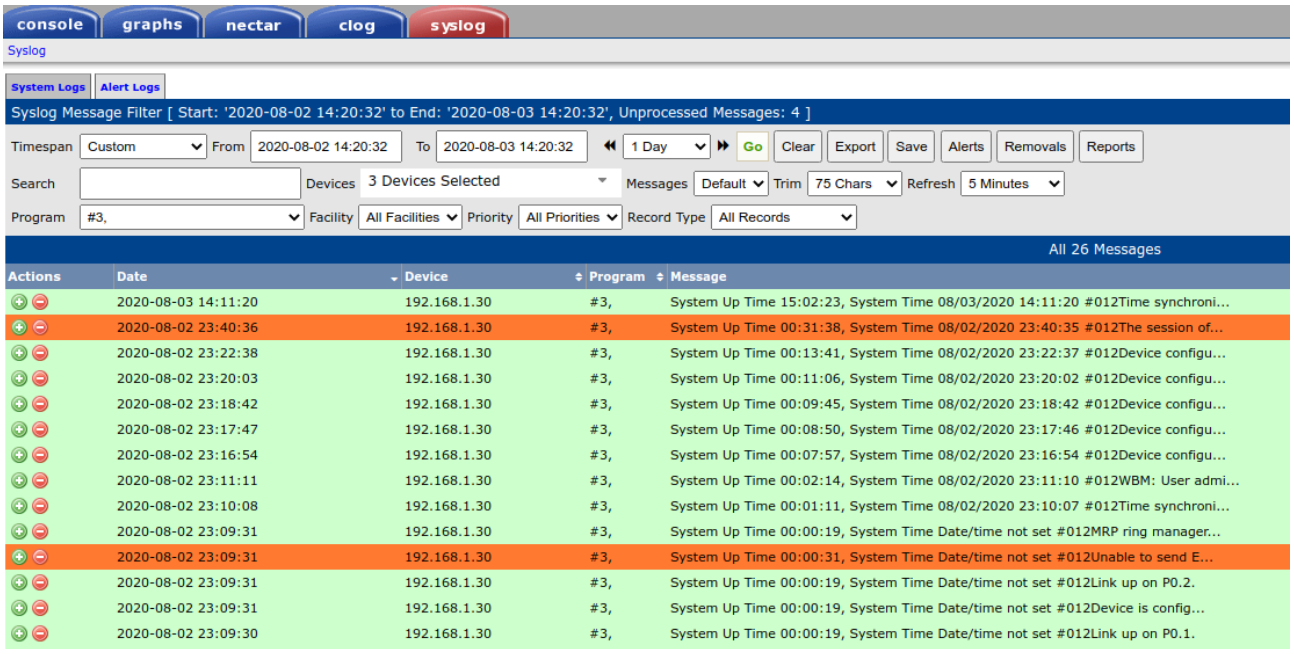
Obrázek 20 Změna MAC adresy

```
michal@XPS-15-7590-Linux:~$ tail -f /var/log/syslog | grep arpwatch
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 d6:7e:07:58:0b:43 (c2:3c:29:08:53:ac)
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: reaper: pid 91745, exit status 1
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 d6:7e:07:58:0b:43 (c2:3c:29:08:53:ac)
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 28 13:11:59 XPS-15-7590-Linux arpwatch: reaper: pid 91746, exit status 1
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 fe:e6:30:a1:99:6d (d6:7e:07:58:0b:43)
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: reaper: pid 91846, exit status 1
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 fe:e6:30:a1:99:6d (d6:7e:07:58:0b:43)
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 28 13:12:38 XPS-15-7590-Linux arpwatch: reaper: pid 91847, exit status 1
Jul 28 13:13:06 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 32:27:a2:26:4f:c7 (fe:e6:30:a1:99:6d)
Jul 28 13:13:06 XPS-15-7590-Linux arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 28 13:13:06 XPS-15-7590-Linux arpwatch: reaper: pid 91923, exit status 1
Jul 28 13:13:07 XPS-15-7590-Linux arpwatch: changed ethernet address 192.168.1.100 32:27:a2:26:4f:c7 (fe:e6:30:a1:99:6d)
```

Obrázek 21 Pozorovaná změna útočníkovi MAC adresy na serveru

Syslog a SNMP

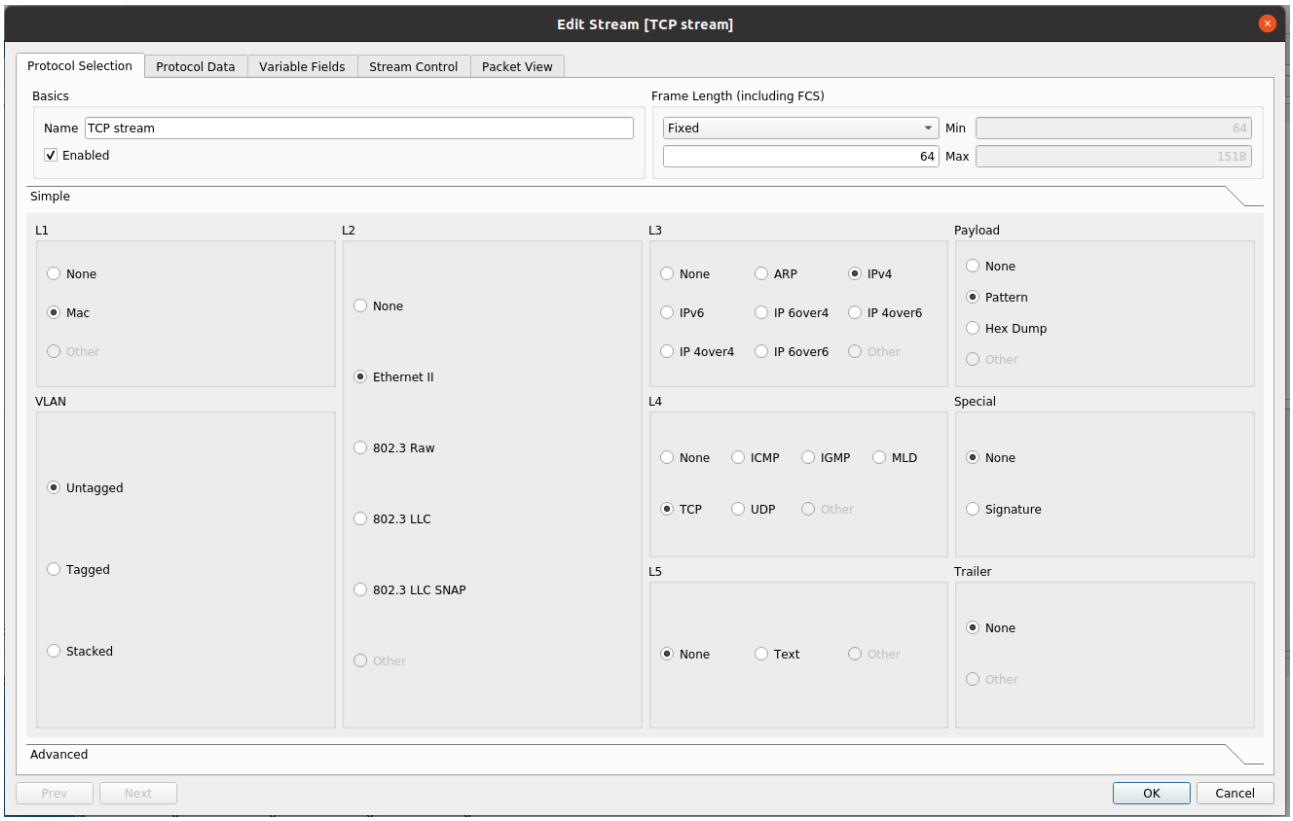
RRD Tool a jeho frontendovou část Cacti lze stáhnout na oficiálních stránkách výrobce. Před samotnou instalací je nutné mít nainstalovaný a nakonfigurovaný jakýkoliv webový server, který využívá PHP a MySQL. Já jsem konkrétně zvolil webový server Apache a pro databázi komunitní nástupnickou větev MySQL s názvem MariaDB. Dále je nutné nakonfigurovat službu SNMP a mít vytvořený syslog server. Pro laboratorní testování jsem zvolil otevřenou rozšiřující implementaci protokolu syslog s názvem rsyslog. Na obrázku 22 je ukázka zařízení SC-3, jehož syslog byl uložen do MariaDB a zobrazen v Cacti. Tyto syslogy všech zařízení umístěných na síti je velmi důležité sledovat, neboť nám můžou poskytnout velmi dobrý přehled událostí, které se v síti dějí, případně z nich extrahovat informace o dlouhodobějším stavu zařízeních.



Obrázek 22 Ukázka syslogu přepínače SC-3

Sledování síťového provozu

Níže uvádím jako ukázku několik grafů z nástroje RRD Tools, resp. jeho frontendové nadstavby Cacti. Grafy vznikly ze sledování uměle vytvořeného síťového provozu v laboratorních podmínkách. Ten jsem vytvářel pomocí výše zmíněných nástrojů hping a Ostinato Packet Generator. Na obrázku 23 je vidět nastavení generovaného provozu. Obrázek 24 pak ukazuje počet vygenerovaného síťového provozu za dobu běhu programu.

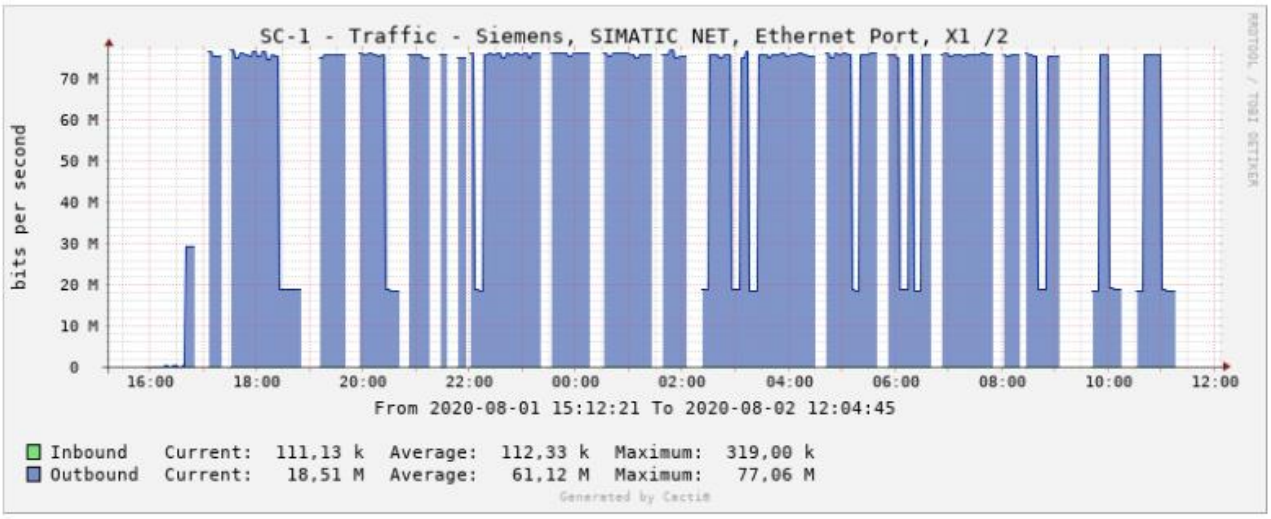


Obrázek 24 Ostinato – ukázka nastavení

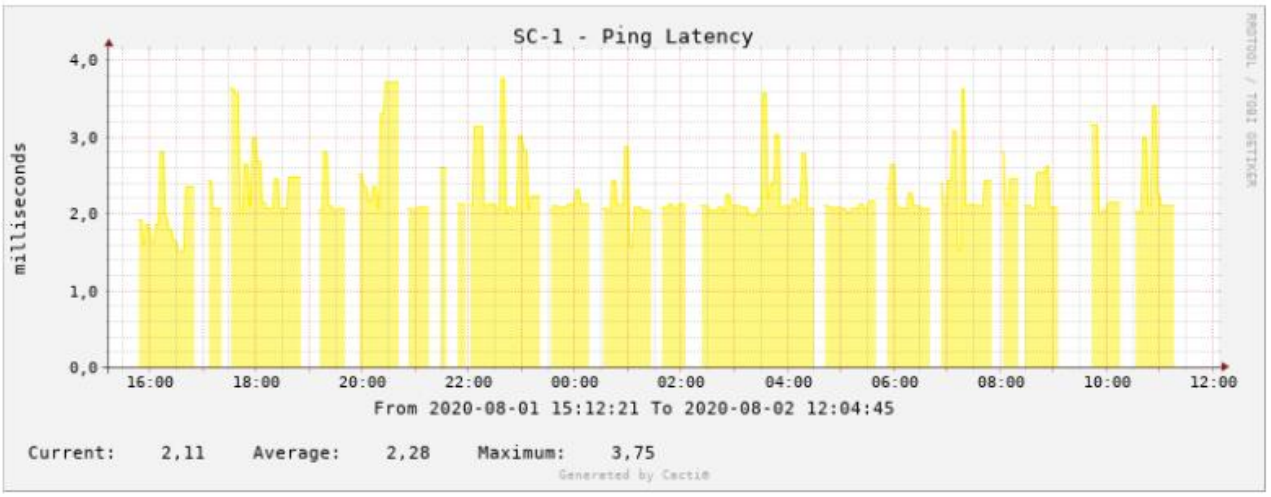
	Port 0-0	**Port 0-1**
Frame Send Rate (fps)	18	148 722
Frame Receive Rate (fps)	16	51
Bytes Received	2 021 157 578	249 124 310
Bytes Sent	112 105 108	603 267 543 825
Byte Send Rate (Bps)	1 836	8 923 320
Byte Receive Rate (Bps)	1 056	3 089
Bit Send Rate (bps)	18 144	99 941 184
Bit Receive Rate (bps)	11 520	34 504
Receive Drops	0	2

Obrázek 23 Ostinato – statistika vygenerovaného síťového provozu

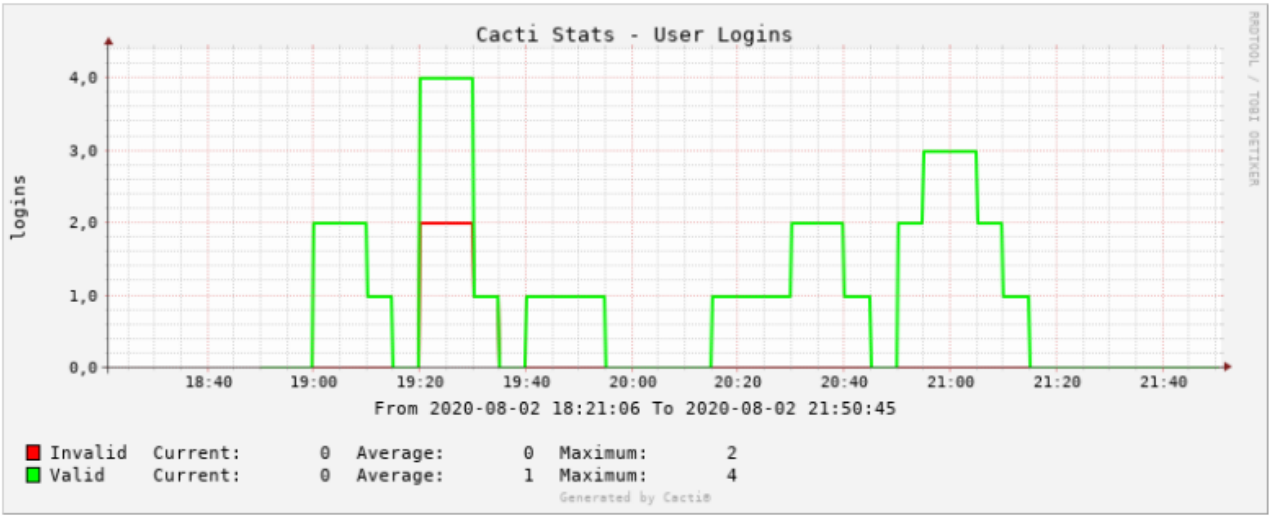
Generování a sledování síťového provozu jsem prováděl zhruba 20 hodin (jak lze vidět z grafů). Jako ukázku jsem vybral tok dat, který procházel síťovým přepínačem SC-1, konkrétní na jeho portu 2 (obrázek 25), dále jsem sledoval ping latenci na stejném přepínači (obrázek 26) a počet přihlášených uživatelů na přepínači SC-2 (obrázek 27).



Obrázek 25 Cacti – tok dat na portu 2 přepínače SC-1



Obrázek 26 Cacti – ping latence přepínače SC-1



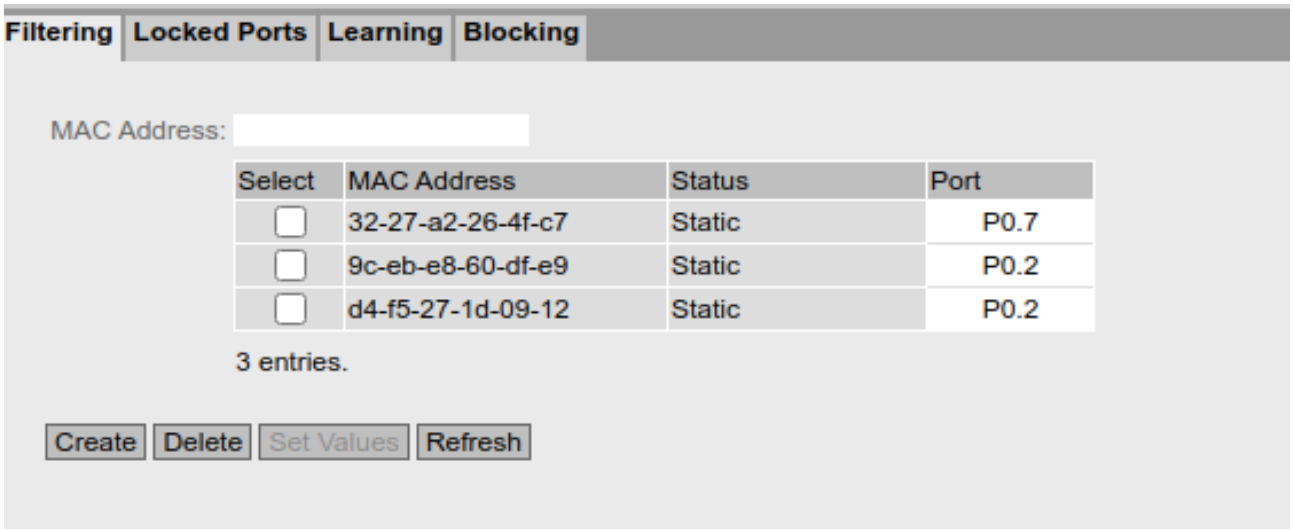
Obrázek 27 Cacti – Počet přihlášení na přepínači SC-2

Tato vizualizace různých parametrů síťových zařízení je velice důležitá pro vytvoření normálového provozu, který ukazuje běžný síťový provoz bez bezpečnostních incidentů. Pokud se nějaký bezpečnostní incident objeví (typicky DoS útok), je poté velice snadné odhalit tyto špičky grafu (např. v grafu toku dat přes určité rozhraní) a následně dále postupovat.

6.5 Port security

Filtry na MAC adresy

Tuto funkcionalitu nazývá Siemens jako Locked port, níže na obrázku 28 lze vidět konfiguraci, kterou využívám v testovací síti. Na portu 7 útočník, který má MAC adresu 32-27-a2-26-4f-c7. Tato funkce je důležitá především z linkového pohledu na bezpečnost, neboť účinně blokuje výskyt (resp. možnou přítomnost) neznámých zařízení připojených do sítě.

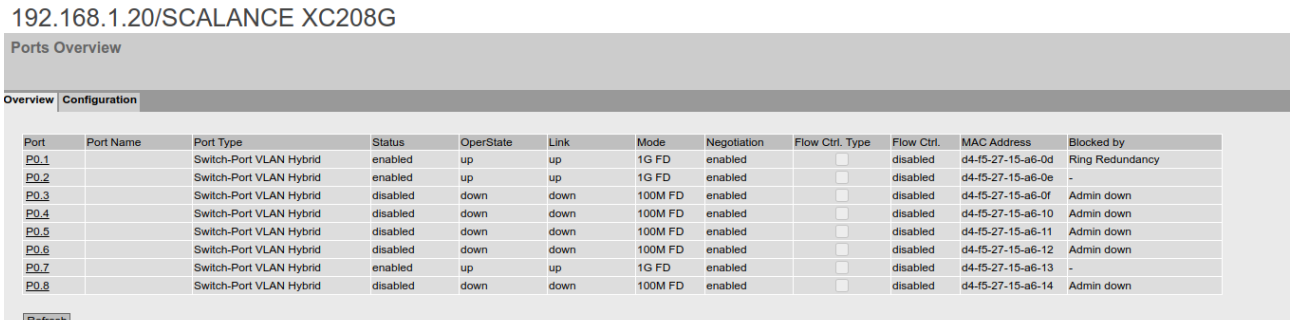


Obrázek 28 Povolené MAC adresy u jednotlivých portů přepínače

Pokud ji pomocí nástroje Macchanger změním na jinou, přepínač dle ACL začne filtrovat dle MAC adresy a zařízení a framy (resp. pakety) s neznámou adresou zahazuje.

Deaktivace nepoužívaných portů

Další doporučení je všechny nepoužívané porty na konkrétním přepínači administrátorsky deaktivovat, aby bylo nutné pro připojení dalšího zařízení ručně port aktivovat. Toto opatření je také účinné z pohledu blokace přítomnosti neznámých zařízení v síti, které by mohli eventuálně být využity k nějakému útoku.



Port	Port Name	Port Type	Status	OperState	Link	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MAC Address	Blocked by
P0.1		Switch-Port VLAN Hybrid	enabled	up	up	1G FD	enabled		disabled	d4-f5-27-15-a6-0d	Ring Redundancy
P0.2		Switch-Port VLAN Hybrid	enabled	up	up	1G FD	enabled		disabled	d4-f5-27-15-a6-0e	-
P0.3		Switch-Port VLAN Hybrid	disabled	down	down	100M FD	enabled		disabled	d4-f5-27-15-a6-0f	Admin down
P0.4		Switch-Port VLAN Hybrid	disabled	down	down	100M FD	enabled		disabled	d4-f5-27-15-a6-10	Admin down
P0.5		Switch-Port VLAN Hybrid	disabled	down	down	100M FD	enabled		disabled	d4-f5-27-15-a6-11	Admin down
P0.6		Switch-Port VLAN Hybrid	disabled	down	down	100M FD	enabled		disabled	d4-f5-27-15-a6-12	Admin down
P0.7		Switch-Port VLAN Hybrid	enabled	up	up	1G FD	enabled		disabled	d4-f5-27-15-a6-13	-
P0.8		Switch-Port VLAN Hybrid	disabled	down	down	100M FD	enabled		disabled	d4-f5-27-15-a6-14	Admin down

Obrázek 29 Správa portů – přehled

7. Závěr

Cílem této bakalářské práce bylo analyzovat průmyslovou část vybrané sítě Škoda Auto, zmapovat typy použitých technologií, klasifikovat různé potenciální útoky a navrhnout soubor protiopatření, pro zajištění síťové kybernetické bezpečnosti tohoto provozu. Dle možné součinnosti se Škoda auto ověřit metodiku v praxi.

Ve své bakalářské práci jsem definoval jsem několik pojmů, které úzce souvisí s bezpečností, dále jsem využil řadu metod pro zjištění zranitelností sítě, včetně vypracovaných modelů hrozeb, které v průmyslové síti Škoda auto mohou být uplatněny. Největší hrozby, kterým průmyslová síť čelí jsou především DoS a Sniffing charakteru.

Analýza sítě odhalila nedostatky, které se dají snadno vyřešit, ačkoliv jejich dopad na síť jako takovou by byl velice dramatický. Na základě analýzy zranitelností a hrozeb jsem navrhl topologii sítě, která vztažmo k té současné má několik velmi významných výhod.

U každé klasifikované zranitelnosti jsem také navrhl protiopatření, které by mělo buď tyto zranitelnosti sítě odstranit, případně odhalit, že se útočník snaží této zranitelnosti využít pro útok. Část těchto protiopatření je poměrně snadno aplikovatelná, protože zakládá na správné konfiguraci průmyslových přepínačů a pasivnímu monitorování sítě, což je především obsahem kapitoly páté. Jelikož nebylo možné otestovat fyzickou bezpečnost, provedl jsem pouze její analýzu, ale dále netestoval.

Součástí souboru protiopatření je též několik otevřených síťových nástrojů, které se mi bohužel nepovedlo nasadit do provozu vybrané průmyslové sítě Škoda Auto – vzhledem k velice omezenému přístupu a nemožnosti testovat zranitelnosti v reálném provozu, jsem byl nucen postavit experimentální model sítě ve školním laboratorním prostředí a následně jsem na ní prováděl útoky a zjišťoval, zda navržené nástroje obstojí v praxi.

Pro analýzu zranitelností jsem se rozhodl využít rozdělení podle referenčního ISO modelu, následně jsem vymyslel vlastní klasifikaci pro „jemnější“ rozdělení zranitelností.

Tato bakalářská práce by mohla v budoucnu sloužit jako základ mé diplomové práce – dovedu si totiž představit ještě těsnější spolupráci s firmou Škoda Auto především v oblasti nasazení těchto navrhovaných protiopatření v reálné sítu. Dále by bylo možné tuto práci v rámci diplomové práce rozšířit i o analýzu a testování na aplikační vrstvě.

Pevně věřím, že výsledky mé práce mohou pomoci nejenom Škodě Auto, ale také všem potenciálním zájemcům, podnikům, firmám, které mají zájem udržet si svoje výrobní „know-how“, pověst společnosti i objem výroby.

Seznam zdrojů:

Tištěná kniha

[1] PERDISCI, Roberto, Clémentine MAURICE, Giorgio GIACINTO a Magnus ALMGREN. *Detection of Intrusions and Malware, and Vulnerability Assessment*. 16th International Conference. Gothenburg, Sweden: DIMVA 2019, 2019. ISBN 3030220389.

[2] ZURAWSKI, Richard. *Industrial communication technology handbook*. Second edition. Boca Raton: CRC Press, Taylor & Francis Group, [2015]. Industrial information technology series. ISBN 9781482207323.

Elektronická kniha

[3] PIGAN, Raimond a Mark METTER. *Automating with PROFINET: Industrial Communication Based on Industrial Ethernet*. 2nd Edition. Publicis, 2015. ISBN 9783895789502.

[4] FLAUS, Jean-Marie. *Cybersecurity of industrial systems* [online]. Hoboken, NJ: ISTE Ltd/John Wiley and Sons, 2019. ISBN 9781119644514.

[5] KNAPP, Eric D. *Industrial network security: securing critical infrastructure networks for smart grid, scada, and other industrial control systems* [online]. 2nd edition. Waltham, MA: Elsevier, 2014. ISBN 9780124201842.

Článek v časopisu

[6] PROFINET – Standard pro průmyslový Ethernet v automatizaci [online]. Praha: SIMATIC Guide, 2005, 2005(4) [cit. 2020-01-05]. Dostupné z: http://stest1.etnetera.cz/ad/current/content/data_files/automatizacni_systemy/prumyslova_komunikace/profinet/profinet_04_2005_cz.pdf

[7] *PROFINET Security Guideline: Guideline for PROFINET* [online]. Karlsruhe: PROFIBUS Nutzerorganisation e. V. (PNO), 2013 [cit. 2020-01-05]. Dostupné z: https://www.profibus-profinet.cz/images/Dokumenty/PROFINET/11789_PROFINET_Security_7002_V20_Nov13.pdf

[8] *PROFINET System Description: Technology and Application* [online]. Karlsruhe: PROFIBUS Nutzerorganisation e. V. (PNO), 2014, October 2014, 22 [cit. 2020-01-05].

Dostupné z: http://us.profinet.com/wp-content/uploads/2012/11/PROFINET_SystemDescription_ENG_2014_web.pdf

[9] *PROFINET System Description: Technology and Application* [online]. Karlsruhe: PROFIBUS Nutzerorganisation e. V. (PNO), 2014, June 2011, 22 [cit. 2020-01-05]. Dostupné z: https://www.automation.com/pdf_articles/profinet/PI_PROFINET_System_Description_EN_web.pdf

[10] BURGET, Pavel. Principy komunikace a diagnostika sítí Profinet. Automa [online]. 2013(05) [cit. 2020-04-23]. ISSN 1210-9592. Dostupné z: https://www.automa.cz/SiteContent.aspx?params=L1NpdGVDb250ZW50LmFzcHg%2fcmlkPTcwMTg5JmFwcD1NYWluJmdycD1Db250ZW50Jm1vZD1NYWdhemluZXMmc3RhPU1hZ2F6aW5lQXJ0aWNsZUNvbnRlbnRXZWImcHN0PU1hZ2F6aW5lQXJ0aWNsZUNvbnRlbnRXZWImcDE9WWVhcl9TVFJJTkdfTXQlMmZPTldZRjA3a2dDMWxKYkptTElBJTNkJTNkJnAyPU51bWJlcl9TVFJJTkdfOE1xcXFCUUtnTFUlMmZxaFMzU2xSUGx3JTNkJTNkJnAzPU9pZF9JTlRfMTAzNzcmdG5hbWU9c2l0ZWRlZmF1bHQmYWNvZGU9NWU2Yzk3ZmVlYzQ0ZWJkNzNlNzNkMTI2MDAwMmI0ZTQ%3d

[11] Pfrang, Steffen & Meier, David. (2018). Detecting and preventing replay attacks in industrial automation networks operated with profinet IO. Journal of Computer Virology and Hacking Techniques. 14. 10.1007/s11416-018-0315-0. Dostupné z: https://www.researchgate.net/publication/323384431_Detecting_and_preventing_replay_attacks_in_industrial_automation_networks_operated_with_profinet_IO

[12] Akerberg, Johan & Bjorkman, Mats. (2009). Introducing security modules in PROFINET IO. 14th International IEEE Conference on Emerging Technologies and Factory Automation. 1–8. 10.1109/ETFA.2009.5347205.

[13] DRAHOŠ, Peter a Juraj GABRIEL. Komunikačný systém Profinet IO. *Automa* [online]. 2006(07) [cit. 2020-04-20]. ISSN 1210-9592. Dostupné z: https://www.automa.cz/SiteContent.aspx?params=L1NpdGVDb250ZW50LmFzcHg%2fcmlkPTcwMTg5JmFwcD1NYWluJmdycD1Db250ZW50Jm1vZD1NYWdhemluZXMmc3RhPU1hZ2F6aW5lQXJ0aWNsZUNvbnRlbnRXZWImcHN0PU1hZ2F6aW5lQXJ0aWNsZUNvbnRlbnRXZWImcDE9WWVhcl9TVFJJTkdfNSUyYmZnblFpbUl6WTFWWndFWXElMmZuQUElM2QlM2QmcDI9TnVtYmVyX1NUUklOR19ZSSUyYlk2SHdVWUpqR3VRMVVQYTRxcEElM2QlM2QmcDM9T2lkX0lOVF81NjAmdG5hbWU9c2l0ZWRlZmF1bHQmYWNvZGU9OGFmN2I3ZDIwYjVlM2JlMTIyYzM3NWRlYzUyMWQ1Nzg%3d

Webové stránky

[14] PROFINET Communication Channels – PROFINET University. PROFINET University – PROFINET University [online]. Copyright © 2019 [cit. 05.01.2020]. Dostupné z: https://profinetuniversity.com/profinet-basics/profinet-communication-channels/

[15] DCP – Discovery and Configuration Protocol - PROFINET University. PROFINET University – PROFINET University [online]. Copyright © 2019 [cit. 10.01.2020]. Dostupné z: https://profinetuniversity.com/naming-addressing/profinet-dcp/

[16] Tech Tip: Why Does PROFINET Need an IP Address? - PROFINEWS. PROFINEWS – PROFINET, PROFIBUS, and IO-Link news from around the world [online]. Copyright © copyright 2020 [cit. 05.01.2020]. Dostupné z: https://profinews.com/2015/02/tech-tip-why-does-profinet-need-an-ip-address/

[17] *Profinet IO* [online]. [cit. 2020-01-05]. Dostupné z: https://www.kunbus.com/profinet-io.html

[18] *PROFINET Manual* [online]. [cit. 2020-01-05]. Dostupné z: https://www.felser.ch/profinet-manual/names.html

[19] *Profinet* [online]. Karlsruhe: PROFIBUS Nutzerorganisation e.V., 2020 [cit. 2020-01-05]. Dostupné z: https://www.profibus.com/

[20] AYLLON, Nelly. *ANOTHER RECORD YEAR FOR PI TECHNOLOGIES* [online]. North America, 2020 [cit. 2020-01-05]. Dostupné z: https://us.profinet.com/record-year-profinet-node-count/

[21] *PROFINET IO: PROFINET Unplugged – An introduction to PROFINET IO* [online]. [cit. 2020-01-05]. Dostupné z: https://www.rtautomation.com/technologies/profinet-io/

[22] Baud, Michel & Felser, Max. (2006). Profinet IO-Device Emulator based on the Man-in-the-middle Attack. 437–440. 10.1109/ETFA.2006.355228. Dostupné z: https://ieeexplore.ieee.org/document/4178343

[23] W. Granzer, C. Reinisch and W. Kastner, "Denial-of-service in automation systems," *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, Hamburg, 2008, pp. 468-471. doi: 10.1109/ETFA.2008.4638438. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4638438&isnumber=4638343

[24] Positive Technologies. Ptsecurity [online]. [cit. 2020-06-18]. Dostupné z: https://www.ptsecurity.com/ww-en/analytics/ics-attacks-2018/

[25] Automaton Direct. Library.automationdirect [online]. [cit. 2020-07-18]. Dostupné z: https://library.automationdirect.com/differences-between-it-and-ot-network-security/

[26] TRANCHARD, Sandrine. THE NEW ISO 31000 KEEPS RISK MANAGEMENT SIMPLE. ISOFocus [online]. 2018 [cit. 2020-07-1]. Dostupné z: https://www.iso.org/news/ref2263.html

[27] Trust Boundaries. Cisco Certified Expert [online]. 2018 [cit. 2020-07-1]. Dostupné z: https://www.ccexpert.us/ont/trust-boundaries.html

[28] Nmap Scripting Engine (NSE) [online]. [cit. 2020-07-18]. Dostupné z: https://nmap.org/book/man-nse.html

[29] What is netstat? [online]. 2019 [cit. 2020-07-3]. Dostupné z: https://www.ionos.com/digitalguide/server/tools/introduction-to-netstat/

[30] Chapter 9. Packet Dissection [online]. [cit. 2020-07-3]. Dostupné z: https://www.wireshark.org/docs/wsdg_html_chunked/ChapterDissection.html

[31] Cyber Threat Source Descriptions [online]. [cit. 2020-07-2]. Dostupné z: https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions

[32] Secure works [online]. 2017 [cit. 2020-07-02]. Dostupné z: https://www.secureworks.com/blog/cyber-threat-basics

[33] Future learn [online]. 2019 [cit. 2020-07-15]. Dostupné z: https://www.futurelearn.com/courses/cyber-security/0/steps/19631

[34] Massachusetts Institute of Technology [online]. [cit. 2020-07-15]. Dostupné z: https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-sgs-ov-controls.html

[35] Die [online]. [cit. 2020-07-18]. Dostupné z: https://linux.die.net/man/8/arpwatch

[36] Juniper [online]. 2020 [cit. 2020-07-10]. Dostupné z: https://www.juniper.net/documentation/en_US/junos/topics/concept/port-mirroring-qfx-series-understanding.html

[37] TCPDump [online]. [cit. 2020-07-05]. Dostupné z: https://www.tcpdump.org/manpages/

[38] Wireshark [online]. [cit. 2020-07-03]. Dostupné z: https://www.wireshark.org/docs/wsug_html_chunked/

[39] Zeek [online]. [cit. 2020-07-19]. Dostupné z: https://docs.zeek.org/en/current/intro/

Článek na webu

[40] Neumann, Peter & Pöschmann, Axel. Ethernet-based real-time communications with PROFINET IO. In: ResearchGate, ©2020 [online]. Institut für Automation und Kommunikation Magdeburg, 2005 [vyd. 2005-05]. Dostupné z: https://www.researchgate.net/publication/241909069_Ethernet-based_real-time_communications_with_PROFINET_IO

[41] PAN, Michael. Real time communications over UDP protocol. Code project [online]. 2011, 15 November 2011 [cit. 2020-01-05]. Dostupné z: https://www.codeproject.com/Articles/275715/Real-time-communications-over-UDP-protocol-UDP-RT

[42] HUNTER, Harrington. *PROFINET IO: PROFINET Unplugged – An introduction to PROFINET IO* [online]. 2017 [cit. 2020-01-05]. Dostupné z: https://profinews.com/2017/01/whats-in-a-profinet-device-name/

[43] ZURKUS, Kacy. Infosecurity Magazine [online]. [cit. 2020-08-01]. Dostupné z: https://www.infosecurity-magazine.com/news/most-industrial-networks/

[44] LUCIAN, Constantin. CSO online [online]. 2020 [cit. 2020-07-28]. Dostupné z: https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html

[45] FIRCH, Jason. PurpleSec [online]. [cit. 2020-07-25]. Dostupné z: https://purplesec.us/common-network-vulnerabilities/

[46] MAZE, Taylor. Fair Institute [online]. 2018 [cit. 2020-07-24]. Dostupné z: https://www.fairinstitute.org/blog/how-to-use-dread-analysis-with-fair

[47] MIESSLER, Daniel. Daniel Miessler [online]. 2016, DECEMBER 17, 2019 [cit. 2020-07-24]. Dostupné z: https://danielmiessler.com/study/threats-vulnerabilities-risks/

[48] An Introduction To Information Security Description Of Threat Environment And Information Security Policy. Hack2Secure [online]. [cit. 2020-06-03]. Dostupné z: https://www.hack2secure.com/blogs/an-introduction-to-information-security-description-of-threat-environment-and-information-security-policy

[49] Imperva [online]. ©2020 [cit. 2020-07-24]. Dostupné z: https://www.imperva.com/learn/application-security/defense-in-depth/

Vysokoškolské práce

[50] KROUPA, Jiří. *Návrh ovladače pro PROFINET bus coupler* [online]. Brno, 2015 [cit. 2020-01-05]. Diplomová práce. Vysoké učení technické v Brně, Fakulta strojního

inženýrství, Ústav automatizace a informatiky. Dostupné z: http://hdl.handle.net/11012/40832

[51] BŘEZINOVÁ, Barbora. Vyhodnocení využitelnosti protokolu PROFINET v oblasti medicínské techniky. Praha, 2015. Diplomová práce. ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE, Fakulta elektrotechnická, Katedra kybernetiky. Dostupné z: https://dspace.cvut.cz/handle/10467/61746

[52] DOVICA, Martin. *Testování implementace sběrnice PROFINET do systémů Simotion* [online]. Ostrava, 2010 [cit. 2020-01-05]. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava. Dostupné z: http://hdl.handle.net/10084/78634

[53] C. Krügel. Network Alertness: Towards an Adaptive, Collaborating Intrusion Detection System. PhD thesis, Vienna University of Technology, 2002.

[54] KUNEŠ, Jiří. Detekce vícefázových síťových útoků [online]. Brno, 2017 [cit. 2020-07-04]. Dostupné z: https://is.muni.cz/th/kobgu/. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Martin Husák.

[55] ŠUSTER, Filip. Automatická detekce podezřelého síťového provozu pomocí blacklistů [online]. Praha, 2017 [cit. 2020-07-14]. Dostupné z: https://dspace.cvut.cz/handle/10467/79796. Diplomová práce. České vysoké učení technické v Praze, katedra počítačových systémů. Vedoucí práce Tomáš Čejka.

[56] LENKA, Rakesh Kumar a Prabhat RANJAN. A Comparative Study on DFA-Based Pattern Matching for Deep Packet Inspection. 2012 Third International Conference on Computer and Communication Technology [online]. IEEE, 2012, 2012, 255-260 [cit. 2020-07-12]. DOI: 10.1109/ICCCT.2012.59. ISBN 978-1-4673-3149-4. Dostupné z: http://ieeexplore.ieee.org/document/6394708/

[57] SVOBODA, Jakub, Ibrahim GHAFIR a Vaclav PRENOSIL. Network Monitoring Approaches: An Overview. International Journal of Advances in Computer Networks and Its Security [online]. 2015 [cit. 2020-06-20]. ISSN 2250-3757. Dostupné z: https://www.researchgate.net/publication/305957483_Network_Monitoring_Approaches_An_Overview

[58] Ionita, D. & Hartel, Pieter & Pieters, Wolter & Wieringa, Roel. (2014). Current Established Risk Assessment Methodologies and Tools. 10.13140/RG.2.2.22914.68806. Dostupné z: https://www.researchgate.net/publication/308887387_Current_Established_Risk_Assessment_Methodologies_and_Tools?channel=doi&linkId=57f4c32608ae91deaa5c3ab1&showFulltext=true

Encyklopedie

[59] PROFINET – HMK Wiki. [online]. Dostupné z: http://wiki.hmkdirect.com/mediawiki/index.php/PROFINET

[60] DCE/RPC - The Wireshark Wiki. FrontPage - The Wireshark Wiki [online]. Dostupné z: https://wiki.wireshark.org/DCE/RPC

[61] What is Suricata. In: Open Information Security Foundation [online]. [cit. 2020-02-02]. Dostupné z: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata

Obrázek na webu

A Layer 2 Ethernet Frame. In Profinet University [online]. PROFINET University, © 2019. [cit. 05.01.2020]. Dostupné z: https://profinetuniversity.com/profinet-basics/profinet-communication-channels/

Non Real-Time packet with additional protocol data. In Profinet University [online]. PROFINET University, © 2019. [cit. 05.01.2020]. Dostupné z: https://profinetuniversity.com/profinet-basics/profinet-communication-channels/

Profinet IRT Communication Telegrams. In HMK Wiki, © 2020 [cit. 05. 01. 2020]. Dostupné z: http://wiki.hmkdirect.com/mediawiki/index.php/PROFINET

FAUZI, Rokhman, Suhono H. SUPANGKAT a Muharman LUBIS. The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework. In: Research gate [online]. 2018 [cit. 2020-08-02]. Dostupné z: https://www.researchgate.net/publication/326554343_The_PDCA_Cycle_of_ISOIEC_27005_2008_Maturity_Assessment_Framework/figures?lo=1