VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH MONITORINGU KRITICKÉ KOMUNIKAČNÍ INFRASTRUKTURY PRO ENERGETICKOU SPOLEČNOST

A CONCEPT OF MONITORING CRITICAL INFORMATION INFRASTRUCTURE FOR ENERGETIC COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Michal Ševčík

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michal Ševčík**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh monitoringu kritické komunikační infrastruktury pro energetickou společnost

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem diplomové práce je vytvoření analytického prostředí pro monitoring a mapování kritické informační infrastruktury před nasazením komerčního řešení. Vytvoření analytického prostředí je popsané v analytické časti diplomové práce. Praktická část diplomové práce je tvořená daty sesbíranými z vytvořeného analytického prostředí a skenováním zranitelnosti rozvodny pomocí programu Nessus. Výstup praktické části je návrh počtu a typu sond, které budou případně umístněné v provozní síti.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK P., V. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ISO/IEC 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Revize publikace. Praha: Český normalizační institut, 2017.

JORDÁN, V. Infrastruktura komunikačních systémů II: kritické aplikace. Brno: Akademické nakladatelství CERM, 2015. 232 stran. ISBN 978-80-214-5240-4.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práca sa zaoberá monitoringom kritickej infraštruktúry, kritickej informační infraštruktúry a mapovaním siete v energetike. Cieľom je vytvoriť analytické prostredie pre spracovanie logov danej siete, zmapovať najkritickejšie úseky siete a implementovanie monitorovacích a sieťových prvkov, ktoré zvýšia bezpečnosť a zminimalizujú riziko bezpečnostných udalostí alebo incidentov.

Klíčová slova

SCADA, IDS, IPS, SIEM, ICS, ELK Stack, Netflow, Syslog, Kybernetická bezpečnosť, Kritická infraštruktúra, Kritická informačná infraštruktúra

Abstract

Diploma thesis deals with monitoring critical infrastructure, critical information infrastructure and network monitoring in energetic industry. The goal is to create analytical environment for processing logs from the network, to map the most critical segments of the network and implementation of monitoring and network devices, that increase security and mitigate risks of security events or security incidents

Key words

SCADA, IDS, IPS, SIEM, ICS, ELK Stack, Netflow, Syslog, Cyber-security,Critical infrastructure, Critical information infrastructure

Bibliografická citace vaší práce

ŠEVČÍK, M. *Návrh monitoringu kritické informační infrastruktury pro energetickou společnost.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 90 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil/a autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2018

_____

podpis studenta

Poďakovanie

Chcel by som poďakovať pánovi Ing. Sedlákovi za vedenie mojej diplomovej práce, kolegom v práci za ich cenné rady a čas. Ďalej by som chcel poďakovať rodine a priateľom, ktorí ma podporovali pri písaní tejto práce.

Content

ÚVOD

Bezpečnosť sietí a komunikácie bola vždy doležitým aspektom v informačných a komunikačných technológiach. Avšak masívny rozvoj týchto technológií v sebe skrýva mnohé bezpečnostné riziká, na ktoré sa nebral ohľad, hlavne čo sa týka smart zariadení (IOT), kde nie je implementovaná security by design & default. Tieto zariadenia sa postupom času integrujú všade, kde je to možné a vytvárajú tým nové vektory útoku pre kompromitovanie firemných, provozních alebo domácich sietí. Svet IOT je len jedna časť problému zabezpečenia sietí, ktorým je nutné v tejto dobe čeliť. S rozvojom techniky prichádzajú na scénu sofistikované malwary, ktoré prekonávajú hranice kybernetického sveta a ich dopad sa výrazne prejavuje v reálnom svete napríklad fyzickým poškodením generátorov, zmenie pravidiel dopravnej komunikácie a tým ohrozenie ľudských životov alebo zhodenie energetických sietí → Blackout. Týmito sofistikovaným malwarmi disponujú štáty alebo veľmi dobre financované hackerské skupiny, ktoré ich využívajú ako zbrane pre dosiahnutie svojich politických alebo ekonomických cieľov. Tieto malwary sú teda väčšinou cielené na kritickú infraštruktúru alebo kritickú informačnú infraštruktúru aby ochromili kľučové segmenty štátov (zdravotníctvo, doprava, energetika...atď.), pre túto činnosť využívajú hlavne zranitelnosti zero-days. Zranitelnosti, ktoré zatiaľ neboli detekované a je tým pádom náročné sa proti ním brániť, bez implementácie sofistikovaných nástrojov a opatrení pre monitorovanie a zabezpečenie sietí.

CIEĽ A METODIKA PRÁCE

Diplomová práca sa zameriava na implementáciu nástrojov pre monitoring provoznej siete energetickej spoločnosti, tieto opatrenia zvýšia bezpečnosť siete a znížia dopad rizík spojených s kompromitovaním energetickej siete.

Konktrétne sa jedná o implementácie IDS a Netflow sond, pomocou ktorých sa pokryje sieťová komunikácia v rámci OT siete. Umiestnenie sond vyplýva z analýzy siete na základe interných dokumentácií a konzultácií s provozným a SCADA oddelením.

Dôležitým miľníkom tejto činnosti je vybudovanie testovacieho polygonu, ktorý slúži pre základný monitoring sieťovej komunikácie → zber logov. Jeho výstavba je popísaná v analytickej časti diplomovej práce.

V praktickej časti je na základe analýzy a zozbieraných dát v testovacom polygone vytvorený návrh pre umiestnenie IDS a Netflow sond. Tento návrh sa opiera o ISO normy z radu 27k a metodiku best-practices v danej oblasti.

Slovník

ASI	Asset Inventory
BCM	Bussines Continuity Management
CIT	Firemná sieť
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarizovaná zóna
EOL	End-of-Life
GOOSE	Generic Object Oriented Substation Event
HIDS	Host-based Intrusion Detection System
HMI	Human machine interface
ICS	Industrial Control System
IDS	Intrusion detection system
IPS	Intrusion prevetion system
IT sieť	Vonkajšia sieť / Firemná sieť / Internet
KB	Kybernetický Bezpečnosť
KI	Kritická infrastrštrkúra
KII	Kritická informačná infraštrukúra
MMS	Manufacturing Message Specification
MTBF	Mean time between failure
NIDS	Network-based Intrusion Detection System
OT	Provozná / Procesná sieť
PAC	Process Automation Controller
PIT	Provozná sieť
PLC	Programmable logical controler
RTU	Remote terminal unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operation Center
VPN	Virtual Private Network

1 Teoretická časť

1.1 Kritická infraštruktúra

Kritická infraštruktúra (ďalej iba KI) predstavuje výrobné a nevýrobné systémy a služby, ktorých nefunkčnosť má vážny dopad na kontinuitu riadenia, bezpečnosť, ekonomiku, verejnú správu štátu a zabezpečenia základných životných potrieb obyvateľstva. Pri výpadku niektorého zo segmentov KI môže dôjsť k stratám na ľudských životoch. Medzi segmenty KI patrí napríklad zdravotníctvo, letiská a vo všeobecnosti doprava, energetika atď. To či určitý segment spadá na základe kritérií do KI je možné nájsť vo normách ISO 27k. Ochrany KI je jednou zo základných úloh štátu a provozovateľov KI. (16)

1.2 Kritická informačná infraštruktúra

Kritická informačná infraštruktúra (ďalej iba KII) je komplex informačných a komunikačných systémov KI, ktoré napĺňajú stanovené kritéria a odvetvové kritéria v oblasti kybernetickej bezpečnosti (ďalej iba KB) a ich nefunkčnosť by mohla opäť spôsobiť závažný dopad na bezpečnosť štátu, zabezpečenie základných ľudských potrieb obyvateľstva zdravie a ekonomiku štátu. V pojatí prostredia energetiky sa jedná ochranu SCADA systémov. (16)

1.3 Supervisory Control and Data Acquisition (SCADA)

SCADA alebo dispečerské riadenie a zber dát je všeobecný pojem pre počítačový systém, ktorý je schopný spracovávať dáta operačného riadenia na veľké vzdialenosti. SCADA avšak nie je plnohodnotným riadiacim systémom, ale zameriava sa na úroveň supervisora (dispečera) a dohľad nad priemyselnými a kritickými infraštruktúrami v reálnom čase. Z pravidla je to priemyselný kontrolný systém (ICS), ktorý funguje o úroveň vyššie nad skutočným riadiacim systémom založeným napríklad na PLC (programovateľné logické jednotky), RTU (Remote Terminal Unit) alebo iných HW zariadeniach. Tie sú pripojené a vysielajú povely napríklad na inteligentné elektronické zariadenia (ďalej iba IED) , ovládače, ochrany, senzory, ističe... Slúžia ako prostredník medzi SCADA serverom a koncovým IED zariadením a tvoria kľúčovú úlohu pri riadení kritických procesov.

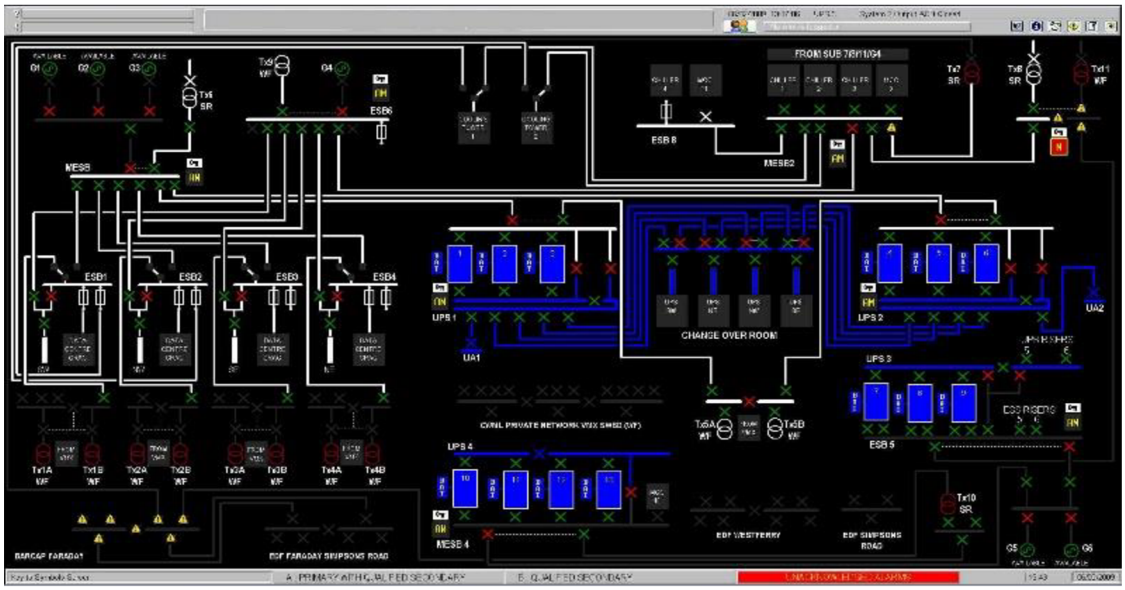
Komplexný SCADA systém sa môže skladať z nasledujúcich komponent:

1. **Operačné zariadenia:** pumpy, ventily, dopravníky a rozdeľovače obvodov v rozvodniach, ktoré môžu byť kontrolované pomocou relé.
2. **Lokálne procesory:** komunikujú s operačným nástrojmi ako sú PLC, RTU, IED a PAC (Process Automation Controller). Jeden lokálny procesor môže byť schopný ovládať a byť zodpovedný za desiatky vstupov a výstupov do operačných zariadení.
3. **Nástroje:** Umiestnené v teréne alebo vo vnútri budovy, ktoré monitorujú teplotu, pH, tlak, množstvo elektrickej energie a prietoky vody.
4. **Krátke komunikácie:** Medzi lokálnym procesorom, nástrojmi a operačnými zariadeniami. Tieto relatívne krátke spojenia, či už káblové alebo wireless komunikácie posielajú analógový a diskrétny signál na báze napätia alebo prúdu, alebo využívajú všeobecné priemyselné protokoly.
5. **Diaľkové komunikácie:** Medzi lokálny procesorom a host computer. Tieto komunikácie bežne pokrývajú niekoľko kilometrové vzdialenosti a využívajú sa prenosové metódy napríklad ako telefóne linky, satelitná komunikácia, mikrovlny, GPRS dáta, optické linky.
6. **Host computer:** Sa správa ako centrálny riadiaci a monitorovací bod. Host computer je umiestnený v dohľadovom centre, kde operátor provozu dohliada na sieť a dostáva prípadne alarmy, kontroluje prijate logy vykonáva kontrolu. Host computer môže byť reprezentovaný ako HMI station alebo Engeneering station viz. obrázok(Obecná architektúra SCADA systému) (3)

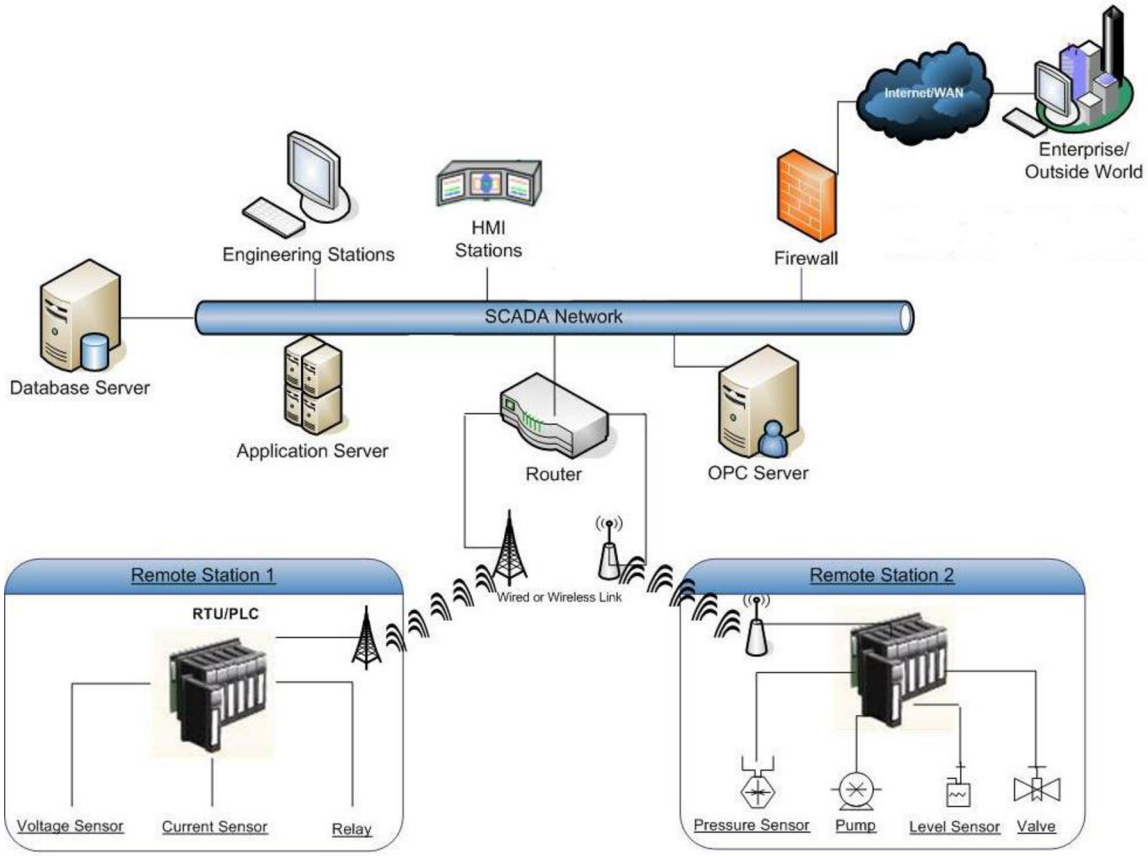
1.4 Human Machine Interface

HMI je skratka pre Human machine interface, rozhranie medzi človekom a strojom, odkiaľ je operátor schopný napríklad prerušiť alebo spustiť elektrický obvod. Alebo inak povedané rozhranie medzi procesmi a operátorom. Je to primárny nástroj pomocou ktorého operátor koordinuje a kontroluje výrobné, priemyselné alebo dohladové procesy. HMI zobrazuje near-real time informácie HMI rozhranie automaticky operátora upozorní keď nastane nejaký problém. V prostredí energetiky sa môže jednať o zlyhanie ochrany, alebo výpadok primárnej trasy obvodu napríklad v rozvodni alebo energetickej sieti. Na tieto abnormálne situácie sú potom nastavené procesy, ktoré je operátor schopný vykonať

na diaľku, alebo v prípadne ak to nie možné, fyzicky sa tým technikov dostaví na určité miesto a problém odstráni. (9)

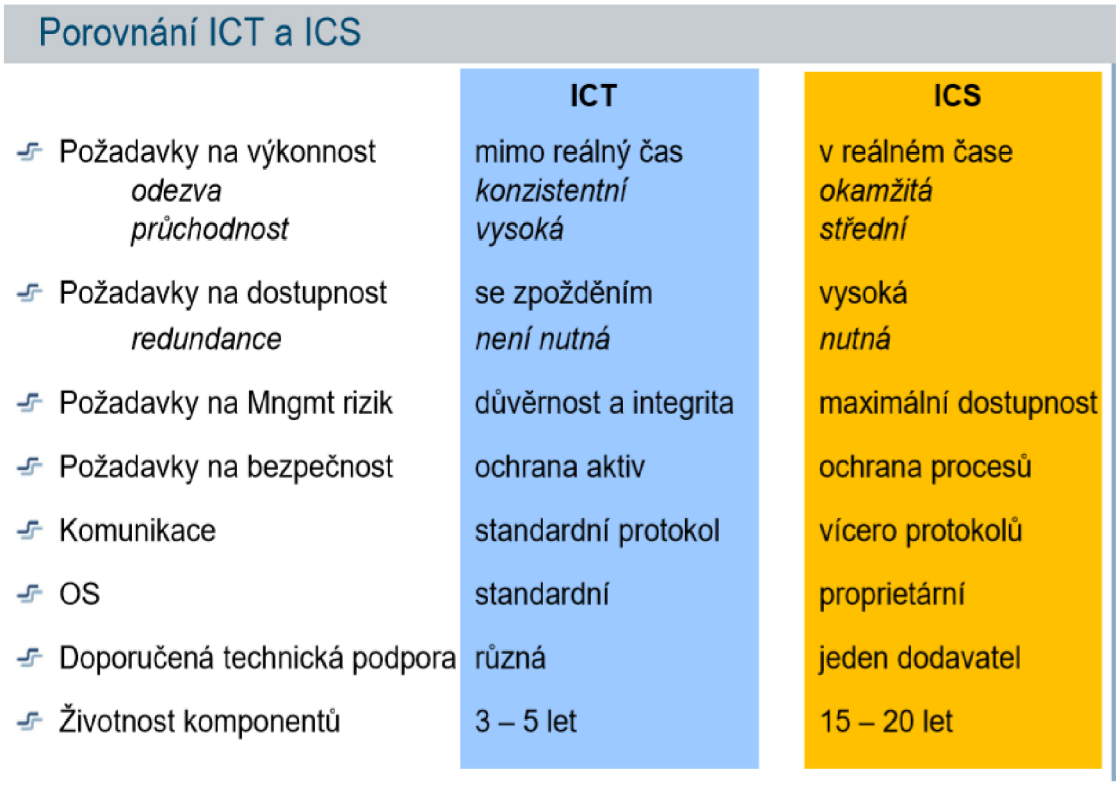


Obrázok 1: HMI rozhranie



Obrázok 2: Obecná architektúra SCADA systému

1.5 ICT a ICS rozdiel



Obrázok 3: Rozdiel medzi ICT a ICS prostredím (zdroj: Ing.Sedlák)

1.6 Kybernetická bezpečnostná udalosť

Je udalosť, ktorá môže spôsobiť narušenie bezpečnosti informácií v kybernetickom priestore. Zatiaľ nemá dopad na aktíva a môže sa jednať o false possitive situáciu. Príkladom takejto bezpečnostnej udalosti môže byť alert log v monitorovacom centre, kde sa zobrazí alert ohľadom sieťovej komunikačnej anomálie. Táto anomália môže byť pripojenie nového zariadenia do siete, napríklad koncové zariadenie (počítač) alebo aktívneho prvku, ktorý sa zatiaľ nenachádza vo whiteliste. Potom je na SOC týme túto udalosť spracovať, spraviť report a overiť či sa jedná a false possitive alebo possitve situáciu a narušenie kybernetickej bezpečnosti. Neriešenie takejto situácie môže viesť ku kybernetickému bezpečnostnému incidentu. (27)

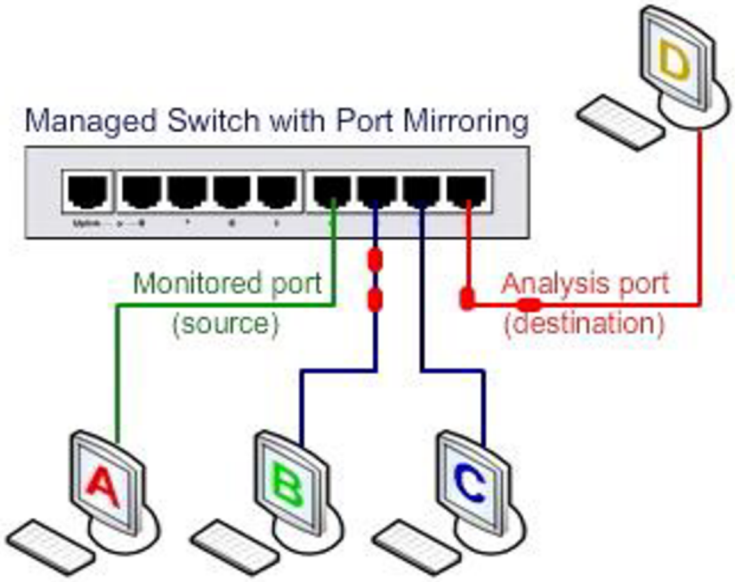
1.7 Kybernetický bezpečnostný incident

Kybernetický bezpečnostný incident je narušenie bezpečnosti informácií v kybernetickom priestore v dôsledku kybernetickej udalosti. Medzi praktické príklady môžeme patriť zhodenie serveru DDoS, odpočutie komunikácie pomocou MITM útoku, alebo zanesenie malwaru do siete. Keď nastane bezpečnostný incident, znamená to

prekonanie všetkých bezpečnostných opatrení, ktoré sa v sieti nachádzajú a ďalším krokom by napadnutá spoločnosť mala vyhodnotiť dopad bezpečnostného incidentu, mať vytvorený BCM, DLP a následne zistiť vektoru útoku. Na to, aby sme zistili vektor útoku je potrebná forenzná analýza, aby mohla byť forenzná analýza úspešná, je nutné poznať detailne sieť, jej prestupy a mať vytvorené čo najpodrobnejšie asset inventory. Bez podrobného asset inventory aj keď je sieť pokrytá mnohými sondami, tak sa nemusí daný priestor pokryť a zistiť vektor útoku, pretože nevieme presne na aké segmenty a prestupy dozerať a čo všetko monitorovať, prípadne čomu jednotlivé odhalené IP adresy prislúchajú (7, 16)

1.8 Port Mirroring

Port mirroring je metóda monitorovania sieťového trafficu. S povoleným port mirroringom, switch odosiela kópie všetkých sieťových paketov prechádzajúcich portom, na ktorom je táto funkcionalita povolená a zrkadlí ich na voľný port switchu, kde je pripojený určitý druh analytického zariadenia, ktoré je schopné daný traffic prijať, zanalyzovať a detekovať sieťové abnormality. Túto funkcionalitu podporujú takmer všetky komerčné switche. Počet portov, ktoré sa dajú mirrorovať na jednom zariadení je individuálny a záleží to od typu zariadenia. (15)



Obrázok 4: Port Mirroring provozu medzi zariadením A a B

Na obrázku 3. je zobrazená komunikácia medzi zariadením A a zariadením B. Zobrazený switch podporuje port mirroring funkcionalitu a administrátor je schopný nastaviť zrkadlenie trafficu prechádzajúceho portami, na ktoré sú pripojené zariadenia A a B do portu, na ktorom je pripojené zariadenia D. Toto zariadenie môže byť využité napríklad na logovanie alebo monitorovanie sieťové provozu cez daný uzol. Za praktický príklad takéhoto zariadenia, alebo analytického nástroja môžeme považovať SIEM, alebo IDS sondu. Týmto spôsobom je možné nahrávať aj napríklad telefónu komunikáciu, ak namiesto počítaču A a B máme VOIP telefóny.

1.9 Port Forwarding

Port forwarding je sieťová technika pomocou ktorej gateway, alebo podobné zariadenie vysiela všetkú prijatú komunikáciu špecifického portu na rovnaký port vnútorného sieťového nodu. Port forwarding sa primárne využíva na segregáciu sieťového provozu, optimalizovanie rýchlosti siete a permanentnému priradeniu sieťovej cesty, konkrétnemu protokolu, alebo sieťovej službe. Vo všeobecnosti port forwarding používa známe (dedikované) čísla portov. Predpokladajme, že router obdrží IP adresu a číslo portu v hlavičke paketu. Ak router nie je nakonfigurovaný na port forwarding, tak najprv identifikuje port pred rozoslaním. Avšak ak port forwrding je nakonfigurovaný, tak automatizovane prenesie paket na vnútornú destináciu nodu. Celý tento proces port forwadingu je transparentý pre všetkých sieťových klientov. (11)

1.10 Security operation center a jeho funkcie

Security Operations Center (SOC) je organizovaný tím ľudí, ktorých cieľom je kontinuálne monitorovanie a zdokonaľovanie bezpečnosti spoločnosti. SOC tím je zodpovedný za implementácie opatrení, ktoré znížia riziko kompromitovania siete. Ich kľúčovou činnosťou je predísť bezpečnostnému incidentu, analyzovať sieťovú komunikáciu a agilne reagovať na bezpečnostné udalosti pomocou dobre zavedených technológií a procesov. Stratégia SOC tímu musí byť presne a jasne definovaná a je veľmi závislá na podpore vedenia z organizačného, ale aj finančného hľadiska. Inak SOC tím nemôže efektívne vykonávať svoju činnosť a nebude vnímaný ako kritické aktívum zvyškom organizácie. SOC tím musí cieliť na adresovanie bezpečnostných požiadavkov a to si vyžaduje silnú podporu z vedenia, zavádzanie opatrení je ekonomicky nákladné a vyžaduje vo väčšine procesov zmeny. Pri výstavbe SOC tímu sa musí brať aj ohľad

napríklad na fyzické zabezpečenie ich pracoviska, pretože primárne narábajú s citlivými informáciami. Ako náhle je jasne definovaný scope SOC tímu je nutné implementovať technológie, pomocou ktorých bude schopný efektívne vykonávať svoju činnosť. Medzi takéto technológie napríklad patrí: firewally, IDS/IPS sondy, breach detetection solutions a najhlavnejšou komponentov je SIEM, ktorý slúži pre efektívny zber informácií z jednotlivých zdrojov. Flow dát, telemetrické údaje, packet capture, syslog, netflow a ďalšie udalosti sa musia zbierať, korelovať a analyzovať z bezpečnostnej perspektívy. Čím viac informáciami SOC tím disponuje, tým efektívnejšie je schopný pracovať, nutnosťou je taktiež vulnerability manažment, ktorý ovplyvňuje všetky nastavené bezpečnostné pravidlá a procesy a je nutné ho zaviesť, pretože nie všetky zraniteľnosti a s nimi spojené riziká sa dajú odstrániť. Vo väčšine prípadov sa SOC tím snaží dohliadať na zraniteľnosti a voliť opatrenia tak, aby dopad rizika bol čo najmenší. (28)

Obrázok 5: Činnosti Security Operation tímu

1.11 Intrusion Detection System

Intrusion detection system (ďalej iba IDS) je systém, ktorý monitoruje sieťový provoz a detekuje podozrivú sieťovú komunikáciu. V prípade výskytu takejto komunikácie je zhotovený log alebo alert, na ktorý je operátor upozornený a musí danú situáciu preveriť. Napriek tomu, že IDS monitoruje sieťovú komunikáciu pre potencionálne škodlivý kód alebo aktivitu, IDS sonda často hlavne v začiatočných fázach implementácie vyhadzuje mnoho false possitive logov. Táto situácia je v skorých štádiach implementácie IDS sondy bežná a je na operátorovi aby sondu nastavil a vyhodnotil, či sa jedná o false possitive log, alebo o bezpečnostnú udalosť. Vo väčšine prípadov sondy majú self-learning module, pomocou ktorého sú schopné sa časom naučiť či sa jedná legitimný provoz, alebo nie. Každopádne, na tento modul nie je dobré sa spoliehať a vždy si vyžaduje kontrolu operátora, pretože problém nastáva, ak sieť je už kompromitovaná nejakým malwarom, tak sonda v ranných štádiách túto komunikáciu môže vyhodnotiť ako false possive situáciu a už ju v budúcnosti nelogovať. Preto je nutné mať podrobne zmapovanú logickú topológiu siete a pre prípadné overenie legitímnosti sieťovej komunikácie vytvoriť napríklad Honeypot. (23)

Rôzne typy IDS systémov

IDS sondy fungujú na viacerých princípoch detekovania podozrivej sieťovej komunikácie. Medzi tieto princípy patrí:

- Sieťová IDS sonda (ďalej iba NIDS) je umiestnená na strategickom bode v sieti odkiaľ môže monitorovať všetok prichádzajúci a odchádzajúci sieťový provoz zo všetkých aktívnych prvkov danej siete.
- HOST IDS sonda (ďalej iba HIDS) sa vyskytuje na jednotlivých koncových zariadeniach, napríklad koncových staniciach (počítačoch) alebo na serveri. HIDS takto môže detekovať priamo, či na koncové zariadenie prichádza nejaká škodlivá komunikácia, ktorú nebola schopná detekovať NIDS sonda. Toto ale platí aj opačne a to v prípade, že z koncového zariadenia je odosielaná škodlivá komunikácia. Avšak osadiť rozsiahlu sieť HIDS sondami je nereálne riešenie a sú využívané NIDS sondy.
- Signature-based IDS sonda je typ sondy, ktorý funguje na báze signatúr. Sonda obsahuje databázu predefinovaných signatúr so škodlivým kódom, voči ktorej

porovnáva obdržaný sieťový provoz. Väčšina sond tohoto typu podporuje funckionalitu napísania si vlastných, alebo upravenie si predefinovaných signatúr a tým pádom ju presne vyladiť na danú sieťovú oblasť / komunikáciu. Písanie signatúr prebieha pomocou regulárnych výrazov.

- Anomaly-based IDS sonda pracuje na základe detekcie anomálií sieťovej komunikácie. Táto funkcionalita sa využíva nie len v priemyselnom prostredí a jej odlišnosť od Signature-based sondy je v tom, že neporovnáva sieťový provoz voči databáze so známymi exploitami, alebo obsahuje white-list sieťových príkazov a komunikácie a porovnáva ich atribúty. Medzi takéto atribúty môže patriť dĺžka určitého komandu na nejaké IED. Týmto spôsobom sa detekujú hlavne zero-day útoky, proti ktorým ešte nie sú vytvorené signatúry a útoky sú neznáme.

Monitorovanie pomocou IDS sondy patrí do kategórie pasívneho monioringu sieťe, kde neobmedzujeme dostupnosť služieb, ktoré sú prioritné pre ICS prostredie. (8, 22, 23)

1.12 Intrusion Prevention System

Intrusion prevetion system (ďalej iba IPS) sa dá najlepšie prirovnať k firewallu. V klasickom firemnom firewalle je niekoľko desiatok alebo stoviek pravidiel. Väčšina z týchto pravidiel sú povoľovacie pravidlá: “allow the traffic through“. Keď firewall obdrží paket, tak hľadá pre daný paket pravidlo, ktoré mu dovolí prejsť firewallom. Ak sa pri prechádzaní zoznamu pravidiel nenájde pravidlo, ktoré danú komunikáciu povolí, tak je tam posledné pravidlo „drop/deny“, ktoré daný paket zahodí a nedostane sa do cieľovej destinácie. IPS pracuje na tomto princípe, ale inverzne. IPS obsahuje tak ako firewall desiatky alebo stovky pravidiel, ktoré sú blokovacie takzvané „deny rules“, napríklad zablokuj tento bezpečnostný problém v komunikácií. Keď sa paket dostane na IPS, IPS prejde zoznam svojich pravidiel od vrchu nadol a hľadá dôvod, prečo daný paket zahodiť. V prípade, že žiadny dôvod nenájde, paket je prepustený a dostane sa do cieľovej destinácie. Hlavný dôvod prečo mať IPS umiestnenú v sieti je možnosť blokovania dobre známych útokov / exploitov naprieč sieťou. Monitorovanie pomocou IPS sondy patrí medzi aktívny prístup monitorovania siete. Tento prístup má ale nevýhodu v rámci obmedzenia dostupnosti služieb a pre vyladenie tohoto systému je nutné podrobne poznať komunikáciu v sieti. (8, 23)

Rozdiel medzi IDS a IPS

Hlavný rozdiel medzi IDS a IPS sondou je ten, že IDS sonda nám neobmedzuje dostupnosť siete služieb a patrí medzi pasívny prístup monitoringu siete a jej umiestnenie aby sa pokryla celá komunikáciu v sieti musí byť na aktívnom prvku cez ktorý všetok traffic prechádza alebo sme schopný z takýchto oblastí pokiaľ ich je viac mirrorovať daný traffic do IDS sondy.

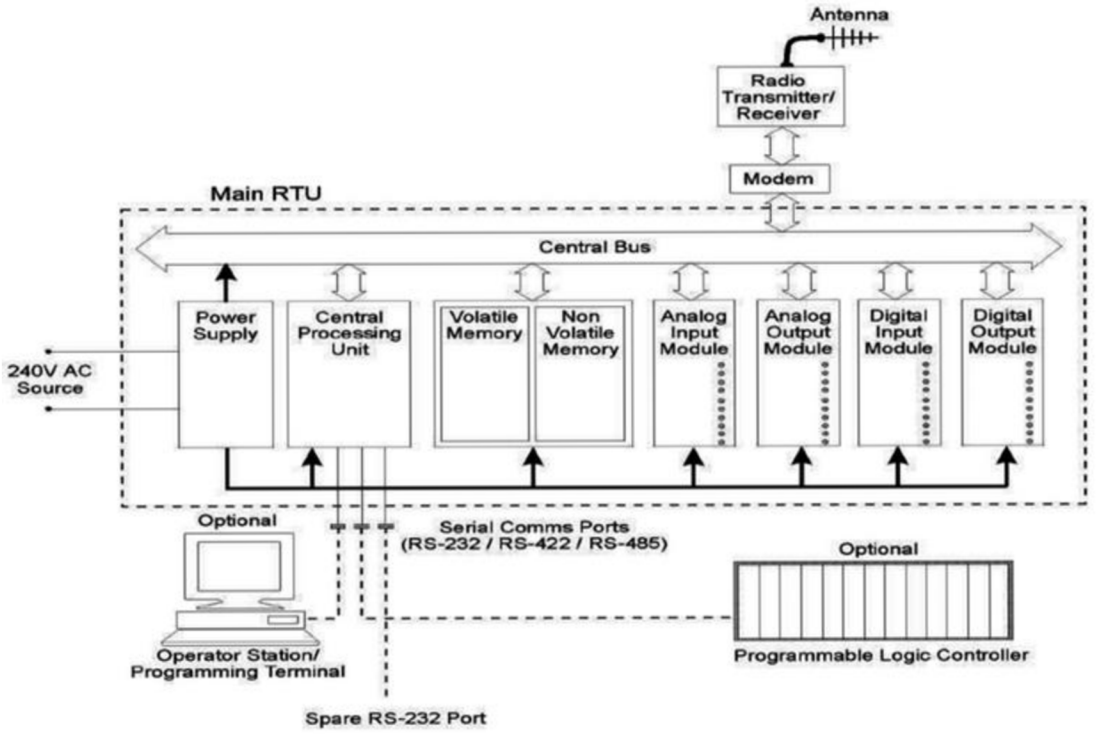
Aby bola IPS sonda validne použitá musí byť umiestnená do priamo v sieťovej ceste ku koncovému zariadenia alebo segmentu siete, ktorý má monitorovať. Týmto spôsobom sa ale značne obmedzuje dostupnosť daného segmentu alebo služby.

1.13 Remote Terminal Unit

Remote terminal unit (ďalej len RTU) je viacúčelové zariadenie využívané na vzdialený monitoring a kontrolu rôznych zariadení a automatizovaných systémov. Typicky je aplikované v priemyselnom prostredí, slúži podobnému účelu ako PLC, ale pracuje na vyššej úrovni. RTU môžeme považovať sa samostatný počítač, pretože všetky jeho časti dohromady spĺňajú definíciu počítača: procesor, pamäť a úložisko. Pre tieto vlastnosti v môže byť využité ako intellignet controller, alebo master controller pre zariadenia, ktoré spolu automatizujú určitý proces, ako výrobná linka v automobilovom priemysle. RTU sú pokročilejšie verzie PLC zariadení, tieto zariadenia komunikujú v binárnom kóde a ich programovanie prebieha pomocou asembleru. RTU sú inteligentné zariadenia schopné kontrolovať a spracovávať množstvo procesov bez intervencie užívateľa, alebo inteligentnejšieho sieťového prvku. Pre tieto vlastnosti je hlavne využívané v distribuovaných kontrolných systémoch (ďalej len DCS) a v SCADA systémoch, odosielaním telemetrických údajov do monitorovacieho centra a príjmaním príkazov z monitorovacieho centra. Vzhľadom na dodávateľa zariadenia, účel a model, RTU môžu byť modulovateľné a obsahovať rôzne obvodové karty a komunikačné rozhrania, záložné zdroje a rôzne druhy analógových digitálnych I/O rozhraní pre rôzne systémy. Pre ich modulárnosť a odlišnosti prostredia v ktorom sa nachádzajú, nemusia byť ani kompaktibilné. RTU využívané v telekomunikáciach nemusí byť použiteľné pri ropných a plynových aplikáciach, pretože procesy, ktoré tieto zariadenia majú riadiť sú kompletne odlišné. (24)

Prostredia v ktorých sa RTU využívajú:

- Petrochemický a ťažobný priemysel
- Jadrové elektrárne
- Vodné elektrárne
- Tepelné elektrárne
- Poľnohospodárstvo
- Kontrola kvality
- Chemická priemysel
- Čističky odpadových vôd
- Automobilový priemysel
- Potravinárska výroba
- Výroba liečiv



Obrázok 6: Príklad schémy RTU zariadenia

1.14 Demilitarizovaná zóna

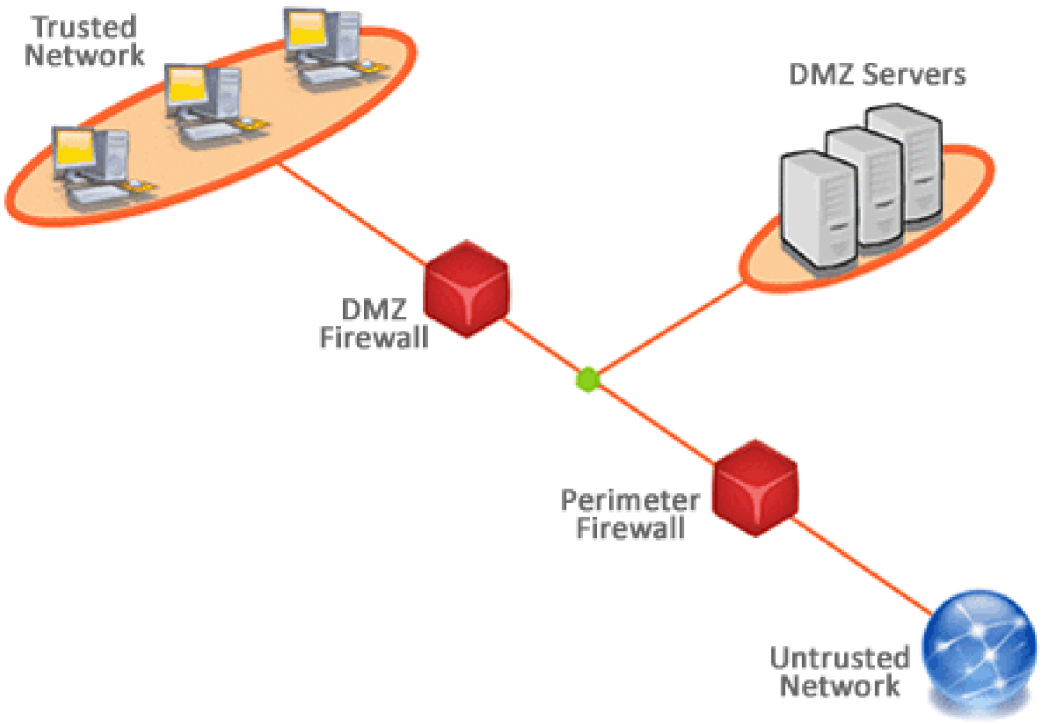
Demilitarizovaná zóna (ďalej iba DMZ) je fyzická alebo logická pod-sieť, ktorá oddeľuje vnútornú sieť od externej siete, väčšinou Internet. DMZ obsahuje servre, ktoré sú vysunuté smerom von a sú prístupné z externej siete, väčšinou sa jedná o:

- Webový server
- Emailový server
- DNS server

Existujú rôzne metódy návrhu DMZ. Najčastejšie metódy obsahujú riešenie s jedným alebo dvomi firewallmi. Architektúra DMZ siete môže byť veľmi široká a obsahovať ďalšie bezpečnostné komponenty, v závislosti od požiadavkov na bezpečnosť siete, pre ktorú je tvorená. Jeden firewall s aspoň tromi sieťovými rozhraniami, môže tvoriť sieť obsahujúcu DMZ. Externá sieť je tvorená od providera na prvom sieťovom rozhraní, na druhom sieťovom rozhraní je vnútorná sieť a DMZ je na treťom sieťovom rozhraní.

Rozdielne druhy firewalloých pravidiel medzi komunikáciou externej siete a DMZ, LAN a Internetom na báze kontroly povolených portov, typu komunikácie povolenej do DMZ z externej siete, limitovaná konektivita na špecifických hostov do vnútornej siete a prevencia nevyžiadaného pripojenia smerom do externej, alebo vnútornej siete je kontrolovaná pomocou DMZ. Viac bezpečné riešenie je využitie dvoch firewallov pre vytvorenie DMZ. Prvý firewall nazývaný aj hraničný firewall je nakonfigurovaný iba na povolenie komunikácie smerom do DMZ z externej siete. Druhý firewall alebo vnútorný firewall povoľuje iba komunikáciu z DMZ do vnútornej siete.

Toto riešenie je pokladané za bezpečnejšie, pretože útočník musí prekonať dve zariadenia s rôznymi pravidlami, aby sa dostal do vnútornej siete. Keďže DMZ segmentuje sieť, bezpečnostné politiky môžu byť špecificky definované pre každý jeden segment. Napríklad IDS/IPS systém umiestnený v DMZ, ktorá obsahuje iba Webový server môže detekovať alebo blokovať všetok provoz, okrem HTTP a HTTPS requestov na port 80 a 443. (25)



Obrázok 7: Obecné schéma DMZ s perimeter firewallom

1.15 Virtual Private Network

Virtuálna privátna sieť (VPN) je technológia, ktorá vytvára bezpečný a zašifrovaný komunikačný kanál cez menej bezpečnú sieť, ako je vo všeobecnosti internet. VPN technológia bola vyvinutá, aby umožnila vzdialeným užívateľom bezpečne sa pripojiť do firemnej siete, aplikácií, alebo iných služieb. Pre zistenie bezpečnosti dáta cestujú cez zabezpečený tunel a užívatelia musia pre prihlásenie do VPN siete využívať autentizačné metódy ako napríklad heslo, token, alebo iné definované unikátne metódy. Využívanie VPN siete má výhody v zaistení určitého levelu bezpečnosti pre pripojenie k určitým systémom, kde samotná infraštruktúra túto funkcionalitu nie je schopná poskytnúť. Nevýhoda využívania VPN je vo výkone, ktorý môžu ovplyvniť rôzne typy faktorov, ako rýchlosť internetu užívateľa, využívanie rôznych typov protokolov a typy šifrovania využívané pre zabezpečenie VPN siete. Existuje niekoľko typov protokolov pre zabezpečenie a šifrovanie dát v rámci VPN siete.

- IP security (IPsec)
- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

- Point-To-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- OpenVPN

Najbežnejším typom VPN sú remote-access VPN a site-to-site VPN

1.15.1 Remote Access VPN

Remote Access VPN využíva verejnú telekomunikačnú infraštruktúru ako internet, pre poskytovanie bezpečného pripojenia užívateľov do firemnej siete. Toto riešenie je veľmi dôležité hlavne v prípade, keď zamestnanci využívajú verejnú Wifi, alebo iné formy pripojenia do internetu pre pripojenie sa do firemnej siete. VPN client na strane užívateľa, ktorý sa snaží nadviazať toto spojenie sa pripojí na VPN gateway firemnej siete. Gateway typicky vyžaduje nejaký prístroj (token) pre autentizáciu daného užívateľa. Následne vytvorí tunel späť k zariadeniu snažiacemu sa o pripojenie do vnútornej siete a umožní mu pripojiť sa do firemnej siete a využívať ju tak, akoby bol pripojený lokálne.

Zabezpečenie remote-access VPN väčšinou využíva IPsec alebo SSL pre bezpečné pripojenie, aj keď SSL VPN sú často využívane a cielené pre vytvorenia bezpečného tunela ku konkrétnej jednej aplikácií ako k celej vnútornej sieti. Niektoré VPN poskytujú Layer 2 access do siete, to však vyžaduje tunneling protokol ako PPTP alebo L2TP fungujúci ponad IPsec pripojením.

1.15.2 Site-to-Site VPN

Tento typ VPN využíva jedno gateway zariadenie pre pripojenie do celej siete z jednej lokality do siete v druhej lokalite. Ako príklad môžeme umiesť pripájanie sa do data centra. Koncový node vo vzdialenej lokalite nepotrebuje VPN clienta, pretože sa o to postará gateway. Väčšina site-to-site VPN, ktoré sa pripájajú cez internet využíva IPsec. Bežné je aj využívanie MPLS cloudov ako verejného internetu. Je možné vytvorenie buď Layer 3 pripojenia (MPLS IP VPN) alebo Layer 2 (Virtual Private LAN Service / VPLS)

VPN siete môžu byť vytvorené aj medzi konkrétnymi počítačmi. Typicky sa môže jednať o servre umiestnené v rôznych datacentrách. (26)

1.16 False Possitive log

Flase possitive log je situácia, kedy v SIEMe sa zobrazí alert s upozornením na nejakú netredičnú činnosť alebo situáciu v sieťovej komunikácií, ktorá avšak neznamená hrozbu nejakej bezpečnostnej udalosti, ale IDS sonda alebo iné zariadenie s bezpečnostnými politikami a pravidlami zodpovedné za monitoring siete ju tak vyhodnotí. Pričom spomínaná činnosť je bežná legitimná situácia, ale definičné pravidlá signatúr IDS sú príliž všeobecné alebo FW pravidlá a politky velmi striktne alebo nepresne definované a tým vznikne tento flase possitive log.

Ako jednoduchý príklad môžeme uviesť prihlasovanie sa cez SSH na určitý aktívny prvok v sieti. Na FW je definované pravidlo, že v prípade troch chybných pokusov o prihlásenie sa pod admin účtom, sa vyhodnotí alert a odošle sa do SIEMu. V skutočnosti sa však deje to, že technik sa snaží iba prihlásiť a tri krát chybne zadal heslo.

No aj napriek tomu je vhodné situáciu preveriť, ideálnejšie je postupom času odstraňovať tieto false possitive logy a vylaďovať pravidlá komunikácie aby ich bolo čo najmenej a SIEM nebol zahltený týmto typom správ.

2 Analytická časť

V tejto časti diplomová práca popisuje nástroje, ktoré bolo nutné implementovať, aby sa mohlo začať mapovanie provoznej siete, konkrétne výstavbu testovacieho polygonu, opis jeho jednotlivých komponentov a analýza aktívnych prvkov provoznej siete. Analýza je zameraná na funkcionalitu aktívnych prvkov, ich plán obmeny a celkovú fyzickú a logickú topológiu siete. Na základe analýzy prostredia je v praktickej časti opísaná voľba opatrení pre zabezpečenie provoznej siete. V analytickej časti diplomovej práce je popísaný proces analýzy prostredia a implementácie opatrení aj z pohľadu projektového riadenia.

2.1 Vybrané oblasti SLEPT analýzy

V tejto sekcií diplomová práca popisuje vonkajšie vplyvy, ktoré nútia energetickú spoločnosť zavádzať príslušné bezpečnostné opatrenia. SLEPT analýza je transformovaná na oblasť energetiky a riadenie bezpečnosti v danej oblasti, jednotlivé časti SLEPT analýzy sa v tomto prípade prelýnajú a nie sú opísané osobitne.(20, 21)

Legislatívne hľadisko

Oblasť energetiky obecne spadá do kategórie kritickej infraštruktúry, definovanie kritickej infraštruktúry je popísané v *Nařízení vlády č. 432/2010 Sb. - Nařízení vlády o kritériích pro určení prvku kritické infrastruktury*. Následne sa na energetickú spoločnosť vzťahuje *Kybernetický Zákon č. 181/2014 Sb.* a *vyhláška č. 316/2014 Sb. o bezpečnostných opatreních.*, preto je spoločnosť nútená prijať opatrenia pre zabezpečenie KI a KII. Voľba opatrení, ktoré zvýšia bezpečnosť siete, je tvorená na základe best practices a ISO noriem z radu 27K.

Dôležitou súčasťou energetiky je regulačný úrad, ktorý pôsobí ako správny úrad pre výkon regulácie v energetike. Hlavné oblasti pôsobnosti úradu sú:

- Regulácia cien
- Vykonávanie dohľadu nad trhom energetického odvetvia
- Monitorovanie a vyhodnocovanie dodržiavania kvality dodávok a služieb v elektriny a plynu
- Rozhodovanie o potrebných licenciách a certifikátoch nezávislosti.

Z ekonomického pohľadu je dodávka elektriny a plynu kľúčová pre energetickú spoločnosť, pretože v prípade nedodania je energetická spoločnosť nútená regulačným úradom platiť svojím zákazníkom odškodné. Ak tento fakt prepojíme na riadenie kybernetickej bezpečnosti, tak zavádzanie opatrení je pre zvýšenie bezpečnosti OT siete nutné jednak pre Kybernetický zákon, pretože pri neplnení si povinností, ktoré z neho plynú sú pokuty v rádoch miliónov korún, a aby sa aj predišlo dodatočným stratám pri neplnení dodávky elektrickej energie.

Technologické hľadisko

Z technologického hľadiska zavádzanie opatrení je nevyhnutnosťou kvôli rozvoju rôznych typov malwaru určených práve na ICS prostredie, pomocou ktorých je možné napríklad zhodiť celú energetickú sieť a tieto malwary prekračujú hranice kybernetického priestoru a ich celkový dopad sa veľmi výrazne odráža v reálnom svete, kde ich následkom vzniká veľká pravdepodobnosť straty na ľudských životoch. Medzi praktické príklady malwaru patrí napríklad: Stuxnet, NoPetya, Industroyer, Crash-Override. Tieto malwary patria medzi najničivejšie z pomedzi tých, s ktorými sme sa zatiaľ stretli. Takýmito malwarmi disponujú štáty, alebo organizácie s veľmi veľkými finančnými zdrojmi a následne ich využívajú ako zbrane na dosiahnutie svojich ekonomických alebo politických cieľov.

Čo nadväzuje na sociálny a politický faktor. Ukážkovým príkladom je využitie malwaru Stuxnet, pomocou ktorého Izrael a USA sabotovali Iránsky jadrový program. Konkrétne, tento malware podvrhoval telemetrické údaje odosielané do dispečerského riadiaceho centra a menil otáčky rotora umiestneného v centrifúgach na obohacovanie uránu. Tým spôsoboval výrobu nekvalitného uránu, ktorý nespĺňal dané kritéria a tým brzdil celý výrobný proces. Toto bola prvá fáza daného malwaru. V druhej fáze sa malware správal agresívnejšie, dochádzalo k častejším poruchám centrifúg, už nie iba ich rotorov tým, ako sa menili otáčky, ale jednotlivé centrifúgy začali praskať v dôsledku nárastu tlaku vo vnútri zariadenia. Stuxnet totižto zablokoval vývod z centrifúgy, kadiaľ mal odchádzať do zberného kontajneru už obohatený urán a odosielal pozmenené telemetrické údaje do riadiaceho centra, kde prístroje vykazovali normálne hodnoty. Stuxnet aj napriek tomu, že sa nevzťahuje na energetické prostredie, tak jeho princíp fungovania je pre napadnutie ICS systémov využiteľný. Princíp je využitie zero-days zraniteľnosti. Ide o využitie

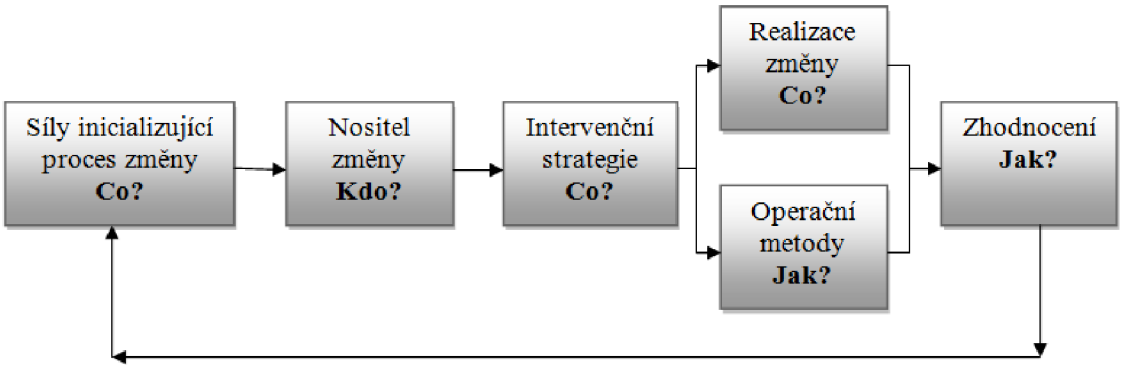
chyby implementovanej do algoritmu, alebo protokolu, podľa ktorého sa riadia kľúčové zariadenia v ICS prostredí. Chyba môže byť spôsobená náhodne, napríklad neošetrením nejakej výstupnej hodnoty procedúry → chyba programátora, alebo sa môže jednať o naschvál implementovaný backdoor dodávateľom zariadení.

Na prostredie energetiky sa vzťahuje hlavne malware Industoryer, ktorý tvorí najväčšiu hrozbu od čias kedy sa vypustil Stuxnet. Industroyer sa vyskytol na Ukrajne a spôsobil v Kyjeve výpadok dodávky elektriny. Tento malware využil zraniteľnosti práve v štandardizovaných protokoloch: IEC 60870-5-101, IEC 60870-5-104, IEC 61850 a OLE for Process Control Data Access (OPC DA). Protokoly a ich komunikácia v rámci siete je opísaná v závere analytickej časti. V dobe, keď tieto štandardizované protokoly vznikali približne pred 20 rokmi sa na bezpečnosť, alebo zabudovanie bezpečnostných prvkov do týchto protokolov nebral ohľad. Bolo to z dôvodu oddelenia OT siete od vonkajšieho sveta (Internetu), čo ale v tejto dobe a s rozvojom technológií nie je možné a vznikajú rôzne prestupy a vektory ako sa do OT siete dostať.

Priemerná doba odhalenia malwaru v sieti pri plne vybudovanej infraštruktúre môže dosiahnuť 230 dní.

Ďalším aspektom je rozširovanie energetickej siete a jej strategický rozvoj. Koncept SmartGrid, kde sa do energetickej siete začínajú implementovať rôzne smart IOT zariadenia, ktoré nemajú v sebe zabudovanú security by default & design a decentralizovanosť energetiky vytvára nové vektory útoku na OT sieť. Hrozby a riziká s nimi spojené sú ťažko manažovateľné bez sofistikovaných bezpečnostných nástrojov a bezpečnostných opatrení.

2.2 Lewinov model riadenej zmeny



Obrázok 8: Lewinov model zmeny

Implementácia bezpečnostných opatrení v energetickej spoločnosti predstavuje zmenu, ktorú je nutné naplánovať a identifikovať jednotlivé činitele zodpovedné za túto činnosť.

Sily inicializujúce proces zmeny

Dôvody, prečo firma pristupuje k zmene, sú popísané podrobnejšie v SLEPT analýze transformovanej na prostredie energetiky v predchádzajúcej kapitole. Hlavné dôvody vyplývajú z nasledujúcich zákonov:

- *Nařízení vlády č. 432/2010 Sb. - Nařízení vlády o kritériích pro určení prvku kritické infrastruktury.*
- *Kybernetický Zákon č. 181/2014 Sb.*
- *Vyhláška č. 316/2014 Sb. o bezpečnostných opatreních*

Kontrolný orgán v tejto činnosti zastáva Národný úrad pro kybernetickou a informační bezpečnosť (NÚKIB), ktorý zároveň aj poskytuje odborné rady v kľúčových procesoch a návrhoch bezpečnostných opatrení.

Nositeľ zmeny

Keďže sa jedná o energetickú spoločnosť s mnohými zamestnancami, je nutné definovať, ktoré oddelenie bude za nasledovné zmeny zodpovedné. Za implementáciu bezpečnostných opatrení a analýzu OT prostredia bude zodpovedné oddelenie kybernetickej bezpečnosti → SOC tím na čele s CSIRT manažérom oddelenia

kybernetickej bezpečnosti. Na to, aby bezpečnostné opatrenia boli efektívne, je nutná spolupráca a dlhoročné skúsenosti ľudí zodpovedných za riadenie provoznej siete. Jedná sa oddelenia SCADA – centrálny dispečerský systém a provozu (sieťarov). Pri implementácií bezpečnostných opatrení je dôležité jednotlivé opatrenia konzultovať so spomenutými oddeleniami a nájsť spoločné riešenia, aby sa naplnili kritéria zároveň pre bezpečnosť a dostupnosť služieb ICS prostredia.

Intervenčná stratégia

Intervencia v rámci implementácie opatrení sa bude týkať nasledujúcich oblastí v spoločnosti:

- Ľudské zdroje
- Organizačná štruktúra
- Technológie
- Komunikačné toky a procesy spoločnosti

Z pohľadu ľudských zdrojov, tak za zmenu bude zodpovedný SOC tím na čele s CSIRT manažérom kybernetickej bezpečnosti, kde CSIRT manažér na základe analýz poskytnutých SOC tímom, jednaním s provozným oddeleným a svojich odborných skúseností v problematike riadenia bezpečnosti bude zodpovedný za voľbu opatrení pre zabezpečenie OT siete, čo vlastne priamo nadväzuje na organizačnú štruktúru a komunikačné toky spoločnosti. Z toho plynú napríklad požiadavky na jednotlivé výberové konania zariadení implementovaných do OT siete, kde za ne bolo zodpovedné doteraz provozné oddelenie. Zmena nastáva priamo v tejto štruktúre spoločnosti. Jednotlivé výberové konania musia byť odsúhlasené CSIRT manažérom a musia spĺňať kritéria definované oddelením kybernetickej bezpečnosti, pričom musí nastať korelácia v rámci nárokov bezpečnostných tak provozných.

Z pohľadu komunikačných tokov a procesov spoločnosti je dôležitá oblasť reportovania bezpečnostných incidentov. V prípade ak SOC tím zaznamená bezpečnostný incident, je povinný oznámiť danú situáciu Národnému Úradu Kybernetickej a Informačnej Bezpečnosti hneď, ako je to možné a vhodné je zdieľať následne túto informáciu aj s dcérskymi a konkurenčnými spoločnosťami.

Stratégia zvolená pre implementáciu opatrení je na základe metodiky best practices a ISO noriem z radu 27K. Konkrétne sa jedná minimálne o nasledujúce normy:

- ISO/IEC 27000 *Information technology - Security techniques - Information security management systems*
- ISO/IEC 27005:2011 *Information technology - Security techniques - Information security risk management*
- *ISO/IEC TR 27019 — Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*
- *ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management*
- *ISO/IEC 27039 — Information technology — Security techniques — Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)*

Keďže energetická spoločnosť patrí medzi nadnárodné spoločnosti a v istých oblastiach, kde daná spoločnosť pôsobí na základe vonkajších vplyvov opísaných v SLEPT analýze, boli dcérske spoločnosti nútené zavádzať podobné opatrenia skôr, tak sa využijú ich poznatky a znalosti v tejto problematike. Na tomto procese sa však nepodieľajú iba dcérske spoločnosti, ale v Českej republike aj medzi konkurenčnými firmami funguje zdieľanie informácií v tejto oblasti, pretože sa jedná o spoločný cieľ a energetické siete sú medzi sebou navzájom prepojené. Zároveň to nadväzuje na strategický rozvoj energetickej sústavy a koncept SmartGrid.

2.3 Časový plán projektu

Pre rozbor časového plánu projektu analýzy provoznej siete a implementácie opatrení je využitá metóda PERT. Časové odhady jednotlivých činností sú vyjadrené v Man-Days, čomu prislúcha hodnota 7,5 hodiny na jeden pracovný deň. Táto hodnota sa však neviaže na jedného pracovníka, ale na oddelenie zodpovedné za túto činnosť.

V tabuľke činností projektu sa nachádza päť časových údajov, pričom odhady doby trvania jednotlivých sa skladajú z troch časových údajov:

- Optimistický odhad (a)
- Najpravdepodobnejší odhad (m)
- Pesimistický odhad (b)

Zvyšné dva časové údaje sú stredná doba trvania činnosti reprezentovaná (y) a smerodatná odchýlka reprezentovaná ako σ^2 , čo odpovedá druhej odmocnine z hodnoty rozptylu.

Pre výpočet strednej doby trvania využijeme nasledujúci vzorec, tento vzorec umožňuje prevod na deterministický model:

$$y = \frac{a + 4m + b}{6}$$

Výpočet hodnoty rozptylu:

$$\sigma\text{^}2 = \frac{(b - a)\text{^}2}{36}$$

Výpočet hodnoty smerodatnej odchýlky:

$$\sigma = \frac{b - a}{6}$$

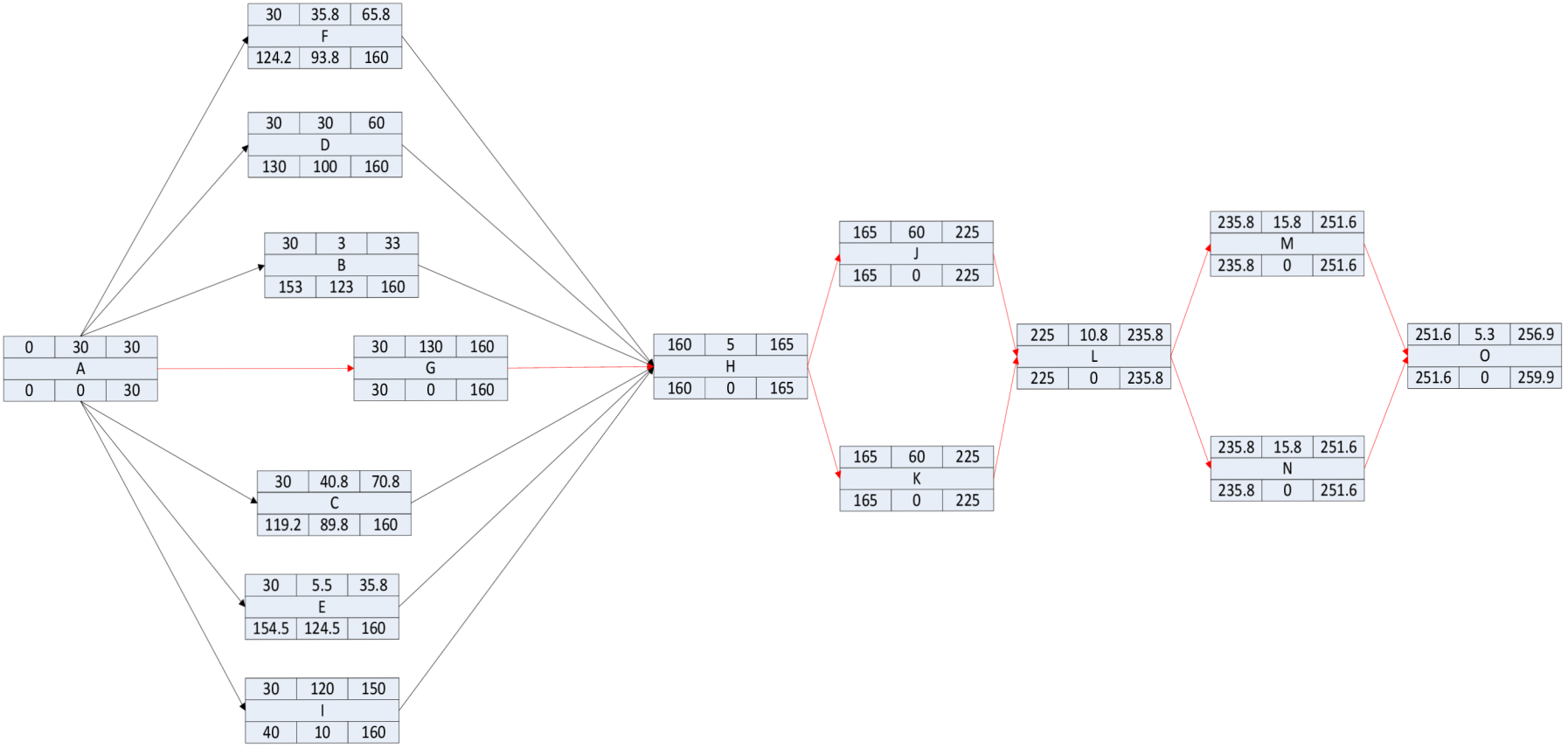
Tabuľka 1: Jednotlivé činnosti projektu

Činnosť	Popis činnosti	Následník	a	m	b	y	σ^2
A	Vybudovanie Testovacieho polygonu	B,C,D,E,F,G,I	20	30	40	30	11.1
B	Forward Syslog trafficu do polygonu	H	1	3	5	3	0.44
C	Forward Netflow trafficu do polygonu	H	30	40	55	40.8	17.36
D	Analýza Centrálnej SCADY	H	20	30	40	30	11.1
E	Analýza prostredia rozvodne	H	3	5	10	5.5	1.36
F	Analýza aktívnych prvkov siete	H	30	35	45	35.8	6.25
G	Analýza komunikácie	H	125	130	135	130	2.78
H	Vyhodnotenie analýzy	J,K	5	10	15	10	2.78
I	Testovanie potenciálneho riešenia	H	110	120	130	120	11.1
J	Výberové konanie pre Hardware	L	50	60	70	60	11.1
K	Výberové konanie pre Software	L	50	60	70	60	11.1
L	Voľba riešenia	M,N	5	10	20	10.8	6.25
M	Implementácia Hardwar riešenia	O	10	15	25	15.8	2.77
N	Implementácia Softwar riešenia	O	10	15	25	15.8	2.77
O	Ukončenie a vyhodnotenie projektu	-	2	5	10	5.3	1.77

Tabuľka 2: Legenda pre výpočet uzlovo orientovaného grafu

Najskorší možný začiatok *ZM = KM predchodcu*	Stredná doba trvania činnosti *(y)*	Najskorší možný koniec *KM = ZM + y*
Názov činnosti		
Najneskorší prípustný začiatok *ZP = KP - y*	Celková rezerva (RC) *RC = ZP – ZM*	Najneskorší prípustný koniec *KP = ZP následníka*

2.4 Metóda PERT



Obrázok 9:Časový diagram projektu: PERT

2.4.1 Kritická cesta

Kritická cesta projektu je najdlhšia cesta v projekte, činnosti ležiace na kritickej ceste majú nulové rezervy a v prípade predĺženia jednej činnosti ležiacej na kritickej ceste dochádza k predĺženiu celého projektu.

Kritickú cestu tvoria činnosti: A → G → H → J + K → L → M+ N → O

Celková doba trvania projektu vychádza na 256,9 MD.

Rozptyl doby trvania projektu je daný súčtom rozptylom hodnôt dôb trvania kritických činností projektu a jeho hodnota je 52,42 (MD)^2. Táto pomerne vysoká hodnota je spôsobená tým, že kritickú cestu v určitých fázach projektu tvoria paralelné činnosti a môžu sa predĺžiť obe zároveň.

Smerodatná odchýlka doby trvania projektu je druhá odmocnina z hodnoty rozpytlu a je rovná hodnote 7,24 MD.

2.5 Analýza rizík mapovania provoznej siete a implementácie opatrení

Pre analýzu rizík daného projektu je zvolená metóda RIPRAN. Nasledujúca tabuľka: „Hodnotenie pravdepodobnosti rizík“ obsahuje kvantitatívne vyjadrenie pravdepodobnosti rizika. Pri tabuľke: „Hodnotenie dopadu rizík“ je vyjadrenie dopadu reprezentované slovne a každému slovnému vyjadreniu prislúcha hodnota z určitého intervalu (viz. tabuľka: Hodnotenie dopadu rizík) .

Celkové hodnotenie rizika je interpretované súčinom hodnôt pravdepodobnosti a dopadu rizika. Pre hodnotenie je zvolená škála v rozmedzí 1 až 5, pričom 1 prislúcha spodná hranica, čiže nízka pravdepodobnosť, alebo dopad a pre hodnotu 5 platí presne opačný princíp.

Tabuľka 3: Hodnotenie pravdepodobnosti rizika

Hodnota	Číselné vyjadrenie
1	0 % - 20 %
2	21 % - 40 %
3	41 % - 60 %
4	61 % - 80 %
5	81 % - 100 %

Tabuľka 4 Hodnotenie dopadu rizika

Hodnota	Slovné Vyjadrenie
1	Veľmi malý
2	Malý
3	Stredný
4	Veľký
5	Veľmi veľký

2.5.1 Celkové hodnotenie rizika

Celkové hodnotenie rizika = hodnota pravdepodobnosti x hodnota dopadu

Tabuľka 5: Vizuálne vyjadrenie hodnoty celkového rizika

Číselné vyjadrenie	Vizuálne vyjadrenie
1-4	
5-9	
10-14	
15-19	
20-25	

Tabuľka 6: Bodové ohodnotenie celkového rizika

	1	2	3	4	5
1 (0 % - 19 %)	1	2	3	4	5
2 (20 % - 39 %)	2	4	6	8	10
3 (40 % - 59 %)	3	6	9	12	15
4 (60 % - 79 %)	4	8	12	16	20
5 (80 % - 100 %)	5	10	15	20	25

Nasledujúca tabuľka obsahuje hlavné identifikované riziká, ktoré môžu v súvislosti s projektom analýzy prostredia a vyhodnotenia informácií nastať. Pre jednotlivé hrozby je stručne popísaný scenár a podľa uvedených stupníc vyššie stavená pravdepodobnosť reprezentovaná v tabuľke ako (P), dopad (D) a celková hodnota rizika ako (H).

Tabuľka 7: Identifikácia a hodnotenie hlavných rizík analýzy provoznej siete a implementácií opatrení

Číslo	Hrozba	Scenár	P	D	H
Technologická rizika					
1	Chybný návrh umiestnenia IDS sond	Zanedbanie bezpečnosti siete	3	5	15
2	Chybný návrh umiestnenia Netflow sond	Nepokrytie celej komunikácie siete	3	5	15
3	Nedisponovanie nástrojom na mapovanie a monitoring siete	Predĺženie doby implementácie opatrení	1	5	5
4	Nedostačujúce znalosti pri stavbe Testovacieho polygonu	Oneskorenie mapovania siete	2	3	6
5	Chybné zanalyzovanie prostredia	Chybná implementácia opatrení	2	5	10
6	Plné vyťaženie aktívneho prvku, ktorý mirroruje traffic do sond	Strata časti vzorku komunikácie	1	5	5
Procesní rizika					
7	Dodanie neúplných podkladov	Predĺženie doby mapovania siete	2	2	4
Bezpečnostné riziká					
8	Strata zozbieraných údajov	Vytvorenie bezpečnosnej udalosti	2	4	8
9	Odcudzenie zozbieraných údajov	Hrozba bezpečnostnej udalosti	2	4	8

V uvedených kategóriach rizík bolo identifikovaných 9 hlavných rizík projektu analýzy prostredia provoznej siete a návrhu opatrení, ktoré zvýšia bezpečnosť a naplnia kritéria novely vyhlášky kybernetickej bezpečnosti.

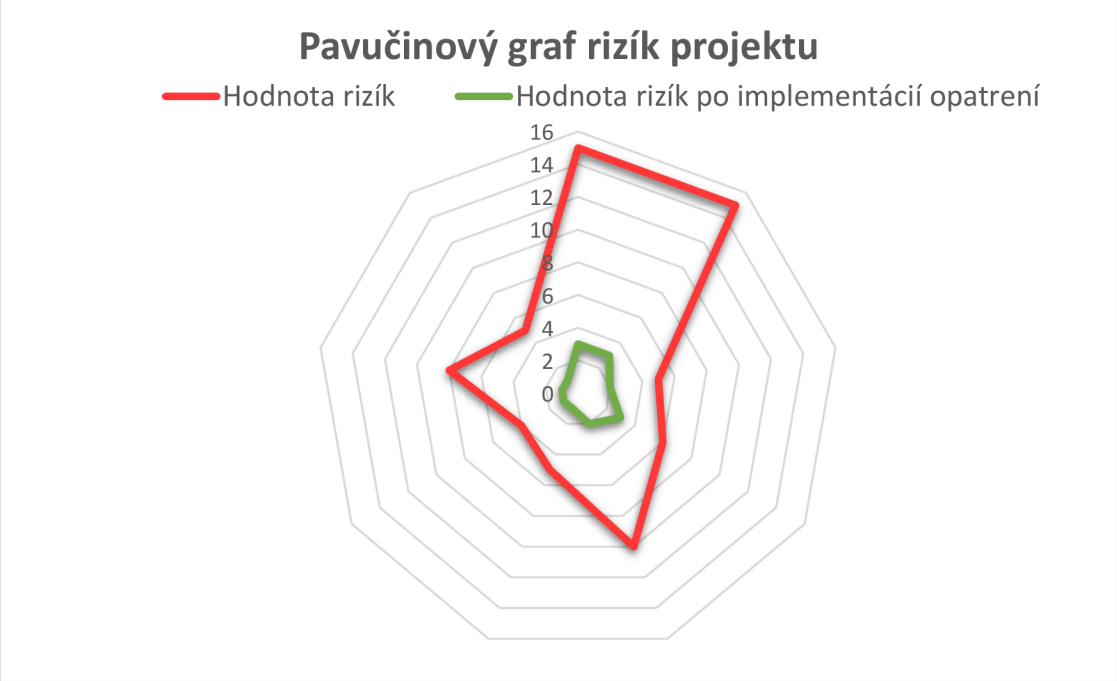
Na nasledujúcej strane sú v tabuľke zhrnuté opatrenia, ktoré znižujú dopad jednotlivých rizík a v stĺpcoch (P), (D), (H) sú uvedené hodnoty rizík po implementácií opatrení.

Cieľom implementácie opatrení riadenia projektu bolo zníženie daných rizík na najnižšiu úroveň, s čo najnižšou finálnou hodnotou. Väčšina opatrení projektu je spojená s finančnými nákladmi ostatné sú formou doporučení, s ktorými sa finančné náklady nespájajú. Ekonomické zhodnotenie jednotlivých činností sa v rámci utajenia informácií na žiadosť a smernice spoločnosti neuvádza v diplomovej práci.

Tabuľka 8: Opatrenia rizík

Číslo	OPATRENIA	P	D	H
Technologická rizika				
1	Detailné zmapovanie provoznej siete a využitie best practices	1	3	3
2	Detailne zmapovanie komunikačných tokov siete	1	3	3
3	Vytvorenie testovacieho polygonu	1	2	2
4	Poskytnutie odborných konzulácií pri implementácií testovacieho polygonu	1	3	3
5	Spolúpráca SCADA a provozného oddelenia	2	1	2
6	Odtestovanie vyťaženia uzlu siete zodpovedného za mirroring trafficu	1	1	1
Procesní rizika				
7	Viacnásobná a čiastková kontrola dodávaných podkladov a technické konzultácie s Provozným a SCADA oddelením	1	1	1
Bezpečnostné riziká				
8	Šifrovanie diskov a jednotlivých podkladov	1	1	1
9	Šifrovanie diskov a jednotlivých podkladov	1	1	1

2.6 Mapa rizík



Obrázok 10: Pavučinový graf rizík projektu

Pre vizuálnu interpretáciu mapy rizík je zvolený pavučinový graf, ktorý je reprezentovaný dvomi krivkami, kde červená krivka reprezentuje hodnotu jednotlivých rizík pred zavedením opatrení a zelená krivka interpretuje zníženú úroveň rizík po aplikovaní opatrení. Všetky riziká sa tak dostávajú na najnižšiu úroveň s nízkym dopadom.

2.7 Testovací polygon

Testovací polygon je dočasné riešenie pre základný monitoring, mapovanie siete a zber logov, pred nasadením komplexného komerčného riešenia. Slúži aj pre porovnanie a uvedomenie si, aké prípadne funkcionality sú vyžadované u komerčného riešenia. Pomocou mapovania siete a príjmania Netflow, sa overí fyzická topológia siete a čo najpodrobnejšie zmapuje aj logickú komunikáciu jednotlivých zariadení v provoznej sieti. Výstupom tejto analýzy je čo najpodrobnejšie zmapovaná logická komunikácia, komunikačné protokoly a návrh umiestenenia prípadných IDS sond a sond určených na Netflow. Návrh riešenia sa popisuje v praktickej časti diplomovej práce

Na to, aby sa mohlo začať s mapovaním a monitoringom siete, je nutné si vybudovať nástroj. Nástroj, alebo nástroje tvoria virtuálne servre, ktoré sú virtualizované na jednom fyzickom servery. Hlavným komponentom pre túto činnosť je vytvorenie ELK Stacku.

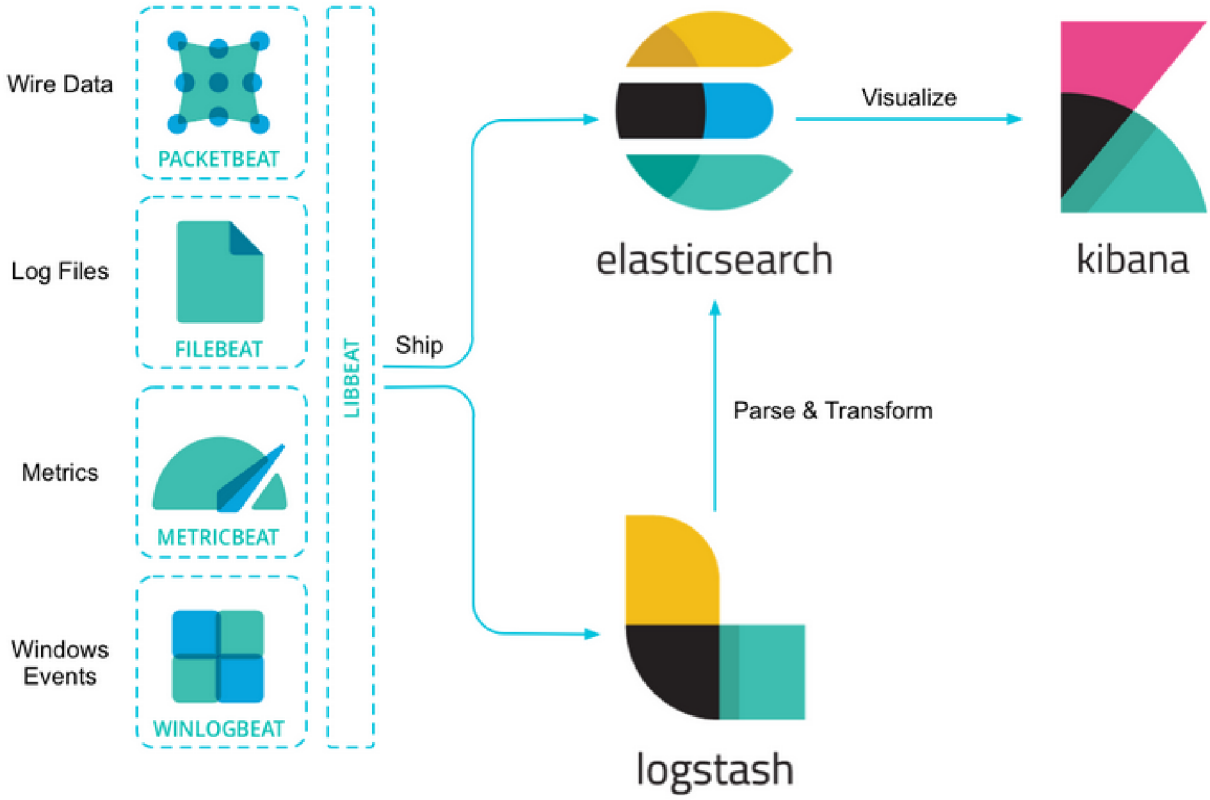
Parametre: Fyzický server

Server typu HP DL580 G7 pre vytvorenie testovacieho polygonu s nasledujúcou konfiguráciou.

- 4x procesor Intel Xeon E7520,
- 128GB DDR3 pamäť,
- 4x PSU1200W,
- 256MB SDRAM P410i,
- pevný disk 300GB SAS2 6Gbit DP 10k,
- rámeček na disk HP G6, G7.

2.7.1 ELK Stack

Nástroj, ktorý je zvolený pre príjmanie Syslogu a Netflow, je open-source riešenie, ELK Stack. Jeho základné tri komponenty tvorí Logstash, Elasticseach a Kibana. Tieto komponenty zároveň tvoria jadro Testovacieho polygonu. Každý táto jeden komponent je virtuálny server, s operačným systémom Centos 7. ELK Stack je jedna z najpopulárnejších open-source log manažment platforiem. (1)



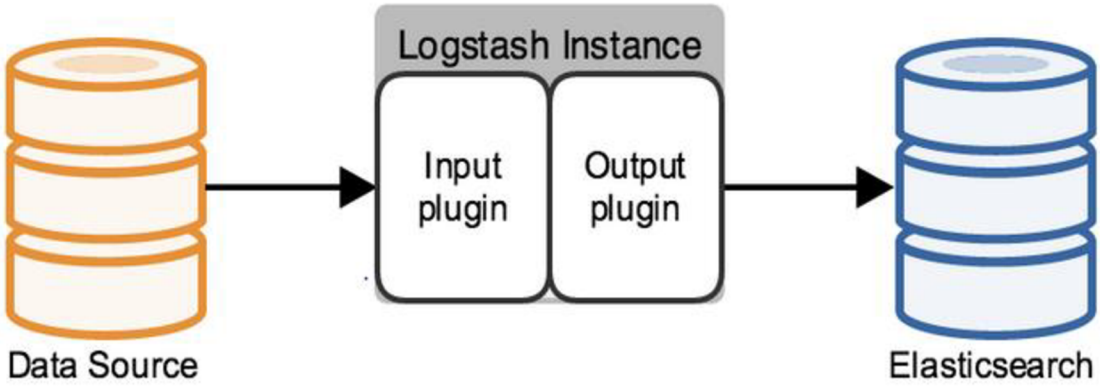
Obrázok 11: Architektúra ELK Stack

2.7.2 Logstash

Parametre virtuálneho serveru **Logstash**:

- **OS:** Centos 7
- **Kernel:** 3.10.0-514.26.2.el7.x86_64
- **Procesor:** 4 CPU
- **Pamäť:** 8 GB
- **Disk:** 50 GB

Logstash je open-source riešenie pre príjmanie a parsovanie logov, ktoré odosiela v upravenej forme na určitý typ úložiska. V tomto prípade Elasticsearch. Logstash je schopný parsovať a transformovať príjmané logy do JSON formátu. Minimálna Logstash inštalácia vyžaduje jednu Logstash instanciu a jednu Elasticsearch instanciu. Tieto instancie sú priamo prepojené. Logstash využíva input plugin na prijatie dát a Elasticsearch output plugin na indexovanie dát v Elasticsearch. Týmto sa pri štarte vytvorí Logstash procesing pipeline, na základe configuračného súboru Logstashu umiestneného vo /etc/logstash/conf.d



Obrázok 12: Minimálna inštalácia a konfigurácia Logstashu

Konfiguračný súbor sa skladá z nasledujúcich častí:

- Input plugin
- Filter plugin (optional)
- Output plugin

V input plugine je dôležité nastaviť akú komunikáciu má logstash príjmať a na akom porte. V tomto prípade ide o nastavenie Syslog a Netflow trafficu, ktoré sú odosielané defaultne pomocou UDP trafficu na port 514 pre syslog a port 9999 pre Netflow.

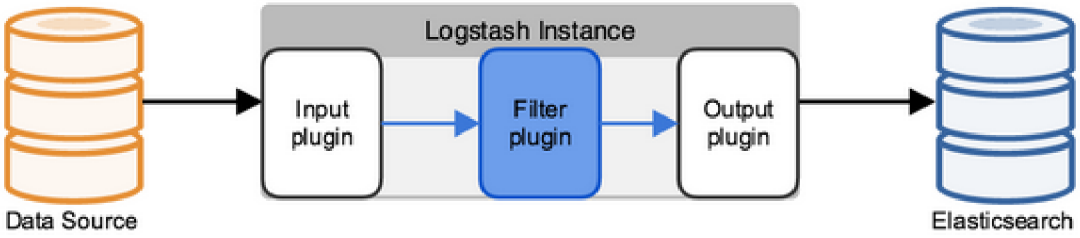
V sekcií Output plugin je nutné nastavenie IP adresy hosťa, na ktorom sa budú logy ukladať a definovať a povoliť príslušný port na Elasticsearch servery. Elasticsearch defaultne načúva na porte 9200. (2)

Nastavenie Logstash Firewallu

Pre príjmanie logov je nutné povolenie portov na firewalle Logstashu. Pomocu príkazu v CLI rozhraní daného servru: *firewall-cmd --list-all* si zobrazíme firewallové nastavenia.

Filter plugin

Keď príjmame logy, tak väčšinou sú v neštrukturovanom tvare a často obsahujú veľmi veľa informácií, ktoré sú pre konkrétne riešnie irelevanté. V tomto prípade je vhodné využitie filter pluginov pre parsovanie, odstránenie nepotrebných informácií a prípadne pridanie dodatočných informácií do konkrétnych logov. Pridanie takéhoto filter pluginu môže mať značný dopad na výkon, záleží to od množstva operácií, ktoré musí plugin vykonať. Toto zaťaženie je riešené pomocou paralelných procesov na viac jadrových serveroch. Pomocou argumentu *-w* je možno zmeniť počet vlákien, ktoré sa majú podielať na filtrovaní logov. Príkaz: bin/logstash -w 16, pridelí 16 vlákien na filtrovanie logov, ktoré su odosielané na Logstash.



Obrázok 13: Logstash a filter plugin architektúra

Logstash väčšinou nekomunikuje s jedným Elasticsearch node, ale sú vytvorené clustre z dôvodu redundancie, čím zamedzíme vytvoreniu „okna“ – neprijímania logov. Defaultne Logstash používa HTTP protokol na presúvanie dát do clustrov. Ale je možné využiť aj Elasticsearch HTTP REST API na indexovanie dát do Elasticsearch clustru. Toto API reprezentuje indexované dáta vo formáte JSON a nie sú potrebné Java client triedy ani dodatočné JAR súbory. Toto riešenie nemá žiadne výkonové nevýhody oproti transportným alebo node protokolom. Zabezpečenie komunikácie je možno vykonať pomocou HTTP REST API, použitým voľne dostupného balíčku X-Pack Security, ktorý podporuje SSL a HTTP základnú autentifikáciu. Pri využití HTTP protokolu je možné nakonfigurovať output plugin na automatické load-balance indexovanie v rámci špecificky stanovených hostov v Elasticsearch clustry. Týmto sa zároveň zvyšuje dostupnosť spomínanej služby.(14)

V tomto prípade však postačí riešenie, kde v testovacom polygone sú vytvorené dva Elasticsearch nodes a vytvárajú jeden cluster. V prípade výpadku jedného nodu je traffic automaticky presmerovaný na druhý, bez obmedzenia dostupnosti. Nie je nutné vytváranie Message Queue, pretože z provoznej siete nie je odosielaný taký veľký objem dát aby sa dané riešenie požadovalo.

2.7.3 Elasticsearch

- **OS:** Centos 7
- **Kernel:** 3.10.0-514.26.2.el7.x86_64
- **Procesor:** 4 CPU
- **Pamäť:** 16 GB
- **Disk:** 300 GB

Elasticsearch je distribuovaný RESTful vyhľadavací a analytický engine, ktorý tvorí jadro ELK Stacku. Centrálne ukladá dáta do NoSQL databázy založenej na Lucene search engine. Do tejto databáze Logstash odosiela Syslog a Netflow. Na túto databázu sa dotazuje napríklad pomocou poslednej komponenty Kibany.

2.7.4 Kibana

- **OS:** Centos 7
- **Kernel:** 3.10.0-514.26.2.el7.x86_64
- **Procesor:** 4 CPU
- **Pamäť:** 16 GB
- **Disk:** 50 GB

Kibana je webové rozhranie pre vizualizáciu dát uložených uložených v Elasticsearch, špecializuje sa na prehľadávanie a reprezentovanie veľkého množstva dát v reálnom čase. Tieto komplexné dáta potom sú agregované a prezentované užívateľovi v pochopiteľnom formáte a umožňuje vytvárať flexibilné a dynamické tabuľky a grafy pri nainštalovaných správnych pluginov. Môžeme tvrdiť, že je to veľmi okresaný SIEM systém, ktorý je v momentálnej fáze implementácie a mapovania provoznej siete dostačujúci a poskytuje aspoň základný monitoring a vyhodnocovanie príjmaných logov.

Nastavenie jednotlivých komponent ELK staku je opísané nižšie v analytickej časti diplomovej práce. Diplomová práca nepopisuje inštaláciu jednotlivých služieb pre ich

rozsah, ale nastavenie firewallových pravidiel a konfiguračných súbor pre spojazdenie ELK Stack.

2.8 Netflow

Netflow je typ data record streamu z aktívnych prvkov siete, ktoré danú funkcionalitu podporujú. Obsahuje informácie o prepojení jednotlivých zariadení v sieti, tieto informácie obsahujú napríklad: zdrojovú IP adresu, cieľovú IP adresu, zdrojový a cieľový port, typ služby, VLANy, množstvo odoslaných paketov a rôzne ďalšie informácie, ktoré môžu byť zakódované do rámcu a hlavičky protokolu. S Netflow dátami, operátori môžu pochopiť viac ako iba objem dát, ktorý prechádza sieťou. Pomocou Netflow je možné pochopi,ť odkiaľ sa daný traffic vzal, kam ide a aká služba, alebo aplikácia mu prislúcha. Z pohľadu bezpečnosti je to základný stavebný kameň, ktorý slúži na detekciu anomálí v sieťovej komunikácií. Pri podrobnom asset inventory, dôkladne zmapovanej logickej topológie siete a správne nastavených aktívnych prvkoch, tvorí prvú bariéru pri detekcií potencionálnej bezpečnostnej udalosti a tým predchádza prípadnému bezpečnostnému incidentu. Ide hlavne o monitoring 2 až 4 vrstvy ISO osi modelu.

2.8.1 Netflow kolektor

Tieto dáta o komunikácií v sieti, ktoré prvky spolu komunikujú sa ukladajú a sú zbierané pomocou Netflow collectoru. Collector aktuálny traffic analyzuje a prezentuje užívateľovi, môže mať podobu hardwaru alebo softwaru.

2.8.2 Netflow sonda

Netflow sondy sú základným predpokladom monitoringu sieťovej infraštruktúry. Sonda je pasívne zariadenie, ktoré nejako nevplyvňuje provádzku v sieti a prekonávajú obmedzenie získavania Netflow pomocu aktívnych sieťových prvkov. Poskytujú základnú viditeľnosť komunikačných tokov v sieti.

2.9 Základná konfigurácia fyzického serveru.

Prvý krok pri budovaní testovacieho polygonu bola inštalácia operačného systému na fyzický server. To znamená vytvorenie boot USB s operačným systémom Centos 7. Keďže na fyzickom servery sa virtualizujú všetky ostatné nodes, ktoré budú zabezpečovať funkcionalitu polygonu je nutné vytvorenie bridge rozhrania. Premostiť preposielanie príjmaného trafficku z fyzického rozhrania do virtuálneho rozhrania serverov, na ktorých pobeží prvá komponenta z ELK Stacku Logstash. Vzhľadom na obmedzenú konektivitu (internet) do provoznej siete, je nutné vytvoriť jednotlivé virtuálne servery lokálne na Laptope s konektivitou a potom preniesť vystavané virtuálne servery na fyzický server umiestnený v provoznej sieti. Pre vytváranie virtuálnych serverov bol zvolený nástroj VirtualBox. Táto služba avšak nepobeží na fyzickom serveri, namiesto nej je zvolený iný nástroj KVM. Preto je potom nutné transformovať jednotlivé virtuálne servery buildnuté na Laptope, aby boli kompaktibilné s KVM. VirtuálBox má výstupné virtuálky vo formáte *vmdk,* KVM podporuje formáte *qcow2*. Konvertovanie prebieha pomocu nasledovného príkazu:

```
qemu-img convert -f vmdk <route_to_file_/file_name>.vmdk -O qcow2
<destiantion_of_file/file_name>.qcow2
```

Konvertovanie v tomto prípade prebieha už na strane VHOSTa, kde pomcou príkazu *scp* bol prekopírovaný vmdk file na fyzický server.

Aby sa vyhlo v neskoršom štádiu implementácie server hardeningu, tak verzie operačných systémov boli v ich minimál verziách a dodatočné tooly, ktoré boli pre spojazdenie funkcionality polygonu potrebné, boli inštalované z lokálne vytvoreného repozitáru. Táto časť riešenia sa však kvôli jeho rozsahu v diplomovej práci neopisuje, tak ako inštalácie jednotlivých služieb testovacieho polygonu. Pre správu virtuálnych serverov je nutná inštalácia virtualizačných balíčkov

```
yum install -y qemu-kvm qemu-img virt-manager libvirt libvirt-
python libvirt-client virt-install
```

- **qemu-kvm** = QEMU emulator
- **qemu-img** = QEMU disk image manager
- **virt-install** = Command line tool pre vytváranie virtuálnych serverov.

- **libvirt** = Poskytuje libvirtd daemon ktorý manažuje virtuálne zariadenia and kontroluje hypervisora.
- **libvirt-client** = poskytuje client-side API pre pristupovanie na servery a taktiež poskytuje virsh utility, ktorá má command line tool pre manažovanie virtuálnych zariadení.

Je možno ešte inštalovať pre grafické rozhranie **virt-viewer,** ale toto riešenie je pre naše prostredie nevhodné a nepotrebné.

Inštalácia virtuálnych serverov prebieha pomocou príkazu: **virt-install** nasledovne:

```
virt-install –virt-type kvm –name <node_name> --ram
<value_in_bites> --disk path=<cesta ku qcow2 súboru pre danú
instanciu>,bus=virtio,size=<velkosť disku v GB> --network bridge
=<názov rozhrania> --graphics vnc,listen=0.0.0.0 –noautoconsole
–os-type=linux –os-variant=rhel7 –
cdrom=<path_to_iso/iso_name>.iso
```

Prebehne inštalácia virtuálneho serveru. Zobrazenie virtuálnych serverov pomocou príkazu:**virsh list –all**. Spustenie jednotlivých virtuálnych serverov, príkaz: **virsh start <node_name>**.

2.9.1 Vytvorenie bridge rozhrania

Aby vedel Logstash spracovávať a príjimať Syslog a Netflow je nutné fyzické rozhranie VHOSTa, na ktorom daný traffic príjma, premostiť do virtuálnej instancie Logstash. Pre vytvorenie bridge rozhrania je nutné sa na fyzickom serveri navigovať do zložky, kde sú uložené konfiguračné súbory jednotlivých sieťových rozhraní. Tie sú uložené v:

```
/etc/sysconfig/network-scripts
```

A jedná sa o konfiguračné súbory ifcfg-<názov rozhrania>

Je nutné vytvoriť konfiguračný súbor bridge rozhrania a názov bridge rozhrania prideliť konfiguračnému súboru fyzického rozhrania portu, na ktorý sa daný traffic príjmá. Príklad takýchto súborov je uvedený na nasledujúcej strane.

Konfiguračný súbor bridge rozhrania

```
DEVICE=“<názov rozhrania>“
ONBOOT=“yes“
TYPE=“Bridge“
STP=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=“<volitelný názov pre rozonanie rozhrania>“
UUID=*určitý_string*
BRIDGING OPTS=priority=32768
IPADDR=<IP adresa virtuálneho rozhrania>
PREFIX=<zaleží od sieťového rozsahu>
```

Pre vytvorenie bridge rozhrania pre virtuálny server fyzickému rozhraniu je nutné do konfiguračného súboru fyzického rozhrania iba priradenie názvu bridge. Názov je v uložený v premennej DEVICE ten sa musí zhodovať s názvom premennej BRIDGE v konfiguračnom súbore fyzického rozhrania.

Konfiguračný súbor fyzického rozhrania

```
DEVICE=<názov fyzického rozhrania>
ONBOOT=“yes“
BRIDGE=<názov bridge rozhrania>
TYPE=ETHERNET
NAME=“<volitelný názov pre rozonanie rozhrania>“
UUID=*určitý_string*
```

V ďalšom kroku je nutné nastavenie firewallu fyzického serveru, konkrétne povolenie portov a protokolov pre jednotlivé porty a vytvorenie port forwarding pravidiel pre forwardovanie trafficu na vnútorné sieťové rozhranie Logstah serveru.

2.10 Nastavenie firewallu fyzického serveru

Zobrazenie firewallových pravidiel sa prevedie pomocou príkazu:

Firewall-cmd --list-all

Keďže sa bude príjmať NetFlow a Syslog traffic je nutné povolenie portov 514 a 9999, zároveň je nutné stanoviť, či sa jedná o TCP alebo UDP traffic. Netflow a Syslog využíva UDP protokol a NTP protokol pre časovú synchronizáciu. NTP protokolu príslúcha defaultne port 123/UDP.

Povolenie portov na firewalle pomcou nasledovných príkazov:

```
firewall-cmd --add-port=514/udp --zone=public --permanent
firewall-cmd --add-port=9999/udp --zone=public --permanent
firewall-cmd --add-port=123/udp --zone=public --permanent
```

Pri povoľovaní portov je dôležitý parameter „permanent“, pokiaľ by firewallové pravidlo tento parameter neobsahovalo, tak v prípade reštartu serveru fyzického alebo virtuálneho by prišlo ku strate firewallových pravidiel.

Forwardovanie portov na virtuálny server Logstash:

```
firewall-cmd--add-forward-port=port=9999:proto=udp:toaddr=
<vnútorná ip adresa Logstash serveru>  --zone=public --permanent
firewall-cmd--add-forward-port=port=514:proto=udp:toaddr=
<vnútorná ip adresa Logstash serveru>  --zone=public --permanent
```

Pre akceptovanie trafficu od zdroja odosielania je ešte nutné vytvorenie takzvaných rich-rules pre danú zónu, kde vlastne je nutné iba zadať parameter source adress, port, zone a posledný parameter accept.

V poslednom kroku pre implementáciu všetkých pravidiel je nutný restart firewallu fyzického serveru pomocou príkazu:

```
firewall-cmd --reload
```

2.10.1 Inštalácia virtuálneho serveru Logstash

Inštalácia prebieha pomocou CLI rozhrania na fyzickom serveri už spomínaným príkazom, týmto spôsobom prebieha inštalácia všetkých virtuálnych serverov:

```
virt-install –virt-type kvm –name <node_name> --ram
<value_in_bites> --disk path=<cesta ku qcow2 súboru pre danú
instanciu>,bus=virtio,size=<velkosť disku v GB> --network bridge
=<názov rozhrania> --graphics vnc,listen=0.0.0.0 –noautoconsole
–os-type=linux –os-variant=rhel7 –
cdrom=<path_to_iso/iso_name>.iso
```

Je nutné dať si pozor pri inštalácií Logstash serveru, aby názov network bridgu sa zhodoval s názom, ktorý je uvedený v konfiguračných súboroch sieťových rozhraní (Bridge rozhranie a fyzické rozhranie).

Inštalácia samotnej služby Logstash a debugovanie sa v diplomovej práci neopisuje. Pre spustenie služby logstash sú nutné po jeho inštalácií nasledovné príkazy:

```
systemctl enable logstash
systemctl start logstash
```

overenie či je služba spustená: `systemctl status logstash`

Nastavenie firewallu

Nastavenia firewallu virtuálneho serveru sú takmer zhodné s nastaveniami firewallu VHOSTa. Je nutné povolenie portov 514, 9999, 123 všetko pre UDP protokol a dodatočné povolenie portu 5514/UDP a forwardovanie komunikácie z portu 514 na port 5514, aby dokázal logstash prijmaný Syslog parsovať. Toto opatrenie je z dôvodu, že porty v rozsahu od 0 po 1024 sú rezervované pre root užívateľa:

```
firewall-cmd --add-port=514/udp --zone=public --permanent
firewall-cmd --add-port=5514/udp --zone=public --permanent
firewall-cmd --add-port=9999/udp --zone=public --permanent
firewall-cmd --add-port=123/udp --zone=public --permanent
firewall-cmd --permanent --add-forward-
port=port=514:proto=udp:toport=5514 --zone=public –permanent
```

```
firewall-cmd --reload
```

Aby Logstash mohol parsovať a ukladať príjmané logy je nutné vytvoriť konfiguračný súbor. Ako už bolo spomenuté konfiguračný súbor sa skladá z troch častí, pričom filter sekcia je voliteľná a je možné ju rôzne upravovať.

- Input
- Filter
- Output

Konfiguračný súbor `logstash.conf` je umiestnený v `/etc/logstash/conf.d` a môže vyzerať nasledovne:

```
input {
        syslog {
                port => 5514
        }
}
#filter {
        #if [type] =="syslog" {
         #grok {
                #match => {"message" =>
"%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[%POSINT:syslog_pid}\])?:
%{GREEDYDATA:syslog_message}"
        #add_field => ["received_at", "%{@timestamp}" ]
        #add_field => ["received_from", "%{host}" ]
#}
output {
        elasticsearch {
                hosts => ["http://<vnútorná ip adresa
elasticsearchu>:9200"]
        }
}
```

V input sekcii je nutné nastavenie portu, ktorý parsuje logy, v tomto prípade sa jedná o port 5514 a typ parsovaných logov čož je syslog. Pre output plugin nastavenie, kam sa majú logy preposielať a ukladať, to je elasticsearch databáza a za parameter hosts je potrebné zadať vnútornú IP adresu servera, na ktorom beží služba Elasticsearch a port pre danú službu.

2.11 Konfigurácia Elasticsearch

Elasticsearch príjma defaultne logy odosielané z Logstashu na TCP porte 9200. Preto je nutné opäť daný port povoliť na firewalle a dodatočne nastaviť ešte konfiguračný súbor `elasticsearch.yml` pre spojazdnenie služby:

```
systemctl enable elasticsearch
systemctl start elasticsearch
```

overenie či je služba spustená: `systemctl status elasticsearch`

Nastavenie firewallu

```
firewall-cmd --add-port=9200/tcp --zone=public --permanent
firewall-cmd --add-port=123/udp --zone=public --permanent
firewall-cmd --reload
```

Nastavenie konfiguračného súboru elasticsearchu

Konfiguračný súbor `elasticsearch.yml` sa nachádza v zložke:

```
cd /etc/elasticsearch/
vi elasticsearch.yml
```

V konfiguračnom súbore je nutné nájsť sekciu Network a pre parameter *network.host* zadať vnútornú IP adresu virtuálneho serveru Elasticsearch. V tej istej sekcií Network definovať aj port pre parameter http.port: 9200.

```
# Set the bind address to a specific IP (IPv4 or IPv6):
network.host: <vnutorna ip adresa elasticsearchu>
# Set a custom port for HTTP:
http.port: 9200 <adresa portu na ktorom príjma logy od logstashu>
```

2.12 Konfigurácia Kibana

Kibana je webové rozhranie pre reprezentovanie dát uložených v Elasticsearch. Slúži pre manažérsky výstup, s rôznymi tabuľkami, grafmy a štatistikami. Kibana defautlne využíva TCP port 5601, ktorý je nutné povoliť na firewalle daného nodu a pre prepojenie dát s Elasticsearchom a zpojazdenie kompletnej funkcionality ELK stacku je nutné v konfiguračnom súbore `kibana.yml` priradiť vnútornú IP adresu Elasticsearchu.

```
systemctl enable kibana
systemctl start kibana
```

overenie či je služba spustená: `systemctl status kibana`

Nastavenie firewallu

```
firewall-cmd --add-port=5601/tcp --zone=public --permanent
firewall-cmd --add-port=123/udp --zone=public --permanent
firewall-cmd --reload
```

Nastavenie konfiguračného súboru elasticsearchu

Konfiguračný súbor `elasticsearch.yml` sa nachádza v zložke:

```
cd /etc/kibana/
vi kibana.yml
```

špecifikovanie portu v yml súbore

server.port: 5601

špecifikovanie URL Elasticsearchu

elasticsearch.url: „http://<vnútorná ip adresa Elasticsearch: default port >“

2.13 Nastavenie časovej synchornizácie

Časová synchornizácia operačného systému Centos 7, môže prebiehať pomocou dvoch služieb a to pomocou NTP, ktorá je aj v tomto riešení využitá, alebo pomocou služby Chrony. Tieto dve služby nemôžu fungovať paralelne, je nutné jednu službu zakázať, aby sa neobmedzila funkcionalita druhej služby.

Zakázanie služby Chrony

```
systemctl disable chronyd
systemctl stop chronyd
```

overenie vypnutia: `systemctl status chronyd`

Povolenie služby NTP

```
systemctl enable ntpd
systemctl start ntpd
```

Pridanie a povolenie UDP/123 trafficu a portu na jednotlivých nodoch (viz. Nastavenie firewallových pravidiel)

Pridanie NTP serveru

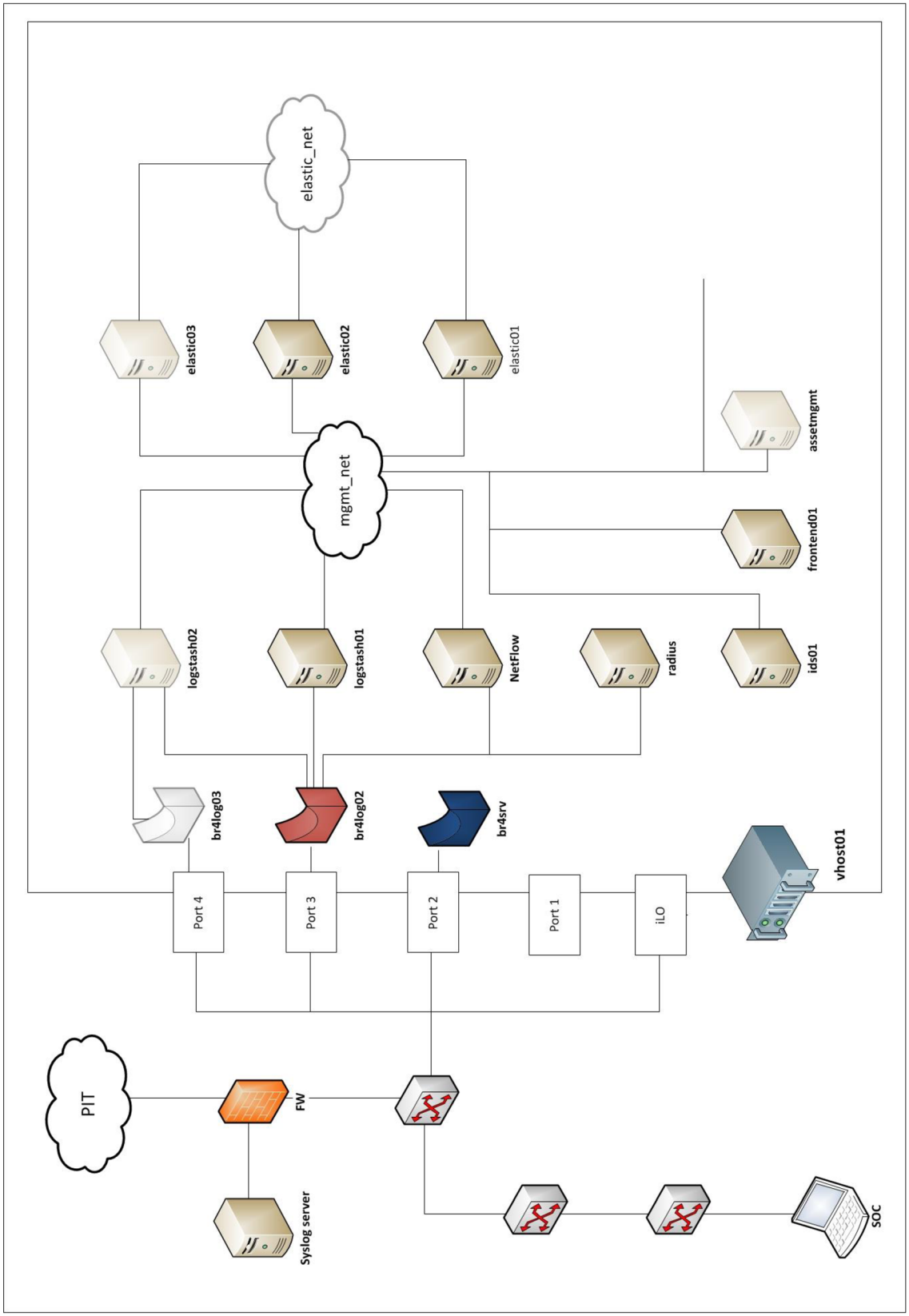
Pre pridanie NTP serveru, voči ktorému sa jednotlivé instancie budú synchronizovať je nutné otvoriť konfiguračný súbor `ntp.conf umiestneného v adresáry etc.` Keďže OT sieť je oddelená od internetu a disponuje vlastným NTP serverom, tak v sekcii konfiguračného súboru zobrazeného nižšie je nutné iba pridanie IP adresy NTP serveru:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool
(http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org iburst
#server 1.centos.pool.ntp.org iburst
#server 2.centos.pool.ntp.org iburst
#server 3.centos.pool.ntp.org iburst
server <ip adresa NTP serveru v OT sieti>

systemctl restart ntpd
```

Následne pomocou príkazu ntpq -p overíme správne nastavenie NTP serveru. Pokiaľ v danej tabuľke vidíme IP adresu NTP serveru a časové hodnoty synchornizácie nastavenie prebehlo úspešne.

2.14 Finálna architektúra testovacieho polygonu

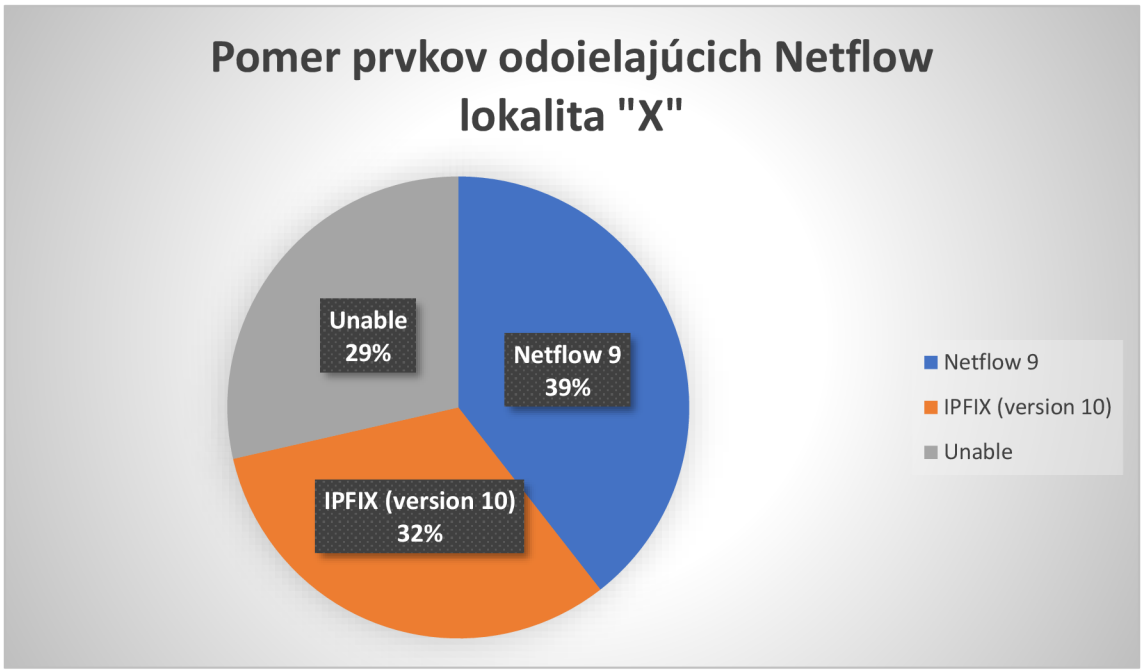


Obrázok 14: Architektúra testovacieho polygonu

2.15 Mapovanie siete

Mapovanie provoznej siete prebiehalo na základe údajov zozbieraných v netflow kolektore, IDS sonde, interných dokumentov spoločnosti a konzultácií s provozným oddelením. Hlavné získané parametre v tejto oblasti sú: lokalita prvkov, ich dátum výroby, ukončenie podpory daných zariadení a akú verziu flow dát sú schopné poskytnúť. V prvej stati sú popísané prvky, ktoré sú schopné odosielať Netflow v lokalite „X“. Podrobnosť informácií je zobecnená kvôli utajeniu informácií o KII.

Analýza prvkov neodosielajúcich Netflow:



Obrázok 15: Pomer prvkov odosielajúcich Netflow v lokalite "X"

V provoznej sieti v lokalite „X“ sa nachádza 29% prvkov, ktoré nie sú schopné odosielať Netflow. Pri tejto podskupine sú dôležité 4 parametre a to:

- Podpora skončila
- Podpora skonči v intervale 1 až 4 rokov
- Podpora skončí v roku 2018
- Podpora skončí za viac ako 5 rokov

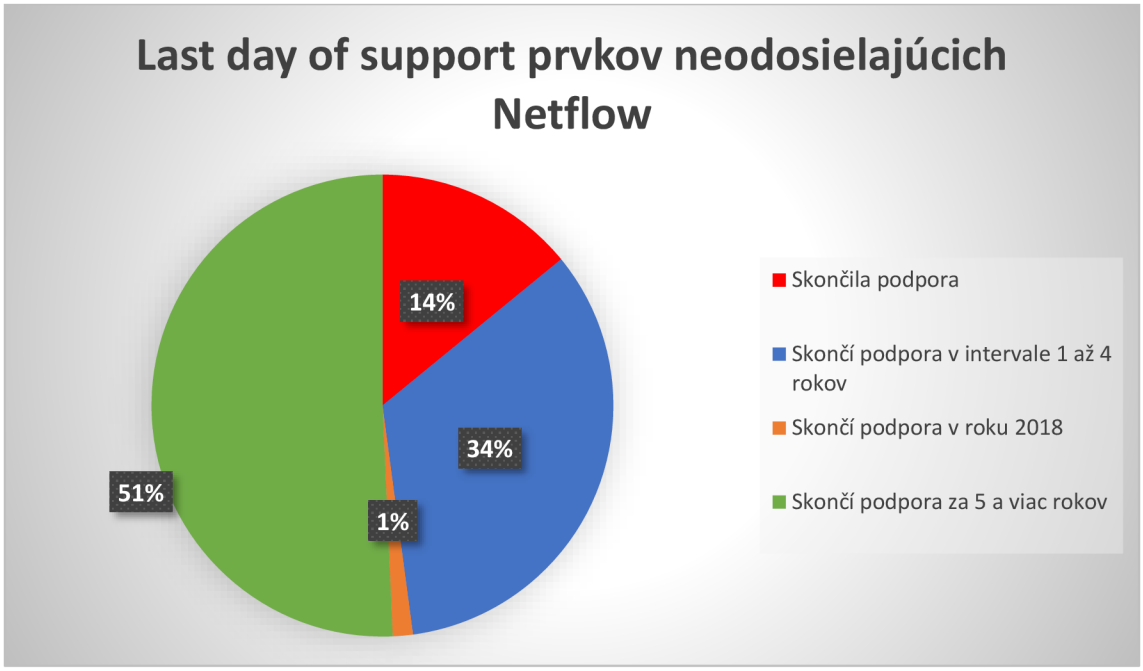
Tieto údaje sú významné z dôvodu umiestnenia sond pre jednotlivé lokality v lokalite „X“, či má zmysel v danej lokalite umiestňovať sondu na Netflow, alebo je výhodnejšie výmena aktívneho prvku, ktorý funkcionalitu odosielania Netflow podporuje. Na túto

analýzu nadväzuje plán rozvoja siete,v ktorom je popísaná výmena určitých zariadení v lokalite „X“ . Agregáciou týchto dokumentov je možno dôjsť k spomínanému záveru.

Z analýzy vyplýva nasledovné:

- Počet prvkov, ktorým skončila podpora v lokalite „X“ tvorí 14%
- Počet prvkov, ktorým skončí podpora v roku 2018 tvorí 1%
- Počet prvkov, ktorým skončí podpora v rozmedzí 1 až 4 rokov tvorí 34%
- Počet prvkov, ktorým skončí podpora za 5 a viac rokov je 51%

Pre manažérsky výstup viz. nasledujúci obrázok (Obr.11: Intervaly podpory prvkov neodosielajúcich Netflow).



Obrázok 16: Intervaly podpory prvkov neodosielajúcich flow data

Analýza prvkov odosielajúcich Netflow:

Analýza prvkov, ktoré sú schopné v lokalite „X“ odosielať Netflow, sa skladá z rovnakých parametrov, ako predchádzajúca analýza a je rozšírená o verziu Netflow.

Verzia príjmaného Netflow:

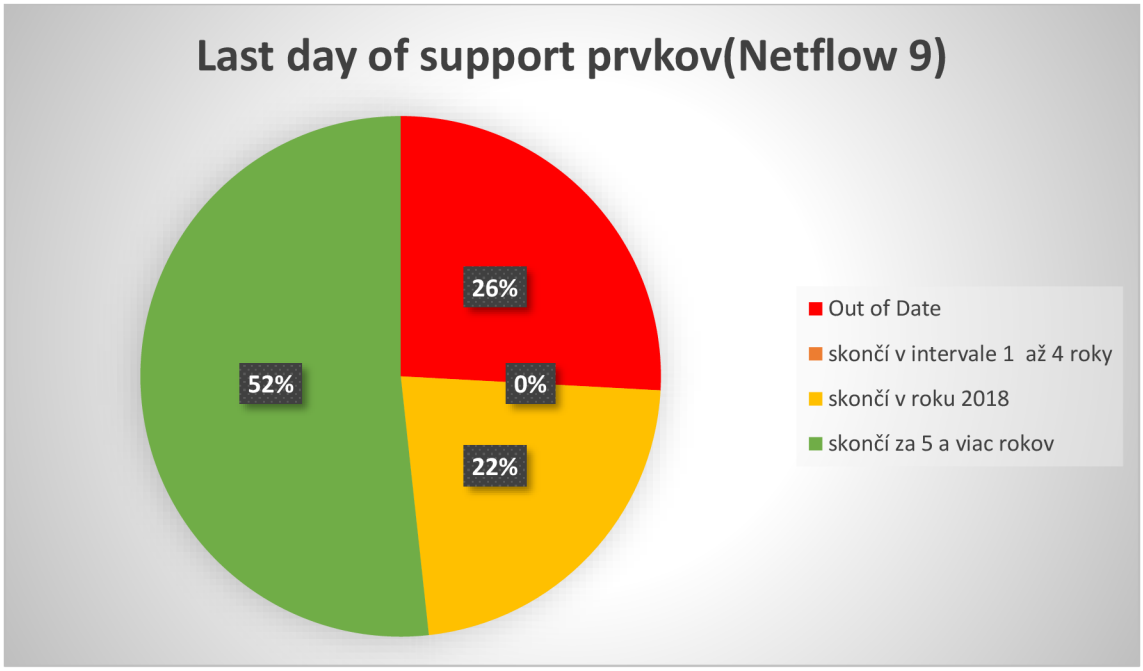
- Netflow 9
- IPFIX (Version 10)

Ideálny stav je príjmanie Netflow vo formáte IPFIX (Version 10), pri týchto dátach nedochádza ku skresleniu príjmaných dát. 100% prvkov v lokalite „X“ odosielajúcich IPFIX (Version 10) skončí podpora za viac ako 5 rokov a nemá zmysel do týchto lokalít osádzať Netflow sondy. Pomer týchto prvkov vzhľadom na celkový počet prvkov v lokalite „X“ tvorí 18%. (viz. Obr.10: Pomer prvkov odosielajúcich Netfow v lokalite „X“)

Pomer prvkov odosielajúcich Netflow verzie 9 vzhľadom na celkový počet v lokalite „X“ tvorí 40%. Flow dáta príjmané z týchto zariadení sú v niektorých prípadoch skreslené a nie plne relevantné.

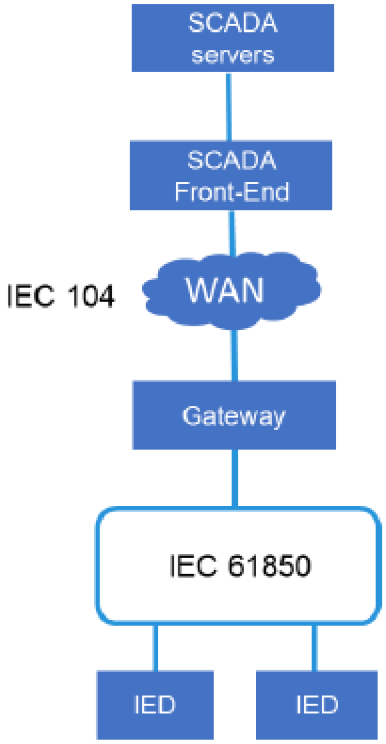
- Pomer prvkov, ktorým skončila podpora 26%
- Pomer prvkov, ktorým skončí podpora v rozmedzí 1 až 4 rokov 0%
- Pomer prvkov, ktorým skončí podpora v roku 2018 22%
- Pomer prvkov, ktorým skončí podpora za 5 a viac rokov tvorí 52%

Pre manažérsky výstup viz. Nasledujúci obrázok (obr.12 Podpora prvkov odosielajúcich Netflow 9)



Obrázok 17:Podpora prvkov odosielajúcich Netflow 9

2.16 Analýza komunikácie SCADA a rozvodňa



Obrázok 18:Obecné zobrazenie komunikácie SCADA-Rozvodňa

Obecne na základe architektúry, ktorú môžeme v prostredí energetiky tak komunikácia prebieha nasledovne:

SCADA centrálny server, je server, z ktorého sa vysielajú príkazy na jednotlivé IED, alebo RTU zariadenia umiestnené vo vnútri rozvodne a z rozvodne sa vysielajú naspäť na centrálny SCADA server telemetrické údaje z jednotlivých zariadení. Pre túto komunikáciu je využívaný vo väčšine prípadov protokol IEC 60870-5-104 (ďalej iba IEC 104) alebo IEC 60870-5-101 (ďalej iba IEC 101). Príkladom takéhoto príkazu môže byť zapnutie vypínaču, alebo elektrického ističa vo vnútri rozvodne. Protokol IEC104 prejde WAN OT sieťou do rozvodne a gateway v danej rozvodni preloží tento protokol na IEC 61 850, protokol pomocou ktorého komunikujú jednotlivé IED zariadenia v rozvodni. Zariadenie (gateway), ktoré tento preklad zabezpečuje je takmer vždy určité RTU s rôznymi rozhraniami. Protokol IEC 61850 využíva ďalšie dva komunikačné protokoly

a to: Manufacturing Message Specification (ďalej iba MMS) a Generic Object Oriented Substation Event (ďalej iba GOOSE).

2.16.1 GOOSE

Protokol GOOSE je kontrolný mechanizmus, v ktorom formát dát (status, value) je združený do data setu a odoslaný s časovou periódou 4 milisekundy. Tento mechanizmus je využívaný pre zaistenie špecifického prenosu, rýchlosti a spoľahlivosti, správy s hard real-time požiadavkami. V prostredí energetiky je využívaný na zapnutie elektrických ochrán.

- GOOSE data sú priamo zapúzdrené do Ethernetového rámcu.
- Využíva prioritné tagovanie VLAN, separuje virtuálne siete vo vnútri rovnakej fyzickej sieti a nastavuje vhodnú úroveň priority správ
- Rovnaká GOOSE správa je znovu odoslaná so zvýšeným odosielajúcim intervalom. Každá nová udalosť využívajúca GOOSE dataset element spôsobí zastavenie znovu odosielanie existujúcich GOOSE správ. To, či sa jedná o novú udalosť alebo udalosť, ktorá sa opakovane odosiela, určuje stavové číslo vo vnútri GOOSE protokolu.
- GOOSE správy sú navrhnuté tak, aby boli univerzálne a kompaktibilné so všetkými dodávateľmi IED zariadení.
- GOOSE protokol nie je IP-based. Využíva Ethernet ako prenosný protokol.

2.16.2 MMS

MMS je štandardizovaný protokol, ktorý odosiela menej urgentné správy ako GOOSE protokol. Pomocou neho sa odosielajú príkazy na jednotlivé IED zariadenia z centrálneho SCADA serveru alebo telemetrické údaje z jednotlivých IED zariadení na centrálny SCADA server. MMS protokol pracuje na vrchnej vrstve TCP protokolu a využíva port 102. Gateway alebo RTU vo vnútri rozvodne ho využíva na zber telemetrických dát a odosielanie príkazov.

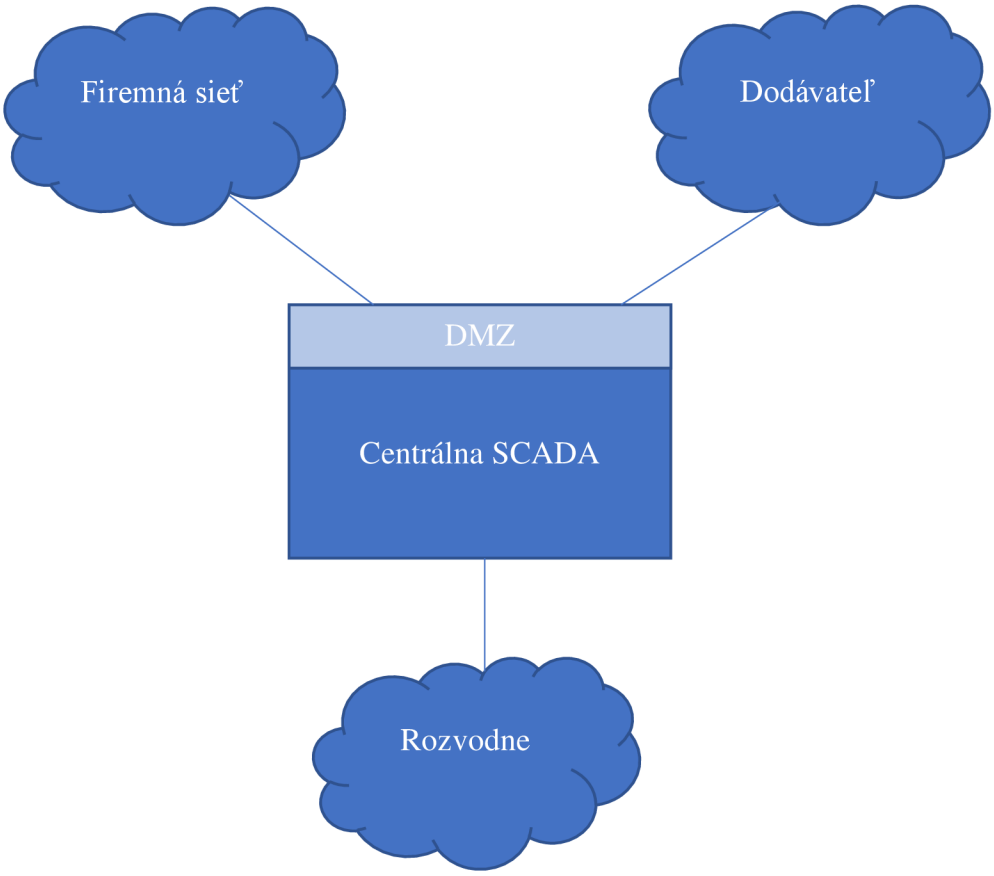
3 Praktická časť

V tejto časti diplomová práca pojednáva o možných technických riešeniach a opatreniach, ktoré zvyšujú zabezpečenie a znižujú riziko kompromitovania OT siete. Výstupom praktickej časti je umiestnenie a typ sond v provoznej sieti. Zvolené riešenie vychádza z analýzy prostredia a metodiky best-practices v tejto problematike. Oblasti, na ktoré je praktická časť zameraná sú možné vektory útoku na SCADA systémy a s nimi spojené hrozby.

3.1 Vektory útoku na centrálny SCADA systém

Kompromitovanie centrálneho SCADA systému o ktorých diplomová práca pojednáva a volí opatrenia je možné pomocou 4 obecných vektorov útoku a to cez: firemnú sieť, kompromitovanie správcovských účtov dodávateľa alebo cez jednotlivé rozvodne a takzvaný Insider Threat.

Vektory útoku na centrálny SCADA Systém



Jednotlivým vektorom prislúcha najhorší možný scenár a to získanie kontroly nad centrálnym SCADA serverom, z ktorého je možné ovládať energetickú sieť.

Vektory:

- Exploit software zraniteľnosti cez firemné rozhranie
- Exploit software zraniteľnosti pomocou vzdialeného prístupu / údržby
- Exploit software zraniteľnosti cez rozhranie rozvodne
- Príkazy vyslané do rozvodne z neautorizovaných zariadení (Insider Threats)

3.2 Opatrenia pre zabezpečenie centrálneho SCADA systému

V tejto časti diplomová práca popisuje návrh obecných opatrení na základe best practices pre štyry obecné vektory útoku na SCADA systém energetickej spoločnosti. Dôvodom tohoto rozdelenia je, že tieto komunikačné kanály so sebou prinášajú rôzne riziká. Komunikácia v rámci SCADA a OT siete je vo väčšine prípadov machine-to-machine a tak povediac pravidelná. Vo väčšine prípadov sa transportujú operačné a telemetrické dáta, nie konfiguračné zmeny alebo binárne súbory. Exploity alebo payloady je ťažké skryť, ak je sieť monitorovaná pomocou sofistikovaných nástrojov. To znamená, že pri dobrom asset inventory, vulnerability manažmente a striktne definovaných komunikačných pravidlách, ktoré sú monitorované pomocou napríklad IDS sond, tak je možné tieto útoky zachytiť a na ne reagovať.

3.2.1 Opatrenia pre prístup cez firemné rozhranie

Obecne platí, že OT sieť a IT sieť je od seba oddelená, ale aj napriek tomu existujú vektory, ako sa do provoznej siete (ďalej iba OT) dostať aj cez IT sieť. Jedná sa o prístup iba určitých skupín ľudí, ktorý majú na starosť OT sieť. Medzi jedno z opatrení, aby sa zvýšila bezpečnosť OT siete, je vybudovanie demilitarizovanej zóny s dodatočnými bezpečnostnými prvkami ako je jump server, active-directory atď... medzi IT a OT, ako je zobrazené na obrázku v sekcií „vektory útoky na centrálny SCADA systém“.

3.2.2 Opatrenia pre zabezpečenie vzdialeného prístupu / údržby

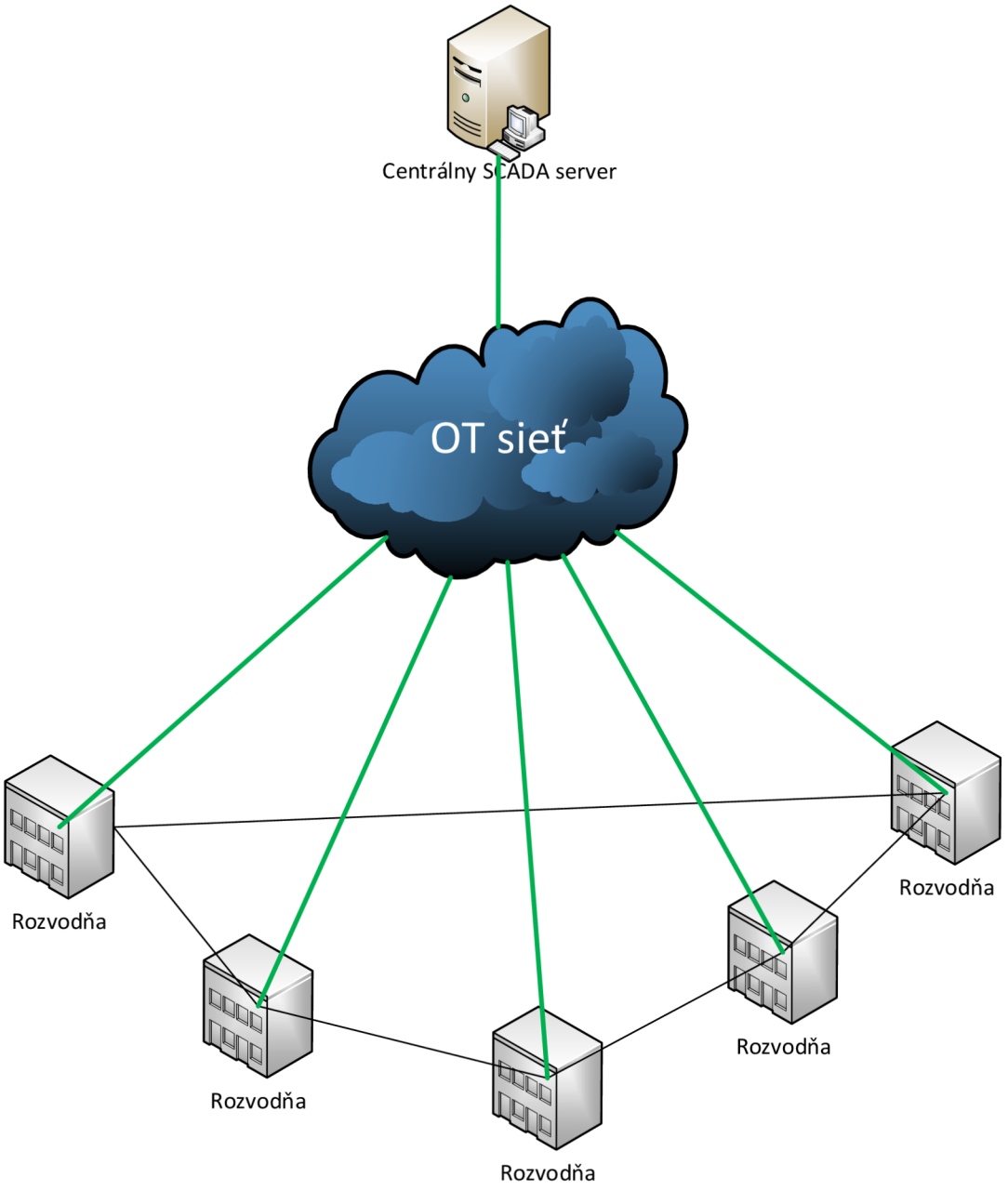
SCADA servery sú bežne pod správou dodávateľov systému, ktorí sa starajú a ručia za ich funkcionalitu. Preto majú vytvorený prístup do OT siete a to vytvára jeden z možných vektorov útoku. Potenciálna hrozba, ktorá môže nastať, je získanie validných credentials

dodávateľa systému a pomocou nich môže útočník získať kontrolu na centrálnym SCADA serverom. Útočníci tak môžu manipulovať so softwarovou konfiguráciou SCADA systému, pokiaľ kompromitujú účet dodávateľa, vytvoriť do systému backdoor, logickú bombu alebo manipulovať treshholdy použité v ochranných systémoch. Tento druh útoku je ťažké detekovať a môže spôsobiť veľké škody, preto je nutné, aby do siete pristupovali dodávatelia systému cez DMZ a cez jump server umiestnený v DMZ, na ktorom bude implementovaná HOST-Based IDS sonda, ktorá môže pomôcť spolu s pravidlami nastavenými na jump serveri detekovať potenciálnu hrozbu. Dodávatelia sa tak logujú na jump server a ten sa následne pripája na hostov v OT doméne. HIDS na jump servery má prístup k udalostiam, ktoré sa dejú priamo na jump servery a tým poskytuje presnejšiu detekciu potenciálnych hrozieb ako samostatná NIDS v DMZ. Tak isto do prostredia centrálnej SCADA je vhodné implementovanie dvoch typov sond pre OT ale aj IT. Podrobnejšie je táto problematika opísaná nižšie v praktickej časti v sekcií „Monitoring OT siete z pohľadu IDS“.

3.2.3 Segmentácia siete

Jedným z najdôležitejších bezpečnostných princípov je správna segmentácia komunikácie v rámci OT siete. Ide o komunikáciu centrálnych SCADA serverov a jednotlivých rozvodní. Ideálny stav je, ak je pre dispečerský riadiaci systém vytvorená VPN a VLAN sieť (prípadne viac záleží od architektúry) a centrálny SCADA server komunikuje s jednotlivými rozvodňami, zároveň rozvodne môžu komunikovať iba s centrálnym SCADA serverom v rámci tejto siete a nie medzi sebou. Týmto opatrením sa zníži počet portov, ktoré je nutné mirrorovať do IDS sondy a zamedzí sa v prípade kompromitovania rozvodne malwarom z iných rozvodní, konkrétne kompromitovanie RTU zariadení, ktoré majú funkcionalitu jednotlivých IED zariadení na starosti a tým rozšírenie malwaru v rámci VLAN dispečerského riadiaceho systému aj do ostatných lokalít. Najhorší scenár, ktorý by v tomto prípade mal nastať je iba lokálny výpadok dodávky elektriny pre danú oblasť, za ktorú je rozvodňa zodpovedná a nie výpadok celej siete. Aby bol útočník schopný spôsobiť celkový blackout musel by kompromitovať malwarom centrálny SCADA server.

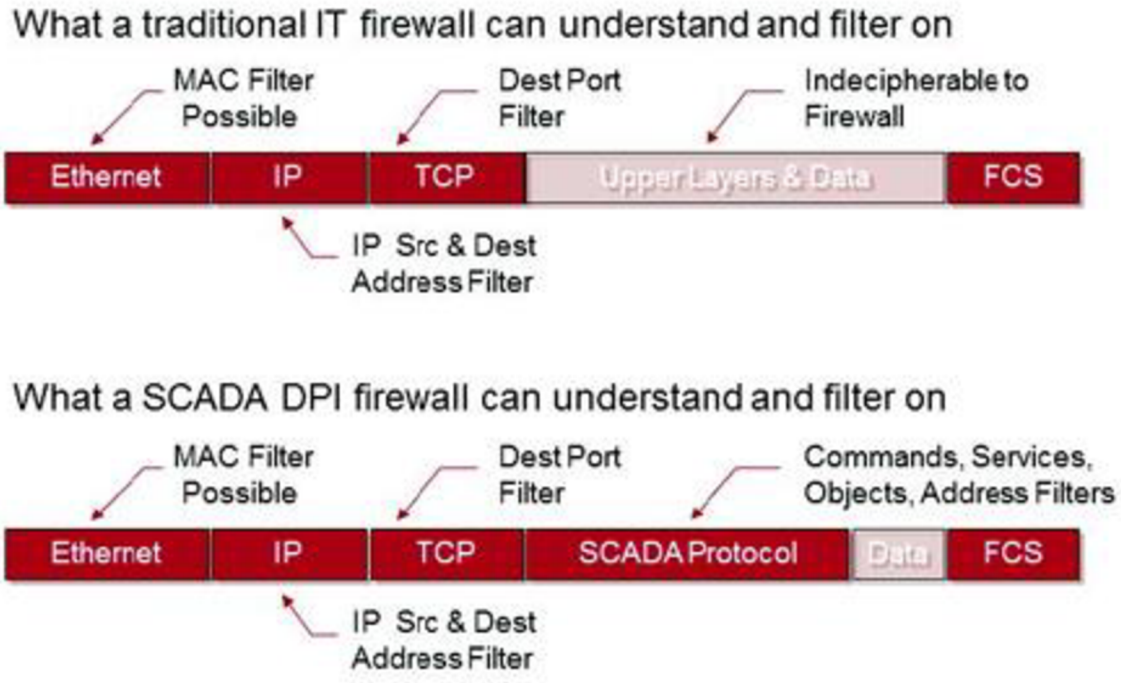
Na nasledujúcom obrázku je zobrazená zelenou spojnicou segmentácia siete v rámci komunikácie dispečerského riadiaceho systému. Čierna spojnica je fyzické prepojenie rozvodní v kruhovej topológií.



Obrázok 19: Komunikácia v rámci dispečerského riadiaceho systému

Segmentácia siete pozitívne ovplyvňuje exploit zraniteľností cez rozhranie rozvodne a obmedzuje prípadný dopad iba na jednu lokalitu, ako už bolo opísané. Pre zvýšenie bezpečnosti rozvodne prichádza do úvahy implementácia aplikačného firewallu na perimeter rozvodne. Toto riešenie však skrýva mnoho úskalí. Výhody, ktoré plynú s implementácie aplikačného firewallu sú, že obsahuje Deep Packet Inspection (DPI) funkcionalitu, ktorá je schopná sa pozrieť do vnútra odosielaných paketov protokolu IEC104 a tým nájsť prípadné malformované pakety odosielané z centrálneho SCADA

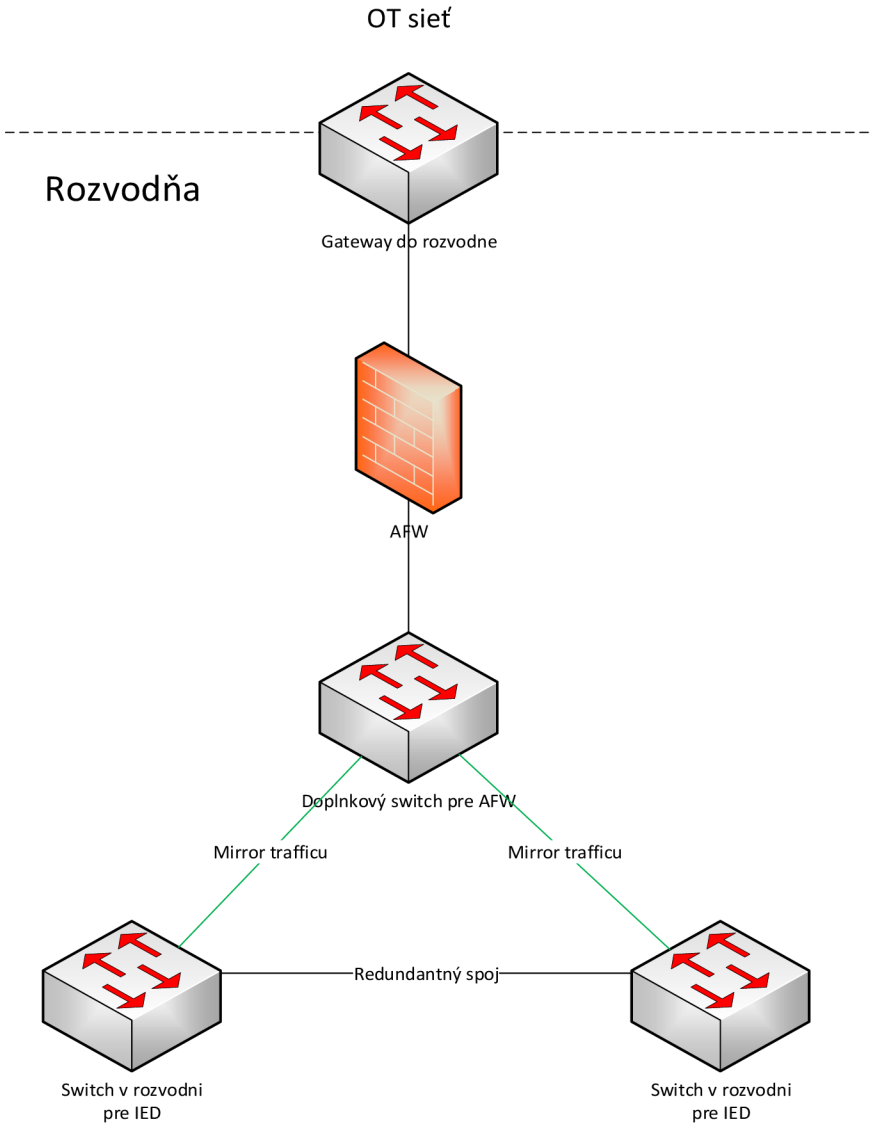
serveru do rozvodne a zároveň sledovať komunikáciu z rozvodne na centrálny SCADA server.



Obrázok 20:Firewall s DPI (zdroj: www.tofinosecurity.com)

Avšak jednotlivé rozvodne obsahujú rôzny počet zariadení, čo by si vyžadovalo nastavovanie FW pravidiel a politík osobitne pre jednotlivé lokality a vyladenie tejto komunikácie by bolo veľmi časovo náročné. Keďže sa jedná o aplikačný firewall, tak v tomto prípade sa správa ako IPS sonda a je veľká pravdepodobnosť, že môže nastať situácia, ktorá nie je nastavená v politikách daného FW a tým sa rovno komunikácia zamedzí. Čo má veľmi negatívny dopad na dostupnosť, ktorá je v prostredí energetiky kľúčová. V prvej fáze implementácie toto riešenie určite nie je vhodné a patrí do kategórie aktívneho monitoringu. Ďalším argumentom proti implementácií AFW je, že pokiaľ je nutné ošetrenie, aby nejaký škodlivý kód nebol spúšťaný z prostredia rozvodne, tak je to skôr prípad pre fyzické zabezpečenie rozvodne. Čo znamená prekonanie fyzickej bezpečnosti. Ak by išlo o kompromitáciu cez kybernetický priestor, tak to znamená prekonania všetkých bezpečnostných politík a opatrení OT siete a obídenie signatúr IDS sondy implementovanej v centrálnej SCADA (táto problematika je opísaná v kapitole „Monitoring OT siete z pohľadu IDS“). Nasadenie AFW má zmysel po zozbieraní a podrobnom zanalyzovaní jednotlivých komunikačných tokov uložených v IDS sonde.

Aplikačný FW väčšinou obsahuje iba dve sieťové rozhrania pre internú a externú sieť, čo by zaznamenalo dokúpenie aktívneho prvku (switch), aby sa mohla celá komunikácia mirrorovať do AFW a to predstavuje ďalšie náklady. Finálna architektúra v rámci rozvodne by potom musela vyzerať nasledovne:



Obrázok 21: Architektúra zapojenia aplikačného firewallu do rozvodne

3.2.4 Monitoring OT siete z pohľadu IDS

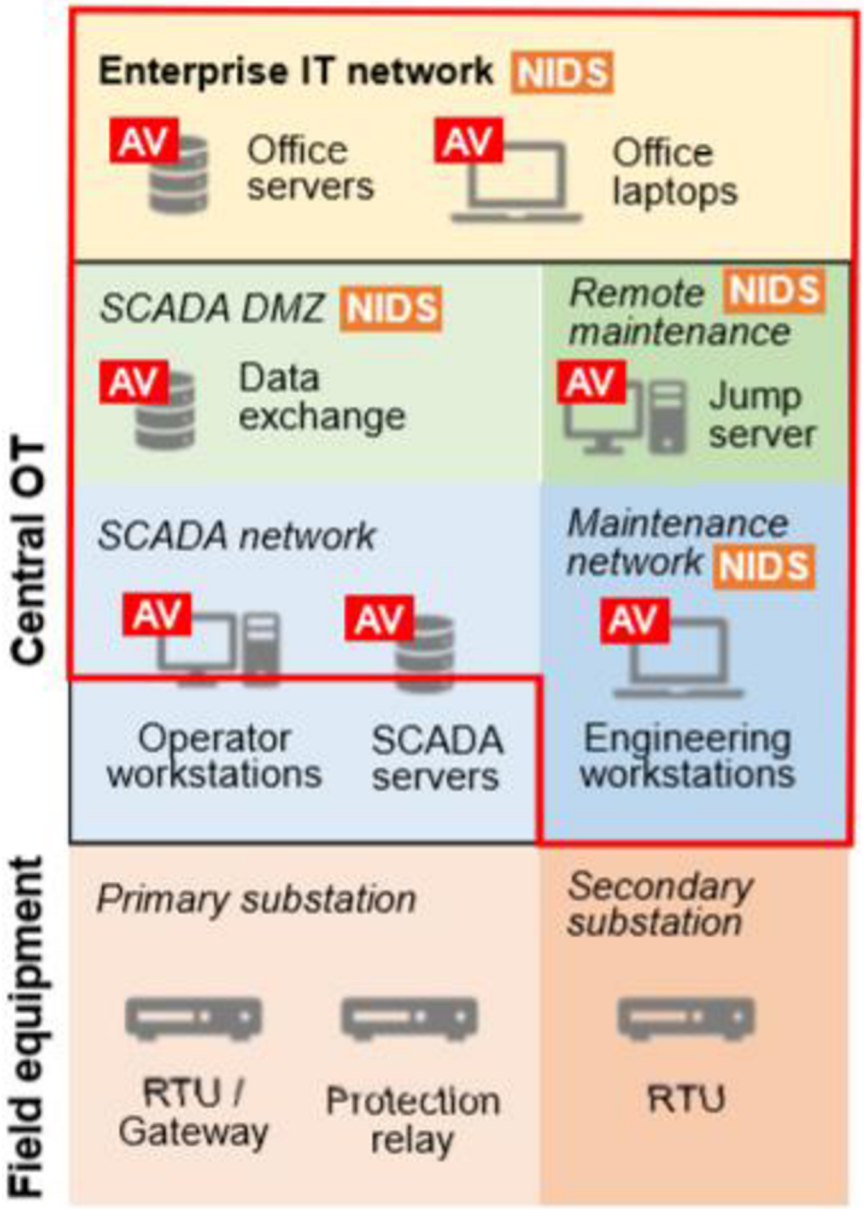
Pre monitoring OT siete je možné zvoliť dva prístupy: a to aktívny alebo pasívny monitoring. Do kategórie aktívneho monitoringu spadajú opatrenia implementácie IPS sond. IPS sonda v prípade detekcie nezvyčajnej komunikácie ihneď danú komunikáciu zablokuje. Nevýhoda tohoto riešenia je, že sonda za anomáliu môže považovať aj legitimnú komunikáciu, ktorá doteraz neprebiehala (zapojenie redundantnej trasy, pripojenie nového aktívne prvku alebo IED zariadenia) a automaticky ju zakáže → false possitive log. Toto riešenie má veľký dopad na dostupnosť, ktorá je v ICS prostredí prioritou. Vyladenie IPS sondy by stálo veľa úsilia a aj tak nie je zaručená maximálna dostupnosť služieb. Pokrytie OT siete týmto typom sond by vyžadovalo ich veľké množstvo, pretože musia byť umiestnené priamo v trase komunikácie a ich pridaná hodnota by bola minimálna.

Preto je výhodnejšie riešenie osadenie IDS sondy. Jedná sa o pasívny monitoring siete, ktorý nemá dopad na dostupnosť a vyťaženie siete, v prípade detekcie anomálii v komunikácií, vyhodí iba log alebo alert a nezakáže danú komunikáciu. Logy sa následne zbierajú v centralizovanom systéme určenom pre monitoring nazývaný SIEM. Pre zabezpečenie OT siete a hlavne centrálneho SCADA systému je nutné si uvedomiť, aké všetky služby a protokoly sa v komunikácií nachádzajú. Z analýzy vychádza takzvaný detection gap, kde zabezpečenie centrálnej SCADY sa nedá pokryť IDS sondami, ktoré sú bežné v IT prostredí. To, kde tradičný prístup IT prostredia funguje aj v OT prostredí je zobrazené na nasledujúcom obrázku.

Legenda k obrázku:

AV Signature – a host-based detekcia je účinná na moderných serveroch a pracovných staniciach, ale nie na embedded zariadeniach

NIDS Signature – a network-based IDS fungujú pre protokoly použité v IT ale nie pre SCADA protokoly



Obrázok 22: Tradičný prístup zabezpečenia IT (Zdroj: ENCS OT Monitoring training)

Detekcion gap tvorí neohraničená časť obrázku: Field equipment, operátorské stanice a SCADA server. V tejto oblasti nám sondy využívané v IT nepomôžu a je nutné osadiť sondy určené pre SCADA protokoly, ktoré fungujú na princípe detekcie anomálii komunikácie. Keďže útoky na ICS systémy sú takmer vždy zero-day, tak tento spôsob detekcie patrí medzi najúčinnejšie. Príkladom takejto anomálie môže byť pozmenená dĺžka príkazu odoslaného na RTU zariadenie. Aby sonda vedela tieto informácie spracovávať musí obsahovať funkcionalitu deep packet inspection (DPI). Keďže OT prostredie nie je také variabilné ako IT a príkazy a komunikácia v rámci OT siete je pevne daná a má nemennú štruktúru, tak vyladenie sondy je jednoduchšie a minimalizuje sa tým

počet false possitiv logov. Z toho vyplýva, že pre zabezpečenie centrálneho riadiaceho systému je nutné z pohľadu IDS sond osadiť dva typy.

- IDS pre IT protokoly
- IDS pre OT protokoly

Sondou určenou pre IT protokoly sa bude detekovať komunikácia do centrálneho riadiaceho systému od dodávateľov, teda z vonku siete a zároveň Insider Threat, pre zabezpečenie a detekciu potenciálnych malwarov v rámci OT siete a centrálnej SCADY sonda určená pre OT protokoly. Výhodou segmentácie siete a IDS OT-based sondy je, že pre pokrytie bude stačiť jedna IDS sonda.

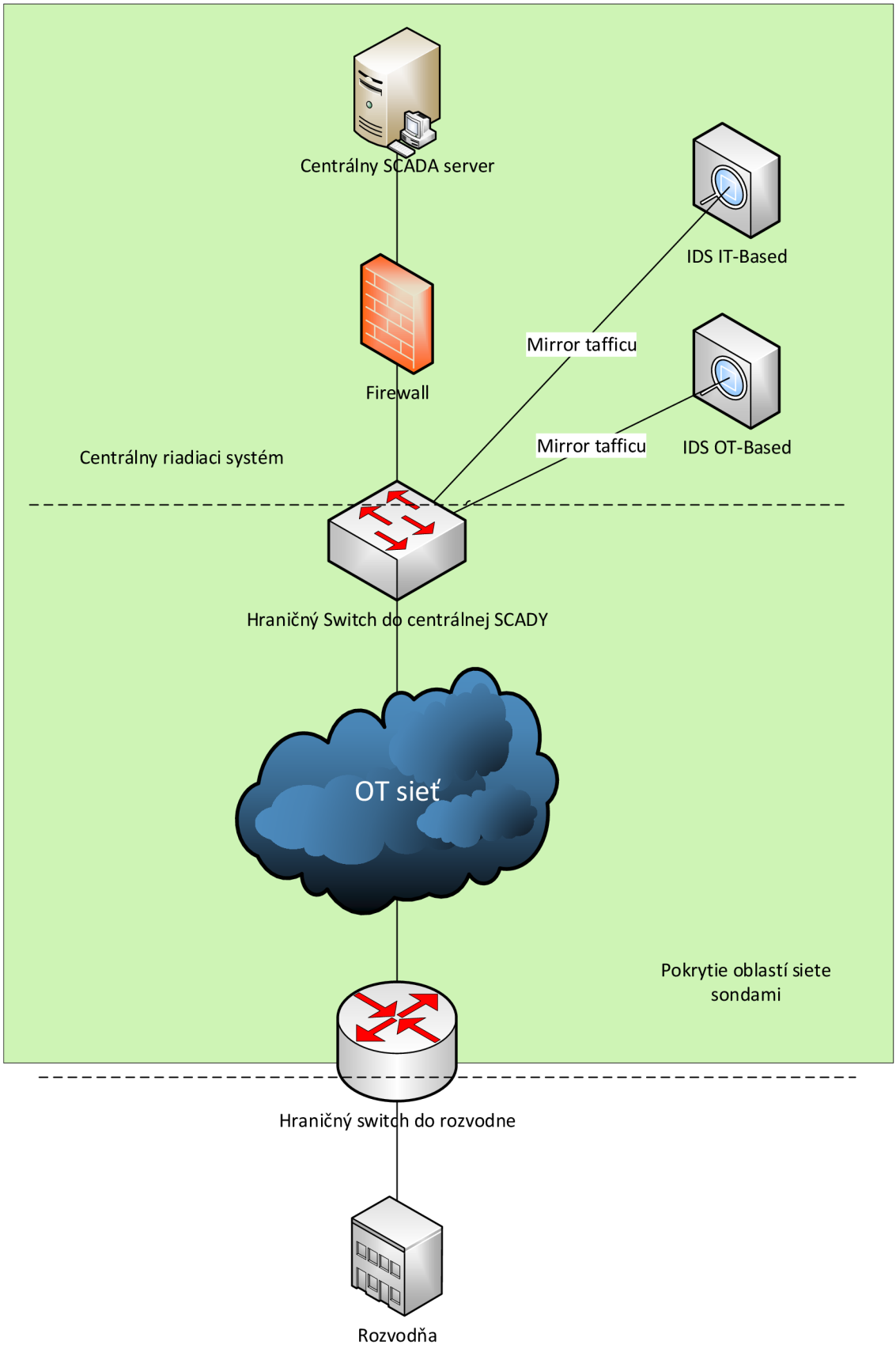
3.2.5 Identifikácia umiestnenia IDS sondy

Na základe analýzy siete bolo nutné nájdenie uzla, cez ktorý ide všetok traffic smerom z centrálnej SCADY do OT siete a naopak. Po identifikácií uzla, alebo konkrétneho switchu zodpovedného za túto komunikáciu je nutné zohľadniť jeho vlastnosti a parametre. Jedná sa o:

- priepustnosť portov
- šírku pásma
- schopnosť vykonávať port mirroring

Preto je nutné daný switch otestovať a vyskúšať, či je schopný tieto parametre splniť, aby nenastala situácia, že z dôvodu plného vyťaženia šírky pásma dôjde k strate dát a tým pádom neúplným údajom v IDS sonde.

Týmto umiestneným IDS sond sa pokryje komunikácia po hraničný switch do rozvodne. V prípade monitoringu anomálii v rámci rozvodne je nutná implementácia sondy aj do vnútra rozvodne. Aby sa dosiahlo plnej funkcionality sondy určenej pre OT protokoly, konkrétne využitia DPI komunikácia v rámci OT siete, nesmie byť šifrovaná. Zároveň existuje niekoľko typou IDS sond popísaných v teoretickej časti diplomovej práce. Z analýzy a vlastností IDS sond teda vyplýva, vhodné osadenie IDS sondy, ktorá je Network-based a detekciu vykonáva na základe anomálii.



Obrázok 23: Pokrytie oblasti komunikácie implementáciou IDS OT-based sondy

3.2.6 Porovanie typov IDS sond

Signature-based sonda upozorňuje na konanie dátovej komunikácie, ktorá zodpovedá určitému modelu. Modelu už známych zraniteľnosti → signatúry, tieto signatúry sú už vo väčšine prípadov preddefinované a manuálne naskriptované. Takmer všetky sondy dovoľujú vytváranie vlastných signatúr, čo umožňuje technikom pomocou regulárnych výrazov upraviť signatúru pre dané prostredie. Avšak treba zachovať to, aby signatúra bola čo najvšeobecnejšia, písanie príliš špecifických signatúr nie je vhodné, pretože útok sa môže v priebehu času mierne pozmeniť a potom ho sonda nezaznamená.

Výhody:

- Sonda môže byť vyladená, aby zaznamenávala málo false possitiv logov
- Alerty dávajú nápovedu o aký typ útoku sa jedná

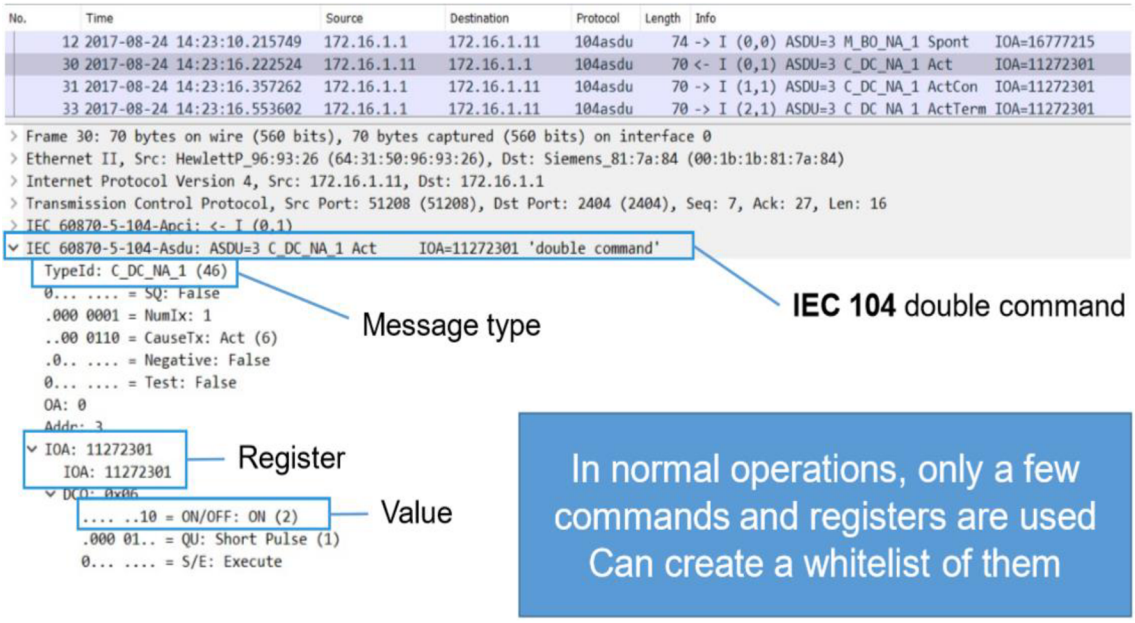
Anomaly-based: Ako už bolo opísané vyššie, komunikácia v rámci priemyselných protokolov je stála a nie tak variabilná ako v IT. Čo má kladný dopad, pretože tento typ sondy upozorňuje technika na abnormality v sieťovej komunikácií. Často tieto sondy majú samo-učiaci sa algoritmus, ktorý nie vždy je výhodou a je nutné, aby bezpečnostný technik detailne poznal komunikáciu v rámci OT siete a tým správne vedel vyhodnotiť alerty a logy.

Výhody:

- Detekuje nový druh útokov (zero-day), ktorý nezodpovedná štruktúre protokolov v OT sieti bez vytvárania nových signatúr

3.3 Praktický príklad IDS sondy s DPI

Na obrázku [Ukážka DPI IDS sondy (Zdroj: ENCS OT monitoring training)] na nasledujúcej strane je zobrazená komunikácia SCADA serveru s riadiacou jednotkou (RTU) umiestnenou v rozvodni. Centrálny SCADA server vyslal pomocou protokolu IEC104 double command na RTU zariadenie. Týmto jednotlivým typom príkazov vysielaných na RTU odpovedá určitý Message Type a hodnota I/O registra RTU zariadenia a následne jeho hodnota už len v boolean tvare. Jednotlivé príkazy majú pridelené špecifické číslo definované v registri RTU zariadenia a majú pevne definovanú dĺžku. Tento podrobný rozbor práve poskytuje funkcionalita DPI, ktorá hľadá anomálie v takomto druhu komunikácie.



Obrázok 24: Ukážka DPI IDS sondy (Zdroj: ENCS OT monitoring training)

3.3.1 Detekcia zero-day

Práve takýto typ útoku bol využitý pomocou malwaru Industroyer, kde využili neošetrenú podmienku - vracanie hodnoty určitých procedúr Interrogation commandu vyslaného na RTU zariadenie → a spôsobili tzv. null pointer dereferenciu. V podstate skrátili dĺžku tohoto commandu o 3 byty a tým zamedzili dostupnosť určitej služby, ktorá bola kľúčová pre dodávanie elektrickej energie.

```
68 0e 30 00 be 00 64 01 06 00 01 00 00 00 00 14 (normal)
68 0b 34 00 ce 00 64 01 06 01 00 14 (malformed)
```

Obrázok 25: Malformovaný packet Interrogation command C_IC_NA_1 (Zdroj: ENCS OT monitoring training)

Celkovo tento príkaz má dĺžku 70 bytov a útočníci ho skrátili a 3 byty. Prvé dva tučne vyznačené byty sú zodpovedné za adresu RTU zariadenia a zvyšné tri tučne vyznačené za konkrétnu hodnotu v I/O registry pre daný príkaz. V malformovanom pakete sú zastúpené každé po jednom byte čo spôsobilo spomínanú situáciu.

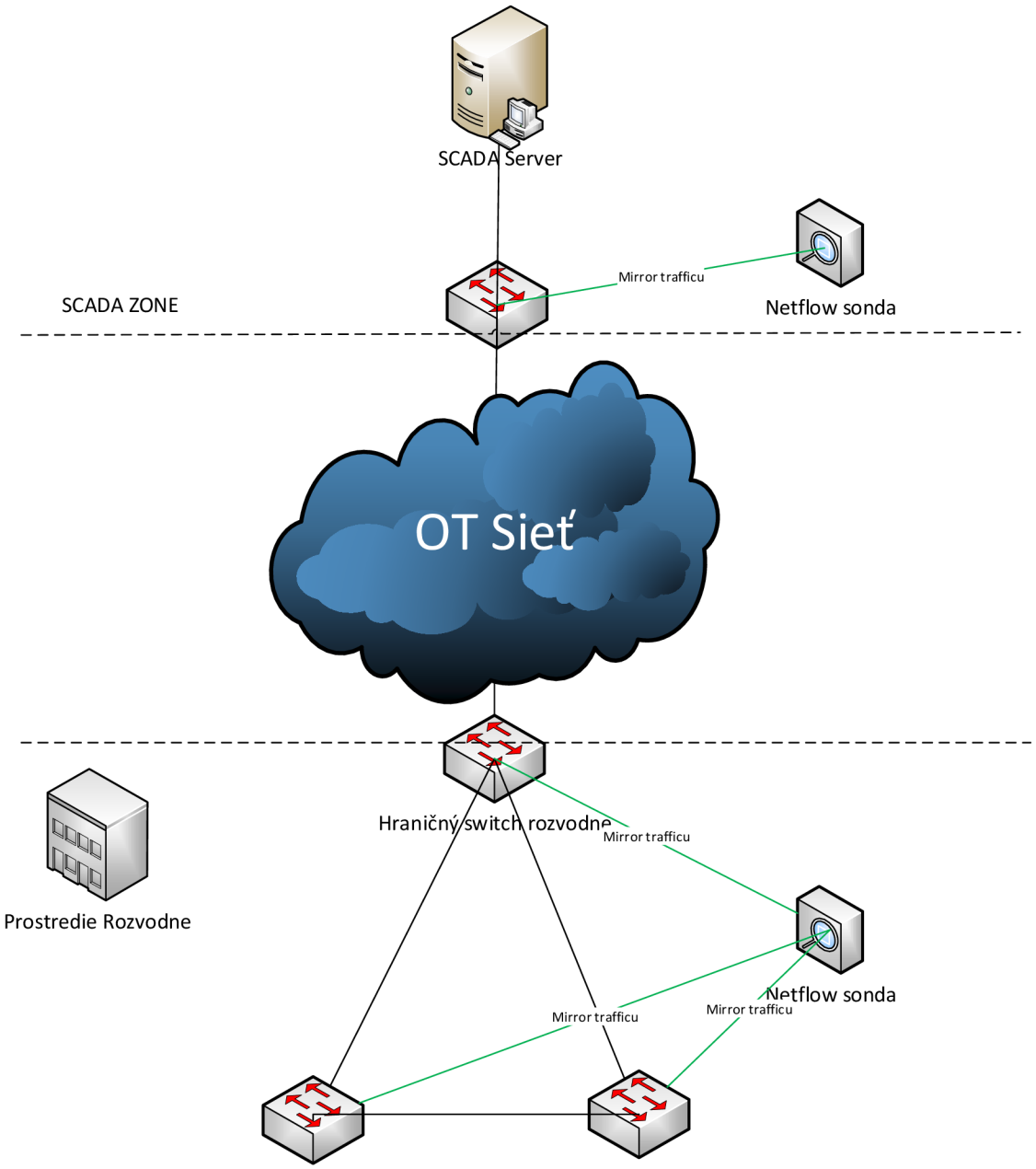
Pomocou typu sond, ktoré detekujú anomálie a sú určené pre OT protokoly, tak je možné tieto útoky detekovať a agilne jednať.

3.3.2 Implementácia Netflow sond

Monitorovanie komunikácie na základe Netflow je ďalším a zároveň základným bezpečnostným opatrením pri monitorovaní siete, kde je monitorovaná druhá až štvrtá vrstva ISO osi modelu. Tento spôsob monitoringu poskytuje zjednodušene povedané informácie, aká IP adresa s kým komunikovala a port ktorý daná komunikácia využila. Zároveň vytvára štatistické údaje o jednotlivých komunikáciach. Samozrejme z časti túto funkcionalitu podporujú IDS sondy, ale nie je to ich primárne využitie skôr je to ich doplnok a nevykonávajú túto činnosť v reálnom čase, tak ako netflow sondy. Korelácia týchto opatrení je významná pre nutnosť prípadnej forenznej analýzy pri výskyte bezpečnostnej udalosti alebo bezpečnostného incidentu. Je dobré disponovať pri tejto činnosti čo najväčším počtom dát. Navyše IDS sonda nemusí ani odhaliť anomáliu v komunikačných tokoch tak promptne ako Netflow sonda.

Implementácia Netflow sond je v tomto návrhu rozčlenená na dve fázy. Odosielanie flow dát sú schopné aj niektoré aktívne prvky a tým pádom nie je nutné implementovanie Netflow sond do týchto lokalít. Podrobnejší rozbor tejto problematiky je opísaný v analytickej časti diplomovej práce. V prvej fáze implementácie pre pokrytie Netflow komunikácie je vhodné osadiť Netflow sondu do rovnakého segmentu siete, ako sú umiestnené IDS sondy. Týmto riešením sa pokryje komunikácia OT siete od centrálneho riadiaceho systému po hraničný switch jednotlivých rozvodní. Nevýhoda tohoto riešenia je, že nebudú dostupné flow dáta, z jednotlivých uzlov (aktívnych prvkov), ktoré tvoria OT sieť, cez ktoré komunikácia prešla a tým pádom neúplné dáta pre forenznú analýzu. Tomu riešeniu sa dá pomôcť tým, že prvky ktoré tvoria OT sieť a vedia odosielať Netflow dáta verzie IPFIX version 10 sa funkcionalita povolí a budú ich odosielať do Netflow kolektoru. Následne sa budú obmieňať aktívne prvky OT siete za nové s kritériom pre odosielanie IPFIX verzie 10. To spadá do druhej fáze implementácie. Nevýhoda však tohoto riešenia je, že nebudú obsiahnuté flow dáta z vnútra jednotlivých rozvodní.

Preto sa ponúka druhé riešenie nákup Netflow sond pre každú lokalitu (rozvodňu) a mirrovať traffic z gateway switchu do rozvodne a switchov vo vnútri rozvodne do sondy v každej jednej lokalite. Avšak toto riešenie môže byť v konečnom štádiu omnoho nákladnejšie a pre voľbu riešenia tejto problematiky sa vyžadujú dodatočné analýzy.



Obrázok 26: Varianta 2 osadenia Netflow sond

3.4 Skenovanie rozvodne

V nasledujúcej časti práca popisuje analýzu rizík spojenú so skenovaním rozvodne a voľbu opatrení pre jednotlivé riziká spojené s touto činnosťou. V prípade odhalenia zraniteľnosti jednotlivých zariadeniami umiestnenými v rozvodni práca popisuje návrh riadenia rizík a voľbu opatrení na zníženie dopadu odhalených zraniteľnosti.

3.4.1 Analýza rizík

Pre analýzu rizík je využitá metóda RIPRAN, pričom nasledujúce tabuľky obsahujú kritéria pre kvantitatívne hodnotenie pravdepodobnosti, dopadu rizík a celkovú závažnosť rizík projektu.

Pre hodnotenie pravdepodobnosti a dopadu rizík je zvolená škála v rámci intervalu od 1 do 5, pričom 1 má najnižšiu hodnotu dopadu a pravdepodobnosti a 5 reprezentuje najväčšiu pravdepodobnosť a dopad rizika spojeného s činnosťou skenovania rozvodne. Pri dopade jednotlivých rizík je hodnotám pridelené slovné hodnotenie. Celková hodnota rizika je následne vyjadrená pre jednoduchšie orientovanie jak číselne a to vynásobením hodnoty pravdepodobnosti a hodnoty dopad tak vizuálne viz. tabuľka celkové hodnotenie rizika.

3.4.2 Hodnotenie pravdepodobnosti rizika

Tabuľka 9: Hodnotenie pravdepodobnosti rizika

Hodnota	Číselné vyjadrenie
1	0 % - 20 %
2	21 % - 40 %
3	41 % - 60 %
4	61 % - 80 %
5	81 % - 100 %

3.4.3 Hodnotenie dopadu rizika

Tabuľka 10 Hodnotenie dopadu rizika

Hodnota	Slovné Vyjadrenie
1	Veľmi malý
2	Malý
3	Stredný
4	Velký
5	Veľmi velký

3.4.4 Celkové hodnotenie rizika

Celkové hodnotenie rizika = hodnota pravdepodobnosti x hodnota dopadu

Tabuľka 11: Vizuálne vyjadrenie hodnoty celkového rizika

Číselné vyjadrenie	Vizuálne vyjadrenie
1-4	
5-9	
10-14	
15-19	
20-25	

Tabuľka 12: Bodové ohodnotenie celkového rizika

	1	2	3	4	5
1 (0 % - 19 %)	1	2	3	4	5
2 (20 % - 39 %)	2	4	6	8	10
3 (40 % - 59 %)	3	6	9	12	15
4 (60 % - 79 %)	4	8	12	16	20
5 (80 % - 100 %)	5	10	15	20	25

3.4.5 Analýza rizík skenovania rozvodne

Tabuľka 13: Analýza rizík spojených s činnosťou skenovania rozvodne

Číslo	Hrozba	Scenár	P	D	H
Technologická rizika					
1	Výpadok HMI	Obmedzenie riadenia rozvodne z lokálnej SCADY	2	3	6
2	Výpadok RTU	Obmedzenie riadenia rozvodne a jednotlivých IED zariadení	2	4	8
3	Výpadok ochrán	Obedzenie funckioanlity rozvodne	2	4	8
4	Zhodenie celej rozvodne	Výpadok elektickej energie pre danú lokalitu	1	5	5
5	Vypnutie / poškodenie zariadení zbierajúcich vzorky komunikácie v rámci rozvodni	Nezíkanie potrebných údajov pre vyhotovenie analýzy prostredia	1	2	2
Procesní rizika					
6	Chybné podklady k danej rozvodni	Predĺženie doby skenovania	1	1	1
Bezpečnostné riziká					
7	Strata zozbieraných údajov	Opakovania skenovania rozvodne	1	2	2
8	Odcudzenie zozbieraných údajov	Hrozba bezpečnostnej udalosti	1	1	1
9	Nájdenie zraniteľnosti zariadení	Voľba opatrení	4	5	20

Opatrenia:

Aby sa predišlo rizikám obmedzenia dostupnosti jednotlivých zariadení v rozvodni prípadne celej rozvodne je nutná účasť ochranárov a servisných technikov, ktorí sú schopní obnoviť funkcionalitu jednotlivých zariadení promptne v intervale niekoľkých minút. Táto situácia môže nastať, pretože aktívne skenovanie môže spôsobiť zamrznutie starších zariadení.

3.5 Nástroje použité pri skenovaní

- Nessus Vulnerability Scanner
- Nmap
- Wireshark
- Špecializované embedded zariadenie pre zbieranie sieťovej komunikácie

Pre zozbieranie sieťovej komunikácie bola komunikácia zbieraná z 3 switchov umiestnených v rozvodni. Prvé zariadenie sa umiestnilo na hraničný switch (gateway) rozvodne, kde sa pokryla celá komunikácia smerujúca do a z rozvodne. Zvyšné dve zariadenia boli osadné a traffic bol mirrorovaný z redundantne zapojených switchov, ku ktorým sú pripojené jednotlivé IED zariadenia. Tým sa pokryla komunikácia v rámci rozvodne. Pre zber sieťovej komunikácie sa využil nástroj Wireshark, ktorý ju ukladal do PCAP súborov s postupným ukladaním po časových intervaloch 10 minút po dobu dvoch dní. Následne sa zozbieraná komunikácia analyzovala, a vytvárala sa štatistika komunikačných tokov, tieto detailné informácie sa však v diplomovej práci kvôli ochrane údajov neuvádzajú.

Pre aktívny sken zraniteľnosti bol využitý softwarový nástroj Nessus s rozšíreniami pre priemyslové siete. Skenované zariadenia:

- RTU
- HMI
- NTP server
- Hraničný switch rozvodne
- Priemyslové switche v rozvodni

Cieľom bolo oskenovať zariadenie a detekovať potenciálne zraniteľnosti jednotlivých firmwarov, operačných systémov zariadení a zmapovať otvorené porty. Pomocou aktívneho skenovania sa overila zároveň dodaná dokumentácia k príslušnej lokalite a povolená komunikácia.

Aktívny sken prebehol úspešne bez narušenia dostupnosti služieb, alebo celkovej dostupnosti rozvodne. Sken zraniteľnosti odhalil určité zraniteľnosti, na ktoré je nutné dohliadať a manažovať → to spadá do činnosti: vulnerability manažment. Podrobnosť informácií je na žiadosť spoločnosti obmedzená.

Vnútorný sken zraniteľnosti riadiacej jednotky neprebehol z obavy o funkčnosť zariadenia v aktívnom provoze. Prebehol iba externý sken zraniteľností.

3.6 Zhrnutie opatrení pre zabezpečenie OT siete

3.6.1 Zabezpečenie centrálnej SCADA

- Implementácia NIDS sondy pre OT s DPI
- Implementácia NIDS sondy pre IT
- Implementácia Netflow sondy

Všetky spomenuté sondy sa musia implementovať na hraničný switch vedúci do centrálnej SCADA, tým sa pokryje komunikácia v rámci centrálnej SCADA po gateway switch rozvodne. Pri Netflow sonde sa obdržia flow dáta smerované do a z centrálnej SCADA, avšak nie z jednotlivých uzlov, ktoré tvoria OT sieť.

Pre získanie flow dát z uzlov, ktoré tvoria OT sieť je nutné obmeniť prvky, ktoré neodosielajú flow dáta verzie IPFIX 10, alebo na tieto uzly osadiť Netflow sondu.

3.6.2 Zabezpečenie rozvodní

Z kybernetického hľadiska zabezpečenie všetkých rozvodní je veľmi ekonomicky nákladná činnosť a je závislá na fyzickej bezpečnosti. Bez korelácie týchto dvoch oblastí dochádza k zanedbaniu celkovej bezpečnosti a na tento aspekt treba brať ohľad. Aby sa znížilo riziko kompromitácie siete cez rozvodňu, tak je vhodné osadenie tak isto Netflow sond a IDS OT-Based sond do rozvodní 1. priority definovaných energetickou spoločnosťou.

3.6.3 Prvá fáza implementácie

V prvej fáze implementácie bezpečnostných opatrení ide hlavne o pokrytie sieťovej komunikácie do OT siete z IT prostredia → prístup na centrálny SCADA server a z tohoto serveru po gateway switch všetkých rozvodní energetickej spoločnosti. Do tejto fázy spadá tak isto zabezpečenie a monitorovanie komunikácie rozvodní 1. priority a to vyžaduje implementáciu Netflow a IDS sond OT – based aj do vnútra jednotlivých rozvodní tejto kategórie.

Čo sa týka rozhodnutia implementácie týchto opatrení aj pre zvyšné rozvodne, ktoré nie sú definované v kategórii jedna bude predmetom ďalších analýz. A preto diplomová práca o nich nepojednáva.

3.7 Ekonomické zhodnotenie

Jednotlivé ceny uvádzané v ekonomickom zhodnotení sú tvorené na základe verejne dostupných informácií a odborného odhadu. Informácie sa neuvádzajú podrobne ale celkovo k jednotlivým opatreniam.

Tabuľka 14: Ekonomické zhodnotenie

Sondy	**Cena v EUR**
• IDS	600 000
• Netflow	24 000
Support každý ďalší rok (Volitelná položka)	200 000
Servery	
Hardware + Software	204 000
Celkom bez Volitelnej položky	***828 000***

3.8 Prínosy diplomovej práce

Prínosy diplomovej práce spočívajú v návrhu umiestnenia bezpečnostných opatrení, ktoré zvýšia bezpečnosť siete a znížia pravdepodobnosť a dopad rizík spojených s kompromitovania OT siete. Zároveň sa týmito opatreniami naplnia určité kritériá pre splnenie požiadaviek vychádzajúcich z legislatívy, na základe ktorých je energetická spoločnosť nutná konať, aby naplnila podmienky zákona:

- *Kybernetický Zákon č. 181/2014 Sb.*
- *Vyhláška č. 316/2014 Sb. o bezpečnostných opatreních*

Implementácia opatrení tak isto naplní určité kroky, ktoré je nutné splniť, aby spoločnosť splnila podmienky auditu a naplnila stanovené ciele uvedené v listine o POA. Kontrolným orgánom v tejto činnosti vystupuje Národný Úrad Informačnej a Kybernetickej Bezpečnosti (NÚKIB).

4 Záver

Diplomová práca popisuje a definuje opatrenia, ktoré je nutné implementovať pre zabezpečenie OT siete z pohľadu kybernetickej bezpečnosti. Konkrétne sa jedná o implementáciu pravidiel a zariadení, ktoré monitorujú sieť, agregujú jednotlivé udalosti a tým predchádzajú vzniku bezpečnostného incidentu.

Pre analýzu prostredia OT siete bolo nutné vybudovanie testovacieho polygonu, ktorý slúžil na zber a triedenie logov odosielaných z jednotlivých sieťových prvkov. Tým čiastočne poskytoval náhlad na logickú topológiu sieťovej komunikácie a tvoril primárny zdroj informácií pre základný monitoring siete pred nasadením komplexného komerčného riešenia. Zároveň testovací polygon slúžil na testovanie jednotlivých bezpečnostných opatrení, overenie ich funkcionality a účinnosti. Vytvorenie testovacieho polygonu bol jeden z hlavných milníkov projektu. Analýza prostredia následne prebiehala ako na základe dát zozbieraných v polygone, tak pomocou poskytnutých dokumentácií OT siete a jednaním so skúsenými technikmi spoločnosti, ktorí poskytovali cenné informácie a insight do danej problematiky. Bez týchto konzultácií a ich znalostí by sa analýza značne predĺžila.

Praktická časť popisuje už samotné návrhy riešenia pre zabezpečenie a pokrytie OT siete sondami. Vybraný technický návrh pozostáva s implementácie IDS sond, OT a IT based pre zabezpečenie centrálnej SCADY, ktorá tvorí jadro OT siete, a samotnej OT siete. Kľúčová časť bola identifikácia miesta, kde tieto sondy implementovať, aby sa pokryla komunikácia v rámci OT siete v čo najväčšom merítku a bolo možné efektívne detekovať potenciálne hrozby a znížiť dopad rizík, ktorý z nich plynie. Tento istý princíp je aplikovaný pre Netflow sondy a koreláciou týchto opatrení dostávame efektívny monitoring 2 až 7 vrstvy ISO OSI modelu.

Významnou časťou diplomovej práce bolo aktívne skenovanie zraniteľností rozvodne pomocou programu Nessus, podrobnosť výstupu tejto činnosti je však na utajenie informácií značne obmedzená.

5 Zdroje

(1) *Overview* [online]. [cit. 2018-05-07]. Dostupné z: https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html#beats-reference

(2) *Deploying and Scaling Logstash* [online]. [cit. 2018-05-07]. Dostupné z: https://www.elastic.co/guide/en/logstash/5.0/deploying-and-scaling.html

(3) CARDWELL, Les a Annie SHEBANOW. *The Efficacy and Challenges of SCADA and Smart Grid Integration: Supervisory Control and Data Acquisition* [online]. Journal of Cyber Security and Information Systems, 2016 [cit. 2018-05-07]. Dostupné z: https://www.csiac.org/journal-article/the-efficacy-and-challenges-of-scada-and-smart-grid-integration/

(4) *ISO/IEC 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*. Revize publikace. Praha: Český normalizační institut, 2017.

(5) *ISO/IEC 27005: Information technology - Security techniques - Information security risk management poskytuje doporucení a techniky pro analýzy informacních rizik*. 1. Praha: Český normalizační institut, 2011.

(6) I*SO/IEC 27032: Information technology - Security techniques - Guidelines for cybersecurity*. 1. Praha: Český normalizační institut, 2012.

(7) *ISO/IEC 27035: Information technology – Security techniques – Information security incident management*. 2. Praha: Český normalizační institut, 2016.

(8) *ISO/IEC 27039: Information technology — Security techniques — Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)*. 1. Praha: Český normalizační institut, 2015.

(9) JANÍČEK, František. *Digitálne ochrany v elektrizačnej sústave*. Bratislava: Slovenská technická univerzita, 2004, 360 s. ISBN 80-227-2135-2.

(10) JORDÁN, Vilém. *Infrastruktura komunikačních systémů II: kritické aplikace*. Brno: Akademické nakladatelství CERM, 2015, 232 stran : ilustrace. ISBN 978-80-214-5240-4.

(11) Port-forwarding. *Techopedia* [online]. [cit. 2018-03-17]. Dostupné z: https://www.techopedia.com/definition/4057/port-forwarding

(12) *Elastic: netflow-module* [online]. [cit. 2018-03-17]. Dostupné z: https://www.elastic.co/guide/en/logstash/current/netflow-module.html

(13) *Install KVM (QEMU) on CentOS 7 / RHEL 7* [online]. Miarec, 2018 [cit. 2018-05-07]. Dostupné z: https://www.itzgeek.com/how-tos/linux/centos-how-tos/install-kvm-qemu-on-centos-7-rhel-7.html

(14) BERMAN, Daniel. *Logz: complete-guide-elk-stack* [online]. 2018 [cit. 2018-05-07]. Dostupné z: https://logz.io/learn/complete-guide-elk-stack/?utm_source=google&utm_medium=cpc&utm_campaign=2Tier_ELK_Learning&utm_content=2Tier_elk_what_is_guide_elkstackGuide&utm_term=elk_what_is&gclid=CjwKCAiA8bnUBRA-EiwAc0hZk4j64rMv1AuVvUi5smeNVSM6cEfw242TsGzKnEBvX0Biumd-lfn-shoC3ToQAvD_BwE#intro

(15) *What is port mirroring* [online]. Miarec [cit. 2018-05-07]. Dostupné z: https://www.miarec.com/faq/what-is-port-mirroring

(16) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014

(17) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací. Praha:* Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(18) Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon) ze dne 28. listopadu 2000.

(19) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014

(20) RAIS, K. a R. DOSKOČIL. Risk management: Studijní text pro kombinovanou formu studia. 1. vydání. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80214-3510-0.

(21) RAIS, K. a R. DOSKOČIL. Operační a systémová analýza 1: Studijní text pro prezenční a kombinovanou formu studia. 1. vydání. Brno: Akademické nakladatelství CERM, 2011. ISBN 978-80-214-4364-8.

(22) *European Network for Cyber Security: ENCS OT Monitoring Training*. Schipol, 2017.

(23) ROSENCRANCE, Linda. *Intrusion Detection System* [online]. January 2018 [cit. 2018-05-07]. Dostupné z: https://searchsecurity.techtarget.com/definition/intrusion-detection-system

(24) HAUGHN, Mathew. *Remote Terminal Unit (RTU)* [online]. September 2017 [cit. 2018-05-07]. Dostupné z: https://whatis.techtarget.com/definition/remote-terminal-unit

(25) COBB, Mike. *DMZ (demilitarized zone)* [online]. June 2015 [cit. 2018-05-07]. Dostupné z: https://searchsecurity.techtarget.com/definition/DMZ

(26) BURK, John. *Virtual Private Network (VPN)* [online]. July 2015 [cit. 2018-05-07]. Dostupné z: https://searchnetworking.techtarget.com/definition/virtual-private-network

(27) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013, 377 s. : il, grafy, tab. ISBN 978-80-7204-872-4.

(28) PAGANINI, Pierluigi. *What is a SOC (Security Operations Center)?* [online]. May 24, 2016 [cit. 2018-05-07]. Dostupné z: https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

Zoznam obrázkov

Zoznam tabuliek