VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Audit kyberbezpečnosti řídících systémů v organizaci

Cyber Security Audit of Industrial Control Systems in Organization

Student: Robert Kolich
Vedoucí bakalářské práce: Ing. Jan Ministr, Ph.D.

Ostrava 2022

Obsah

1 Úvod

V dnešní době se potýkáme s čím dál vyšší mírou optimalizace, sledováním a sběrem dat výrobních postupů průmyslových organizací, což je primárně zajišťováno nasazením řídících systémů. Toto řešení nabízí nespočet výhod v oblasti efektivity výroby optimalizace a načasování procesů. Avšak zvýšený proud dat z a do řídících systémů také skýtá různá úskalí primárně v podobě obtížnosti kybernetického zabezpečení procesu práce s řídícími systémy.

Cílem bakalářské práce je tedy analýza zabezpečení řídících systémů a systémů, které jsou přímo ovlivněny nebo ovlivňují tyto systémy a procesy. Za další cíle práce si autor klade vypracování analýzy rizik a doporučení návrhu zabezpečení proti potencionálním hrozbám nalezeným v analýze rizik.

Práce se zaměřuje na audit kybernetické bezpečnosti řídících systémů v organizaci působící v sektoru výroby a distribuce technických plynů používající řídící systémy pro řízení výrobních procesů a akvizici výrobních dat pomocí řídících systémů.

Dále je bakalářská práce rozdělena do dvou částí, na teoretickou a praktickou část. Teoretická část přibližuje termíny spojené s operačními technologiemi, rozdílem mezi operačními a informačními technologiemi, řídícími systémy, kybernetickou bezpečností a auditem kybernetické bezpečnosti řídících systémů. V neposlední řadě je představen audit, jeho celkový průběh, osoby zodpovědné za vykonávání auditu a jaké náležitosti musí splňovat pro vykonávaní pozice auditora.

Praktická část se skládá z kapitol tři a čtyři, kde v třetí kapitole je popsáno fungování organizace, na kterou je audit zaměřen, čím se organizace zaobírá, je zde ilustrován současný stav využití řídících systémů, stav zabezpečení zmíněných systémů a v neposlední řadě jsou zde vypsány požadavky na zdokonalení kybernetické bezpečnosti v organizaci.

Ve čtvrté a poslední kapitole se bakalářská práce opět zaobírá řešením praktické části, a to primárně nalezením kritických procesů a zařízení v rámci řídcích systémů a vyhodnocením jejich potencionálních hrozeb. Poté se autor

práce zaměřil na pravděpodobnost výskytu hrozeb. Tyto poznatky sloužící jako vstup do části návrhu kybernetického zabezpečení nejpravděpodobnějších hrozeb. Závěrem autor navrhuje případné sugesce na zlepšení vypozorovaných slabých míst. Samotná implementace kybernetického zabezpečení je podřízeno schválením vedení organizace, proto tedy není předmětem zpracování bakalářské práce.

2 Teoretická a metodická východiska kyberbezpečnosti řídících systémů

Tato kapitola se zaobírá formulací řídících systémů, rozdíly mezi informačním systémem a řídícím systémem, jeho dělením na specifické segmenty, nahlíží na případné hrozby jejich kategorizaci, metodiku hodnocení hrozeb, případný dopad na jednotlivé systémy, pracovníky a celou organizaci. Popisuje postupy a aspekty zabezpečení jednotlivých částí řídících systémů.

Další část kapitoly se věnuje definici auditu, jeho primárním členěním, dále specifikací auditu řídících systémů, jednotlivými metodikami auditu. Práce se dále věnuje standardům ISO a ISA/IEC, které definují postupy pro implementaci kybernetického zabezpečení řídících systémů. Dále se zabývá řízením rizik, jeho principy, analýzou a vyhodnocení jednotlivých rizik.

2.1 Definice řídícího systému

Řídící systém – dále jen ICS (Industrial Control System) je pojem zastřešující blíže specifikovanou skupinu programovatelných zařízení, který se zabývá škálou obchodních praktik souvisejících s průmyslovou výrobou, avšak hlavním účelem ICS je snížit případnou chybu lidského faktoru optimalizací a automatizací procesů v průmyslové výrobě. Řídící systémy jsou využívány téměř ve všech odvětvích kritické infrastruktury, což jsou ku příkladu tepelné, jaderné, vodní elektrárny, řídící centra elektrické sítě, čističky vod. ISC je také používáno k řízení procesů v průmyslové výrobě.

Jak již bylo zmíněno v předchozích odstavcích, lidský faktor je majoritní příčinnou chyb vyskytujících se ve výrobních procesech, a přesně z toho důvodu se začaly implementovat řídící systémy do různých oblastí výroby. Cílí na automatizaci, distribuci a také na samotný monitoring vykonávaných procesů. Distribuce procesů umožnuje zvýšit efektivitu jednotlivců a s tím je spojena zkrácená doba, kterou jedinec stráví nad vykonáváním daného pracovního úkonu v určeném čase. Zároveň zaručuje standardní a konzistentní kvalitu výstupů výroby a snižuje cenu vynaloženou na výrobu. Monitoring procesů zabezpečuje kontrolu nad částmi i celými procesy, poskytuje zaměstnancům kontrolu

nad řízením produkčních procesů a rychlou reakci na deviaci od obvyklých hodnot.

2.2 Informační a operační technologie

Technologii dnešní doby lze klasifikovat mnoha způsoby. Jedním ze způsobů, jak lze klasifikovat technologie je na informační technologie (IT) a operační technologie (OT). Informační technologie využívá hardware a software pro vytváření, ukládání, odesílání a přijímání dat, typicky zahrnuje počítače, které nabývají roli klienta, serveru, síťového zařízení, jež sloužící ke směrování provozu v síti, virtuálního softwaru pro redukci potřeby užití hardwaru a v neposlední řadě aplikace zabezpečující fontend klientovi, aby mohl provádět různorodé úkoly.

Naopak, operační technologie zahrnuje zařízení a technologii, která poskytuje kontrolu nad reálným světem. Řadíme zde obojí fyzické zařízení, a systémy je kontrolující, monitorující, a které s nimi vytvářejí rozhraní. Jinými slovy, je to hardware a software potřebný pro kontrolu a monitoring průmyslových procesů napříč škálou aplikací a průmyslů kde jsou klíčovými faktory efektivita a provozuschopnost po celou dobu stanoveného času běhu výroby a procesů.

Do těchto technologií řadíme:

- PLC
- CNC Systémy
- Vědecké vybavení jako např. digitální osciloskoly
- Automatizační systémy budov BAS (Building Automation Systems) za použití protokolu BAC net
- Ovládání světelné signalizace
- Monitoring využití energie
- Dopravní systémy

V současné době je pozorován fenomén integrace informačních a operačních technologií propojením subsystémů z obou kategorií v jeden celek, umožňující zlepšení efektivity, snížení výskytu chyb, snížení vynaložených finančních prostředků, což způsobí výhodu oproti konkurenci. Integrací je myšleno propojení v různých směrech IT a OT prostředí, které je přizpůsobeno cílům organizace.

Integraci můžeme dále rozdělit do tří hlavních kategorií. První kategorií je procesová integrace nebo také integrace technologických postupů. IT a OT oddělení spolu při tvorbě procesů komunikují a obě se podílejí na tvorbě, aby vzniklý proces byl vyhovující oběma stranám a splňoval požadavky pro správu obou oddělení. Druhou kategorii lze nazvat softwarová a datová integrace zabírající se, jak přesunout data a software do a ze serverů do specifických lokací kde se OT zařízení nachází. Poslední kategorií je fyzická integrace, která se zabývá integrací softwaru do fyzických zařízení a nástrojů pro implementaci nových IT řešení na starších OT zařízeních, které doposud byly opatřeny OT specifických softwarem nekompatibilním s novými IT požadavky na zařízení.

2.3 Rozdíl mezi informační a operační technologií

V předchozím odstavci byla každá z technologií charakterizována, a i když jsou v některých aspektech totožně, existují klíčové oblasti, kde se právě tyto dvě technologie zcela zásadním způsobem liší. Pokud je nahlíženo na tyto oblasti z pohledu na zabezpečení, jsou rozdíly patrné, kde je IT z pohledu dat prioritně zaměřeno na ochranu dat, poté až na integritu, a nakonec na dostupnost. V případě OT je na prvním místě dostupnost a integrita, ochrana dat zaujímá pomyslnou poslední příčku důležitosti práce s daty.

Patrné rozdíly se vyskytují i v síťové topologii těchto technologií. IT prostředí je velké s relativně velkým počtem klientů a serverů. Servery jsou rozděleny na základě důležitosti a potřeby, prostředí je dynamického charakteru – IP adresy jsou dynamicky alokovány DHCP serverem. Na rozdíl od IT, je OT komparativně menšího charakteru s limitovaným počtem klientů, serverů a většinově statickými IP adresami.

Fyzické komponenty jednotlivých technologií také dosahují určitých rozdílů. IT prostředí se skládá ze serverů, síťových komponentů, zařízení a pracovních stanicí. Tyto komponenty jsou často chráněny firewally, antivirovými programy, IPS – systémy prevence průniku do systému a firewally webových aplikací, OT systémy jsou postaveny na specifických produktech, mají komponenty jednoho výrobce a limitované zabezpečení z důvodu jednoduššího hardwarového vybavení, které je primárně určeno pro zaznamenávání

a přeposílání dat. Oba systémy mají odlišnou plánovanou dobu provozu, kdy se u IT komponentů předpokládá doba životnosti od tří do pěti let, kdežto u komponentů hardwarových technologií je časový horizont životnosti nad patnáct let. Je to primárně z důvodu praktičnosti, kdy jsou jednotlivé komponenty zapojeny do průmyslových provozů a jejich úkolem je bezchybné plnění stále stejných operací a procesů. V porovnání s IT, kde je kladen důraz na výkon a cenová dostupnost jednotlivých komponentů je zlomková v porovnání s řídícími systémy.

Z pohledu implementace změn v obou systémech je nesmírně důležité, aby oba systémy podléhaly neustálé inovaci a aktualizaci softwaru. Neaktualizovaný software je jedním z primárních slabých míst obou systémů. Softwarové aktualizace v IT softwaru, jsou běžně prováděny ihned jakmile je aktualizace k dispozici, navíc jsou tyto aktualizace často automatizovány na serverové straně systému. Oproti tomu, v OT se nemůžou být aktualizace automaticky řízeny ani ihned nainstalovány. Zprvu musí být naplánována odstávka provozu v řádů dnů nebo týdnů dopředu, aby neafektovala další související procesy. Dalším rozdílem je, že operační technologie jsou komparativně s IT nasazeny v provozu po delší časový úsek a tedy software na nich nasazený už nemusí dostávat podporu ze strany výrobce daného řídícího systému nebo softwaru na něm. Poslední překážkou v aktualizaci softwaru na řídících systémech je samotný proces schválení aktualizace managementem z důvodu odstávky provozu to často není možné a proto na řídících systémech běžící neaktualizovaný software.

2.4 Typy řídících systémů

Různá průmyslová odvětví využívají určitý typ řídících systémů v každodenním provozu. Téměř všechny obdoby kritické infrastruktury a oblasti průmyslové produkce, čističky vod, přepravy a elektrické sítě vyžadují k provozu jeden z typů řídících systému k tomu, aby byly schopny provozu.

Avšak každý z řídících systémů je specifický svými vlastnostmi a využitím, proto je důležité specifikovat pro obeznámení s jejich architekturou případně využitím. Nejběžnější typy řídících systémů budou diskutovány v následujících odstavcích.

2.4.1 Programovatelný logický automat (PLC)

PLC neboli programovatelný logický automat je programovatelný počítač používán k automatizaci různých elektro-mechanických procesů v průmyslové výrobě. Je implementován jako řešení k vznikajícímu problému vysoké spotřeby energie v důsledku využívání elektrický spínačů k ovládání výrobních procesů. PLC se skládá z několika hardwarových komponentů, což jsou:

- Procesor (CPU) – provádí aritmetické a logické operace a periodicky kontroluje, zda se v PLC na úrovni softwaru nevyskytují chyby
- Paměť – systémová ROM (paměť pouze pro čtení) permanentně ukládá data využívána procesorem, kdežto RAM (paměť s náhodným přístupem) ukládá informace ze vstupů a výstupů zařízení, časové hodnoty a další interní měřené hodnoty
- Fyzická kontrola zařízení – sekce, vydávající příkazy fyzickým částem zařízení, mezi něž řadíme pumpy, motory, světla
- Sekce vstupů a výstupů – zaznamenává informace z komponentů jako jsou senzory a přepínače
- Programové zařízení – sloužící k importu programu do paměti procesoru

PLC jsou používány v obou SCADA a DCS systémech jako kontrolní komponenty celkového systému, které poskytují lokální vykonávání procesů. V případě SCADA systému zabezpečují stejnou funkcionalitu jako RTU komponent, naproti tomu, pokud jsou použity v DCS systémech, sloužící pro lokální ovladače. PLC mají programovatelnou paměť, která primárně sloužící k uložení instrukcí pro účel implementaci specifických funkcí jako jsou například kontrola vstupů a výstupů, logické funkce, časovače, počítadla. K PLC paměti se lze standardně dostat pomocí programovatelného rozhraní alokovaného přímo na pracovní stanici, data jsou pak uložena v lokální síti v databázi data historian, tyto dvě části jsou pak spojeny lokální sítí LAN.

2.4.2 Distribuovaný kontrolní systém (DCS)

Distribuovaný kontrolní systém je charakterizován jako průmyslový řídící systém, který je nasazen a řízen distribuovaným způsobem, což znamená, že je řízení dosaženo pomocí příkazů, které jsou distribuovány kolem procesu,

který je řízen individuálně nežli centrálně. DCS systémy jsou integrované jako kontrolní architektura poskytující dohled nad několika integrovanými subsystémy, které jsou odpovědné za kontrolu fungování lokalizovaných procesů ve výrobě. DCS používá centralizovanou kontrolně řídící smyčku pro ovládání množiny lokalizovaných ovladačů, které mají společný úkol vykonávání výrobního procesu. Kontrola produktu a procesu je pomocí DCS zajištěna kontrolní smyčkou, kdy je stav produktu a procesu kontrolován a stabilně udržován v konstantním stavu.

Distribuované kontrolní systémy se skládají ze tří komponentů, které zajišťují funkcionalitu zařízení. Prvním komponentem je kontrolní modul. Kontrolní modul je kontrolní centrum neboli mozek celé části procesní kontroly, tento modul vykonává výpočetní procesy algoritmů a logických výrazů. Funkce kontrolního modulu je práce se vstupní proměnou, která je poté modulem kontrolována, hodnota vstupní proměnné je kalkulována a výsledky této kalkulace budou porovnány s hodnotou uložené standardní proměnné. Tato standardní hodnota je očekávanou hodnotou výstupu procesu, proto jestli se vstupní hodnota liší od standardní hodnoty, musí být vstupní hodnota manipulována a parametry procesu musí být automaticky pozměněny, aby vstupní hodnota byla totožná s hodnotou standardní. Hodnota je odeslána do vstupně výstupního modulu a poté do pohonné jednotky.

Druhým základním komponentem DCS je stanice operátora. Stanice operátora je místo, ze kterého operátor monitoruje proces. Je používána jako rozhraní pro kontrolu a monitoring systému, která probíhá pomocí množiny několika stanicí lidského rozhraní (HIS). His je počítač, který získává data z kontrolní stanice. Stanice operátora sloužící k zobrazení procesních proměnných, kontrolních parametrů a upozornění, které pracovník používá k zobrazení statusu procesu, dalšími využitími jsou zobrazení trendů výrobních dat, zpráv systému a procesních dat.

Posledním základním komponentem DCS je vstupně výstupní modul, což je rozhraní mezi kontrolním modulem a samotným mechanickým komponentem zařízení. Funkce vstupně výstupního modulu zahrnují manipulaci na vstupu a výstupu s daty procesu, převod signálu z digitálního na signál analogový a naopak. Vstupní modul dostane proměnnou z vysílače a poté

ji poskytne kontrolnímu modulu, mezitím co výstupní modul zajišťuje odeslání již upravené proměnné do pohonné jednotky. Každý fyzický instrument komunikující s DCS musí být ve vstupně výstupním modulu zaznamenán, a je přiřazeno unikátní identifikační číslo, aby neproběhla chyba v komunikaci mezi zařízeními.

2.4.3 Dispečerské řízení a sběr dat (SCADA)

Dispečerské řízení a sběr dat neboli SCADA je typ systému pro řízení procesů používající počítače, komunikaci po síti a HMI (rozhraní člověk-stroj) pro kontrolu nad procesy. SCADA systém komunikuje s ostatními přístroji, jako je například již dříve zmíněné PLC, za účelem interakce s přístroji řídícími výrobu.

Tyto systémy sbírají data z procesu, který je analyzován in real-time. Dále zapisuje a provádí analýzu dat. Tato analýza umožnuje individuálním operátorům výroby vidět data, která můžou pocházet přímo z výroby a upravovat výrobu odesláním řídících požadavků do vzdálené lokace pomocí SCADA systému. Systémy mohou být provozovány virtuálně, což právě umožnuje operátorovi řídít celý proces i ze vzdálené lokace, operátor nemusí být přítomen přímo v konkrétní továrně, ale může procesy řídít z velícího střediska z pohodlí kanceláře.

SCADA systémy se skládají z hardwaru i softwaru. Typický hardware SCADA systém obsahuje MTU (master terminal unit), který vytváří komunikaci v řídícím centru. V geografické lokaci se nachází přímá kontrola fungování systému v podobě RTU(vzdálená terminálová jednotka) a PLC, které kontroluje mechanické součásti jako jsou motory zařízení. MTU ukládá a zpracovává data z vstupu a výstupu RTU jednotky, mezitím co RTU a PLC kontrolují lokální procesy ve výrobě. Komunikační komponenty hardwaru umožňují komunikaci mezi RTU, MTU a PLC komponenty. Softwarová složka SCADA systému je naprogramována, aby říkala systému, kde, kdy a co má systém monitorovat, jaké parametry jsou akceptovatelné a jakou zvolit odpověď v případě, že se parametry liší od předpokládaných hodnot. IED (inteligentní elektronické zařízení), například ochrané relé, je schopno přímo komunikovat s MTU nebo s lokálním RTU pro následný sběr a vyhodnocení dat, které jsou poté odeslány do řídící jednotky SCADA systému. Komponenty IED, poskytují přímé rozhraní pro kontrolu a monitoring senzorů a zařízení.

2.4.4 Další řídící systémy

- Vzdálené terminálové jednotky (RTU) – zařízení na bázi mikroprocesoru, používáno v řídících systémech pro propojení hardwaru v distribuovaných řídících systémech nebo SCADA systémech. Jsou také využívány pro telemetrii, RTU přeposílají data ze sensorů řídící smyčky do výstupního proudu tak, aby mohly být data následně odeslány do centralizovaného řízení.
- Programovatelné automatizační ovladače (PAC) – Programovatelný automatizační ovladač představuje jakékoliv zařízení, které disponuje instrukcemi vyšší úrovně.

2.5 Kybernetické hrozby řídících systémů

Jak již bylo zmíněno v předchozích podkapitolách o řídících systémech, jsou využívány především v průmyslových procesech a kritické infrastruktuře, kde se hardware obměňuje jednou za několik desítek let, a právě tento starší hardware na kterém často běží software staršího vydání bez implementace novějších patchů je nejčastějším cílem útoků. Jsou specifické tím, že jsou to v podstatě starší techniky, jak proniknout nebo se zmocnit kontroly nad systémem jež byly využívány v IT sféře, ale kde jsou již neúčinné. V posledních letech jsou na vzestupu útoky specificky zaměřené na řídící systémy, primárně na SCADA a DCS. Malware vyvinutý čistě pro řídící systémy se poprvé objevil zhruba před deseti lety. útoky cílené čistě na ICS se čím dál více zaměřují na bezpečnostní komponent řídících systémů. Jakákoliv organizace věnující se správě a provozu kritické infrastruktury by měla mít tyto hrozby a jak jim předejít na paměti již při plánování a implementaci architektury ICS.

Kvůli vzrůstající frekvenci útoků a nově objevených slabin systému je nutno tyto potencionální hrozby v co nejkratším čase adekvátně adresovat, proto je vhodné využít analýzy rizik potencionálních hrozeb, o které bude práce pojednávat v pozdějším paragrafu. Toto se vztahuje především na infrastrukturu přímo napojenou na síť a na části, které můžou být kyberútoky přímo ovlivněny. Útoky jsou také směřovány na služby a zařízení provozující správu ICS protokolů. V IT jsou využívány protokoly, jež jsou standardizovány v TCP/IT. Naproti tomu

ICS využívají celou řadu protokolů specifických lokací, funkcí. Zároveň i druhem průmyslu, už jen tato specificita způsobuje problémy se samotným zabezpečením, navíc v mnoha řídících systémech jsou zanedbávána bezpečnostní opatření z různých důvodů, jimiž jsou například nedostatek budgetu pro zabezpečení, adekvátní pracovníky rozumějící zabezpečení operační technologie a jiné. Nejčastějšími hrozbami ve ICS sféře jsou následující:

Nákaza malwarem přes intranet a internet – V úzkém spojení s lidským faktorem se malware dostane do sítě díky chybě člověka, což je ale jen jedním z vektorů proniknutí malwaru. Dalším takovým případem je nesprávná konfigurace a práce se síťovými komponenty – konkrétně servery a databázemi. Právě tyto de facto slabiny v systému jsou hojně využívány pro nasazení malwaru, což umožní útočníkovi přístup k jinak nepřístupným datům. Díky čím dál většímu propojení IT a ICS prostředí útočníkovi proniknout do IT sítě, která je integrována s ICS sítí, a tudíž pronikne z jednoho prostředí do druhého. Dalšími vektoru útoku se stávají takzvané zero day exploits – útok pomocí slabiny v systému, která byla právě objevena a na kterou ještě není bezpečnostní patch nebo také drive-by download kdy stačí na webovou stránku vstoupit a ta okamžitě zahájí skryté stahování malwaru do systému klienta, bez toho, aniž by to tušil. Mez vektory útoku, který u této hrozby stojí za zmínku řadíme také SQL injekci, worms a cross-site scripting. Tuto hrozbu lze minimalizovat strategií patchování operačních systémů a aplikací působících na front i backendu IT sítě, jestliže je ICS síť jakýmkoliv způsobem propojená s IT sítí nebo snad s internetem, jsou nutná nasazení stejných zabezpečení, a navíc je zde přidán aspekt monitorování logovaných souborů nestandardní aktivity v síti a v neposlední řadě Hardening (odinstalování všech nepotřebných aplikací, procesů a služeb) fyzických a virtuálních stanic v ICS síti.

Lidský faktor – Lidé jako jsou zaměstnanci, externí pracovníci jako oprava nebo stavební dělníci bývají potencionální hrozbou pro kybernetickou bezpečnost v ICS prostředí, hrozbou v tomto směru je špatně nakonfigurovaný, nainstalovaný software nebo hardware. Zaměstnanci mohou nevědomky nainstalovat malware kliknutím na odkaz v emailu, stáhnutím hry, filmu, souboru na pracovní počítač, pomocí flash disku nebo dokonce i pomocí skrytého flash disku, který se jeví jako napájecí kabel nebo klávesnice. Tým spravující IT a ICS

prostředí se také potýká s novou překážkou v podobě takzvaných firewallů nové generace, které musí být pravidelně nastaveny a aktualizovány. Změna, nesprávná konfigurace nebo neověřená instalace aktualizace může vést k celé řadě problémů s funkcionalitou nebo dokonce i ke kritickým problémům jako jsou například login bez nutnosti autorizace a autentifikace. Je zřejmé, že nestačí pouze adekvátně nastavit systémy zabezpečení, ale je potřeba zavést pravidla pro práci s řídícími systémy v organizaci a také proškolit personál o kyberbezpečnosti, používání a zabezpečení těchto systémů. Dále je důležité nastavit adekvátní firemní strategii, jak postupovat v kybernetickém zabezpečení řídících systémů a kritických procesů obecně, není nasnadě tyto kroky podcenit. Často probíhá kontraktování externích expertů z důvodu školení zaměstnanců a auditu kybernetické bezpečnosti v organizaci.

DDOS útok a IoT zařízení – Organizace stále více implementují do svého IT a ICS prostředí IoT technologie, které jak již název napovídá, jsou připojeny do sítě, ať už to je GPS, RFID a různé druhy senzorů. Tyto zařízení používají mnoho komunikačních protokolů a každý z nich vyžaduje individuální přístup k zabezpečení čemuž navíc nenapomáhá to, že zařízení nejsou často adekvátně zabezpečena a v jejich kódu se vyskytuje celá řada bezpečnostních slabin jako jsou například backdoory, správa hesel uložena přímo ve firmwaru, nemožnost instalace aktualizací a další. Známou praktiku, jak zamezit předávání, měření dat je zahltit komponent obrovským množstvím dotazů (queries), což způsobí nemožnost poslat odpověď v přijatelném časovém horizontu. Tento útok nazýváme DDoS útokem. V současné době se využívávají IoT zařízení čím dál více a s novou generací sofistikovanějších DDoS útoků, na operační technologii jako celek, ale i na řídící systémy a jejich komponenty. Je klíčové těmto potencionálním hrozbám předcházet. Zdánlivým řešením této situace je korektní konfigurace pravidel firewallu, nastavení přístupu v cílových zařízeních a také CDN (content delivery network), což je síť vzájemně propojených počítačů, která umožnuje rozložit dotazy do více serverů a tímto zmírňuje dopad DDoS útoku.

Nákaza malwarem pomocí externího hardwaru je používáním rozšiřitelných uložišť, jako jsou například USB flash disky, je stále prevalenčním trendem v kancelářském prostředí. Pro správu řídících systémů v místě, kde se nachází jsou využívány notebooky pro přenos externích dat a instalaci

aktualizací. V ICS bezpečnosti je nejdůležitější zabezpečit dostupnost spojení a fyzické zabezpečení zařízení, a z toho důvodu je důležité školit zaměstnance o dopadech malwaru a technikách jakými se malware do řídících systémů dostává. Potencionální hrozby mohou být spustitelné programy a aplikace obsahující škodlivý kód, což může spět k úniku dat a infikování zařízení malwarem. Při připojení do firemní sítě může dojít k tomu, že infikovaný notebook nebo flash disk rozšíří malware do ostatních zařízení a síťových komponentů ICS prostředí. Proti této hrozbě nestačí již dříve zmíněné firemní strategie ani zavádění antivirové programy, které jsou schopny detekovat škodlivý malware a školení zaměstnanců o správném zacházení a hrozbách využívání externího hardwaru, ale je nutno používat nástroje pro správu přístupů a nastavení adekvátních práv konkrétním uživatelům.

Spoofing – IP spoofing je používáno k získání neautorizovaného přístupu k počítači, serveru nebo zařízení používajícím IP protokol. Probíhá tak, že útočník pošle paket do cíle útoku s pozměněnou cílovou adresou indikující, že paket pochází z ověřeného systému nebo portu, avšak útok není z pohledu útočníka zcela jednoduchou záležitostí a útočník musí splnit několik kroků, aby měl útok vůbec šanci na úspěch. Průběh útoku je následující. V prvé řadě si musí útočník určit konkrétní cíl v podobě počítače nebo serveru. Poté je nutno získat IP adresu daného zařízení a současně musí dosáhnout odpojení počítače od internetu. Následujícím krokem je vypozorovat průběh komunikace v síti, a to modifikovat hlavičku paketu podle vypozorované komunikace v síti. V posledním kroku zkusí navázat komunikaci s cílovým zařízením a paket mu odeslat. V případě, že je celá operace úspěšná a pakety dorazí do cílového zařízení, vytvoří útočník pomocí dat odeslaných paketů zadní vrátka pro pozdější přístup do počítače nebo serveru. V případě, že se jedná o ARP (Address Resolution Protcol) spoofing, postup odlišný. ARP slouží jako protokol, který mapuje IP adresu na hardwarovou adresu, v tabulce, které se standardně říká ARP cache jsou zaznamenány a přidávány přiřazené IP adresy k hardwarovým adresám. Protokol poskytuje pravidla pro párování těchto adres s koncovými zařízeními. Proces přiřazení probíhá následovně. V prvé řadě příchozí paket ze zařízení dorazí do směrovače, který odešle dotaz na ARP program, pro nalezení MAC adresy. Program se podívá do ARP cache, zdali je zařízení

již uvedeno v tabulce, jestliže ano, odešle odpověď do směrovače a ten zařízení přidělí již platnou adresu. Ovšem může nastat právě taková situace, že se útočník dostane k datům ARP cache, které pozmění ve svůj prospěch tak, že změní MAC adresu zařízení za adresu zařízení útočníka, tím pádem, když se bude chtít připojit do sítě, ARP mylně útočníkovo zařízení uvede jako již registrované v síti a tím také získá přístup do celé sítě.

Ransomware – dělící se do dvou kategorií, kdy první kategorií ransomware je šifrovací ransomware kombinující šifrovací algoritmy mající za cíl zablokovat přístup k souborům a následně za odemknutí požadují vyplatit částku. Druhým typem ransomwaru je zamykací ransomware. Ten způsobuje změnu hesla celého operačního systému, kdy uživatel není schopen se vůbec do systému přihlásit, příkladem takového ransomwaru je winlocker, který jak již název napovídá změní heslo u operačních systémů windows a tedy zamezí uživateli přístup. Nejčastějším případem je případ infekce ransomwarem přes email, kdy útočník navrhne email, který vypadá jako email od blízké osoby nebo ověřené instituce a do přílohy připojí soubor v zdánlivě neškodném formátu. Osoba, která email přijme a otevře danou přílohu nevědomky na pozadí spustí program, který zapříčiní již zmíněnou zašifrování dat nebo dokonce změnu hesla celého systému.

Phishing – patří mezi jeden z nejstarších druhů kybernetických útoků a jež je stále populární vzhledem ke svému poměrně nenáročnému provedení a vysokou účinností. Tento pojem referuje o procesu, kdy je cílový uživatel kontaktován prostřednictvím emailu nebo telefonu útočníkem, který se vydává za legitimní instituci za účelem získání osobních dat, nejčastěji to jsou bankovní údaje, čísla na kreditní kartě, hesla. Obvykle jsou informace získány pod nátlakem ze strany útočníka, který prezentuje cíli informace například, že se účet bude uzavírat nebo potřebuje k vyplnění formuláře doplňující informace.

2.6 Kybernetické zabezpečení řídícího systému

Kybernetická bezpečnost je definována jako: „*Souhrn technologií, procesů a praktiky, jejichž cílem je ochrana sítí, počítačů, programů a dat před útoky,*

zničením nebo neautorizovaným přístupem. Jde o součást informační bezpečnosti.“ (Svatá, 2016, s. 49).

Zabezpečení ICS systémů je komplexní sbírkou procesů a praktik, které jsou implementovány k prevenci, minimalizaci a odrazení potencionálních hrozeb a slabých míst řídících systémů. Tyto kybernetické zabezpečení jsou specifická a v některých aspektech se lišící se oproti typickému zabezpečení IT systémů, avšak IT a ICS systémy jsou v organizaci nedělně propojeny a je potřeba koordinace obou týmů a implementaci zabezpečení s ohledem na oba tyto prvky organizace. Rozdíl v kybernetické bezpečnosti oproti informační bezpečnosti vyplývá z normy ISO 27032, když uvádí, *že bezpečnost informací se zabývá ochranou důvěrnosti, integrity a dostupnosti informací všeobecně tak, aby sloužila potřebám uživatelů příslušných informací* (ISO 27032, 2013, s. 18), zatímco kybernetická bezpečnost je *zachování důvěrnosti, integrity a dostupnosti informace v kybernetickém prostoru* (ISO 27032, 2013, s. 12).

Následující podkapitoly budou na kybernetické zabezpečení řídících systémů pohlížet z různých vektorů, jimiž jsou:

- Architektura kybernetického zabezpečení,
- Segmentace a segregace sítě,
- Firewally,
- Autentifikace a autorizace,
- Zabezpečení hranic systému

2.6.1 Architektura kybernetického zabezpečení

Jediný nástroj, technologie nebo řešení nemůže adekvátně ochránit ICS, je nutno být seznámen s konceptem Hloubkové obrany (Defense-in-Depth), což je strategie zahrnující dvě a více vrstev překrývajících se mechanismů nebo technik ochrany. Tím, že se vrstvy překrývají v okruzích působnosti ochrany, minimalizují možnost selhání ochrany systému v jednom bodě. Strategie hloubkové obrany zahrnuje použití firewallů, vytvoření demilitarizovaných zón, mechanismy detekce vniknutí do systému, využívání optimální bezpečnostní politiky, tréninkových programů, ale také například krizových plánů a fyzického zabezpečení hardwaru. Od pracovníků, kteří se o tuto sekci zabezpečení starají

je očekávána znalost systému, jeho potencionálních vektorů útoku a slabých míst, které by mohly být útočníkem využity proti ICS systému.

2.6.2 Segmentace a segregace sítě

Je potřeba rozdělit ICS na bezpečnostní domény a oddělit řídící systémy od dalších sítí, jako je kupříkladu korporátní síť. K odhalení kritických částí ICS systémů lze využít analýzu operačního rizika a pomocí nabytých poznatků je příhodné definovat ty části ICS systému, které by měly být segmentovány. Segmentace sítě v podstatě znamená rozdělení sítě do několika menších celků, koncept segmentace a segregace sítě se řadí mezi jeden z nejefektivnějších procesů, které může organizace implementovat k zabezpečení ICS. Segmentace rozčlení sítě do kategorií, které se řídí stejnými bezpečnostními principy, jsou spravovány totožnou skupinou pracovníků a typicky nabývají stejné úrovně zabezpečení. Segmentace také minimalizuje způsob a stupeň přístupu k citlivým informacím, ICS komunikaci a konfiguraci hardwaru a značně omezit vektory využitelné útočníkem, ale také zmírní dopady chyb a nehod, které neochromí zbylé segmenty sítě. Cílem segmentace a segregace sítě je tedy minimalizovat přístup k citlivým informacím pro neautorizované osoby a systémy a zároveň ujištění, že organizace může pokračovat v činnosti bez narušení. Tohoto je běžně docíleno implementací vhodné technologie nebo použití techniky, výběr optimální technologie nebo techniky je realizován na základě architektury a konfigurace sítě.

Tradičně je segmentace a segregace sítě implementována v bráně mezi doménami. Prostředí ICS mají běžně definované domény jako jsou provozní LAN, kontrolní LAN, provozní DMZ, a navíc také brány do domén, které se neřadí do ICS anebo nemají stejnou úroveň zabezpečení což jsou například internet a korporátní LAN. Segregace sítě vyžaduje vytvoření a používání souboru pravidel pro kontrolu jaká komunikace je povolena přes bránu do jiného segmentu. Tyto pravidla jsou obvykle založena na povaze komunikujících segmentů, ale také na datech, která jsou mezi nimi přenášena.

Nehledě na výběru technologie použité k implementaci segmentace a oddělení sítí, z pravidla se vyskytují čtyři koncepty implementace hloubkové obrany pro dobrou síťovou segmentaci a separaci, jimiž jsou:

Použití technologií ve více vrstvách, nejen v síťové vrstvě, načež by měl být systém oddělen v každé vrstvě, pokud je to tedy možné, to znamená od linkové vrstvy až po vrstvu aplikační, uvažujeme-li v prostoru OSI modelu.

Implementace principu nejmenšího možného přístupu uživatelům a dalším systémům. Jestliže systém nenavazuje komunikaci s dalším systémem, není důvod pro to, aby byly systémy navzájem propojeny a je žádoucí, aby byly segmentovány. V případě, že systém si potřebuje předávat data s dalším systémem, není žádoucí, aby tak dělal přes libovolné porty a neoptimálně zvolené protokoly, a proto je vždy lepší, když mají dva a více systémů nastavená určitá pravidla interakce na kterých portech a jakými protokoly mohou komunikovat. V neposlední řadě by také měly být ošetřen formát dat jakými spolu komunikují, aby se zamezilo neoptimálnímu využití sítě a omezil možný prostor pro nežádoucí zásah útočníka.

Informace a infrastruktura by měla být rozděleny na základě nutnosti ochrany dat, se kterými pracuje. Toto opatření může zahrnovat použití jiných hardwarových komponentů nebo nasazovaných platforem pro každou segmentovanou síť. Čím kritičtější část infrastruktury, tím je více žádoucí, aby tyto části měly být striktněji izolovány od ostatních částí kritické infrastruktury. V případě, že není možno využít segmentace nasazením softwaru na jiném hardwaru a následnou segmentaci, lze pracovat s možností odlišné části systému virtualizovat pro dosažení potřebné izolace jednotlivých částí.

Posledním bodem je implementace takzvaného whitelistu, namísto blacklistu. Whitelist je seznam povolených programů a uživatelů, kteří mohou do konkrétní segmentované sítě přistupovat, naopak blacklist je jakýmsi protikladem, kdy jsou pouze zaznamenány programy a uživatelé, kteří by přístup mít neměli. Lze vidět, že takzvaný whitelisting je pracnější na implementaci, ale nesmírnou výhodou je, že pouze autorizovaní uživatelé a programy mohou přistupovat do sítě.

2.6.3 Firewally

Síťové firewally jsou nástroje nebo systémy pro kontrolu toku síťového provozu, mezi jednotlivými sítěmi používající různé pravidla a omezení pro zabezpečení tohoto procesu. Ve většině moderních aplikací jsou firewally

používány v kontextu internetového spojení a UDP/IP souboru protokolů, ale v případě ICS se využívají firewally i v prostředí, které není propojeno s internetem. Například, mnoho korporátních sítí využívá firewally pro omezení spojení v rámci interní sítě pro přístup aplikacím a databázím pracujícími s citlivými daty. Firewally mohou dále omezit komunikaci mezi jednotlivými sítěmi v rámci ICS a fyzickými zařízeními, nasazením firewallů do těchto oblastí může organizace dosáhnout vyššího stupně zabezpečení omezením přístupu neautorizovaným subjektům a systémům. Firewally můžeme obecně rozdělit do tří kategorií jimiž jsou:

Firewally filtrující pakety jsou nejběžnější a nejzákladnějším typem firewallů, jež jsou také nazývány paket filtrem. Jak již název napovídá, jedná se o směrovací zařízení, která obsahují funkcionalitu řízení paketů v rámci systémů a probíhající relací. Přístup je kontrolován pravidly a omezeními, tyto firewally operují v třetí vrstvě OSI modelu, což je sítová vrstva. Tento typ firewallu kontroluje základní informace příjmového paketu, jako je IP adresa a porovnává je s pravidly, jestliže paket projde kontrolou, je dále odeslán do vyšší síťové vrstvy. Vzhledem k posouzení paketu s pravidly firewallu, může nastat jedna z následujících situací: paket může být zahozen, poslán dále, vrácen zpět odesilateli. Firewall filtrující pakety poskytuje vysoký stupeň zabezpečení, ale může zapříčinit zpomalení množství dat, která protečou v síti za určitý časový úsek.

Firewall inspekce stavu, je firewall, pomocí kterého probíhá filtrace paketů na čtvrté úrovni OSI modelu, v transportační vrstvě. Firewall inspekce stavu filtruje pakety v síťové vrstvě, rozhodne, zdali jsou pakety relace legitimní a poté přejde na evaluaci složky paketu transportní vrstvy. Inspekce stavu paketu sleduje aktivní relace a tuto informaci používá k rozhodování, zdali by měl paket být odeslán do další vrstvy nebo blokován. Tento druh firewallu rovněž poskytuje vysokou úroveň zabezpečení, jestliže je korektně implementován, a navíc nezapříčiňuje zpomalení toku dat v čase, avšak oproti firewallu filtrujícím pakety je náročnější na správu a komplexnější na implementaci pravidel firewallu.

Aplikační proxy firewally, tato množina firewallů se zabývá evaluací paketů v aplikační vrstvě a filtruje provoz na základě stanovených aplikačních pravidel jako jsou využívání pouze specifikovaných aplikací a protokolů. Firewally

tohoto typu jsou velmi efektivní v ochraně před útoky na vzdálený přístup a konfigurační služby ICS zařízení.

V rámci ICS prostředí jsou nejčastěji nasazeny firewally mezi ICS sítí a korporátní sítí, v případě správně konfigurace mohou značně omezit nechtěný vstup do sítě, výstupem je zlepšení kybernetické bezpečnosti systému, potencionálně také mohou vylepšit tok dat v síti odstraněním nepotřebných částí dat v komunikaci mezi sítěmi. Existuje taky hardware přímo určený k implementaci firewallů, který může výraznou mírou pomoci v zabezpečení ICS prostředí, pokud je tedy optimálně nasazen, navrhnut a spravován, jestliže ne, stává se pouze dalším potencionálním vektorem, který může útočník využít pro proniknutí do sítě nebo získání citlivých dat. Firewally poskytují celou řadu nástrojů pro vynucení dodržování nastavených pravidel, disponují těmito schopnosti a to konkrétně:

Schopnost blokovat veškerou komunikaci s výjimkou speciálně povolené komunikace mezi přístroji mezi nechráněnou LAN sítí a chráněnou ICS sítí. Blokování může být uplatněno na základě zdrojové a konečné IP adresy, druhu služby, portů nebo také druhů užitých protokolů. Blokování se také může vyskytnout v obou směrech komunikace, to znamená ať už na příchozích nebo na odchozích paketech, je možné tuto techniku kombinovat což je přínosné ve zmírnění rizika ve vysoko rizikových případech jakou jsou například odesílání a přijímání emailů.

Zajištění bezpečné autentifikace všech uživatelů, kteří jsou v interakci s ICS sítí. Zde se naskýtá implementace různých stupňů ochrany autentifikace což mohou být, jednoduchá hesla, komplexní hesla s pravidly, vícefaktorové ověření, využití tokenů k autentifikaci, biometrické údaje uživatele a takzvané chytré karty (smart cards).

Zajištění autorizace na základě geolokace. Uživatelé mohou být omezeni a povoleni se přihlásit v uzlech sítě jen v konkrétní pracovní geolokaci. Toto opatření zamezí nedovolenému přihlášení z jiné lokace útočníkem, který se vydává za zaměstnance s povolením vstupu do sítě.

Užití pravidel nastavení firewallu pro specifické služby umožňuje kromě obecného nastavení firewallu pro systémy i konfigurovat jednotlivé protokoly.

Jelikož není nejvhodnější užívat pouze obecné nastavení a pravidla pro efektivní zabezpečení řídících systémů pomocí firewallu, rozhodl se autor práce popsat jednotlivá doporučená nastavení v přístupu k jednotlivým protokolům.

2.6.3.1 Systém doménových jmen

Systém doménových jmen, dále jen DNS, nachází primární využití v překladu doménových jmen a IP adres. Většina internetových služeb závisí a často využívá DNS, ale jeho využití v kontrolní síti je poměrně vzácné, ve většině případů není důvod povolit DNS požadavky ze sítě organizace do kontrolní sítě a žádný důvod pro DNS požadavky z kontrolní sítě do DMZ, proto by tyto ojedinělé případy měly být posuzovány individuálně a měl by být dobrý důvod k jejich povolení, avšak lokální DNS je doporučeno využívat.

2.6.3.2 Hypertext Transfer Protokol

Hypertextový transport protokol, dále jen HTTP, je protokol určený pro komunikaci s webovými servery. Podobně jako DNS je tento protokol naprosto klíčový ve fungování internetových služeb. Naneštěstí má tento protokol nedostatky v zabezpečení a mnoho aplikací používajících HTTP protokol má slabiny, které jsou dobře zmapované a tím pádem jsou často využívány jako jeden z vektorů útoku. Díky vysokému riziku hrozeb není doporučeno, aby byl protokol použit v kontrolní síti nebo v komunikaci mezi sítí organizace a kontrolní sítí.

2.6.3.3 File Transfer Protokol

File transfer Protokol, dále jen FTP a triviální verze tohoto protokolu nazývaná TFTP jsou používány pro transfer souborů mezi individuálními zařízeními. Tyto dva protokoly jsou využívány na téměř všech platformách zahrnujících SCADA systémy, DCS, PLC z důvodu využívání minimálního procesního výkonu. Jednou z nevýhod užití těchto dvou protokolů je, že při vytváření těchto protokolů byla bezpečnost uvažována až na posledním místě. V FTP není přihlášení a heslo nijak šifrováno, některé z implementací tohoto protokolu trpí slabinou potencionálního buffer overflow, a pro TFTP platí, že dokonce ani žádné přihlášení nevyžaduje. Z těchto důvodů je žádoucí, zablokovat jakoukoliv TFTP komunikaci, zatímco FTP může být povoleno jen za podmínek využití jiné úrovně autentifikace a autorizace a komunikace přes

šifrovaný tunel. Alternativním řešením je využití SFTP protokolu, kde **S** znamená zabezpečený.

2.6.3.4 Telnet

Telnet protokol vytvářející interaktivní, textovou komunikaci mezi klientem a hostem, primárním využitím telnetu je vzdálený login a kontrola služeb v systémech s limitovanou výpočetní kapacitou nebo v systémech s omezenou potřebou zabezpečení. Užití tohoto protokolu bychom se měli zcela vyhnout z důvodu, že veškerá komunikace v telnetu je nešifrovaná, a navíc poskytuje připojenému aktérovi kontrolu nad systémem, k němuž je připojen. Pro vzdálenou správu systému je doporučováno použití Secure Shell Protokolu (SSH). Stejně jako u FTP protokolu, jestliže má být použit v měl by obsahovat stejné bezpečnostní opatření, které jsou využití jiného autentifikačního a autorizačního programu a komunikace probíhající pouze přes šifrovaný tunel.

2.6.3.5 Dynamic Host Configuration Protokol

Dynamic Host Configuration Protokol, zkratkou DHCP, je používán v internetových sítích k dynamické distribuci konfiguračních parametrů jako jsou IP adresy pro zařízení a služby. Základní DHCP neobsahuje žádnou možnost autentifikace serverů a klientu, což je velkou slabinou protokolu, útočník může realizovat útok pomocí falešného DHCP serveru poskytujícího klamavé konfigurační parametry připojovaným zařízením a službám. Neautorizovaní klienti mohou získat přístup k serveru a zapříčinit nedostatek automaticky přidělovaných IP adres. Naštěstí tomuto problému se lze vyhnout využitím statické konfigurace namísto dynamické alokace adres, statická konfigurace by měla být standardní konfigurací u ICS zařízení. Pokud je skutečně nutno využít dynamické alokace konfiguračních parametrů, doporučuje se implementace nástroje pro identifikaci a autentifikaci DHCP serverů, DHCP servery by měly být umístěny ve stejném segmentu sítě ve kterém se nacházejí konfigurovaná zařízení.

2.6.3.6 SCADA a průmyslové protokoly

SCADA a průmyslové protokoly jako jsou Modbus/TCP, EtherNet/IP, IEC 61850, jsou kritické pro komunikaci s většinou řídících systémů, tyto protokoly byly opět navrhnuty s primární myšlenkou funkcionality, načež na zabezpečení byl při návrhu protokolů brán minimální ohled. Nepožadují žádnou autorizaci

a autentifikaci při interakci se systémem a zadáváním příkazů, proto by tyto protokoly měly být nasazeny pouze v interní kontrolní síti.

2.6.4 Zabezpečení hranic systému

Zařízení na ochranu hranic systému kontrolují tok informací mezi propojenými bezpečnostními doménami, aby chránily ICS proti kybernetickým útokům a zároveň poskytovaly ochranu proti chybovým stavům a incidentům. Přenos dat mezi systémy, které disponují různými úrovněmi zabezpečení s jinými bezpečnostními politikami prezentuje nebezpečí, že data při transferu poruší některá nastavená bezpečnostní pravidla. Nástroje pro ochranu hranic jednotlivých systémů jsou komponenty řešící tento problém. Organizace mohou izolovat komponenty ICS a podnikových systémů jež se soustředí na vykonávání různých procesů. Tyto izolace jednotlivých systémů limitují neautorizovaný tok dat mezi systémovými komponenty a zároveň umožňuje vyšší míru ochrany individuálních systémových komponent.

Zabezpečení hranic systému zahrnuje brány, směrovače, firewally, síťovou analýzu kódu a virtualizačních systémů, systémy detekce narušení systému, šifrované tunely a emailové brány. Zařízení pro zabezpečení hranic systému určují, jaký tok dat je povolen tím způsobem, že analyzují přenášená data a s nimi asociovaná metadata.

Architekti sítě a ICS zabezpečení se musí rozhodnout, které domény budou mít mezi sebou povolenou přímou komunikaci, pravidla komunikace, vybrat zařízení, která budou použity pro dohled nad určenými pravidly komunikace a v neposlední řadě na topologii sítě, která bude podporovat nasazení těchto pravidel. Zařízení zabezpečující ochranu hranic individuálních systémů jsou zapojena v souladu s nastavenými pravidly bezpečnostní politiky organizace. Často uplatňovaný koncept demilitarizované zóny, dále jen DMZ, je segment sítě vložen mezi bezpečnostní domény, působící jako jakási neutrální zóna, jejímž účelem je poskytnutí ochrany ICS domény před externími hrozbami a zároveň umožňuje vynucení dodržování bezpečnostní politiky organizace týkající se toku dat mezi jednotlivými systémy. Dalšími funkcemi zabezpečení hranic systému jsou následující:

Zamezení jakémukoliv průběhu transferu dat a pouze povolení navázání komunikace na základě výjimky zapsané v takzvaném whitelistu, což je seznam uživatelů a systému, kteří mají povolení navázat komunikaci se systémem, toto zabezpečení zajišťuje to, že pouze systémy a osoby zaznamenané na whitelistu jsou autorizovány navázat komunikaci a vyměňovat data s daným zařízením nebo systémem.

Implementace proxy serverů, které slouží jako prostřední člen mezi komunikaci externích domén se zabezpečovaným systémem. Komunikací je myšleno požadování a přijímání služeb, souborů a navázání spojení z a do ICS domény. Externí požadavky navázány pomocí připojení k proxy serveru jsou evaluovány na straně proxy serveru, a ne přímo v ICS, tímto je umožněna vyšší míra zabezpečení.

Zamezení neautorizované inserce informací. Techniky použity pro tento způsob zabezpečení jsou například inspekce paketů firewallem a XML brány. Tyto zařízení verifikují, že formát a specifikace protokolů v aplikační vrstvě odpovídá zvoleným standardům a slouží k identifikací slabých míst, které nemohou být detekovány pomocí procesů operujících na síťové a transportní vrstvě. Limitují počet povolených formátů, obzvláště blokování užití free textu v emailové komunikaci ulehčuje použití těchto technik při zabezpečení hranic ICS.

2.7 Postup aplikace bezpečnostních opatření v rámci řídících systémů

Jediný bezpečnostní produkt nebo technologie nemůže adekvátně ochránit ICS, implementace zabezpečení řídících systémů je kombinací efektivně selektovaných bezpečnostních pravidel a optimálního nastavení bezpečnostních procedur. Výběr a implementace bezpečnostních kontrol v rámci prostředí ICS má velké dopady na bezchybné fungování procesů, proto je nutno zamyslet se nad tím, které bezpečnostní prvky je nutno implementovat, aby byl adekvátně sníženo případné riziko a zároveň nebyl afektován chod procesů, systémů a celé organizace. Nabízí se další otázka, zdali jsou vybrané bezpečnostní postupy již implementovány a pokud ne, jestli je realistická možnost implementace vybraných opatření, popřípadě s jakou jistotou by opatření byly korektně implementovány a nastaveny, tak aby dosáhly požadované úrovně zabezpečení.

Následující paragrafy podkapitoly postupu popisují doporučený postup aplikace bezpečnostních opatření v ICS prostředí, avšak není nutno se systematicky řídit pořadím daných kroků, je pouze klíčové implementovat množinu všech možných dále zmíněných postupů na zabezpečované řídící systémy.

2.7.1 Kategorizace informačního systému

První aktivitou je kategorizace informací a informačního systému z pohledu scénáře dopadu při potencionální ztrátě dat. Pro každou informaci a informační systém pohlížíme na bezpečnostní aspekty, což jsou důvěrnost, integrita, dostupnost a zkoumaným faktorem je, případný dopad na systém zabezpečení při situaci, kdy jeden z těchto aspektů chybí.

2.7.2 Výběr bezpečnostních procesů a pravidel

Tento krok obsahuje prvotní výběr minimálních bezpečnostních požadavků vzhledem k ICS. Úvodní bezpečnostní požadavky jsou počáteční událostí procesu výběru množiny bezpečnostních kontrol systému, jsou vybírány na základě výstupu prvního kroku obsahujícím výčet bezpečnostních kategorií a dopad na informace a informační systémy determinované v prvním kroku. Pro potřebu specializovaných nástrojů napomáhajících zabezpečení informačních systémů a organizací slouží koncept s anglickým názvem overlays – volně přeloženo jako překryvy nebo překrytí, dále se bude o konceptu zmiňovat jako o overlay. Overlay je specifikovanou množinou bezpečnostních procesů a aplikací, vylepšení kontroly a pomocných pravidel. V obecné rovině overlay slouží jako nástroj pro zjednodušení specifického návrhu minimálních požadavků pomocí selekce množiny bezpečnostních procesů a aplikací, které odpovídají obecným okolnostem potřeb zabezpečení v organizaci. Ovšem není to tak, že organizace dále nepotřebují dále specifikovat podmínky zabezpečení, ale je nutno na základě jedinečnosti systému podmínky, procesy a pravidla doplnit o již zmíněné procesy a pravidla nacházející se ve zvoleném Overlayi.

Speciálně v ICS prostředí se Overlay dělí do tří kategorií, dle dopadu na zabezpečení, jimiž jsou: nízký, střední a velký dopad incidentů na ICS. Selekcí jedné z kategorií Overlaye jsou poskytnuty základní specifikace, požadavky a doporučení, které mohou být implementovány příslušným

personálem provádějícím aplikace bezpečnostních opatření. Jak již bylo jednou zmíněno v předchozím odstavci, použití Overlaye neposkytuje kompletní návod pro řešení zabezpečení všech systémů, avšak nutno na základě jedinečnosti systému podmínky, procesy a pravidla doplnit o již zmíněné procesy a pravidla.

2.7.3 Implementace bezpečnostních procesů a pravidel

Tento krok zahrnuje implementaci bezpečnostních procesů a pravidel v ICS a informačních systémech. Tento proces může být v rámci ICS aplikován dvěma způsoby, prvním způsobem je nový vývoj anebo aplikace na již existující systém.

V případě systému nového vývoje je proces výběru aplikován z pohledu požadavků na zabezpečení systému, je to dáno tím, že systém ještě neexistuje, a proto se vývoj systému může přizpůsobit bezpečnostním požadavkům. Bezpečnostní procesy a pravidla zahrnuty v bezpečnostním plánu sloužící jako specifikace bezpečnostních požadavků a jsou zahrnuty do systému v průběhu vývojové a implementační fáze životního cyklu projektu.

Naopak u zpětné implementace, do již existujícího systému je aplikace bezpečnostních procesů a pravidel aplikována v době, kdy je systém vyřazen z provozu z důvodu opravy nebo přidání funkcionalit. Z důvodu předcházející existence systému, budou již organizace mít vypracován průzkum kategorizace bezpečností a výběr bezpečnostních procesů a pravidel pro diskutovaný systém.

2.7.4 Posouzení bezpečnostních procesů a pravidel

Tento bod návrhu bezpečnosti nahlíží na míru efektivity aplikovaných bezpečnostních procesů a pravidel. Hodnotí, zdali jsou aplikovaná bezpečnostní opatření efektivní v minimalizaci slabých míst zabezpečení, nahlíží na jednotlivé procesy a pravidle bezpečnosti a každé z pravidel je evaluováno separátně. Poté je na systém nahlíženo na systém jako celek a hodnoceno splnění minimálních požadavků na zabezpečení systému. Jestliže některý komponent zabezpečení nebo i celý systém je vyhodnocen jako neefektivní v potírání hrozeb a slabých míst, je nutno přijmout dodatečná opatření v rámci neefektivní části.

2.7.5 Autorizace informačního systému

V sekci autorizace informačního systému je výčet opatření, procesů a pravidel bezpečnosti předložen managementu, jestli nejsou ze strany managementu organizace žádné požadavky na změnu nebo vylepšení těchto bezpečnostních praktik

2.7.6 Monitoring bezpečnostních opatření

V posledním kroku návrhu probíhá neustálý monitoring a vyhodnocování aktivit systému, dále je sledováno chování bezpečnostních opatření při změně nebo aktualizaci části systému. V případě abnormálního chování bezpečnostních procesů po změně nebo aktualizaci je nutno všechny body postupu aplikace bezpečnosti na systém zopakovat.

2.8 Definice Auditu

Audit může být charakterizován jako nezávislá inspekce situace firmy, organizace nebo jednotlivce. Avšak definice mohou být různé, například Svatá (2012, s. 16) *tvrdí, že audit je objektivní ověření stavu, jevu, záměru, skutečnost se stavem nebo jevem žádoucím, tj. modelem, normou, standardem apod.* Audit je prováděn osobou specializující se na vykonávání auditu, jmenovitě auditorem, jehož cílem je auditorská zpráva o průběhu a výsledcích auditu. Další definicí auditu lze uvést jak (Slámečka, 2012) *uvádí, že hlavní vlastností auditu je kritický pohled na systém, objektivní získávání a vyhodnocování důkazů, zjišťování souladu mezi zjištěným stavem a stanovenými kritérii a ujištění druhé strany o kvalitě. „V rámci významu auditu pro organizaci představuje nezastupitelný nástroj zpětné vazby mezi vlastníky různých aktiv, okolím organizace, managementem a zaměstnanci, na které management deleguje svoje pravomoci.“ (Svatá, 2016, s. 13)*. Primárním druhem auditu je tedy audit finanční.

Konkretizovaným cílem auditu je tedy podle (Poslání a smysl auditu, 2018) *vyjádření názoru nezávislého, kvalifikovaného odborníka, který podává věrný a poctivý obraz skutečnosti s dostatečnou vypovídající schopností v rámci kontextu auditu a jeho zjištění.* Přínosy auditu (dále už jen v kontextu bezpečnosti informací) spočívají podle (Lidinský, a kol., 2008) *v poskytnutí skutečného obrazu o fungování ve srovnání s obvyklým standardem a výstupy jsou průkazné,*

správné a obsahují doporučení pro rozvoj bezpečnosti informací systémů a akční plán jejich implementací, včetně popisu, požadavků, časové a finanční náročnosti a očekávaných přínosů. Výstupy z auditu pak mohou být pro management východiskem pro změny v systému.

Kontrola a audit ICT představují klíčový krok vedoucí k posílení zabezpečení v organizaci. Procesy a výstup auditu bezpečnosti ICS tedy přispívá k porozumění fungování a vyšší míře zabezpečení v rámci organizace, kde je audit prováděn. Jak uvádí (Svatá, 2016) *audit musí splňovat základní vlastnosti, jako je:*

- *komplexnost – musí postihnout všechny relevantní aspekty,*
- *objektivnost – musí se opírat o existující standardy, případně zkušenosti, pokud standardy neexistují,*
- *nezávislost – auditor nemá s objektem auditu ani se zadavatelem auditu žádné spojení, které by představovalo konflikt zájmů,*
- *formalizace – proces auditu se musí řídit metodikou a existujícími standardy.*

2.9 Audit kybernetické bezpečnosti

Audit kyberbezpečnosti je systematické a nezávislé přezkoumání kyberbezpečnosti v organizaci. Audit zajišťuje to, že v organizaci jsou nastaveny řádné kontroly bezpečnosti, firemní politiky, procedur tak, aby fungovaly bezproblémově a minimalizovaly rizika spojená s útoky na systém. Každá organizace má nastavena určitá pravidla, jak postupovat při zabezpečení, prevenci a samotném útoku. Právě audit těchto pravidel a procedur má za úkol odhalit případné nedostatky a slabiny systému. Cílem auditu kyberbezpečnosti organizace je poskytnout managementu a vedení organizace přehled o tom, jaká je bezpečnostní situace v podniku. Audit hraje zásadní roli v prevenci před útoky na IT a ICS prostředí organizace. Identifikují a testují zabezpečení a pomáhají identifikovat slabiny jednotlivých komponentů i systému jako celku, které by mohly být využit potencionálním útočníkem.

Audit kyberbezpečnosti řídících systémů se zaměřuje na bezpečnostní pokyny, standardy, plavidla. Nejen, že probíhá hodnocení, zda prvek zabezpečení odpovídá nebo ne, ale navíc evaluuje míru optimalizace

jednotlivých zabezpečení. Oproti posouzení kybernetické bezpečnosti, které pouze poskytuje náhled do stavu systému, je audit soustředěn na hloubkovou kontrolu všech aspektů kybernetické bezpečnosti v organizaci. Audit se zaměřuje na hodnocení těchto částí:

část	hodnotí
Operační bezpečnost	Pravidla, pokyny, procedury zabezpečení
Bezpečnost dat	Šifrování, přístup k datům, bezpečnost dat během přenosu
Systémová bezpečnost	Proces instalace aktualizací, hardening
Bezpečnost sítě	Síťovou bezpečnost, konfigurace antiviru, firewallu, monitoring bezpečnosti

Zdroj: vlastní zpracování

Audit je největší zárukou kontroly stavu, kterou může nezávislá auditorská firma nabídnout, poskytuje organizaci a zákazníkům dané organizace zárukou kvality kybernetického zabezpečení organizace. ICS audit přináší výhody v evaluaci a zlepšení bezpečnosti řídících systémů, tyto výhody jsou:

- nalezení slabých míst v zabezpečení,
- dodržování pravidel,
- zlepšení bezpečnostní pozice,
- náskok před potencionálními útočníky,
- důvěra v kybernetické zabezpečení,
- poskytnutí záruky bezpečnosti dat zákazníkům

2.9.1 Audit podle vyhlášky o kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti nařizuje zúčastněným stranám provedení auditu kybernetické bezpečnosti. Výstupem tohoto auditu jsou pak podklady pro zlepšení bezpečnosti a inovaci současných systémů. Vyhláška také klade určité požadavky na obsazení aktérů prováděného auditu. Auditor musí splňovat standardy odborné způsobilosti, nezávislost posudku kybernetické bezpečnosti a také přijímá primární zodpovědnost za provedení auditu. Dle

vyhlášky je audit uskutečňován v pravidelných časových intervalech nebo také v případě změny částí zabezpečovacích mechanismů. Vyhláška říká, že audit je nutno dokumentovat a také konkretizuje specifikace, které mají být v dokumentaci auditu obsaženy. Výstupním dokumentem je výsledná zpráva o provedení auditu, jež se poté stává součástí bezpečnostní dokumentace auditu. Pokud je audit prováděn třetí stranou je auditor povinen s výsledky seznámit správce systému. Závěr auditu sloužící jako zpětná vazba pro oddělení kybernetické bezpečnosti v organizaci a zároveň je vstupem do budoucí fáze identifikace zlepšení zabezpečení.

2.10 Role auditora

Auditor je zodpovědný za provádění analýzy a zhodnocení technologické infrastruktury podniku, aby bylo zajištěno, že systémy zabezpečení pracují přesně a efektivně, přičemž dodržuje firemní pokyny a pravidla. Jestliže auditor nalezne slabinu v zabezpečení, je zodpovědný za oznámení, popis a případný návrh řešení, jak se s potencionálním slabým místem vypořádat. Role auditora kybernetické bezpečnosti obnáší vývoj, implementaci, testování a evaluaci auditních procedur. Je zodpovědný za provedení auditu kybernetické bezpečnosti pomocí zavedených bezpečnostních standardů auditu v organizaci. Proces auditu zahrnuje sítě, software, aplikace, komunikační systémy, bezpečnostní systémy, a především řídící systémy, když je audit aplikován na sektor operačních technologií. Auditor zastupuje zásadní roli v organizaci, kde je kladen důraz na využívání technologie, jeden technický nedostatek nebo chyba mohou mít katastrofální následky na chod organizace. Bezpečnostní audity jsou důležité pro evaluaci zabezpečení interní kontroly a procesů k zabezpečení bezpečnosti dat organizace proti interním a externím hrozbám.

Kvalifikační požadavky, které musí auditor splňovat, uvádí ve svých přílohách novelizovaná vyhláška kybernetické bezpečnosti. Doložením odborné kvalifikace může být uznávaná certifikace auditora označovaná jako CISA (Certified Information Security Auditor), kterou nabízí organizace Isaca stejně jako certifikace CRISC (Certified in Risk and Information System Controls). Kromě těchto certifikací vyhláška považuje za relevantní certifikace auditora také CIA (Certified Internal Auditor) a Lead Auditor ISMS (Lead Auditor Information

Security Management System), která má velmi blízko k ISO normě 27001. Přesněji se jedná o certifikaci způsobilosti vést audit bezpečnosti informací právě podle normy ISO 27001. Důvěryhodnost procesu auditu a schopnost dosahovat jeho cílů závisí na kompetencích jednotlivců zapojených do plánování a provádění auditu včetně auditorů a vedoucích týmu auditorů (ISO 19011, 2018, s. 41) „*Důvěryhodnost procesu auditu a schopnost dosahovat jeho cílů závisí na kompetencích jednotlivců zapojených do plánování a provádění auditu včetně auditorů a vedoucích týmu auditorů“* (ISO 19011, 2011, s. 41).

2.11 Provádění auditu kyberbezpečnosti

V předchozích odstavcích bylo objasněno, co je to kyberbezpečností audit, typicky tento úkon zaznamenává míru zabezpečení, která je kontrolována pomocí kontrolního seznamu takzvaných best practices, uznávaných standardů nebo státních regulací. Postup provádění bezpečnostního auditu je následující:

Zvolit kritéria bezpečnostního auditu – Rozhodnout, které kritéria potřebuje organizace splnit, a toto použít při tvorbě kontrolního seznamu oblastí, které budou analyzovány a testovány.

Zhodnotit úroveň znalostí zaměstnanců – čím více lidí má přístup k citlivým datům, tím se zvyšuje šance, že ve ztrátě nebo odcizení dat bude hrát roli lidský faktor. Je důležité se ujistit, že se zaznamenávají přístupy jednotlivých zaměstnanců k citlivým informacím a také, že zaměstnanci, kteří s citlivými daty pracují jsou pro tuto práci adekvátně proškoleni.

Monitorování síťových logů – monitorování aktivity v síti a logů událostí je důležitým nástrojem v ujištění se, že pouze zaměstnanci s adekvátní úrovní povolení můžou přistupovat k citlivým datům.

Identifikace slabin – než auditor přistoupí k penetračnímu testování konkrétních komponentů prostředí, měl by se zaměřit na snadno identifikovatelné slabiny systému, může to být například zpoždění instalace bezpečnostní aktualizace nebo zastaralý management hesel v organizaci.

Testování komponentů systému – auditorský tým testuje potencionální slabá místa systémů pomocí penetračního testování, hodnotí úroveň

zabezpečení jednotlivých částí, kontroluje správnost nastavení síťových prvků, VPN, pravidla firewallu.

Implementace ochranných prvků – poté co jsou identifikovány slabiny, je nutno implementovat adekvátní opatření pro odstranění anebo zmírnění.

2.12 Auditorská zpráva

Auditorská zpráva bezpečnosti je zevrubným dokumentem obsahující hodnocení zabezpečení organizace. Cílí na identifikaci slabin v bezpečnosti organizace, proto je tento dokument důležitým výstupem auditu, který dopomáhá dosáhnout vyšší úroveň zabezpečení organizace. Standardně je zpráva výčtem všech nálezů auditorů jako jsou chyby, slabiny nebo další bezpečnostní vady v auditovaném systému, také obsahuje doporučení, jak tyto nedostatky napravit. Jedním z hlavních úkolů auditorské zprávy je poskytnout feedback, a to takovým způsobem, aby klient mohl nedostatky napravit.

Auditorská zpráva může obsahovat několik sekcí, může zde být sekce s informacemi o harmonogramu, rozsahu auditu, detaily o testovacím procesu, doporučení a dále. Vyskytují se různé druhy auditorských zpráv, ale všechny mají určité části společné, těmito částmi jsou:

- Název – název auditorské zprávy
- Obsah – obsah zprávy, poskytuje rychlou cestu, jak se ve zprávě zorientovat
- Rozsah auditu – referuje o širším popisu co se v auditu událo
- Popis – detailní popis bezpečnostních rizik, obsahuje relevantní detaily o problému, jak problém opakovaně vyvolat, jak moc je problém nebezpečný pro chod organizace
- Doporučení – poskytuje doporučení o krocích, které by měly být provedeny k odstranění nalezeného problému

2.13 Řízení rizik kybernetické bezpečnosti

Organizace se musí vypořádávat s riziky při každodenním provozu, tyto hrozby zahrnují finanční rizika, riziko selhání zařízení, lidský faktor a další, proto se organizace snažící se implementovat procesy, které potencionální riziko evaluují a rozhodují, zdali je riziko nutno řešit a jak s ním naložit v případě,

že se riziko promění v realitu. Tento proces řízení rizik je řešen jako součást iterativních a stále probíhajících procesů za chodu organizace. Organizace používající ICS se v minulosti vypořádávaly s rizikem pomocí užitím ověřených postupů (best practices) zabezpečení. Zhodnocení bezpečnosti je ve většině případů stanoveno regulacemi ze strany interních předpisů firmy, ale i příslušného státu působnosti organizace. *V ISO normě zabývající se managementem rizik je pak riziko chápáno jako účinek nejistoty na dosažení cílů* (ISO 31000, 2010).

Proces řízení rizik by měl být implementován v rámci struktury organizace pomocí využití tříúrovňového přístupu, který v první úrovni působí v rámci organizaci, druhá úroveň pokrývá procesy a třetí úroveň se zabývá informačním systémem ICS. Tento proces prostupuje všemi třemi úrovněmi v primárním cílem stálého zdokonalovaní vyhledávání a potírání případných rizik.

Řízení rizik se skládá ze čtyř částí, jimiž jsou: rámování, hodnocení, reakce a monitorování. Tyto aktivity jsou nezávislé a často se vyskytující současně v jedné organizaci. Například výstup z monitorování bude sloužit jako vstup pro rámování. Jelikož prostředí, kde organizace působí se neustále mění, je nutno aby se tomuto faktu přizpůsobil i proces řízení rizik, je nutno mít také na paměti, že všechny tyto části jsou aplikovatelné nejen na kybernetickou část organizace, ale i na fyzickou a finanční bezpečnost.

Rámování se v řízení rizik zabývá vytvoření frameworku, ve kterém se rozhoduje, jaké kroky mají být podniknuty v rámci řízení rizik. tato část se skládá z přezkoumání existující dokumentace.

V případě hodnocení rizik je vyžadováno, aby organizace identifikovaly hrozby a slabá místa, případnou míru škody, kterou tyto hrozby a slabá místa mohou způsobit a také míru pravděpodobnosti, že se tyto hrozby mohou naplnit.

Reakce se zabývá tím, jak organizace bude postupovat v případě toho, že se hrozba stane realitou a jak na ni budou jednotlivé struktury v organizaci reagovat. Reakce na identifikaci hrozby vyžaduje, aby v prvé řadě organizace vyhodnotila možné způsoby, jak adresovat nalezené riziko následně proběhne evaluace možností s přihlédnutím na možnosti jež byly vytvořeny v průběhu předchozího kroku hodnocení rizik a následnou implementaci vybraného postupu

adresování identifikovaného rizika, což může být jedno z následujících řešení: přijmutí rizika, vyhnutí se riziku, zmírnění dopadu, transfer rizika nebo jakákoliv kombinace z těchto řešení.

Monitoring je čtvrtým a zároveň posledním komponentem řízení rizik, organizace musí monitorovat hrozby a rizika nepřetržitě a zároveň implementovat zvolené strategie řízení rizik, změny v neustále vyvíjející se situaci mohou pozměnit kalkulaci rizik a efektivitu zmírnění rizik.

V ICS sektoru je také prominentní řízení rizik, obzvláště je třeba vyzdvihnout rozdíly mezi přístupu v řízení rizik mezi tradičním IT a ICS, kdy kybernetický incident v ICS může zahrnovat nejen digitální dopad na systém, ale také dopad fyzický, proto je nutno tento aspekt zvážit při řízení rizik.

2.14 Rekapitulace druhé kapitoly

Rekapitulace druhé kapitoly je věnována stručnému shrnutí klíčových poznatků o teoretických a metodických poznatcích východiscích kyberbezpečnosti řídících systémů.

V začátku kapitoly je čtenář této práce obeznámen s pojmem řídící systém, jeho užitečností v automatizaci, redukci chyb ve výrobě a odvětví, ve kterých se primárně využívá, jimiž jsou téměř veškerá odvětví kritické infrastruktury – tepelné, jaderné, vodní elektrárny, ale i řídící centra elektrické sítě, čističky vod a další zařízení věnující se průmyslové výrobě.

Podkapitola informační a operační technologie se zaobírá definicí těchto dvou pojmů, kdy je informační technologie primárně využívá hardware a software pro vytváření, ukládání, odesílání a přijímání dat. Operační technologie je možno popsat jako technologii nebo zařízení poskytující kontrolu nad reálným světem – jsou to fyzické zařízení i systémy kontrolující, monitorující a vytvářející rozhraní mezi fyzickými stroji a softwarem pro kontrolu a monitoring. Je zde i krátce zmíněna integrace IT a OT prostředí, která se dělí do tří hlavních kategorií, jimiž jsou – procesová integrace, softwarová a datová integrace a fyzická integrace.

Další část předchozí kapitoly pojednává mezi jednotlivými rozdíly mezi informační a operační technologií, z hlediska bezpečnosti dat lze poznat rozdíl kdy v IT prostředí je prioritní zaměření na ochranu dat poté integritu a dostupnost. Avšak v OT prostředí je z tohoto pohledu kladen důraz na dostupnost a integritu, kdežto ochrana zaujímá pomyslnou poslední příčku v žebříčku důležitosti. Z hlediska topologie sítě je IT prostředí velké s relativně velkým počtem klientů a serverů, které jsou rozděleny na základě důležitosti a potřeby, prostředí je dynamického charakteru. OT prostředí je komparativně menší s limitovaným počtem klientů, serverů a se staticky alokovanými IP adresami. Poslední zmíněným rozdílem jsou fyzické komponenty použité v jednotlivých prostředích, kdy největším rozdílem bude specifický hardware používaný pouze v operačních technologiích, které je popsáno a vyjmenováno v následujícím odstavci.

Každý z typu řídících systémů má své specifické uplatnění na různých úrovních průmyslového monitoringu a výroby. Jsou jimi PLC – programovatelný logický automat využívaný k automatizaci elektromechanických procesů, DCS – distribuovaný řídící systém, je průmyslový systém,
který je nasazen a řízen distribuovaným způsobem, SCADA – dispečerské řízení a sběr dat je typ systému pro řízení procesů používající počítače a kontrolu nad procesy.

Kybernetické hrozby a útoky na kritickou infrastrukturu, které se primárně zaměřují na řídící systémy začínají být stále frekventovanějšími, proto je nutno tyto hrozby adekvátně a v co nejkratším čase adresovat, k tomu je vhodné využít analýzu rizik potencionálních hrozeb. Nejčastěji se jedná o infrastrukturu přímo napojenou na síť a na části, které mohou být přímo kyberútoky ovlivněny. Nejčastější hrozby ohrožující ICS jsou: Nákaza malwarem přes internet, DDOS útok na IoT zařízení, nákaza malwarem pomocí externího hardwaru.

Kybernetické zabezpečení ICS je komplexními procesy a praktikami využívanými k prevenci, minimalizaci a odrazení potencionálních hrozeb, zabezpečení se lišící od zabezpečení IT systému, a to hlavně v architektuře kybernetického zabezpečení. Zabezpečení ICS se primárně

zaměřuje na koncepty: Architektury kybernetického zabezpečení, segmentaci a segregaci sítě, firewally, autentifikaci a autorizaci.

Další část se již věnuje stránce auditu obecně, kdy audit představuje nezastupitelný nástroj pro organizaci zpětné vazby mezi managementem a zaměstnanci, audit kybernetické bezpečnosti je systematickým a nezávislým přezkoumáním kybernetické bezpečnosti v organizaci, tento specifický audit se zaměřuje na operační bezpečnost, bezpečnost dat, systémovou bezpečnost a bezpečnost sítě. Audit podle vyhlášky o kybernetické bezpečnosti stanovuje, jak se audit provádí, kdo ho provádí, co je vstupem a výstupem auditu a jaká dokumentace je vyprodukována.

Auditorem je osoba zodpovědná za provedení analýzy a zhodnocení technologické infrastruktury podniku, aby bylo zajištěno, že systémy zabezpečení pracují přesně a efektivně. Musí splňovat určité kvalifikační požadavky, jež jsou zmíněny ve vyhlášce o kybernetické bezpečnosti.

Provádění auditu kyberbezpečnosti je realizován za pomoci kontrolního seznamu uznávaných standardů, státních regulací a nejlepších praktik. Postup provádění auditu má tyto kroky: zvolit kritéria bezpečnostního auditu, zhodnotit úroveň znalostí zaměstnanců, monitorování síťových logů, identifikace slabin, testování komponentů systému, a nakonec implementace ochranných prvků. Výstupem auditu kybernetické bezpečnosti řídících systémů je auditorská zpráva, která cílí na identifikaci slabin v bezpečnosti organizace. Má tyto části: název, obsah, rozsah auditu, popis, doporučení.

Poslední podkapitola se věnuje řízením rizik, což je nástroj pro kontrolu a zmírnění rizik. Proces řízení rizik by měl být implementován pomocí využití tříúrovňového přístupu, kdy první úroveň je působení řízení rizik v rámci organizace, druhá úroveň je soustředěna na řízení rizik procesů a poslední úroveň se zaobírá informačním systémem ICS. Na každé z těchto úrovní je pak uplatněna metodika řízení rizik složena ze čtyř částí, jimiž jsou: rámování, hodnocení, reakce a monitorování.

3 Popis současného stavu kyberbezpečnosti řídících systémů

Tato kapitola se zaměřuje na organizaci, která se v každodenním fungování neobejde bez využití řídících systémů. Tato práce se poté zaměří na konkrétní organizaci, působícím ve výrobním a logistickém průmyslu využívající řídící systémy k řízení, kontrole výroby, automatizaci specifických procesů ve výrobě a v neposlední řadě akvizici dat.

Dalším oddílem této kapitoly bude popis fungování organizace a poté se bude zaobírat důležitosti kybernetického zabezpečení řídících systémů a jednotlivým požadavkům kybernetické bezpečnosti v organizaci.

3.1 Organizace využívající řídící systémy

Organizace, jejíž část je předmětem auditu kybernetické bezpečnosti řídících systémů je globální, mezinárodní společnost primárně se zabývající výrobou industriálního plynu, dodává plyn zákazníkův v rozličných odvětvích jako jsou například zdravotnická zařízení, výroba nafty, potravinářský průmysl a mnoho dalších průmyslových a civilních odvětví. Organizace je v současné době řazena do žebříčku Fortune Global 500, což je roční hodnocení 500 největších korporací hodnoceno na základě zisku společnosti. Organizace se zaměřuje na dvě průmyslová odvětví, jimiž jsou výroba industriálního a medicínského plynu a inženýring, což je sekce věnující se návrhu, realizaci a správě chemických továren na výrobu plynů.

Autor se v bakalářské práci zaměřil na realizaci auditu kybernetické bezpečnosti v jednom z dálkových řídících center ROC (Remote Operations Center), které se soustředí detekci abnormalit ve výrobním procesu pomocí strojového učení, optimalizaci provozu skrze datovou analýzu, implementaci automatického a prediktivního řízení výroby pomocí řídících systémů, mezi další hlavní činnosti patří řízení a správa necelé stovky menších i větších výrobních center, která jsou rozmístěna v oblasti východní Evropy, blízkého východu, Ruska, severní Afriky.

Pracovní tým ROC se skládá z přibližně osmdesáti specialistů a inženýrů, kteří mají za úkol zpracovávat, kontrolovat a vyhodnocovat data výrobních závodů v zemích zmíněných v předchozím odstavci. Na základě přijatých dat jsou vytvářeny nástroje, matematické modelování a prediktivní řízení výroby, za pomoci strojového učení jsou získávány podrobné informace o odchylkách od standardního stavu a poté probíhá proces optimalizace výrobních parametrů na základě výstupu ze zpracovaných dat. Zároveň se centrum podílí na vývoji softwarových aplikací a na vizualizaci zpracování výsledků dat.

3.2 Význam kybernetické bezpečnosti pro organizaci

Otázka kybernetické bezpečnosti se během posledních let dostává stále více do popředí, téměř všechny firmy, podniky a organizace k práci využívají komponenty informačních a operačních technologií. Žádná organizace se nechce stát obětí kybernetického útoku, který může mít značné ekonomické dopady na fungování firmy, obzvláště pokud firma pracuje s citlivými údaji, jež jsou chráněny zákonem.

Ani organizace, která je zmíněna v praktické části není výjimkou, a to obzvlášť kvůli jejímu zaměření, což je výroba plynů. Proto je pro organizaci klíčové zabezpečení kritické infrastruktury jako takové obzvláště s důrazem na řídící systémy. V organizaci je na denní bázi používána celá řada technologií, které se mohou stát potencionálním vektorem útoku. ROC komunikuje, sbírá data a řídí externí továrny téměř vyloženě pomocí internetového spojení. Většina zařízení, se kterými komunikuje se vyskytuje v zahraničí, proto je pro organizaci prioritní internetové spojení s okolím, dalším cílem, kterého se organizace snaží dosáhnout je správnost přijatých a odchozích dat. Zde je toto ošetřeno využitím specifických protokolů pro komunikaci se servery nebo přímo protokoly specifickými pro ICS prostředí.

Pro fungování organizace je proto nezbytné bezchybné a nepřetržité fungování technologií jako jsou servery, řídící systémy, interní síť a další komponenty.

3.3 Přehled kyberbezpečnosti ICS v organizaci

Primární činností organizace výroba plynů, proto používá celou řadu systémů a zařízení ze sféry operačních technologií, jmenovitě to jsou PLC, DCS a SCADA systémy, avšak při dálkové komunikaci s řídícími systémy jsou data vedena přes internet. Toto spojení nemůže probíhat přes volně dostupné sítě, a proto organizace využívá virtuální privátní sítě pro zvýšení zabezpečení přenosu dat do a z fyzických zařízení operačních technologií.

Dále jsou implementovány Firewally, které jak již bylo zmíněno v teoretické části poskytují soubor pravidel průtoku paketů v síti za účelem lepšího kybernetického zabezpečení. Síť je zde pochopitelně segmentovaná a separovaná do jednotlivých kategorií dle potřeby zabezpečení, jsou zde tři sítě, první slouží pro běžnou komunikaci a přístup na internet, druhá síť je pro hosty a je omezena nižšími privilegii přístupna určité stránky a servery, poslední sítí je síť, s nejvyšší úrovní zabezpečení, z této sítě lze přistupovat na jinak běžně nedostupné servery, stránky a ke komunikaci s řídícími systémy.

Následujícím zabezpečením je nastavení různých stupňů privilegií přístupu zaměstnanců, podle toho, s jakým řídícím systémem pracují, ne každý zaměstnanec potřebuje přístup do všech systémů organizace a je lepší variantou odepření irelevantního přístupu, nežli když je všechno povoleno všem.

V neposlední řadě je nutno zvážit fyzické zabezpečení přístupu k přístrojům, ne úplně z důvodu poškození, ale primárně kvůli možnosti připojení neznámého zařízení do portů, není zcela nutné, aby porty byly fyzicky zabezpečené proti možnosti připojení. Fyzické zábrany jsou mnohem snadněji překonatelné nežli implementace autorizačního a autentifikačního programu nebo případně programové zakázání funkcionality portů.

Řídící systémy, které se vyskytují ve výrobních zařízeních musí být správně nakonfigurovány pro zabezpečení bezchybného a bezpečného fungování, proto organizace využívá manuál poskytnutý výrobcem, který sloužící ke správné konfiguraci otevřených portů, nastavení privilegií, whitelisting povolených IP adres a nastavení autorizace a autentifikace povolených entit, které se mohou navázat kontakt se zařízením. Poslední jmenované nastavení sloužící k prevenci DDoS útoků, s tím souvisí i implementace firewallových

pravidel přímo v zařízeních, načež firewall není vyvinut výrobcem zařízení, ale interně v organizaci. V tabulce pod tímto paragrafem je možno nalézt výčet opatření kybernetické bezpečnosti jež jsou již aplikovány na řídících systémech v organizaci.

Opatření	**Účel opatření**
VPN	Obecná prevence před DDoS útokem
Segmentace a separace sítě	Zabránění neautorizovaného přístupů do segmentů sítě
DMZ	Vytvoření další vrstvy ochrany mezi dvěma sítěmi
Privilegia uživatelů	Zabránění přístupu pracovníkům do částí systémů, které nejsou v jejich kompetenci
Fyzické a virtuální zabezpečení portů	Zamezení nechtěnému přenosu dat do a z řídící jednotky
Optimalizace konfigurace řídících systémů	Minimalizace slabých míst řídících systémů
Whitelisting IP adres	Omezení přístupu z neznámých IP adres
Autorizace a autentifikace uživatelů	Zabránění přístupu osobám nepracujícím v organizaci

Zdroj: vlastní zpracování

3.4 Požadavky na zabezpečení řídících systémů

Jedním z nejdůležitějších požadavků na zabezpečení je ochrana před útoky zvenčí, jež napomáhá minimalizovat hrozby DDoS, a malwarových útoků. Dalším požadavkem je ochrana citlivých dat, na serverech se nalézají data z výroby, která by mohly posloužit konkurenci nebo případným útočníkům při manipulaci fyzických zařízení. Nejsou zde uložena jen a pouze výrobní data, ale je zde i databáze zaměstnanců s osobními údaji, což by mělo být jednou z priorit ochrany před útočníky.

Pokud jde o prostředí týkající se čistě operačních technologií, a to řídících systémů, je žádoucí pravidelně instalovat aktualizace vytvořené výrobcem,

některé řídící systémy, a to zejména SCADA běží na virtuálním počítači, a proto se potýká se stejnými překážkami zabezpečení jako IT technologie, je zde nutnost instalovat a pravidelně aktualizovat antivirový software společně s aktualizacemi systému.

V neposlední řadě je zcela klíčové korektní nastavení funkcionality všech systémů, nesprávné nastavení často vede k bezpečnostním slabinám což otevírá celou řadu možností, jak se útočník může do řídících systémů dostat.

Dále je potřeba dodržování pravidel spojených s užíváním internetu, a s tím související následující bod, což je pravidelné školení zaměstnanců stávajících i nových hrozbách, bezpečnostní politice firmy a jak tyto pravidla používat v praxi.

Při řízení zabezpečení není radno zapomínat na zjišťování a odhalování chyb, reporting a následné vytvoření adekvátního dokumentu zaznamenání zjištěných chyb, který bude předán týmu pracujícím na zabezpečení a bude sloužit jako vstup pro opravu nalezené chyby.

3.5 Rekapitulace třetí kapitoly

Kapitola pojednává o organizaci, na kterou je aplikována praktická část bakalářské práce. V první části třetí kapitoly autor práce představuje organizaci, jež je globální, mezinárodní organizací věnující se výrobě industriálního plynu, který je dodáván do zdravotnických zařízení, do výroby nafty, potravinářského průmyslu a dalších odvětví. Dále je zmíněno dělení organizaci do dvou částí, jimiž jsou výroba industriálního plynu a inženýring. Praktická část je aplikována na část organizace, konkrétně Remote Operations Center, zabývající se dálkovým řízením výrobních procesů, akvizici výrobních dat a optimalizaci výrobních procesů.

Podkapitola nazvaná význam kybernetické bezpečnosti pro organizaci představuje roli a obecnou filozofii organizace v implementaci, kontrole a aktualizaci kybernetické bezpečnosti. Organizace působí ve výrobním průmyslu, kde je nezbytné používat řídící systémy, je prioritou bezchybné a nepřerušované fungování těchto systémů, byť jen malý výpadek nebo

nesprávné fungování může narušit návaznost výrobních procesů, což v nejlepším případě zapříčiní zpoždění ve výrobě, ale už i tento problém má na organizaci negativní finanční dopad. Pro organizaci je důležitá akvizice výrobních dat, proto se velká váha klade na zabezpečení internetového spojení a s ní spojených procesů.

V přehledu kyberbezpečnosti ICS v organizaci je popsáno fungování a výčet zabezpečení implementovaných v řídících systémech a procesech s nimi spojenými. Bezpečnostními opatřeními jsou užití virtuální privátní sítě, firewally, segmentace a separace sítě, autorizace a autentifikace pracovníků, whitelisting zaměstnanců a procesů, kteří mohou přistupovat k řídícím systémům, fyzické a virtuální zabezpečení portů v zařízeních. Posledním bezpečnostním prvkem, který je neméně důležitý je správná konfigurace samotných řídících systémů.

Poslední podkapitola tohoto paragrafu se zaobírá konkrétními požadavky na zabezpečení, jimiž jsou ochrana před útoky zvenčí, minimalizace hrozby DDoS a malwarových útoků, dále je to ochrana citlivých dat, zabezpečení řídících systémů a správná konfigurace virtuálních počítačů, dodržování pravidel spojených s užíváním internetu ze strany zaměstnanců a posledním je testování zařízení pomocí specializovaných nástrojů pro odhalení chyb a slabých míst.

4 Audit kyberbezpečnosti řídících systémů

Kapitola nesoucí název audit kyberbezpečnosti řídících systémů pojednává o procesech a postupech návrhu zabezpečení řídících systémů. Jednotlivé kroky jsou podrobně popsány v následujících podkapitolách nesoucí názvy priority zabezpečení ICS, potencionální hrozby, analýza rizik, strategie zabezpečení, nástroje pro ověření kybernetické bezpečnosti.

V poslední části se tato kapitola bude věnovat následnému doporučení opatření pro zlepšení kybernetické bezpečnosti řídících systémů, dále pak auditu a následné kontrole. Zdali bude vypracovaná strategie implementována je čistě na vedení firmy, a proto implementace není součástí této práce.

4.1 Priority zabezpečení řídících systémů

Řídící systémy jsou součástí sféry operačních technologií, ale jak je známo z předchozích kapitol, informační a operační technologie jsou v dnešní době propojené, a proto se zabezpečení soustředí na obě tyto oblasti, avšak vyšší priorita je stále kladena na množinu zařízení operujících v OT, avšak stránka zabezpečení střetu těchto dvou sfér se nesmí zanedbat a je zcela klíčovou složkou zabezpečení. Ve fázi určení si priorit zabezpečení je nutno zvážit veškeré okolnosti a dostupné informace, jaké má organizace k dispozici. Jelikož organizace působí ve výrobním průmyslu, kde jsou procesy řízeny řídícími systémy, aby jednotlivé navazující procesy probíhaly včas a bezchybně, i malý výpadek jednoho procesu na krátkou dobu může způsobit zdržení procesů ostatních a velké finanční ztráty, je třeba minimalizovat interní i externí hrozby, které by právě tyto události mohli vyvolat.

Jsou proto vynaloženy značné finanční i lidské zdroje pro minimalizování těchto hrozeb, organizace, jež se zabývá průmyslovou výrobou má dedikované oddělení odborníků a relativně rozsáhlý rozpočet na realizaci zabezpečení řídících systémů. Přesto je nutno uvědomění si, s jakými daty organizace pracuje, které je nutno ošetřit vyšším stupněm ochrany a kolik finančních prostředků je ochotna vynaložit na ochranu systému.

Prioritou u řídících systémů bude nepřetržitá provozuschopnost a současně bezchybné fungování, ochrana dat obzvlášť těch, které nepodléhají utajení, tedy bude na nižší úrovni důležitosti.

Jak již bylo zmíněno, operační and informační technologie jsou provázány, a proto je potřeba nahlížet i ze strany zabezpečení IT oddělení, kdy by se mohlo stát, že útočník získá autorizační a autentifikační údaje zaměstnance a přes IT síť se dostane k řídícím systémům a už i jen malými změnami jediného řídícího prvku může ohrozit celou výrobu a způsobit velké finanční škody.

4.2 Potencionální hrozby

Na základě analýzy implementace zabezpečení řídících systémů v organizaci lze vybrat množinu možných řídících systémů a IT procesů, které jsou potencionálně v ohrožení. Ke každému zvolenému řídícímu systému bude přiřazena množina hrozeb, které se mohou vyskytnout.

Řídící systém a informační technologie	**Hrozby**
SCADA	• Nákaza malwarem přes internet • DDoS přes IoT
DCS	• Nákaza malwarem pomocí externího hardwaru
PLC	• Nákaza malwarem pomocí externího hardwaru
Emailová služba	• Spoofing • Phishing • Ransomware
Komunikační aplikace	• Guest users • Phishing • Malware
Datové servery	• Ztráta dat, DNS útok • DDoS přes IoT • Cache poisoning

Zdroj: vlastní zpracování

Jelikož se SCADA věnuje primárně akvizici dat a navazuje spojení s databází, které je přes internet, je zde relativně velké nebezpečí nákazy malwarem přes internet. Neoptimální nastavení portů nebo chyba ve spojení by mohla způsobit, že malware pronikne přes internet do dalších síťových struktur, které jsou nějakým způsobem se SCADOU ve spojení.

DDoS přes IoT je podobného charakteru, kdy při špatném nastavení http protokolu nebo nevyužití VPN může dojít k cílenému množství přijímaných žádostí o spojení a tím pádem dojde k omezení funkcionality toku dat z a do databáze a monitoringu.

Oproti řídícímu systému SCADA, PLC ani DCS nejsou přímo propojeny s internetem, což je výhodou omezující určité vektory útoku. Co však ale může nastat je, že neautorizovaná osoba přijde do fyzické lokace, kde se DCS a PLC systémy vyskytují a zapojí do nich nevyžádaný hardware, který v sobě může nést malware a jelikož tyto systémy nedisponují ochranou proti malwaru nebo antivirovým programem, malware snadno pronikne do systému.

Spoofing a phishing jsou podobné koncepty, kdy se v obou případech snaží útočník získat autorizační a autentifikační údaje od zaměstnance, aby získal přístup do sítě organizace a případně se pokusil přesunout do
sítě, kde sídlí řídící systémy.

Ransomware, Guest users a DNS útok jsou v tomto případě méně pravděpodobnými variantami možného vektoru útoku na organizaci.

K efektivní eliminaci hrozeb je nutno si uvědomit pravděpodobnost toho, že daná hrozba nastane, proto budou výše zmíněná rizika uvedena pro přehlednost v tabulce a ohodnocena stupnicí nula až deset, kdy nula je nejmenší pravděpodobnost, že riziko nastane a deset je pravděpodobnost největší. Pokud jsou hrozby ohodnoceny stejným bodovým ohodnocením, jsou uvedeny ve stejné buňce tabulky.

Hrozba	Pravděpodobnost výskytu hrozby
Spoofing, Phishing, Guest users, Ransomware	6
Malware, DDOS přes IoT	4
Nákaza malwarem přes internet, DNS útok	3
Ztráta dat, Cache poisoning	2
Názaka malwarem pomocí externího hardwaru	1

Zdroj: vlastní zpracování

Z tabulky je zjevné, že žádná případná hrozba není ohodnocena extrémně vysokou pravděpodobností, že se vyskytne, avšak hrozby spadající do sféry informačních technologií mají vyšší hodnocení, pravděpodobně tomu tak je kvůli častější interakcí uživatelů s tímto systémem a také využívání některých prvků tohoto systému pro komunikaci, kde se pochopitelně může vyskytnout největší příležitost pro útočníka, jak se zmocnit akreditace pracovníků.

4.3 Analýza rizik

V přechozí podkapitole o potencionálních hrozbách bylo zjištěna množina potencionálních hrozeb a poté ohodnoceny jednotlivé hrozby dle pravděpodobnosti, že se daná hrozba promění ve skutečnost. Pro lepší pochopení a seřazení hrozeb dle více parametrů bude provedena analýza rizik pro každou hrozbu dle více kritérií. Prvním krokem bude ustanovení kritérií, dle kterých budou rizika hodnocena kdy vstupem jsou hrozby s pravděpodobností výskytu čtyři a více.

Pravděpodobnost výskytu hrozby šest			
Hrozba	**Priorita**	**Závažnost**	**Finanční dopad**
Spoofing	Střední	5	6
Phishing	Střední	6	6
Guest users	Malá	2	2
Ransomware	Vysoká	8	9
Pravděpodobnost výskytu hrozby čtyři			
Hrozba	**Priorita**	**Závažnost**	**Finanční dopad**
Malware	Vysoká	9	7
DDOS přes IoT	Vysoká	8	5

Zdroj: vlastní zpracování

V tabulce bylo určeno kvalitativní hodnocení pro prioritu řešení hrozby, kdy byla určena třístupňová škála: malá, střední, vysoká. Parametr priorita řešení hrozby byl vybrán z důvodu důležitosti identifikovat, které hrozby potřebují být vyřešeny nejdříve, protože v kombinaci s vysokou pravděpodobností výskytu hrozby mohou způsobit velké problémy.

Druhým zvoleným parametrem byla závažnost, která je ohodnocena na kvantitativní škále, kdy nula je nejmenší závažnost toho, když se hrozba naplní. Třetím vybraným parametrem je finanční dopad na společnost, který je také bodově ohodnocen stupnicí nula až deset, kdy nula je nejmenší finanční dopad na organizaci a deset největší. Všechny tři parametry mají určitou návaznost jeden na druhý, kdy se priorita odvíjí od kombinace hodnocení závažnosti a finančního dopadu.

4.4 Návrh zabezpečení řídících systémů

Návrh zabezpečení řídících systémů se bude odvíjet od výsledků předchozí kapitoly a jako vstup použije tabulky, ve kterých byly kvalitativně ohodnoceny jednotlivé hrozby, výstupem poté bude doporučení zabezpečení proti těmto již dříve zmíněným hrozbám. Tedy cílem podkapitoly přiblížit se optimálnímu řešení a co jak nejvíce pomocí preventivních opatření a implementovaných postupů minimalizovat potencionální výskyt hrozeb, které převyšují čtyřku na stupnici hodnotící pravděpodobnost výskytu hrozby.

Hrozba	**Navrhnuté opatření**
Spoofing	Real-time link click ochrana Real-time detekce, semináře pro zaměstnance Instalace antivirového programu Přednášky pro zaměstnance
Phishing	
Guest users	
Ransomware	Instalace antivirového programu Přednášky pro zaměstnance
DDOS přes IoT	Cloudová služba chránící před DDOS útokem
DNS útok	Implementace izolovaných DNS serverů
Ztráta dat	Správná konfigurace databázových serverů
Cache poisoning	Aktualizace DNS softwaru
Malware přes hard.	Fyzické zabezpečení portů na zařízeních Přednášky pro zaměstnance
Malware	Instalace antivirového a anti-malware programu Přednášky pro zaměstnance
Malware přes internet	

Zdroj: vlastní zpracování

V předchozí tabulce jsou přednášky pro zaměstnance, protože je nejdůležitější, aby zaměstnanci pracující s řídícími systémy a technologiemi jimi spojenými získali povědomí o možných hrozbách a byli informováni, jak se jim vyvarovat, případně jak postupovat, když se hrozba promění ve skutečnost, například komu incident nahlásit, co dělat ihned po nalezení hrozby a další užitečné informace.

Druhým nejfrekventovanějším opatřením je instalace antivirového programu na zařízení, kde je to možno a tam, kde to má smysl. Antivirový program zabraňuje velkému spektru hrozeb, o kterých nemá běžný pracovník tušení, proto je klíčové korektní nastavení antivirového programu a pravidel, aby se antivirový program nedostával do konfliktu s pravidly firewallu, ale aby se tyto dva nástroje minimalizující hrozby doplňovaly.

4.5 Nástroje a techniky pro ověření bezpečnosti

V dnešní době se vyskytuje nespočet nástrojů pro testování IT systémů, ale tyto nástroje nejsou nejvhodnější pro použití v ICS prostředí, z důvodu možného narušení procesů. Během aktivního testování se zvyšuje zatížení sítě a tím, že řídící systémy mají často omezenou procesní kapacitu, může dojít k selhání komponentu a na to navazujícím dalším problémům. Z tohoto důvodu se v při ICS testování používají specializované nástroje a testovací techniky. Tyto metody jsou přizpůsobeny tak, aby minimalizovali risk selhání systému, ale zároveň poskytli potřebný vystup testování. Příkladem zmíněného nástroje je:

- Sophia což je nástroj navrhnut a vyroben speciálně pro testování ICS kontrolních systémů. Program funguje tak, že vytvoří digitální otisk sítě a v reálném čase otisk porovnává se současným stavem sítě. Program je schopen zasílání alarmů v reálném čase, má funkci blacklistu i whitelistu a stále monitoruje síť pro nalezení abnormalit.

Další kategorií jsou techniky vyvinuté na testování bezpečnosti informačních technologií, vzhledem k tomu, že většina interakce zaměstnanců se systémem probíhá ve sféře IT a ta je integrovaná s operačními technologiemi, je žádoucí využít standardní testovací nástroje bez specializace na jedno či druhé prostředí, tyto techniky jsou:

- Externí testování je testování prováděno externí firmou, která nejsou podány informace o interní síti. Externí tester prověří slabá místa a snaží se najít chybu v systému, která by mu pomohla proniknout do organizace.
- Interní testování probíhá v síti organizace, cílem tohoto typu testování je zjistit, co by se mohlo stát, kdyby útočník měl přístup k síti. Tester

se připojí do sítě a používá různé techniky a nástroje, aby odhalil, k jakým datům je schopen získat přístup.

4.6 Bezpečnostní politika organizace

Bezpečnostní politika organizace snažící se o identifikaci pravidel a procedur pro všechny zaměstnance používající zařízení nebo síť na kterou se bezpečnostní politika vztahuje.

Organizace má interní soubor sepsaných best practices, procedur a postupů, které poskytují instrukce, jak postupovat v nakládání s daty, jaké úrovně zabezpečení jsou žádoucí u konkrétních systémů a jak má být síť segmentována a separována pro optimalizaci zabezpečení všech komponentů řídících systémů. Bezpečnostní politika je publikována v tištěné i elektronické formě a distribuována zaměstnancům. Veškerý obsah je konzultován s experty na zabezpečení pracujícími v organizaci a současně i externími kontraktory, tento dokument je schválen vedením organizace a každým rokem prochází novelizací, kdy jsou části přidány, odebrány nebo upraveny z důvodu implementace nejnovějších postupů a praktik. Obsahem bezpečnostní politiky jsou i havarijní a krizový plán, který řešící, jak přesně postupovat při nově vzniklém riziku.

4.7 Doporučení na zlepšení kybernetické bezpečnosti

Kybernetické zabezpečení je v organizaci vzhledem k potřebě nepřetržité výroby na vysoké úrovni, existuje dedikované oddělení, které se zabývá pouze kybernetickou bezpečností a jedna sekce tohoto oddělení se zabývá pouze zabezpečením řídících systémů. Proto lze říct, že jsou téměř všechny slabá místa pokryta.

Jedním z nedostatků, který není zcela ošetřen je nedostatečné nastavení komplexity hesel a nevyužívání procesu vícefázového ověření obzvlášť k přihlášení do organizační sítě z domova, v organizaci jsou také používány RFID karty, které nejsou nijak ošetřeny proti odcizení informací nacházejících se na kartě, proto by mohlo dojít k přechodu na modernější technologii, jako je například UWB RTLS.

4.8 Kontrola a audit

Po implementaci strategie kybernetického zabezpečení řídících systémů je nutná vytvoření časového plánu pravidelných kontrol v podobě auditu systému. Nejvhodnější variantou, jakou zvolit je provedení auditu externí firmou vzhledem k tomu, že interní zaměstnanci často využívají stejné techniky a postupy pro každý prováděný test a audit, proto může externí firma se svými vlastními zavedenými postupy odhalit slabá místa a potencionální rizika, které zaměstnancům organizace mohou uniknout, další výhodou využití externí firmy je, že organizace nemusí permanentně zaměstnávat pracovníky, kteří se věnují pouze testování a auditu bezpečnostních systémů, nýbrž vše je v gesci externí firmy.

4.9 Shrnutí čtvrté kapitoly

Čtvrtá kapitola se zaměřuje na praktickou aplikaci kybernetického zabezpečení řídících systémů. V první části pojednává o prioritách zabezpečení v organizaci, kterými jsou, nepřetržitá provozuschopnost, minimální množství chybových incidentů při provozu a ochrana citlivých dat.

Dále je proveden výčet systémů a zařízení zapojených do procesu řízení jimiž jsou SCADA, DCS, PLC, emailová služba, komunikační aplikace, datové servery a k nimž jsou následně přiřazeny potencionální hrozby, které se mohou vyskytnout u daného systému nebo zařízení. Získané hrozby jsou ohodnoceny na kvantitativní bodové škále podle toho, jak pravděpodobný výskyt hrozby je, v pravděpodobnostním hodnocení se na nejvyšší příčce se skóre šest umístily hrozby Spoofing, Phishing, Guest users, Ransomware skóre čtyři byly pak ohodnoceny hrozby Malware, DDoS přes IoT, hranice čtyři a víc byla zvolena pro využití v další podkapitole.

Analýza rizik se zabývá hodnocením rizik dle tří kritérií a to priorita, kritérium ohodnoceno na kvalitativní stupnici o třech hodnotách a to: malá priorita, střední priorita, vysoká priorita řešení hrozby. Druhým zvoleným kritériem je závažnost, kritérium, které hodnotí na stupnici od nula do deseti, jak závažná nastane situace, pokud se hrozba skutečně v organizaci vyskytne. Třetím

a posledním kritériem je finanční dopad, toto kritérium je opět hodnoceno od nuly do deseti a určuje jaký finanční dopad na organizaci by nastal v případě incidentu jedné z hrozeb. Nejdůležitějším kritériem je priorita, avšak všechny tři kritéria na sebe jistým způsobem navazují. Vysoká priorita k zabezpečení slabého místa byla udělena: Ransomware, Malware a DDOS přes IoT, avšak jediný ramsomware je jedinou hrozbou s pravděpodobností výskytu šest a zároveň mající vysokou prioritu.

Kapitola poté přechází k návrhu zabezpečení vycházejícího z výsledků přechozího oddílu, jako vstup je použitá vypracovaná množina hrozeb a cílem je najít navrhnout zabezpečení minimalizující potenciál hrozeb. Jako nejčastější navrhnuté opatření se opakovalo školení pro zaměstnance, patrně z důvodu, že zaměstnanci jsou nejfrekventovanějším aktérem navazujícím interakcí se systémy, procesy a sítí. Na druhé příčce se pak umístilo nasazení antiviru tam, kde se nebudou pravidla antiviru dostávat do konfliktu s pravidly firewallu.

Po návrhu zabezpečení následuje sekce Nástroje a techniky pro ověření zabezpečení, v níž jsou popsány specifika ICS testování a je uveden jeden nástroj speciálně navrhnut k tomuto účelu jménem Sophia. Dalšími technikami, které jsou spíš obecného charakteru jsou techniky vyvinuté na testování bezpečnosti informačních technologií, které se dělí na interní a externí testování.

Bezpečnostní politika organizace hraje stěžejní roli v implementaci bezpečnosti systémů v organizaci, je to interní soubor sepsaných nejlepších oborových praktik, procedur a postupů, který poskytuje instrukce a pojednává o tom, jak postupovat při nakládání s citlivými daty. Bezpečnostní politika organizace zahrnuje havarijní i krizový plán, které řeší, jak přesně postupovat při nově vzniklém incidentu.

V podkapitole doporučení na zlepšení kybernetické bezpečnosti řídících systémů je pojednáváno o určitých možných zlepšeních, které napadly autora práce a o kterých si myslí, že můžou pozitivní mírou přispět k optimalizaci zabezpečení, těmito doporučeními je zavedení pravidel pro vytváření komplexních hesel k přihlašování do systému, vícefázové ověření při práci

v terénu nebo z domova a v neposlední řadě obměna technologie RFID karet za UWB RTLS technologii. Závěr informuje čtenáře o doporučení provádění testování a auditu bezpečnosti v pravidelných intervalech prováděných externí firmou, zejména této kapitole by měl čtenář této práce věnovat zvýšenou pozornost.

5 Závěr

Cílem bakalářské práce byla analýza organizace a následný rozbor stavu kybernetického zabezpečení řídících systémů. Na základě analýzy potencionálních hrozeb byl proveden návrh zabezpečení hrozeb, které s největší pravděpodobností mohou nastat v rámci řídících a na ně navazujících systémů v organizaci.

S rozvojem automatizace průmyslové výroby jsou čím dál více implementovány řídící systémy, které mají na starosti řízení procesů akvizici a controlling dat, automatizování jednotlivých procesů. Vzhledem k čím dál většímu propojení technologií a přidávání funkcionalit zařízením fungujících v operační technologické sféře, se operační technologie neobejdou bez připojení k internetu, avšak to přináší celou řadu problémů v podobě neadekvátního zabezpečení těchto zařízení, která nebyla navrhnuta s myšlenkou připojení k internetu, které skýtá mnoho hrozeb pro mnohdy nedostatečně zabezpečené řídící systémy.

K efektivnímu řízení bezpečnosti je proto vhodné využívat osvědčené techniky a nástroje, které si kladou za cíl nejen adekvátně zabezpečit zařízení a systémy, ale zároveň informovat odpovědné zaměstnance o přehledu a současném stavu zabezpečení, jedním z nejkomplexnějších nástrojů pro ověření stavu zabezpečení je audit kybernetické bezpečnosti, a to konkrétně zaměřený na řídící systémy operačních technologií. Klíčovými prvky tohoto auditu jsou prověření operační bezpečnosti, bezpečnosti dat, systémové bezpečnosti a v neposlední řadě bezpečnosti sítě. Audit se také musí řídit určitými regulemi ošetřenými ve vyhlášce o kybernetické bezpečnosti. Audit je prováděn auditorem, který opět musí splňovat kvalifikační požadavky, jež jsou opět uvedeny ve vyhlášce kybernetické bezpečnosti, dále by se měl vyznačovat kvalifikací, kterou může být CISA, CRISC, CIA nebo ISMS.

Práce seznamuje čtenáře s konceptem řízení rizik, tříúrovňového přístupu k řízení rizik dělícího se na řízení v rámci organizace, procesů a v informačních systémech, řízení rizik je poté nastíněno z pohledu rozebrání na jednotlivé části a identifikací hrozeb.

Organizace, na kterou je aplikována praktická část se zabývá průmyslovou výrobou plynů, při níž používá řídící systémy k controllingu, akvizici dat, a monitoringu výrobních procesů. Hlavními hrozbami zabezpečení řídících systémů v organizaci, definovanými na základě sestavení hodnotící škály kritérií jsou spoofing, phishing, ransomware a DDoS přes IoT. Jejich kompletní výčet je zaznamenán ve čtvrté kapitole, ale pro organizaci je žádoucí tento seznam hrozeb neustále rozvíjet o další potencionální hrozby.

Je žádoucí stanovit a implementovat bezpečnostní strategii a cíle, zhodnotit výstup analýzy rizik, projít současnou bezpečnostní politiku, zde začlenit nové poznatky a poupravit neaktuální pravidla, návrh opatření pro minimalizaci hrozeb jako nejčastější věci zahrnuje pravidelné školení personálu pracujícího s řídícími systémy také implementaci nejnovější verze antivirového softwaru, ostatní aspekty jako firewall a zálohování dat jsou v organizaci na dobré úrovni. Implementace návrhu je závislá na vedení organizace, a proto není předmětem této bakalářské práce, řešení je proto částečně navrhnuto jako spolupráce interního oddělení zabývajícího se kybernetickou bezpečností a externí firmy z důvodu více pohledů a přístupů k auditu, testování a samotné implementaci zmíněných prvků zabezpečení.

Seznam použité literatury

Odborná kniha

SVATÁ, Vlasta. *Audit informačního systému.* V Praze: Oeconomica, nakladatelství VŠE, 2016. 9 s. ISBN 978-80-245-2168-8.

SHAW, William T. *Cybersecurity for industrial scada systems.* 2nd ed. Tulsa: PennWell Books, 2020. ISBN 978-1-593-70506-0.

STOJANOVIĆ, Mirjana D. and Slavica V. BOSTJANCIC RAKAS. *Cyber security of industrial control systems in the future internet environment.* Hershey: PA – Information Science Reference, 2020. ISBN 978-1-799-82910-2.

ŠULC, Vladimír. *Kybernetická bezpečnost. Plzeň:* Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-8-073-80737-5.

SLÁMEČKA, Vladimír. *Manažerská etika: vysokoškolská učebnice.* Praha: České vysoké učení technické v Praze, 2012. ISBN 9788001050057.

KAFKA, Tomáš. *Průvodce pro interní audit a risk management.* Praha: C.H. Beck, 2009. 54 s. ISBN 978-80-7400-121-5

DOUCEK, Petr et al. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publisching: 2019. 54 s. ISBN 978-80-88260-39-4.

POŽÁR, Josef. *Základy teorie informační bezpečnosti.* Praha: Vydavatelství PA ČR, 2007. 58 s. ISBN 978-80-7251-250-8.

Elektronické dokumenty a ostatní

LIDINSKÝ, Vít. *EGovernment bezpečně* [online]. Praha: Grada, 2008 [cit. 2022-05-04]. ISBN 978-80-247-6355-2. Dostupné z: https://www.bookport.cz/kniha/egovernment-bezpecne-1710/

ISO 19011. *Guidelines for auditing management systems* 3. Geneva, Switzerland: International Organization for Standardization, 2018. https://www.iso.org/standard/70017.html

ISO 27032. *Security techniques* 1. Geneva, Switzerland: International Organization for Standardization, 2012. https://www.iso.org/standard/44375.html

ISO 31000. *Risk Management* 1. Geneva, Switzerland: International Organization for Standardization, 2010. https://www.iso.org/iso-31000-risk-management.html

Seznam zkratek

ISO	International Organization for Standardization
ISA	International Society of Automation
IEC	International Electrotechnical Commision
IT	Informační technologie
OT	Operační technologie
ICS	Industrial Control Systems
BAS	Building Automation Systems
DNS	Domain Name System
DHCP	Dynamic host configuration protocol
IPS	Intrusion Protection System
PLC	Programmable logic controller
RAM	Random-access memory
CPU	Central processing unit
SCADA	Supervisory Control and Data Aquisition
RTU	Remote terminal unit
DCS	Distributed control systems
HMI	Human-machine intervace
CND	Content delivery network
IoT	Internet of Things
ARP	Address Resolution Protocol
LAN	Local Area network
DMZ	Demilitarized zone
HTTP	Hypertext Transfer Protocol
FTP	File transfer protocol

TFTP	Trivial File Transfer Protocol
ROC	Remote Operations Center
UWB RTLS	UltraWideband Real-Time Location System