Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Systém pravidelné kontroly bezpečnostních nastavení řídicího systému MicroSCADA

Diplomová práce

Autor: Bc. Matěj Boura
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Ing. Vladimír Soběslav Ph.D.

Odborný konzultant: Ing. Michal Andrejčák
Hitachi Energy

Hradec Králové Prosinec 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 21.4.2024

Matěj Boura

Poděkování:

Děkuji vedoucímu diplomové práce doc. Ing. Vladimíru Soběslavi Ph.D. za metodické vedení práce a konzultantovi Ing. Michalu Andrejčákovi a celé firmě Hitachi Energy za spolupráci při tvorbě této práce.

Abstrakt

Klíčová slova: Kybernetická bezpečnost, Pravidelná kontrola, Hardening, Automatizace, Bezpečnostní audit

Tato diplomová práce se zaměřuje na vývoj automatizovaného systému pro kontrolu bezpečnostních nastavení systémů založených na platformě Windows, ve spolupráci s firmou Hitachi. Cílem je identifikovat a dokumentovat veškeré změny v bezpečnostních nastaveních od poslední kontroly a prezentovat je uživatelům ve srozumitelné formě. S ohledem na neustále se vyvíjející kybernetické hrozby a bezpečnostní rizika, zdůrazňuje tato práce důležitost pravidelného monitorování a aktualizace nastavení systému. V metodologii byl upřednostněn vývoj skriptů v PowerShellu, díky lepší integraci s Windows prostředím a efektivitě v automatizaci kontroly a analýzy. Dále se práce věnuje teoretické části, která poskytuje komplexní přehled o základech kyberbezpečnosti, s důrazem na její význam pro řídicí systémy v průmyslových aplikacích. Kromě toho je zde detailně rozebrána problematika kybernetických hrozeb vztahujících se k řídicím systémům. Tato sekce obsahuje analýzu různých typů kybernetických útoků, s kterými se mohou tyto systémy setkat, včetně případových studií a historických příkladů, které ilustrují potenciální dopady těchto hrozeb na průmyslové a infrastrukturní operace. Výstupem praktické části je poté systém, který zvyšuje efektivitu bezpečnostních kontrol a snižuje potenciál lidské chyby. Technikům, kteří ho používají, poskytuje přehled o stavu systémových nastavení a jejich změnách, což přispívá k lepší ochraně proti kybernetickým hrozbám a zvyšuje celkovou kybernetickou bezpečnost.

Abstract

Title: Regular control of safety settings of the MicroSCADA control system

Key words: Cybersecurity, Periodic Review, Hardening, Automation, Security Audit

This diploma thesis focuses on the development of an automated system for checking the security settings of Windows-based systems, in collaboration with Hitachi. The aim is to find and document any changes in security settings since the last check and present them to users in an understandable form. Given the ever-evolving cyber threats and security risks, the work emphasizes the importance of regularly checking and updating system settings. Script development in PowerShell was preferred method, due to its better integration with the Windows environment and its efficiency in automating scanning and analysis. Furthermore, the theoretical part of the thesis provides a comprehensive overview of the basics of cybersecurity, with emphasis on its relevance to control systems in industrial applications. In addition, the issue of cyber threats related to control systems is discussed in detail. This section includes an analysis of the diverse types of cyber-attacks that these systems may encounter, including case studies and historical examples that illustrate the potential impact of these threats on industrial and infrastructure operations. The outcome of the practical section is then a system that increases the effectiveness of security controls and reduces the potential for human error. It provides the technicians who use it with visibility into the status of system settings and changes to them, which contributes to better protection against cyber threats and enhances overall cybersecurity.

Obsah

1 Úvod ... 1

2 Cíl a metodika práce ... 3

2.1 Cíl práce ... 3

2.2 Metodika ... 3

3 Kybernetická bezpečnost průmyslových systémů ... 5

3.1 Základy kybernetické bezpečnosti ... 5

3.1.1 Historie ... 5

3.1.2 Teorie kybernetické bezpečnosti ... 9

3.1.3 Hardening systému ... 14

3.2 Řídící systémy ... 15

3.2.1 Architektura a zranitelnosti ICS ... 16

3.2.2 MicroSCADA ... 19

3.3 Kybernetické hrozby ... 21

3.3.1 Obecné ... 21

3.3.2 Specifické hrozby pro řídící systémy ... 24

4 Systém pravidelné kontroly s využitím nástrojů CIS ... 30

4.1 Tvorba systému ... 31

4.1.1 Výběr nástrojů ... 31

4.1.2 Skripty ... 37

4.2 Průzkum doporučených nastavení CIS ... 40

4.2.1 Inventář a kontrola podnikových aktiv ... 41

4.2.2 Inventář a kontrola softwarových aktiv ... 41

4.2.3 Ochrana dat ... 41

4.2.4 Zabezpečená konfigurace podnikových aktiv a softwaru ... 42

4.2.5 Správa účtů ... 42

4.2.6 Správa přístupových práv ... 42

4.2.7 Trvalá správa zranitelností ... 42

4.2.8 Správa protokolů auditu 43
4.2.9 Ochrana e-mailů a webových prohlížečů 43
4.2.10 Obrana proti malwaru 43
4.2.11 Obnova dat 43
4.2.12 Správa síťové infrastruktury 43
4.2.13 Monitorování a obrana sítě 43
4.2.14 Školení a zvyšování bezpečnostního povědomí 44
4.2.15 Správa poskytovatelů služeb 44
4.2.16 Bezpečnost aplikací 44
4.2.17 Řízení incidentů 44
4.2.18 Testování penetračními testy 44
4.2.19 Závěrečná doporučení 45
4.3 Průzkum výsledků CIS-CAT® Pro Assessor 46
5 Výsledky a závěr 49
6 Seznam použité literatury 51
7 Přílohy 54
7.1 Odkaz na adresář práce na GitHubu 55
7.2 Odkaz na adresář kontroly bezpečnostních nastavení na GitHubu 56
8 Zadání práce z IS (eVŠKP) 57

1 Úvod

Motivací pro vznik této práce byl zájem o kyberbezpečnost, který se skloubil se zájmy firmy Hitachi Energy, díky přednášce od odborného asistenta této práce Ing. Michaela Andrejčáka. Ten v rámci práce firmy Hitachi Energy identifikoval několik zajímavých problémů, které by si zasloužily bližší zkoumání. Jedním z nich byl právě systém automatické kontroly bezpečnostních nastaveních řídicích systémů, který mě zaujal nejvíce.

Bezpečnost řídicích systémů je v dnešní době klíčovým tématem, které si získává stále větší pozornost jak v průmyslových, tak v informačních technologiích. Řídicí systémy, jako je například MicroSCADA, představují kritickou infrastrukturu pro řízení a monitorování průmyslových procesů, energetických sítí, dopravních systémů a dalších oblastí. Jejich spolehlivost, dostupnost a bezpečnost jsou nezbytné pro udržení kontinuity provozu a minimalizaci rizik.

Důvody, proč je důležité se zabývat bezpečností řídicích systémů, jsou několikanásobné:

1. **Kybernetické hrozby:** S nárůstem propojenosti a digitalizace průmyslových systémů se zvyšuje i jejich exponovanost vůči kybernetickým útokům. Řídicí systémy mohou být cílem různých hrozeb, jako jsou ransomware, malware, nebo cílené útoky na kritickou infrastrukturu.
2. **Průmyslová bezpečnost:** Přerušení provozu nebo poškození průmyslových zařízení může mít vážné důsledky nejen ekonomické, ale i environmentální a lidské. Bezpečnostní opatření jsou nezbytná pro minimalizaci těchto rizik a ochranu před potenciálními nebezpečími.
3. **Regulační požadavky:** Státní orgány a regulační agentury po celém světě stanovují přísné požadavky na bezpečnost průmyslových systémů a kritické infrastruktury. Dodržování těchto předpisů je nejen povinností, ale i zárukou ochrany a stability.
4. **Důvěra a reputace:** Důvěra uživatelů a zákazníků v bezpečnost a spolehlivost řídicích systémů je klíčová pro úspěch podniku. Ztráta důvěry může mít vážné dlouhodobé dopady na reputaci organizace.

MicroSCADA je pokročilý softwarový systém pro řízení a monitorování průmyslových procesů, který byl vyvinut právě výše zmíněnou společností Hitachi Energy. Jedná se o robustní a spolehlivý řídicí systém, který poskytuje komplexní funkce pro správu a automatizaci energetických distribučních sítí, podzemních a nadzemních rozvodů elektrické energie a dalších infrastruktur.

V rámci řídicích systémů hraje MicroSCADA klíčovou roli, protože umožňuje monitorovat a řídit širokou škálu zařízení a procesů v energetickém sektoru. Jeho význam spočívá v několika klíčových bodech:

1. **Centralizovaná správa a kontrola:** MicroSCADA poskytuje uživatelům centrální místo pro správu a kontrolu všech zařízení a procesů v energetické infrastruktuře. To umožňuje operátorům efektivně monitorovat provoz a přijímat rychlé rozhodnutí v případě potřeby.
2. **Automatizace a optimalizace:** Díky pokročilým automatizačním funkcím MicroSCADA umožňuje optimalizaci provozu energetických sítí. Systém může automaticky řídit a optimalizovat různé procesy, což vede ke zvýšení efektivity a spolehlivosti provozu.
3. **Diagnostika a analýza:** MicroSCADA poskytuje uživatelům rozsáhlé diagnostické a analytické nástroje pro monitorování stavu zařízení a detekci případných problémů. To umožňuje provádět preventivní údržbu a minimalizovat riziko výpadků.
4. **Integrace:** MicroSCADA je navržen tak, aby byl snadno integrovatelný s dalšími systémy a zařízeními v energetickém sektoru. To umožňuje organizacím vytvářet komplexní a integrované řešení pro správu a řízení svých infrastruktur.

2 Cíl a metodika práce

2.1 Cíl práce

Cílem této práce je ve spolupráci s firmou Hitachi vyvinout automatizovaný systém, který by umožnil důkladnou prohlídku nastavení systémů, především pak systémů založených na platformě Windows. Hlavním úkolem tohoto systému je detekovat a zaznamenat veškeré změny, které nastaly v těchto nastaveních od poslední kontroly. Poté je ve srozumitelné formě prezentovat uživateli systému.

Kontrola bezpečnostních nastavení je klíčovým prvkem každé kybernetické bezpečnostní strategie. Vzhledem k neustálému vývoji hrozeb a bezpečnostních rizik je důležité pravidelně monitorovat a aktualizovat nastavení systému, aby byla zajištěna maximální úroveň bezpečnosti.

Tento automatizovaný přístup má několik výhod. Za prvé, eliminuje lidský faktor a možnost chyb, které by mohly vzniknout při manuálním prozkoumávání nastavení. Za druhé, umožňuje pravidelnou a systematickou kontrolu bezpečnostních nastavení, což je klíčové pro udržení vysoké úrovně kybernetické bezpečnosti. A za třetí, výrazně snižuje dobu potřebnou k dané kontrole.

2.2 Metodika

Ze začátku spolupráce vzniklo několik skriptů v jazyce Python, který byl vybrán jakožto pravděpodobně nejmohutnější skriptovací jazyk. Ale z důvodu plánu Hitachi používat tento software na širokém množství počítačů a nepohodlnost, kterou by přinášela nutnost na nich instalovat Python, bylo od této metodiky odpuštěno.

Místo toho se hlavní částí této práce stal vývoj skriptů v PowerShellu, což bylo motivováno potřebou efektivního nástroje pro automatizovanou kontrolu a analýzu bezpečnostních nastavení. PowerShell byl zvolen kvůli jeho silné integraci s Windows prostředím a schopnosti přímého interagování s WMI (Windows Management Instrumentation) a dalšími Windows API pro získání detailních informací o systémových nastaveních a konfiguracích.

Skripty pracují na principu extrakce aktuálních nastavení systému, která jsou následně srovnávána s předchozími stavy tohoto nastavení. To umožňuje identifikovat neautorizované nebo podezřelé změny, které by mohly naznačovat bezpečnostní rizika nebo probíhající útoky. Srovnávací mechanismus je klíčový pro detekci odchylek, které

jsou následně analyzovány a prezentovány administrátorům nebo bezpečnostním týmům využívající tento program.

Z obdobného důvodu jako změna na PowerShell vznikl konečný způsob pro ukládání výsledků kontroly i rozdílů. Jelikož firma Hitachi silně preferuje nástroje Microsoftu, které jsou integrované do operačního systémů Windows, tak se výsledky a následně i porovnání výsledků a tabulky s jejich rozdíly ukládají do databáze Access. Nutno také podotknout, že toto byla první zkušenost autora s touto databází.

Automatizace procesu srovnávání nastavení pomocí vytvořených skriptů výrazně zvyšuje efektivitu a tím umožňuje větší pravidelnost bezpečnostních kontrol. Eliminuje se tím lidský faktor a potenciální chyby při manuální analýze, kde je snadné některou změnu ve velkém množství dat přehlédnout nebo opomenout.

Kritická revize existující literatury a výzkumných prací v oblasti kybernetické bezpečnosti a automatizovaných systémů kontroly byla nezbytná pro definování problému a navržení řešení. Zdroje zahrnovaly odborné články, bezpečnostní bulletiny, jakožto i dokumentaci od předních výrobců softwaru a bezpečnostních řešení.

V rámci této práce byl kladen důraz na využití pokročilých nástrojů umělé inteligence (AI), zejména velkých jazykových modelů, jako jsou ChatGPT, Perplexity.AI a SciSpace, pro podporu v diskusi o obsahu a výběru vhodných zdrojů. Tyto nástroje umožňují efektivně prozkoumávat a analyzovat rozsáhlé objemy literatury a výzkumných materiálů s vysokou přesností a v krátkém čase. ChatGPT byl využíván pro generování návrhů textů, získávání přehledů o specifických tématech a odpovědí na otázky týkající se kyberbezpečnosti a řídicích systémů. Perplexity.AI poskytovala podporu při hledání nejnovějších výzkumných článků a publikací, zatímco SciSpace umožňoval přístup k širokému spektru akademických databází a publikací. Integrace těchto AI nástrojů do procesu výzkumu a analýzy zvýšila schopnost identifikovat relevantní teoretické rámce, aktuální výzkumy a nejnovější poznatky v oblasti.

3 Kybernetická bezpečnost průmyslových systémů

V této kapitole je prezentován komplexní přehled základů kyberbezpečnosti, který je zásadní pro pochopení a řešení bezpečnostních výzev souvisejících s řídicími systémy, jako je MicroSCADA. Historický kontext kyberbezpečnosti, který je zde uveden, nám poskytuje ucelený pohled na vývoj a evoluci bezpečnostních hrozeb a obranných strategií. Následně je podrobně zkoumána teorie kyberbezpečnosti, včetně důležitých principů, modelů a standardů, které formují současné bezpečnostní praxe.

Dále je věnována pozornost řídicím systémům, s detailním pohledem na MicroSCADA, jeho význam, funkce a místo v infrastruktuře průmyslových a energetických podniků. Speciální pozornost je věnována tomu, jak jsou principy kyberbezpečnosti aplikovány na tyto kritické systémy k zajištění jejich bezpečného a spolehlivého provozu.

V poslední části této kapitoly jsou zkoumány kybernetické hrozby, přičemž je rozlišováno mezi obecnými hrozbami, kterým čelí většina IT systémů, a specifickými hrozbami pro řídicí systémy. Různé typy útoků, s kterými se mohou tyto systémy setkat, jsou zde zkoumány, a jsou prezentovány strategie a opatření, které mohou pomoci tyto hrozby zmírnit nebo odvrátit.

Cílem této kapitoly je poskytnout čtenářům pevný teoretický základ, na němž mohou být postaveny praktické znalosti pro návrh a implementaci efektivních bezpečnostních řešení, specificky orientovaných na ochranu a obranu řídicích systémů před narůstajícími kybernetickými hrozbami.

3.1 Základy kybernetické bezpečnosti

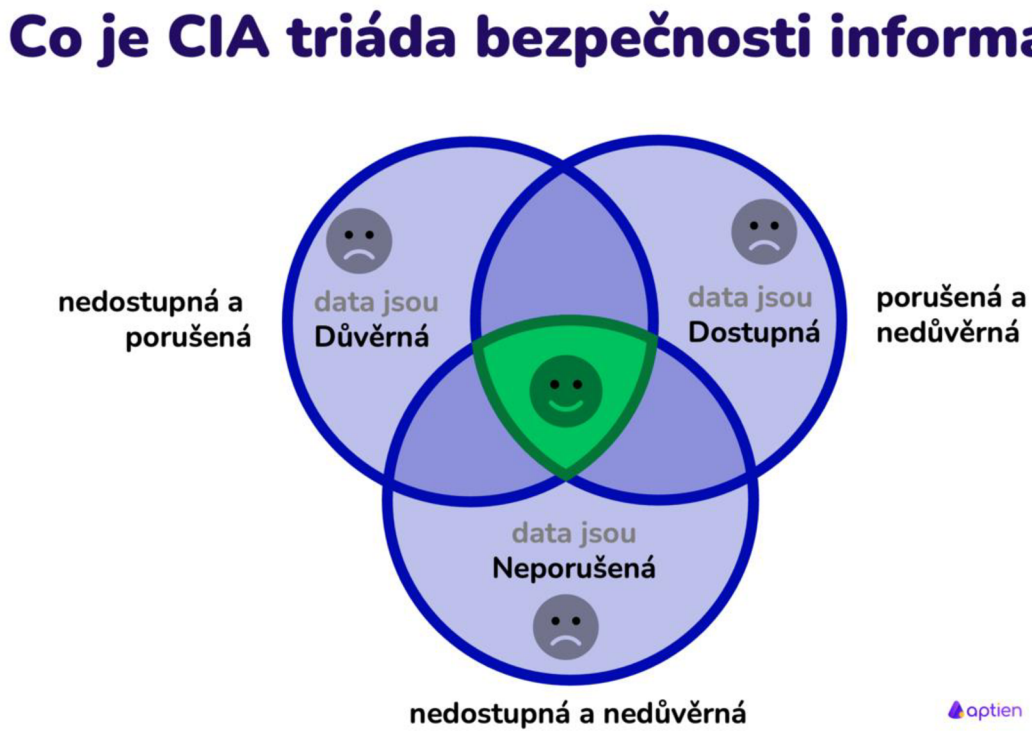
3.1.1 Historie

Historie kybernetické bezpečnosti sahá až do 70. let 20. století, kdy Bob Thomas vytvořil první počítačový virus "Creeper virus". Tento experimentální samo replikující se program nebyl škodlivé povahy; byl vytvořen za účelem demonstrace šířící se aplikace. Creeper se pohyboval po síti ARPANET (předchůdce internetu) a zobrazoval zprávu: "I'm the creeper, catch me if you can!". To vedlo k vytvoření programu "Reaper", který lze považovat za první antivirový software, protože jeho účelem bylo odstranit Creepera následovala i první formalizace termínu kyberbezpečnosti v 80. letech (Tarhan, 2023).

Vznik programů Creeper a Reaper upozornil na možnost autonomního šíření softwaru v sítích a připravil půdu pro odvětví kybernetické bezpečnosti. Ukázal potřebu

mechanismů na ochranu sítí a systémů před neautorizovaným nebo škodlivým softwarem. V průběhu let, kdy se počítačové sítě stávaly složitějšími a rozšířenějšími, se vyvíjela i povaha hrozeb, což si vyžádalo vývoj sofistikovanějších opatření kybernetické bezpečnosti. Postupem času se kybernetická bezpečnost vyvinula v kritický globální bezpečnostní problém, na němž se podílejí různí aktéři, jako jsou státy, technologické společnosti a uživatelé. Vznik kyberprostoru jako základního životního prostoru dále zdůraznil význam kybernetické bezpečnosti při ochraně kritické infrastruktury a sítí. Kybernetická bezpečnost přešla z primárního zájmu armády a zpravodajských služeb do širší oblasti zahrnující nestátní aktéry, jako jsou zločinci a teroristé, a také soukromé podniky (Alam, 2024).

V roce 1977 vznikla triáda CIA, práce Ruthberga a McKenzieho. CIA triáda je základním konceptem v oblasti kybernetické bezpečnosti, který definuje tři základní cíle ochrany informací. Každý prvek této triády představuje klíčovou složku, která je nezbytná pro celkovou bezpečnost informačních systémů a sítí (Alam, 2024), jak lze vidět na Obrázek 1.



Obrázek 1: CIA triáda (Aptien, 2023; převzato a upraveno)

Tato triáda je dodnes velmi oblíbeným způsobem, jak jednoduše informovat zákazníky, nebo jiné méně zdatné jedince v oblasti informačních technologií, jaké základní prvky by měla kyberbezpečnost zajišťovat (Bhagwani & Balasinorwala, 2023). Proto bude

představena blíže i zde. Bližší popis jejích stavebních kamenů i se základy, jak je uvést do praxe:

- Důvěrnost (=Confidentiality)
    - Potřeba zabránit tomu, aby se důvěrné informace a údaje dostaly do nepovolaných rukou. Důvěrnost se zabývá přístupem, provozem a zveřejněním prvků systému.
    - V praxi dnes obvykle zajištěno šifrováním dat, které zajistí, aby neoprávnění uživatelé nemohli získat nebo zpřístupnit data, ke kterým nemají oprávnění. Řízení přístupu je také nezbytnou součástí zachování důvěrnosti tím, že řídí, kteří uživatelé mají oprávnění k přístupu k datům (Bhagwani & Balasinorwala, 2023).
- Integrita (=Integrity)
    - Informace a data by neměla být poškozena nebo upravena třetí stranou bez oprávnění. Integrita se zabývá úpravou, manipulací a zničením prvků systému.
    - V praxi je pro zajištění integrity dat důležitá správa protokolů událostí (Event Log), kde lze zpozorovat kdykoli dojde k bezpečnostnímu incidentu. Zavedení kontroly verzí a auditů v IT struktuře organizace je dalším způsobem, jak lze zajistit, že jsou data původní (Bhagwani & Balasinorwala, 2023).
- Dostupnost (=Availability)
    - Informace a data by měly být neustále k dispozici a měly by být zavedeny adaptivní mechanismy obnovy pro obnovení systému a služeb poskytovaných systémem. Dostupnost se zabývá přítomností, dostupností, připraveností a kontinuitou služeb prvků systému.
    - V praxi může pomoci s dostupností udržování softwarových aktualizací, Monitorování šířky pásma sítě a Vytváření a aktualizace plánů kontinuity podnikání, které v případě výpadku minimalizují dobu výpadku a udržují dostupnost kritických systémů (Bhagwani & Balasinorwala, 2023).

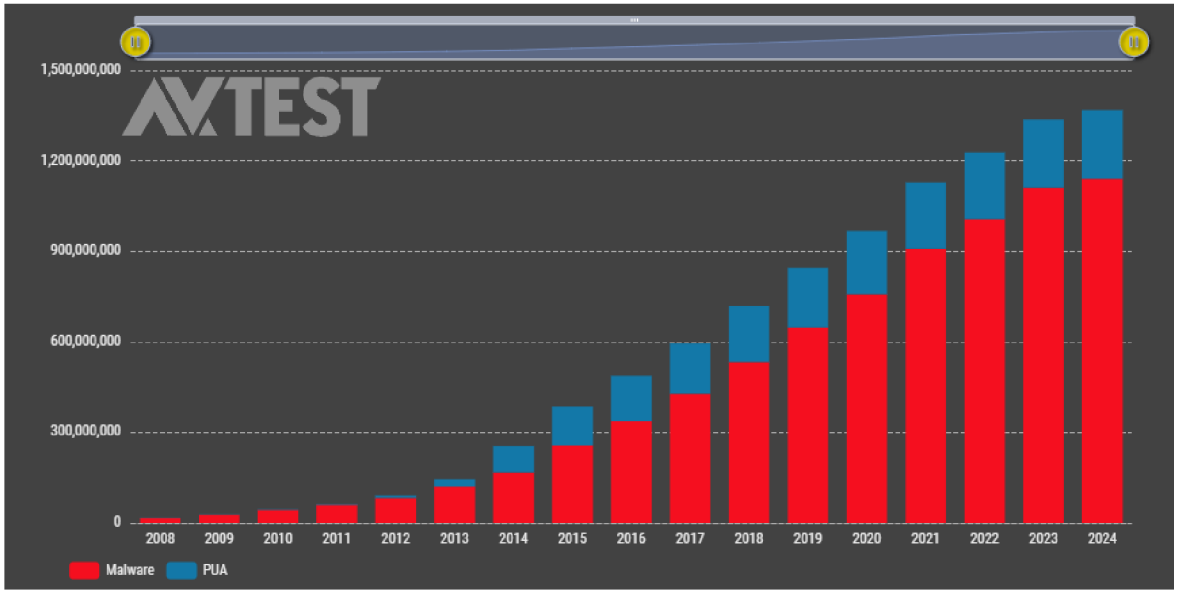
V 80. letech se z ARPANETu (první rozsáhlé sítě) stal internet. S tím, jak se počítače začaly více propojovat, se zdokonalovaly počítačové viry. Morrisův červ vyvinutý v roce 1988 se stal výchozím bodem pro tvorbu účinnějších červů a virů. Tento vzestup

vedl k vývoji antivirových řešení jako prostředku proti útokům červů a virů (Alam, 2024).

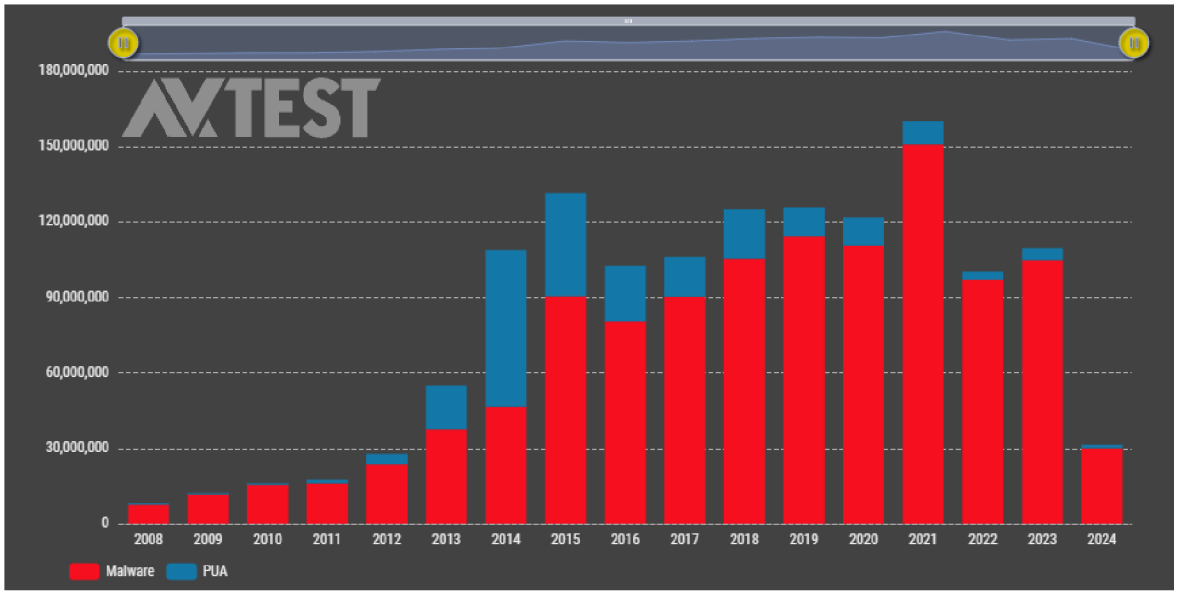
V 90. letech 20. století způsobily viry jako Melissa selhání e-mailových systémů tím, že infikovaly desítky milionů počítačů. Tyto útoky mají většinou finanční a strategické cíle. V 90. letech 20. století také došlo k prudkému nárůstu antivirových společností. Tyto antivirové produkty trpěly spotřebou velkého množství dostupných zdrojů a produkovaly velké množství falešně pozitivních výsledků (Alam, 2024).

S rostoucím výpočetním výkonem počítačů se v roce 2000 objevil sofistikovaný škodlivý software, například polymorfní a metamorfní škodlivé programy. Tyto dva typy mohou měnit svůj tvar a strukturu pomocí různých složitých modulů a provádět tak škodlivé činnosti. Tyto a další skryté škodlivé programy pronikly i na nové platformy, jako jsou chytré telefony a IoT (internet věcí) atd. Stuxnet vytvořený v roce 2010 byl prvním armádním malwarem a jedním z prvních případů, kdy byly kybernetické útoky využity ke špionáži. Stuxnet se šířil pomocí infikovaného vyměnitelného disku, například USB flash disku. Tento disk obsahoval soubory zástupců systému Windows, které iniciovaly škodlivý spustitelný kód (Alam, 2024).

V poslední době se zvyšuje počet útoků tzv. ransomwaru (škodlivého softwaru, který vyhrožuje oběti zveřejněním nebo zablokováním přístupu k jejím datům, pokud nezaplatí výkupné), např. WannaCry, Clop Ransomware a Mount Locker. Vzhledem k probíhající digitalizaci a zrychlování hardwaru se útočníci začali zaměřovat také na hardware, a to pomocí zadních vrátek, trojských koní a side-channel útoky. S rozvojem nových technologií, jako je umělá inteligence, začali výzkumní pracovníci i průmysl tyto nové technologie používat k analýze a pochopení kybernetických útoků a ke zlepšení obrany proti nim. Zároveň ale i útočníci využívají podobné techniky k rozvoji svých kybernetických útoků. Jak lze vidět na Obrázek 2, tak absolutní počet malwaru a potenciálně nechtěných aplikací (PUA = potentially unwanted applications) neustále roste. Lepší zprávou je, že růst přestal akcelerovat s rychlostí, kterou měl před rokem 2015, jak lze vidět na Obrázek 3.



Obrázek 2: Absolutní počty malwaru (=červená) a PUA (=modrá) (AV-ATLAS, 2024; převzato a upraveno)



Obrázek 3: Růst malwaru (=červená) a PUA (=modrá) (AV-ATLAS, 2024; převzato a upraveno)

3.1.2 Teorie kybernetické bezpečnosti

Nejdříve je třeba definovat co termín kyberbezpečnost znamená, dle práce C. P. Pfleegera, S. L. Pfleegera a J. Margulies by se dala kyberbezpečnost definovat takto: "Počítačová bezpečnost je ochrana cenných věcí, tzv. aktiv počítače nebo počítačového systému. Existuje mnoho typů aktiv zahrnujících hardware, software, data, lidi, procesy nebo jejich kombinace. Abychom mohli určit, co je třeba chránit, musíme nejprve určit, co má hodnotu a pro koho." (Pfleeger et al., 2015)

Podobnou definici lze vyčíst i z novější práce Ujjwala Raa. "Kybernetická bezpečnost je soubor nástrojů, politik, bezpečnostních koncepcí, bezpečnostních záruk, pokynů,

přístupů k řízení rizik, opatření, školení, osvědčených postupů, zajištění a technologií, které lze použít k ochraně kybernetického prostředí a majetku organizace a uživatelů. Aktiva organizace a uživatele zahrnují připojená výpočetní zařízení, personál, infrastrukturu, aplikace, služby, telekomunikační systémy a souhrn přenášených a/nebo uložených informací v kybernetickém prostředí."(Ujjwal Rao, 2023)

Tato definice je již více prakticky zaměřená, což je i směr, kterým se vydává tato práce. Jak bylo ukázáno na konci předešlé podkapitoly, počet útoků stále roste, a proto nastává otázka, co je nejlepší kyberbezpečností strategií. Dle Ujjwala Raa je potřeba silná bezpečnostní infrastruktura, která zahrnuje více vrstev ochrany rozptýlených v počítačích, programech i počítačových sítích. Vzhledem k tomu, že ke kybernetickým útokům dochází každých 14 sekund (Ujjwal Rao, 2023), musí firewally, antivirový software, antispywarový software a nástroje pro správu hesel pracovat v souladu, aby přelstily překvapivě kreativní útočníky. Vzhledem k tomu, že v sázce je tolik věcí, není nadsázkou si myslet, že nástroje a odborníci na kybernetickou bezpečnost fungují jako poslední obranná linie mezi našimi nejdůležitějšími informacemi a digitálním chaosem (Ujjwal Rao, 2023).

Zbytek práce se bude později věnovat primárně zabezpečení operačního systému skrze tzv. hardening, česky kalení nebo zpevnění, kdy dochází k odstraňování a eliminaci možných bezpečnostních rizik skrze minimalizaci zranitelností operačního systému přes vhodné nastavení tohoto OS. Proto nyní budou jen stručně představeny zbylé části, které by měla tato struktura obsahovat.

3.1.2.1 Firewall

Protipožární stěny, což je překlad anglického slova Firewall, v budovách, jak už jejich název napovídá, jsou stěny, které mají bránit šíření požáru z jedné části budovy do druhé, například mezi jedním a druhým bytem. Protipožární stěny jsou postaveny z materiálů, které odolávají požárům určité intenzity nebo trvání, čímž brání šíření požáru, ale nezaručují ani nejsou určeny k zastavení obzvláště intenzivního požáru. Síťové brány firewall jsou podobná zařízení pro zabezpečení počítačů, která chrání jednu podsíť před poškozením z jiné podsítě. Primárním účelem firewallu je chránit vnitřní podsíť před hrozbami z internetu. Firewally lze také použít k oddělení segmentů vnitřní sítě, například k zachování vysoké důvěrnosti citlivé výzkumné sítě v rámci větší organizace (Pfleeger et al., 2015).

Firewall se běžně implementuje ve více místech. V rámci operačních systémů (jako jsou Windows, macOS, Linux) má integrovaný firewall, který chrání zařízení před nežádoucím přístupem z internetu nebo lokální sítě. Tento se týká také hardeningu OS, takže bude probrán podrobněji v dalších kapitolách. Dalšími místy kde se používá firewall jsou:

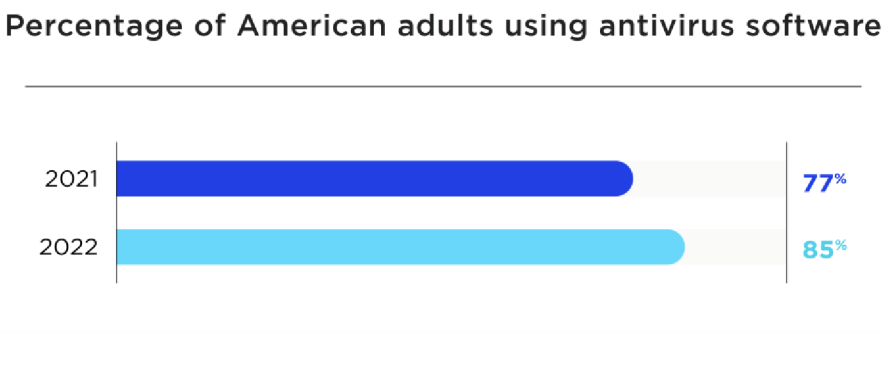
1. Domácí a kancelářské routery: Mnoho domácích a kancelářských routerů má vestavěné firewally, které chrání celou síť před vnějšími hrozbami. Tyto firewally mohou být konfigurovány k blokování nebo povolení provozu na specifických portech.
2. Podnikové sítě: V podnikovém prostředí se firewally implementují na hranicích mezi vnější sítí (např. internetem) a interní podnikovou sítí. Tyto firewally jsou často robustnější a nabízejí rozsáhlejší možnosti konfigurace než domácí routerové firewally.
3. Datová centra: V datových centrech jsou firewally používány k ochraně uložených dat a zajištění bezpečného přístupu k cloudovým službám a hostovaným aplikacím. Mohou být implementovány jako součást fyzické infrastruktury nebo jako virtuální firewally v cloudovém prostředí.
4. Cloudové služby a infrastruktura: Cloudoví poskytovatelé nabízejí firewally jako součást svých bezpečnostních služeb pro ochranu cloudových aplikací a služeb. Tyto firewally lze konfigurovat k ochraně virtuálních serverů a služeb běžících v cloudu.
5. Aplikační firewally (WAF – Web Application Firewalls): Tyto firewally jsou speciálně navrženy pro monitorování, filtrování a blokování škodlivého provozu k webovým aplikacím. Implementují se buď na hardwarových zařízeních, nebo jako cloudové či softwarové řešení (Cloudflare, 2024).

3.1.2.2 Antivirový, antispywarový software a skenery malwaru

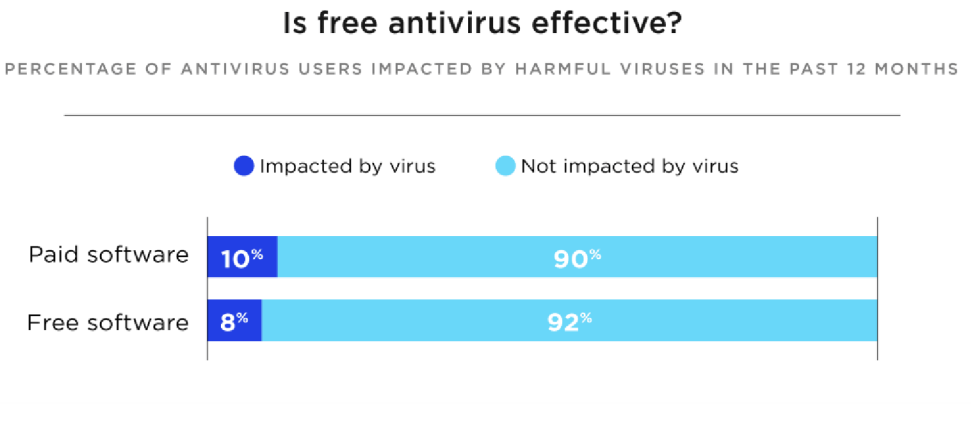
Antivirový software je počítačový program, který detekuje škodlivé programy, jako jsou viry a červy, zabraňuje jim a přijímá opatření k jejich zneškodnění nebo odstranění. Většina antivirových programů obsahuje funkci automatické aktualizace, která umožňuje programu stahovat profily nových virů, aby mohl kontrolovat nové viry, jakmile jsou objeveny (cs.theastrologypage.com, 2024). Antivirový program je nezbytnou a základní potřebou každého systému (Ujjwal Rao, 2023).

Antispywarový software je typ bezpečnostního programu určený k ochraně počítačů a mobilních zařízení před spywarem a dalšími druhy škodlivého softwaru. Spyware je druh malware, který se tajně instaluje na počítači nebo mobilním zařízení bez vědomí uživatele s cílem shromažďovat informace o jeho aktivitách, sbírat osobní údaje, zachytávat klávesové údery atd. a posílat tyto informace třetím stranám bez souhlasu uživatele.

Skenery malwaru jsou software, který obvykle skenuje všechny soubory a dokumenty přítomné v systému a hledá v nich škodlivý kód nebo viry. Viry, červi a trojské koně jsou příklady škodlivého softwaru, které se často sdružují do skupin a označují jako malware. (Ujjwal Rao, 2023) Obvykle jsou součástí antivirového softwaru jako takového. Často obsahují i možnost hloubkové kontroly, která probíhá mimo operační systém. Ze statistik (Security.org Team, 2023) webu security.org provedených v roce 2023 lze vyčíst několik zajímavých informací o používání antivirového softwaru. Ty pozitivnějších z nich poukazují na růst v používání tohoto druhu softwaru, viz Obrázek 4, nebo na vysokou míru efektivity neplacených verzí softwaru Obrázek 5, kde se nejčastěji používá Microsoft Defender, který je defaultně předinstalovaným řešením u operačních systémů Windows.



Obrázek 4: Trend používání antivirového softwaru (Security.org Team, 2023; převzato a upraveno)



Obrázek 5: Efektivita neplacených vs placených antivirových softwaru (Security.org Team, 2023; převzato a upraveno)

3.1.2.3 Šifrování dat

Další velmi důležitou součástí kyberbezpečnosti je šifrování, což je proces, při kterém jsou data převedena do formy, kterou nelze snadno přečíst bez odpovídajícího dešifrovacího klíče. Používá se k ochraně důvěrnosti dat jak v off-line prostředí (uložených na disku), tak on-line prostředí (odesílaných přes internet). Dnes je šifrování nezbytnou součástí ochrany osobních údajů, finančních informací, a obchodních tajemství před kyberzločinci. Kromě toho je šifrování klíčovým prvkem pro zajištění integrity a autentizace, což zabraňuje neoprávněným změnám dat (Boura, 2022).

Typy šifrování:

- Symetrické šifrování: Používá stejný klíč pro šifrování a dešifrování. Je rychlé a vhodné pro šifrování velkého množství dat, ale sdílení klíče může být výzvou (Boura, 2022).
- Asymetrické šifrování (veřejný a soukromý klíč): Používá dva klíče – jeden pro šifrování (veřejný klíč) a druhý pro dešifrování (soukromý klíč). Toto řešení umožňuje bezpečné sdílení šifrovacího klíče, ale je pomalejší než symetrické šifrování (Boura, 2022).

Použití v praxi:

- HTTPS: Používá šifrování pro zabezpečení komunikace mezi webovým prohlížečem a serverem (Boura, 2022).
- VPN (Virtuální soukromá síť): Šifruje data odesílaná mezi uživatelem a VPN serverem, čímž chrání data při přenosu přes veřejné sítě (Boura, 2022).

- Šifrování disku: Chrání data uložená na fyzických médiích, zajišťuje, že data jsou nečitelná bez správného šifrovacího klíče (Boura, 2022).

3.1.3 Hardening systému

Zabezpečení prostřednictvím hardeningu systému je klíčovým krokem v ochraně informačních systémů a sítí před kybernetickými útoky. Kalení systému zahrnuje soubor opatření a technik zaměřených na snížení potencionálního povrchu útoku a eliminaci známých slabých míst v systému. Tato kapitola se věnuje analýze hardeningu na různých úrovních informačních systémů. Zahrnuje to implementaci bezpečnostních opatření a konfigurací na hardware, software i síťové komponenty. Tento proces je nezbytný pro ochranu informačních systémů a infrastruktury před kybernetickými útoky. Představeny budou konkrétní aplikace na IoT zařízeních a elektrických distribučních systémech, které jsou rovněž i specifickým cílem Hitachi Energy (Fard et al., 2022).

3.1.3.1 Hardening IoT zařízení

IoT zařízení představují značné bezpečnostní riziko kvůli rychlému nasazení a často nedostatečným bezpečnostním funkcím. Seul-Ki Choi, Chung-Huang Yang a Jin Kwak (Choi et al., 2018) zdůrazňují význam hardeningu a monitorování bezpečnosti pro IoT zařízení, která postrádají bezpečnostní design, což je činí náchylnějšími k útokům, jako byl Mirai Botnet, tento útok dokázal plně převzít kontrolu nad vestavěnými Linux zařízeními a poté je použít k DDOS útokům. Navrhované schéma v práci (Choi et al., 2018) má za cíl minimalizovat bezpečnostní zranitelnosti tím, že na IoT zařízeních nasadí základní bezpečnostní funkce, čímž se zlepší bezpečnost prostředí služeb IoT prostřednictvím hardeningu systému a monitorování bezpečnosti.

3.1.3.2 Hardening elektrických distribučních systémů

Zaměřením se na elektrické distribuční systémy, se skupina složena z Mahan Fakouri Fard, Mostafa Sahraei-Ardakani, Ge Ou a Mingxi Liu, snažila řešit výzvu zajištění bezpečnosti energetických systémů před katastrofickými přírodními událostmi, zejména před zemětřeseními. Navrhují nový rámec pro hardening hardwaru distribučních sítí, který využívá křivky křehkosti síťového vybavení k reprezentaci pravděpodobností selhání při zemětřeseních. Práce má za cíl zlepšit odolnost distribučních sítí tím, že identifikuje optimální strategie hardeningu prostřednictvím analýzy odolnosti a ekonomických analýz. Navrhovaný přístup zvyšuje odolnost a

zajišťuje dodávku základní zátěže během zemětřesení a po něm, jak bylo prokázáno simulacemi na zkušebním napáječi IEEE 33 (Fard et al., 2022).

3.1.3.3 Hardening jako multiobjektivní optimalizační problém

Poslední prací pomáhající definovat problémy a rámce hardeningu je práce Rinku Dewri, Nayot Poolsappasit, Indrajit Ray a Darrell Whitley. Ta představuje přístup k hardeningu systému jako k multiobjektivnímu optimalizačnímu problému, kde rozhodnutí o implementaci bezpečnostních opatření vyvažuje náklady a potenciální snížení rizika. Tento pohled umožňuje organizacím nalézt optimální rovnováhu mezi zabezpečením a provozními omezeními, což zdůrazňuje význam strategického plánování v úsilí o zpevnění systému. Studie rovněž zdůraznila důležitost pochopení vlivu hodnot vah na cíle společností při rozhodování (Dewri et al., 2007).

3.2 Řídící systémy

Moderní průmyslové řídicí systémy (Industrial Control Systems – ICS) hrají klíčovou roli v automatizaci a kontrole průmyslových procesů napříč různými sektory, včetně výroby elektrické energie, chemické produkce a distribuce vody. Tyto systémy se stále více propojují s internetem, což přináší zvýšenou pozornost k jejich kybernetické bezpečnosti. Bezpečnost ICS je komplikována používáním mikroprocesorů, adopcí komunikačních standardů a protokolů, a složitými distribuovanými síťovými architekturami, což činí ICS zranitelnými vůči kybernetickým útokům (McLaughlin et al., 2016).

ICS se odlišuje od tradičních IT systémů v mnoha ohledech, včetně jejich primárního cíle udržet integritu průmyslových procesů a potřeby vysoké dostupnosti. Interakce s fyzickými procesy jsou zásadní a často komplexní, což znamená, že tradiční IT bezpečnostní řešení nemusí být vhodná pro ICS. To zdůrazňuje potřebu specifických bezpečnostních postupů pro ochranu těchto systémů (McLaughlin et al., 2016).

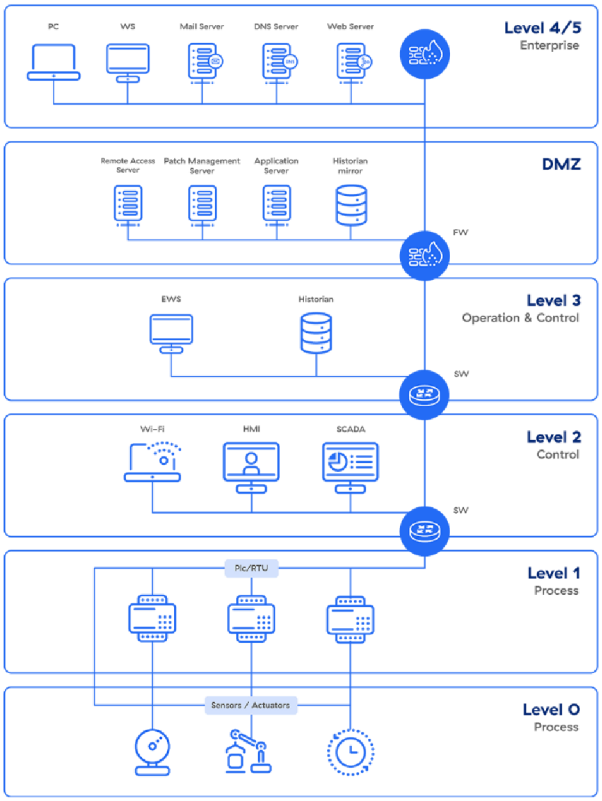
Kromě toho, přestože se moderní směrnice pro kybernetickou bezpečnost zaměřují na ochranu IT infrastruktur, často nezohledňují unikátní aspekty a potřeby řídicích systémů. V důsledku toho vzniká potřeba vytvořit základní směrnice pro zvýšení kybernetické bezpečnosti ICS. To zahrnuje znalost, omezení a monitorování přístupu k systémům, implementaci odpovídající bezpečnosti pro každou úroveň řídicího systému, nepřetržité monitorování systému na všech úrovních a mít kontingenční plán pro případ kybernetických útoků (Smith et al., 2016).

3.2.1 Architektura a zranitelnosti ICS

Architektura průmyslových řídicích systémů je založena na Purdue Enterprise Reference Architecture, známé také jako Purdue Model. Tento model rozděluje systémy typických ICS do úrovní a zón, přičemž každá zóna představuje samostatnou funkční oblast systému:

- Úroveň 0: Fyzické procesy probíhající v zařízení, včetně senzorů, motorů, čerpadel a ventilů.
- Úroveň 1: Inteligentní zařízení monitorující a kontrolující fyzické procesy, jako jsou programovatelné logické regulátory (PLC) a systémy pro bezpečnostní instrumentaci (SIS).
- Úroveň 2: Systémy pro dohled a monitorování fyzických procesů, včetně rozhraní člověk-stroj (HMI) a inženýrských pracovišť.
- Úroveň 3: Systémy pro řízení výroby na úrovni celého závodu, jako jsou systémy pro historii dat a řídicí servery.
- Průmyslová demilitarizovaná zóna (DMZ): Odděluje IT a OT prostředí a obsahuje služby jako jsou proxy servery.
- Úroveň 4: Systémy pro plánování a logistiku, včetně serverů aplikací a e-mailových klientů.
- Úroveň 5: Síť podniku pro výměnu dat o výrobě a zdrojích.

Purdue Model zjednodušuje komplexitu ICS tím, že je rozděluje do spravovatelných částí, umožňuje lepší porozumění a zabezpečení jednotlivých komponent. Adaptace Purdue Modelu na vysoké úrovni a hlavní prvky této architektury jsou znázorněny na Obrázek 6. Na základě výše uvedené adaptace Purdueova modelu lze typické prostředí rozdělit na sítě IT a OT. První zahrnuje běžné osobní počítače, aplikační servery, e-mailové servery, systémy ERP atd. V současné době pozorujeme zřetelné sbližování dělení sítí OT a IT. Proto lze v oblasti OT nalézt standardní IT komponenty, jako jsou stolní počítače, a průmyslová zařízení komunikující buď prostřednictvím standardních protokolů, jako je TCP/UDP, nebo prostřednictvím průmyslových protokolů (Makrakis et al., 2021).



Obrázek 6: Purdue Model (ZscalerTM, 2024; převzato a upraveno)

Zranitelnosti těchto systémů se dají stejně dobře zařadit do vrstev:

1) Hardwarová vrstva: Vložené komponenty, jako jsou PLC a RTU, jsou hardwarové moduly provádějící software. Do těchto modulů lze zavést hardwarové útoky, jako je například fault injection a backdoors. Tyto zranitelnosti v hardwaru mohou protivníci zneužít k získání přístupu k uloženým informacím nebo k odepření služeb. Zranitelnosti na úrovni hardwaru se týkají celého životního cyklu ICS od návrhu až po likvidaci. Bezpečnost v dodavatelském řetězci procesorů je velkým problémem, protože hardwarové trojské koně mohou být vloženy v kterékoli fázi dodavatelského řetězce, což přináší potenciální rizika, jako je ztráta spolehlivosti a bezpečnosti (McLaughlin et al., 2016).
2) Vrstva firmwaru: Firmware se nachází mezi hardwarem a softwarem. Obsahuje data a instrukce schopné řídit hardware. Funkce firmwaru sahají od zavádění hardwaru a poskytování služeb pro běh až po načítání operačního systému (OS). Vzhledem k omezením souvisejícím s v reálném čase fungujícími integrovanými bezpečnostními systémy, používají systémy řízené firmwarem obvykle operační systém reálného

času (RTOS), jako je např. VxWorks. V každém případě mohou být zranitelnosti ve firmwaru zneužity protivníky k abnormálnímu ovlivnění procesu ICS. V nedávné studii byly zneužity zranitelnosti ve firmwaru bezdrátového přístupového bodu a řídicí jednotky recloseru. Škodlivý firmware může být distribuován z centrálního systému v pokročilé měřicí infrastruktuře (AMI) do inteligentních měřičů. Je zřejmé, že zranitelnosti ve firmwaru mohou být využity k útokům DOS, které narušují provoz ICS (McLaughlin et al., 2016).

3) Softwarová vrstva: Zranitelnosti v softwarové základně mohou sahat od jednoduchých chyb v kódování až po špatnou implementaci mechanismů řízení přístupu. Podle ICS-CERT je nejvyšší procento zranitelností v produktech ICS nesprávná validace vstupu softwarem ICS, známá také jako zranitelnost přetečení bufferu. Na druhém místě je špatná správa pověření a na třetím slabiny v autentizaci. Tyto zranitelnosti v implementaci softwarových rozhraní (např. HMI) a konfiguracích serverů mohou mít fatální důsledky na řídicí funkce ICS. Například proprietární software průmyslové automatizace pro historické servery měl zranitelnost přetečení zásobníku haldy, která mohla potenciálně vést k útoku typu Stuxnet. Sofistikovaný malware často zahrnuje jak hardware, tak software. Zranitelnosti WebGL jsou příkladem softwarových útoků s hardwarovou podporou: přístup ke grafickému hardwaru GPU nejméně privilegovanou vzdálenou stranou vede k odhalení paměťových obsahů GPU z předchozích pracovních úloh (McLaughlin et al., 2016).
4) Síťová vrstva: Zranitelnosti mohou být do sítě ICS zaneseny různými způsoby: Přes firewally, které chrání zařízení v síti monitorováním a kontrolou komunikačních paketů pomocí zásad filtrování. Nebo přes modemy, které převádějí sériová digitální data na signál vhodný pro přenos po telefonní lince, aby zařízení mohla komunikovat. Další možností je sběrnicová síť, která propojuje snímače a další zařízení s PLC nebo jinou řídicí jednotkou. Komunikační systémy a směrovače, které přenášejí zprávy mezi dvěma sítěmi mohou být další cestou pro malware do sítě, stejně jako vzdálené přístupové body. I protokoly a řídicí síť, které propojují úroveň supervizora s řídicími moduly nižší úrovně,

mohou mít slabinu. Proto při návrhu síťové architektury pro ICS je třeba oddělit síť ICS od podnikové sítě. V případě, že sítě musí být propojeny, mělo by být povoleno pouze minimální propojení a spojení musí probíhat přes firewall a DMZ (McLaughlin et al., 2016).

5) Procesní vrstva: Všechny výše uvedené vrstvy ICS se vzájemně ovlivňují pro implementaci cílových procesů ICS. Pozorované dynamické chování procesů ICS musí odpovídat dynamickým charakteristikám procesů na základě navrženého modelu ICS. Útoky zaměřené na procesy ICS mohou vnášet nepravdivé informace (prostřednictvím speciálně vytvořených zpráv), aby snížily výkonnost nebo omezily účinnost řízeného procesu. Útoky zaměřené na procesy mohou také narušit stav procesu (např. pád nebo zastavení) modifikací proměnných běhu procesu nebo řídicí logiky. Tyto útoky mohou odepřít službu nebo změnit průmyslový proces bez vědomí operátora. Proto je nezbytně nutné určit, zda jsou odchylky v procesu systému nominálními důsledky očekávaného provozu, nebo signalizují anomálii/útok. Analýza zranitelností zaměřená na procesy může přispět k postupům, které umožní bezpečné fungování celé ICS. Je třeba určit zranitelnosti související s tokem informací (např. závislosti na hardwaru/softwaru/síťovém vybavení s jediným bodem selhání) (McLaughlin et al., 2016).

3.2.2 MicroSCADA

Systémy SCADA jsou klíčovým prvkem průmyslové automatizace, umožňující kontrolu a vizualizaci procesů na dálku. Klasické systémy založené na DCS (Distributed Control System) a PLC jsou vhodné pro velké průmyslové aplikace, avšak jejich složitost a vysoké náklady je činí nepraktickými pro menší aplikace. Proto vznikl systém MicroSCADA X, který poskytuje všechny funkce, které se od moderního systému SCADA/DMS očekávají. Tyto funkce jsou založeny na pokročilých a osvědčených algoritmech, například pro lokalizaci poruch, obnovu a rekonfiguraci sítě. Tradiční funkce SCADA, jako je on-line monitorování dat sítě, jsou doplněny pokročilou databází sítě DMS. To umožňuje nové aplikace v reálném čase pro lepší monitorování sítě a řízení výpadků. Lze okamžitě určit polohu poruchy podél napáječe a prezentovat přesnou polohu poruchy na geografické mapě (Hitachi Energy, 2022).

Nabízí několik důležitých prvků pro bezpečnost:

Efektivita provozu při zachování bezpečnosti sítě

Funkce inteligentní správy objednávek přepínačů podporuje plánování, simulaci, provádění a hlášení plánovaných odstávek údržby. Inteligentní algoritmy automaticky optimalizují pořadí spínání s cílem minimalizovat počet postižených zákazníků. Prostřednictvím funkce plánování provozu umožňuje MicroSCADA X plánovat ovládání spínačů pro vzdálené i ruční spínání zařízení v distribuční síti nebo provádět další volně definovatelné činnosti během odstávky. Dokumenty spínacích příkazů s uživatelsky definovanými činnostmi lze vytvářet na základě šablon Microsoft Word specifických pro danou společnost. Plánování spínání zohledňuje technická omezení sítě, jako je pokles napětí a úroveň zatížení pro každý úsek vedení. Kromě toho eliminuje poškození primárních zařízení a sítě během odstávek údržby tím, že zajišťuje vždy správnou činnost reléové ochrany (Hitachi Energy, 2022).

Spolehlivá provozní bezpečnost

MicroSCADA X zabraňuje současnému provozu primárních zařízení. Rezervuje zařízení a před provedením příkazu zkontroluje, zda lze vybraný objekt provozovat. Blokovací schémata navíc zabraňují nebezpečným operacím, které by jinak mohly poškodit primární zařízení. Blokování a další blokované operace mohou zrušit pouze oprávnění uživatelé. Běžné bezpečnostní postupy vyžadují, aby každé mechanické nebo elektrické zařízení mohlo být před zahájením práce uzamčeno a označeno. MicroSCADA X, která je zodpovědná za splnění bezpečnostních požadavků, pravidel a předpisů, obsahuje funkci lock-out/tag-out. Funkce lock-out/tag-out zajišťuje, že ovládání objektů v aplikaci nebo jiné operace jsou řádně zajištěny před a během například údržbářských nebo servisních prací. Objekt aplikace ve stavu tag-out lze na HMI snadno identifikovat pomocí intuitivního symbolu tag-out na displeji. Funkce dynamického obarvení sítě systému MicroSCADA X poskytuje obsluze rychlý přístup k informacím o napájených, nenapájených a uzemněných částech sítě. Vizualizovány jsou také objekty, které vyvolávají poplach. Zabarvení sítě v kombinaci se simulací ovládání objektů systému MicroSCADA X zajišťuje bezpečný a správný provoz elektrické sítě (Hitachi Energy, 2022).

V portfoliu MicroSCADA X je dále zabudováno velké množství funkcí kybernetické bezpečnosti, které chrání systémy před zneužitím nebo vandalismem. Mezi tyto funkce přísluší např:

- Ověřování uživatelů a oblasti odpovědnosti (AOR)
- Centrální správa účtů (CAM)
- Flexibilní autorizace uživatelů
- Vypršení platnosti relací
- Šifrování komunikace
- Protokolování událostí a aktivit uživatelů
- Reportování

Systémy MicroSCADA X mohou být také vybaveny standardními řešeními ochrany proti malwaru a narušení, jako je ochrana proti virům a whitelisting aplikací. Kybernetická bezpečnost je zohledňována během celého životního cyklu produktů, počínaje fází požadavků a vývoje a konče fází provozu. Nové funkce kybernetické bezpečnosti jsou navrženy tak, aby splňovaly a překračovaly požadavky norem, jako jsou IEC 62351, IEEE 1686 a NERC-C. MicroSCADA X splňuje přísné požadavky na zabezpečení systémů SCADA/DMS a zároveň umožňuje sdílení informací mezi odděleními a jednotlivci v rámci podniku. Moderní bezpečnostní technologie, jako jsou komerční firewally, zajišťují nepřetržitou bezpečnost systému a zakazují škodlivé útoky a neoprávněný přístup. Například databáze hlášení, ke které musí mít přístup velké množství lidí, může být umístěna mimo síť SCADA/DMS a chráněna firewallem (Hitachi Energy, 2022).

3.3 Kybernetické hrozby

3.3.1 Obecné

Kybernetické hrozby jsou identifikovány jako neustále se vyvíjející pole rizik, které mohou mít devastující dopady na jednotlivce, organizace a celé státy. Tyto hrozby ohrožují nejen ochranu citlivých informací, ale mohou také narušit kritickou infrastrukturu a služby, od kterých je společnost závislá. S rostoucí závislostí na digitálních technologiích je kybernetická bezpečnost uznávána jako zásadní prvek národní a mezinárodní bezpečnosti.

V rámci zkoumání kybernetických hrozeb bylo zjištěno, že problém není omezen pouze na technickou sféru, ale zahrnuje také behaviorální a organizační aspekty. Lidské chyby, jako jsou nedostatečně silná hesla, klikání na škodlivé odkazy nebo nedostatek povědomí o bezpečnostních hrozbách, jsou často využívány kybernetickými útočníky.

Proto bylo uznáno, že klíčovým prvkem v boji proti kybernetickým hrozbám je vzdělávání uživatelů a budování silné bezpečnostní kultury v organizacích.
Vzhledem k neustálým změnám v povaze kybernetických hrozeb je zdůrazněna nutnost, aby se bezpečnostní opatření neustále vyvíjela a adaptovala. To zahrnuje nejen implementaci technických řešení, jako jsou antivirové programy a firewally, ale také strategie pro řízení rizik, například průběžné hodnocení a aktualizace bezpečnostních protokolů, incidentní reakce a zotavení po poruše.
Kybernetické hrozby byly klasifikovány do několika kategorií, včetně kybernetické kriminality, kybernetických útoků a kyberterorismu. Motivace pachatelů může variovat od finančního zisku, přes politické cíle, až po úmysl způsobit fyzické škody nebo strach. Bez ohledu na to, zda je útočníkem jednotlivec, organizovaná skupina nebo stát, bylo uznáno, že kybernetické hrozby vyžadují komplexní a multidisciplinární přístup k jejich identifikaci, prevenci a řešení.
V následující podkapitole bude prezentováno zkoumání kybernetických hrozeb specifických pro řídicí systémy, kde bude zdůrazněna jedinečnost výzev, kterým tyto systémy čelí kvůli jejich kritickému významu pro fungování moderní společnosti a jejich specifickým technickým a operačním charakteristikám.

3.3.1.1 Typy kybernetických hrozeb

“Hrozby, kterým kybernetická bezpečnost čelí, jsou trojího druhu:

1. Kybernetická kriminalita – zahrnuje jednotlivé aktéry nebo skupiny, které se zaměřují na systémy s cílem získat finanční zisk nebo způsobit narušení.
2. Kybernetický útok – často zahrnuje politicky motivované shromažďování informací.
3. Kyberterorismus – má za cíl narušit elektronické nebo jiné systémy s cílem vyvolat paniku nebo strach.“ (Bhagwani & Balasinorwala, 2023)

Většina těchto útoků probíhá za pomocí malwaru, což je škodlivý software. Malware je jednou z nejběžnějších kybernetických hrozeb, je to software, který vytvořil kyberzločinec nebo hacker, aby narušil nebo poškodil počítač legitimního uživatele. Malware, který se často propaguje prostřednictvím nevyžádané přílohy e-mailu nebo legitimně vypadajícího souboru ke stažení, mohou kyberzločinci používat k vydělávání peněz nebo k politicky motivovaným kybernetickým útokům (Bhagwani & Balasinorwala, 2023). Existuje řada různých typů malwaru, např:

- “Viry: Samo replikující se program, který se připojí k čistému souboru a propaguje se po celém počítačovém systému, přičemž infikuje soubory škodlivým kódem.“ (Bhagwani & Balasinorwala, 2023).
- “Trojské koně: Typ malwaru, který je maskován jako legitimní software. Kybernetičtí zločinci lstí přimějí uživatele k nahrání trojských koní do počítače, kde způsobí škodu nebo shromažďují data.“ (Bhagwani & Balasinorwala, 2023).
- “Spyware: Program, který tajně zaznamenává, co uživatel dělá, aby tyto informace mohli kyberzločinci využít. Spyware může například zachytit údaje o kreditní kartě.“ (Bhagwani & Balasinorwala, 2023).
- “Ransomware: Škodlivý software, který uzamkne soubory a data uživatele a hrozí jejich smazáním, pokud nebude zaplaceno výkupné.“ (Bhagwani & Balasinorwala, 2023).
- “Adware: Adware: Reklamní software, který může být použit k šíření škodlivého softwaru.“ (Bhagwani & Balasinorwala, 2023).
- “Botnety: Sítě počítačů infikovaných malwarem, které kyberzločinci používají k provádění úkolů online bez souhlasu uživatele.“ (Bhagwani & Balasinorwala, 2023).
- “Phishing: Phishing je situace, kdy kyberzločinci cílí na oběti pomocí e-mailů, které vypadají jako od legitimní společnosti a žádají o poskytnutí citlivých informací. Phishingové útoky se často používají k oklamání lidí, aby jim předali údaje o kreditních kartách a další osobní informace.“ (Bhagwani & Balasinorwala, 2023).

Znepokojivým zjištěním je, že se kybernetické hrozby neustále vyvíjí a adaptují na proměnlivé bezpečnostní prostředí. To vyžaduje od organizací nejen implementaci statických obranných opatření, ale i průběžný vývoj a aktualizaci jejich bezpečnostních strategií. V poslední době byl pozorován nárůst útoků na dodavatelský řetězec, což představuje významné riziko, neboť útočníci se mohou dostat do interních sítí prostřednictvím třetích stran. Exploatace zranitelností nulového dne, které nebyly předtím objeveny ani opraveny, poskytuje útočníkům možnost využít těchto slabých míst předtím, než budou odhaleny a zabezpečeny.

Důležitost multidisciplinárního přístupu ke kybernetické bezpečnosti, který kombinuje technické, právní a vzdělávací aspekty, se ukázal být klíčový pro účinnou

obranu. Vzdělávání zaměstnanců a uživatelů o rizicích a nejlepších praktikách kybernetické hygieny je nezbytnou součástí prevence proti kybernetickým hrozbám.
Dalším velmi znepokojivým faktem je, že kromě tradičních metod kybernetických útoků, významně narůstá hrozba zneužití umělé inteligence (AI) pro škodlivé účely. S postupujícím vývojem AI technologií se otevírají nové možnosti pro jejich zneužití v kybernetickém prostoru. AI hrozby mohou zahrnovat (Kaloudi & Li, 2020):

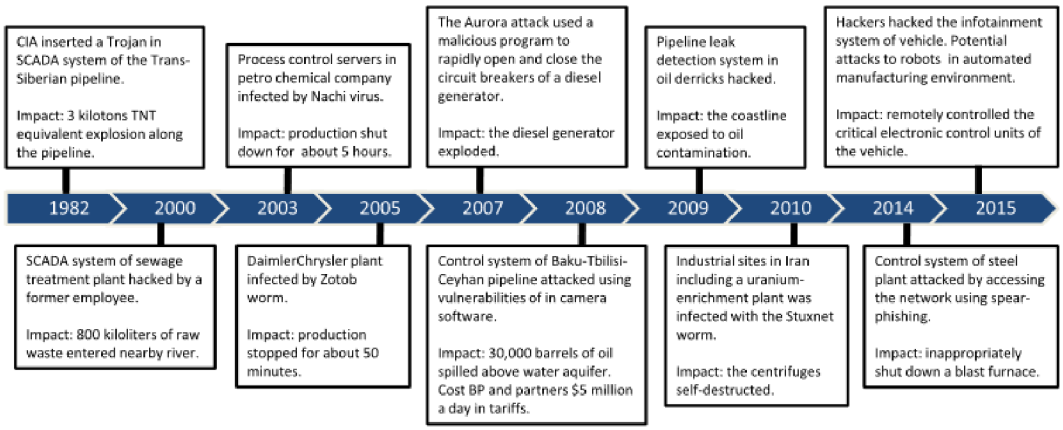
- Generování škodlivého softwaru s AI: Algoritmy AI mohou vytvářet sofistikovanější a obtížněji detekovatelné malwary, které se mohou automaticky adaptovat a měnit své chování k vyhnutí se detekci.
- Sociální inženýrství a AI: AI může být využita k automatizaci útoků sociálního inženýrství, jako je phishing, kde AI generované e-maily nebo zprávy jsou stále přesvědčivější a těžší k odhalení.
- Falešné obsahy a dezinformace: Pokročilé techniky AI, jako je deepfake, mohou vytvářet vysoce přesvědčivé falešné audiovizuální materiály, které mohou být využity k šíření dezinformací nebo manipulaci s veřejným míněním.
- Automatizované útoky proti AI systémům: Útočníci mohou využívat AI k automatizaci a optimalizaci útoků proti bezpečnostním systémům, což umožňuje rychlejší a efektivnější průniky do ochranných bariér.

Rozvoj obranných mechanismů proti AI hrozbám vyžaduje komplexní přístup, zahrnující nejen technologická řešení, ale i širší povědomí o možných rizicích a etických aspektech využití AI. Je zásadní posílit spolupráci mezi akademickým sektorem, průmyslem a vládními institucemi, aby bylo možné čelit těmto nově se objevujícím hrozbám efektivně.

3.3.2 Specifické hrozby pro řídící systémy

3.3.2.1 Historie útoků na ICS

Stabilní provoz ICS může být narušen nejen chybou obsluhy nebo poruchou na výrobní jednotce, ale také chybou softwaru, malwarem nebo úmyslným kybernetickým útokem. Četné kybernetické útoky na ICS jsou shrnuty na Obrázek 7.



Obrázek 7: Shrnutí známých útoků na ICS (McLaughlin et al., 2016; převzato a upraveno)

Podrobněji jsou zde popsány čtyři útoky na ICS, které způsobily fyzické škody. V roce 2007 zinscenovala Idaho National Laboratory útok Aurora, aby demonstrovala, jak může kybernetický útok zničit fyzické komponenty elektrické sítě. Útočník získal přístup do řídicí sítě dieselového generátoru. Poté byl spuštěn škodlivý počítačový program, který rychle otevíral a zavíral jističe generátoru mimo fázi zbytku sítě, což vedlo k výbuchu dieselového generátoru. Vzhledem k tomu, že většina zařízení rozvodné sítě používá starší komunikační protokoly, které nezohledňovaly bezpečnost, je tato zranitelnost obzvláště znepokojivá (McLaughlin et al., 2016).

V roce 2008 došlo v Turecku k silnému výbuchu ropovodu, při kterém se do oblasti nad vodonosnou vrstvou vylilo přes 30000 barelů ropy. Dále to společnost British Petroleum stálo 5 milionů dolarů denně na tranzitních tarifech. Útočníci se do systému dostali využitím zranitelnosti softwaru pro bezdrátovou komunikaci s kamerou a poté se přesunuli hluboko do vnitřní sítě. Útočníci manipulovali s jednotkami používanými k upozorňování dispečinku na poruchy a úniky a kompromitovali PLC (= programovatelný logický automat) na ventilových stanicích, aby zvýšili tlak v potrubí, což způsobilo výbuch (McLaughlin et al., 2016).

V roce 2010 počítačový červ Stuxnet infikoval PLC ve 14 průmyslových závodech v Íránu, včetně závodu na obohacování uranu. Do cílového systému byl zavlečen prostřednictvím infikovaného flash disku USB. Stuxnet se pak nenápadně šířil sítí infikováním vyměnitelných disků, kopírováním do sdílených síťových zdrojů a využíváním neopravených zranitelností. Infikované počítače byly instruovány, aby se připojily k externímu řídicímu serveru. Centrální server pak přeprogramoval PLC tak,

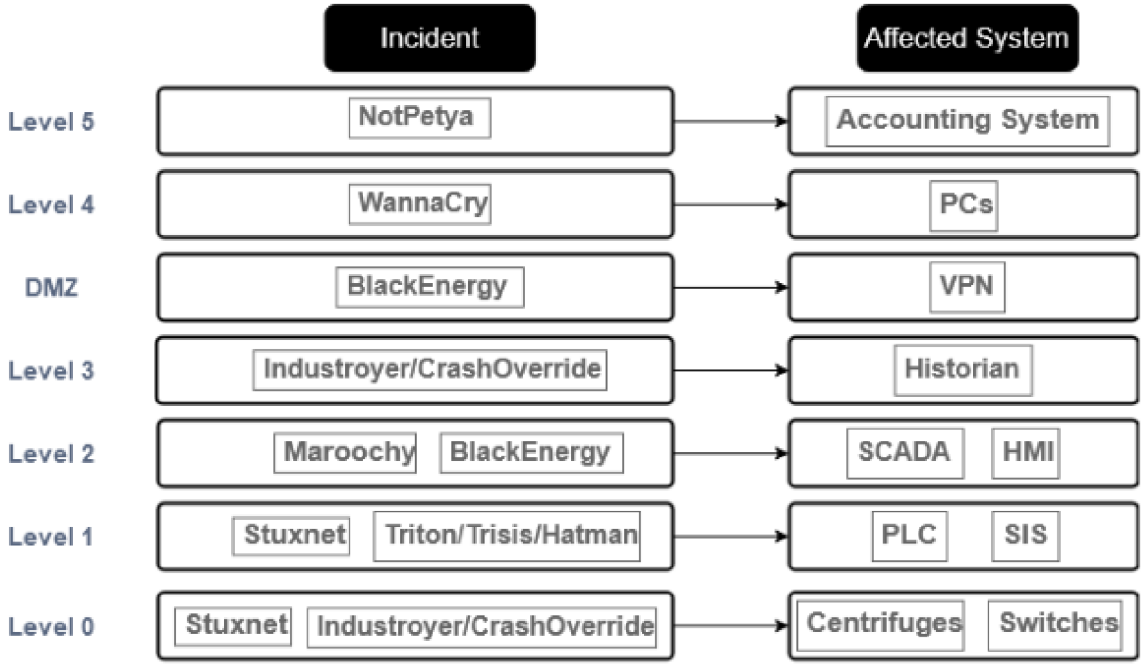
aby upravil provoz odstředivek, které se pomocí infikovaných PLC samy roztrhaly (McLaughlin et al., 2016).

V roce 2015 předvedli dva hackeři dálkové ovládání vozidla. Zneužití zero-day slabiny umožnilo hackerům bezdrátové ovládání vozidel. Softwarové zranitelnosti v entertainment systému vozidla umožnily hackerům jeho vzdálené ovládání, včetně funkcí palubní desky, řízení, brzd a převodovky, což umožnilo provádět škodlivé akce, jako je ovládání klimatizace a audia, vypnutí motoru, brzd i ovládání volantu. Jedná se o předzvěst útoků v automatizovaném výrobním prostředí, kde inteligentní roboti koexistují a koordinují svou činnost s lidmi (McLaughlin et al., 2016).

3.3.2.2 Útoky vzhledem k Purdue modelu

Většina diskutovaných incidentů se týká více úrovní z dříve představeného modelu Purdue. Přehled toho, jaké úrovně se jaký útok týká lze naleznout níže na Obrázek 8. Například Stuxnet infikuje PC a EW (úrovně 4 a 2), které přenesou soubory projektu do PLC (úroveň 1). Zatímco provádí své škodlivé akce proti odstředivkám (úroveň 0), ale ovlivňuje také pohled operátorů (úroveň 2). Duqu infikuje pouze IT systémy, nicméně získané informace (např. přihlašovací údaje) mohou být použity při následných útocích, které se zaměřují na systémy ve více úrovních Purdue. Shamoon ovlivňuje i IT systémy, ale jeho schopnost vymazat data může mít nepřímé dopady na OT stránku organizace. Podobné chování lze pozorovat u útoků WannaCry a NotPetya. Havex vybírá informace z IT systémů, a pokud je to možné, přesouvá se i do 4. úrovně OT prostředí, pokud to podmínky dovolí. BlackEnergy umožnil vybavení protivníků sadou nástrojů, k provádění průzkumu v IT a k přístupu k softwaru, jako jsou VPN a nástroje pro vzdálený přístup. Po získání tohoto typu přístupu se mohou připojit přímo k OT a provádět své škodlivé akce. Jeho součástí je také komponenta wiper, která může ovlivnit jak zařízení v IT, tak i v OT. Industroyer se řídí podobným přístupem. Má však další možnost přístupu k zařízením, která ovládají spínače, jističe na nejnižší z úrovní Purdue. Triton provádí své akce proti řadičům SIS (úroveň 1), vyžaduje však předchozí přístup k EW (úroveň 2). VPNFilter infikuje směrovače, které existují v mnoha úrovních Purdue, a shromažďuje informace z tradičních IT systémů (úrovně 5 a 4) a také z routovatelných průmyslových protokolů (úroveň 3). Při incidentu v německé ocelárně bylo poškozeno zařízení pece, což vyžaduje předchozí přístup protivníka k některé nebo všem předchozím úrovním. V případě Maroochy Water Services incidentu získal útočník přístup do systému SCADA (úroveň 2) a vydal příkazy RTU (úroveň 1), které

umožnily otevření čerpadel a vypuštění odpadních vod (úroveň 0). Při narušení přehrady New York Dam získali útočníci přístup k systému SCADA na úrovni 2 modelu Purdue a získali informace o stavu přehrady. Při incidentu ve vodárenské společnosti "Kemuri" útočníci začali přístupem do systému IT a díky chybné konfiguraci mohli prostřednictvím systému SCADA vydávat příkazy zařízením, která regulují průtok vody a míchají chemikálie. (Makrakis et al., 2021)

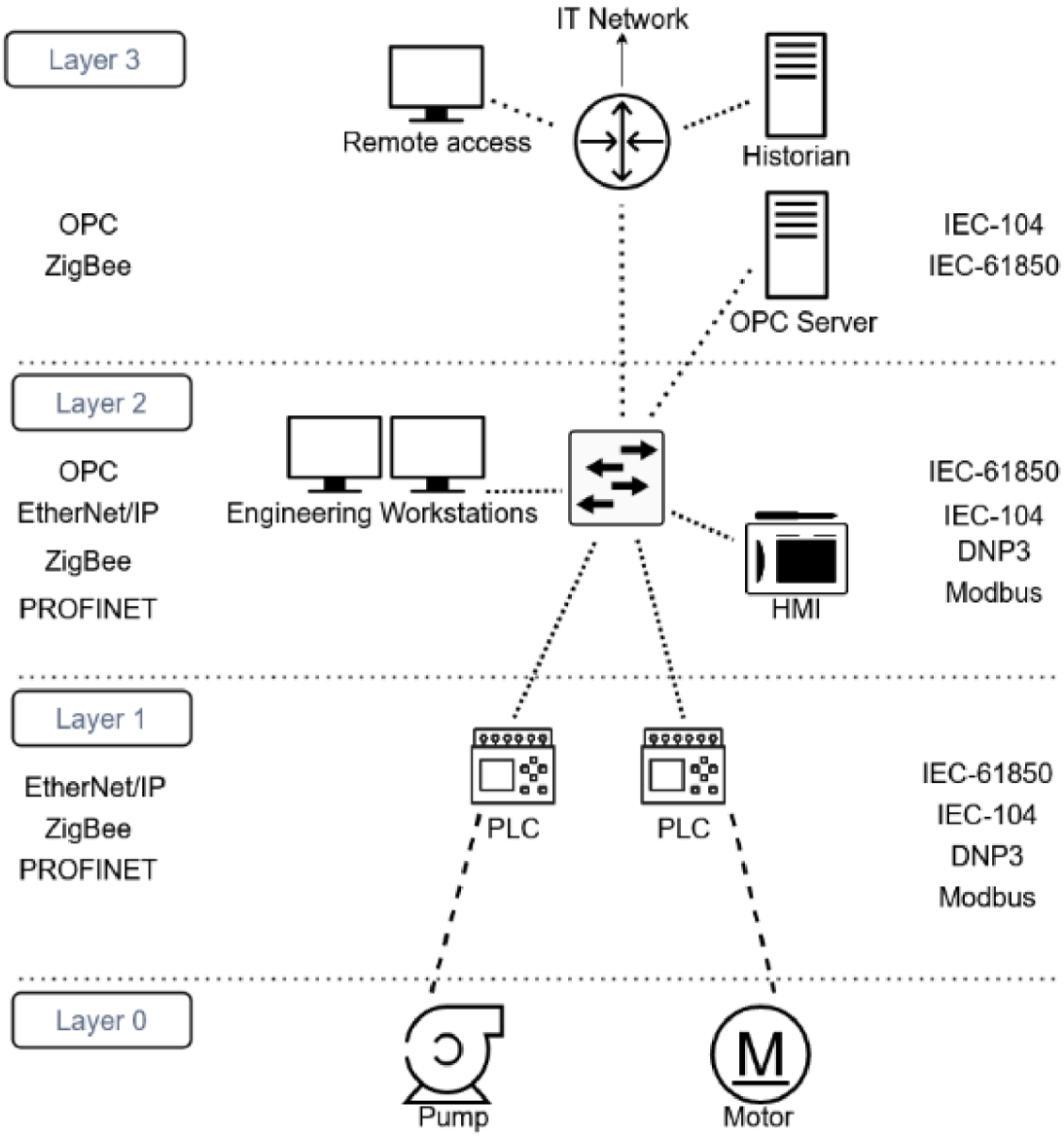


Obrázek 8: Korespondence útoků s dotčenými systémy vzhledem k Purdue modelu (Makrakis et al., 2021; převzato a upraveno)

3.3.2.3 Slabiny ICS

První část této podkapitoly se zabývá známými zranitelnostmi zavedených protokolů ICS. Tyto protokoly se mohou nacházet v různých vrstvách Purdueova modelu, ale obvykle se řídí architekturou znázorněnou na Obrázek 9. Konkrétně protokoly Modbus, DNP3, PROFINET, EtherNet/IP a WirelessHART jsou převážně sběrnicové protokoly, což znamená, že se používají pro komunikaci průmyslových zařízení, včetně PLC a IED, s komponentami, jako jsou senzory, akční členy, spínače ventily atd. Naproti tomu OPC, IEC-104, IEC-61850 a ZigBee jsou označovány jako backendové protokoly. To znamená, že se používají pro interakci různých komponent v ICS na vyšší úrovni, například pro komunikaci mezi řídicí stanicí a rozvodnou v energetické síti. Nicméně některé z backendových protokolů zahrnují funkce pro komunikaci po sběrnici, například specifikaci výrobních zpráv IEC-61850. Komunikace po polní sběrnici je kritická z hlediska času a nákladů, zatímco některé z backendových protokolů mají větší toleranci vůči časovým zpožděním a mohou být implementovány v obecnějším

hardwaru. Stojí za zmínku, že zranitelnosti mohou existovat i v dalších starších IT protokolech, které se rovněž používají v ICS, včetně HTTP, ARP a Telnet (Makrakis et al., 2021).



Obrázek 9: Přehled síťové topologie s protokoly (Makrakis et al., 2021; převzato a upraveno)

Tato druhá část podkapitoly se věnuje specifickým slabinám ICS zařízení. Tato zařízení pracují především na nižších úrovních Purdueova modelu, jak je znázorněno na Obrázek 6. Často jsou zranitelnosti zařízení ICS a někdy i jejich doprovodného softwaru objevovány a zveřejňovány společnostmi a jednotlivci mimo akademickou sféru, některé z těchto organizací dokonce poskytují značné prostředky na identifikaci takových zranitelností. Např. CISA formuje a spravuje seznam identifikovaných zranitelností včetně úrovně závažnosti na základě základního skóre CVSS.

I když byly odhaleny alternativní metody zneužití, můžeme odpovídající útoky rozřadit jako ty, které: (a) provádějí reverzní inženýrství, (b) zaměřují se na neoprávněnou modifikaci řídicí logiky, (c) jsou založeny na žebříkové logice, (d) usilují o instalaci a spuštění malwaru, nativně, na úrovni zařízení ICS, (e) ty, které vyplývají z nedostatku řádných autentizačních mechanismů prováděné řídicí logiky, nebo konečně ty, které (f) dosahují úniku citlivých dat nebo narušení provozu zařízení prostřednictvím zneužití side-channel (Makrakis et al., 2021).

4 Systém pravidelné kontroly s využitím nástrojů CIS

V rámci praktické části této diplomové práce je prezentován vývoj a implementace automatizovaného systému pro kontrolu bezpečnostních nastavení systémů založených na platformě Windows. Tento systém byl ve spolupráci s firmou Hitachi Energy vyvinut s cílem nabídnout efektivní řešení pro identifikaci a dokumentaci změn v bezpečnostních konfiguracích, které byly provedeny od poslední kontroly. Zajištění ochrany systémů před potenciálními hrozbami a zranitelnostmi je v současné digitálně propojené době považováno za zásadní pro zachování bezpečnosti a integrity podnikových informačních systémů.

Jedna z podkapitol se zaměřuje na popis metodologie vývoje systému, včetně vytvoření skriptů v PowerShellu, které umožňují automatizovaný sběr a analýzu dat o nastaveních systému. Klíčovou složkou je práce s databází, která funguje jako základ pro porovnávání aktuálních a předchozích stavů konfigurací a identifikaci potenciálních bezpečnostních rizik. Důraz je kladen na srozumitelnou prezentaci výsledků uživatelům, což umožňuje rychlou a informovanou reakci na identifikované problémy.

Ve vývoji automatizovaného systému pro kontrolu bezpečnostních nastavení na platformě Windows byl jako hlavní ukazatel pro posouzení bezpečnosti zvolen Center for Internet Security (CIS) a jeho nástroje. Tato volba byla učiněna na základě několika klíčových faktorů, které zdůrazňují význam a efektivitu CIS benchmarků a nástrojů v kontextu zajištění kybernetické bezpečnosti.

Hlavním z nich bylo již standardizované použití jejich nástrojů a benchmarků firmou Hitachi. CIS benchmarky jsou uznávány jako zlatý standard pro bezpečnostní konfigurace a poskytují detailní a důkladně ověřená vodítka pro zabezpečení operačních systémů, middleware, softwarových aplikací a síťových zařízení. Pro operační systém Windows CIS nabízí konkrétní doporučení, která jsou navržena tak, aby minimalizovala možný povrch útoku a posílila obranné mechanismy systému proti potenciálním hrozbám. Tyto benchmarky jsou vytvářeny a pravidelně aktualizovány expertní komunitou, což zajišťuje, že reflektují nejnovější hrozby a nejlepší dostupné praktiky v oblasti kybernetické bezpečnosti.

Výběr CIS benchmarků jako základu pro tento systém byl rovněž motivován jejich vysokou adaptabilitou a schopností pokrýt širokou škálu bezpečnostních nastavení. CIS nabízí různé úrovně nastavení, což umožňuje organizacím přizpůsobit bezpečnostní politiky svým specifickým potřebám a rizikům. Tato flexibilita je klíčová

pro implementaci efektivních bezpečnostních strategií, které neohrožují operativní funkčnost ani produktivitu.

Kromě benchmarků poskytuje CIS také nástroj CIS-CAT (CIS Configuration Assessment Tool), který poskytuje automatizované testování a ověřování konformity systémů s doporučenými bezpečnostními konfiguracemi. Licence pro tento nástroj byla propůjčena od firmy Hitachi, pro možnost podrobnějšího prozkoumání nastavení OS Windows. Použití CIS-CAT v rámci vyvinutého systému umožňuje efektivní a přesné zjišťování odchylek od doporučených nastavení. Tento nástroj poskytuje podrobné reporty, které identifikují konkrétní slabá místa a navrhují kroky k jejich odstranění, což výrazně usnadňuje proces hardeningu systému.

4.1 Tvorba systému

Celý vyvinutý systém lze najít jako Přílohu č. 1 - Odkaz na adresář práce na GitHubu.

4.1.1 Výběr nástrojů

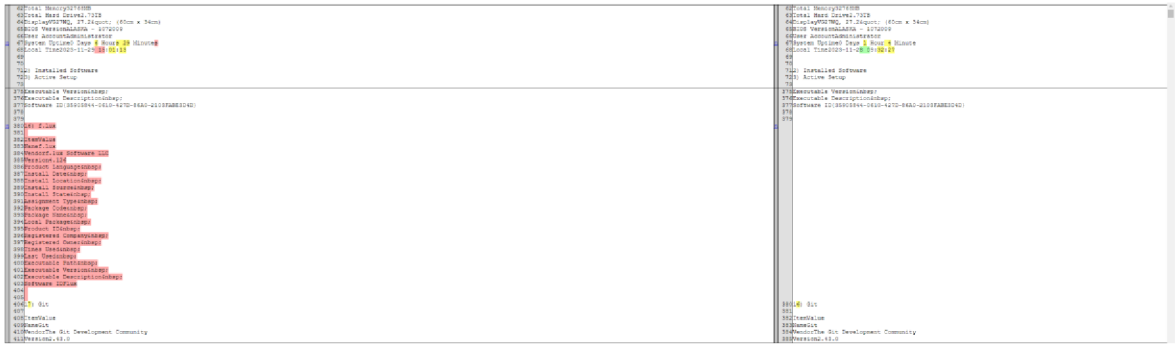
4.1.1.1 Jazyk

Pro implementaci automatizovaného systému kontroly bezpečnostních nastavení v rámci diplomové práce byl jako hlavní programovací jazyk zvolen PowerShell. Toto rozhodnutí bylo motivováno několika důležitými faktory, které převažují výhody použití PowerShellu pro daný účel, zejména v prostředí operačního systému Windows. Jedním z klíčových důvodů byla jednodušší použitelnost a integrace vyvíjeného systému na platformách Windows bez nutnosti instalovat další software. PowerShell, jako nativní skriptovací nástroj pro Windows, umožňuje bezproblémovou a efektivní interakci s operačním systémem a jeho komponentami, což zjednodušuje proces získávání, analýzy a modifikace bezpečnostních nastavení.

Druhým důvodem pro odchýlení od původně zvažovaného Pythonu byla preference společnosti Hitachi používat nástroje Microsoftu. Tato preference má praktický základ v tom, že mnohé podnikové a průmyslové prostředí, ve kterých Hitachi působí, jsou založena na technologiích a produktech Microsoftu. Použití PowerShellu tak přirozeně koresponduje s technologickým ekosystémem firmy a umožňuje lepší kompatibilitu a integraci vyvinutého systému do stávajících procesů a infrastruktury.

To, že zprvu zamýšleným jazykem byl Python, lze pozorovat i na první verzi skriptu pro hledání rozdílů ve výsledcích z auditovacího nástroje. Skript compare.py, který lze nalézt na GitHubu, bral výsledky z auditovacího nástroje WinAudit. Tyto výsledky se

zpočátku tvorby tohoto systému ještě ukládaly ve formátu html, což je defaultní výstup tohoto nástroje. Pro ideální porovnání HTML kódu byla použita knihovna difflib (Python Software Foundation, 2024), která umožnila vytvořit html soubor se shrnutím výsledků vedle sebe a barevným odlišením změn, což nebylo původně dosažitelné s použitím nástrojů PowerShellu. Byla v něm implementována i funkce pro odstranění html tagů, které dělali výstup zbytečně rozsáhlejší a hůře čitelný. Bohužel byl výstup v podobě html i přes tyto snahy stále příliš rozsáhlý, a i proto se od tohoto přístupu opustilo. Na Obrázek 10 níže lze vidět výsledek, kterého bylo dosaženo za pomoci výše zmíněného Python skriptu, kde lze vidět shrnutí původního obsahu dvou cca 400 řádkových výstupů na jeden výstup o pár řádcích a dvou sloupcích, ve kterých jsou shrnuty změny v těchto výstupech vedle sebe. Výsledek i skript je součástí přílohy č. 1 - Odkaz na adresář práce na GitHubu.



Obrázek 10: Výstup Python skriptu (autor)

Navíc PowerShell nabízí rozsáhlou podporu pro automatizaci správy systémů, práci se soubory, správu konfigurací a další, což jsou klíčové aspekty potřebné pro účely této diplomové práce. Jeho schopnost přímo interagovat s Windows Management Instrumentation (WMI) a dalšími Windows API rovněž zvyšuje efektivitu a přesnost operací prováděných systémem.

Tato volba tedy reflektuje strategický přístup k vývoji systému, který je snadno implementovatelný, efektivně integrovatelný a maximálně přizpůsobený potřebám a preferencím společnosti Hitachi, zatímco zároveň minimalizuje požadavky na dodatečnou instalaci a konfiguraci software ve cílovém prostředí.

Z obdobných důvodů byl nakonec zvolen přístup k ukládání dat do databáze Access od Microsoftu. Je to databáze, která používá standardní jazyk SQL a jedná se opět o nativní Microsoft produkt, což zajišťuje dobrou integraci s ostatními produkty Microsoftu, které firma Hitachi aktivně využívá. Tato volba umožňuje využít stávající

infrastrukturu a znalosti pracovníků, což usnadňuje správu dat a integraci s dalšími systémy.

4.1.1.2 Nástroj pro audit operačního systému

V této kapitole se zaměříme na WinAudit, který je oblíbeným nástrojem pro provádění komplexního auditu operačních systémů Windows. WinAudit je bezplatný software, který umožňuje uživatelům snadno shromažďovat informace o hardwaru, softwaru a bezpečnostních nastaveních jejich počítačů. Jeho hlavní přednosti zahrnují jednoduché uživatelské rozhraní a schopnost generovat podrobné zprávy ve formátech, jako jsou HTML, PDF a CSV. Dokonce zvládá i export do databáze a práci s příkazovým řádkem což byly velmi důležité aspekty, které volbu pro tento nástroj usnadnily (Parmavex Services, 2014).

Zároveň jde o software, který se již používal ve firmě Hitachi pro audit systémů, a proto ho je vhodné použít pro zpětnou kompatibilitu s již vytvořenými reporty z tohoto nástroje.

Zde podrobněji vysvětlím jeho hlavní přednosti z informací z jeho dokumentace (Parmavex Services, 2014):

1. Jedná se o jednoduchý nástroj na použití a nevyžaduje instalaci. Funguje na Windows XP a novějších. Jako "ready to run" program nemodifikuje registry systému ani neinstaluje dodatečné soubory. Odstranění WinAuditu je stejně snadné, stačí smazat soubor WinAudit.exe a případně WinAudit.ini, pokud byl vytvořen.
2. Jeho report obsahuje širokou škálu informací o počítači, od základních systémových přehledů, přes detaily o nainstalovaném softwaru, bezpečnostní nastavení, uživatelské účty, plánované úlohy, statistiky provozu, chybové záznamy až po hardwarové zařízení. Bude podrobněji prozkoumáno v následujícím porovnání proti CIS Critical Security Controls (Center for Internet Security®, 2023) doporučením.
3. Umožňuje uživatelům ukládat auditové zprávy ve formátech Comma Delimited, Rich Text a Web Page. Tyto možnosti umožňují snadné zobrazení a analýzu dat v různých aplikacích, jako jsou tabulkové procesory, textové editory nebo webové prohlížeče.
4. Nabízí rozsáhlé možnosti exportu do databází, podporuje verze DBMS jako Microsoft® Access, MySQL®, Microsoft® SQL Server a PostgreSQL. Umožňuje

snadné vytváření a správu databází, export auditovaných dat a jejich údržbu. Poskytuje také jednoduché reportování ze shromážděných dat.

5. Umožňuje spouštění z příkazové řádky pro automatizaci auditů počítačů, což je právě ideální pro použití v dávkových souborech nebo skriptech. Nabízí flexibilní možnosti reportování a export dat do databáze nebo na síťové disky bez nutnosti zobrazování uživatelského rozhraní.
6. Klade velký důraz na ochranu soukromí a bezpečnost. Program nemá schopnost odesílat nebo přenášet informace o vašem počítači na externí servery, což znamená, že žádná data nejsou sdílena s firmou Parmavex Services. Ačkoli WinAudit umožňuje vytváření e-mailových zpráv, vyžaduje k jejich odeslání akci uživatele. Jako freeware a open source program nabízí možnost ověřit si jeho funkčnost prostřednictvím přezkumu zdrojového kódu.
7. Je licencován pod Evropskou veřejnou licencí (EUPL), což znamená, že je zdarma a open source. Nemůže být prodáván, pronajímán, půjčován, sublicencován ani jinak využíván za účelem finančního zisku. Uživatelé si mohou vytvořit libovolný počet kopií a distribuovat je komukoli, včetně komerčních organizací. Použitím softwaru uživatelé souhlasí s podmínkami EUPL. Licence zahrnuje práva na používání, reprodukci, modifikaci, distribuci a další, a platí po celém světě bez poplatků.

4.1.1.3 Firewall

Jedním z požadavků firmy Hitachi bylo také rozšíření výstupu auditu. Jelikož nástroj WinAudit postrádá mimo jiné informace o firewallu a pravidlech, které v něm jsou. K těmto informacím bylo přistoupeno přímo přes funkce od Microsoftu (JasonGerend, 2024).

Pro kompletní výstup těchto pravidel byla použita kombinace tří cmdlets (bude překládáno jako rutiny), konkrétně Get-NetFirewallRule, Get-NetFirewallPortFilter a Get-NetFirewallAddressFilter. Jejich výstupy jsem poté vyfiltroval, aby výstup obsahoval nejdůležitější informace.

Get-NetFirewallRule vrací instance pravidel brány firewall, které odpovídají parametrům hledání zadaným uživatelem. Parametry pro hledání jsou Name (výchozí), DisplayName, nebo vlastnosti pravidla nebo přidružených filtrů či objektů. Dotazovaná pravidla lze umístit do proměnných a předat je dalším rutinám pro další úpravy nebo sledování. Jelikož se ale nezobrazují běžné vlastnosti, jako jsou adresy nebo porty, je

nutné tyto vlastnosti získat z dalších rutin, protože jsou reprezentovány v samostatných objektech nazývaných filtry. Vztah filtr-pravidlo je vždy jedna ku jedné a je spravován automaticky. Proto jsem použil výše zmíněné dva filtry, abych dostal kompletní informace o pravidlech. Kompletní výstup této rutiny pro jedno z pravidel lze vidět na Obrázek 11 níže.

```
Name                          : {39A4DD75-9382-413A-A012-0DDB4BF67899}
DisplayName                   : EA app (EALaunchHelper) (Outbound)
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Outbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
```

Obrázek 11: Výstup rutiny Get-NetFirewallRule (autor)

Rutina Get-NetFirewallPortFilter vrací objekty filtru portů přiřazené ke vstupním pravidlům. Objekty filtru portů představují porty a protokoly spojené s pravidly brány firewall a IPsec. Konkrétně se jedná o parametry Protocol, LocalPort, RemotePort, IcmpType a DynamicTransport.

Rutina Get-NetFirewallAddressFilter vrací objekty adresního filtru přiřazené ke vstupním pravidlům. Objekty filtru adres představují místní a vzdálené adresy přidružené ke vstupním pravidlům. Konkrétně se jedná o parametry LocalAddress a RemoteAddress.

Nyní budou stručně představeny parametry, které jsem zahrnul do kontroly.

- DisplayName = základní parametr názvu pravidla
  - Hodnoty = String
- Protocol = určuje protokol pro pravidlo IPsec
  - Hodnoty
    - určené číslem: 0 až 255
    - určené názvem: TCP, UDP, ICMPv4 nebo ICMPv6
- LocalPort = lokální port na kterém je pravidlo

    - Hodnoty = číslo portu nebo “Any“
- RemotePort = vzdálený port na kterém je pravidlo
    - Hodnoty = číslo portu nebo “Any“
- LocalAddress = lokální adresa pravidla
    - Hodnoty = číselná adresa, nebo některý z LocalSubnet, nebo “Any“
- RemoteAddress = vzdálená adresa pravidla
    - Hodnoty = číselná adresa, nebo některý z LocalSubnet, nebo “Any“
- Enabled = určuje, zda je objekt pravidla administrativně povolen nebo administrativně zakázán
    - Hodnoty = True nebo False
- Profile = určuje rozsah sítě kde pravidlo funguje
    - Hodnoty = Domain, Private a Public
- Direction = určuje směr daného pravidla
    - Hodnoty = Inbound nebo Outbound
- Action = určuje co se stane s provozem odpovídajícím tomuto pravidlu
    - Hodnoty = Allow nebo Block

4.1.1.4 BIOS

Další z informací, o kterých WinAudit nedokáže získat dostatek informací je BIOS. Bohužel se v rámci této práce nepodařilo zajistit dostatečně kvalitní způsob, který by významně rozšířil rozsah informací, které lze získat.

K získání informací byl znovu použit defaultní nástroj od firmy Microsoft a sice rutina Get-CimInstance, která jako povinný parametr vyžaduje ClassName, který určuje, jakou instanci objektu CIM získáme. Pro získání dat o BIOS se využila třída Win32_BIOS. Výstup záleží na konkrétní implementaci BIOS, minimální informace, které lze získat vždy jsou:

- SMBIOSBIOSVersion = verze aktualizace systému BIOS
- Manufacturer = výrobce systému BIOS/základní desky
- Name = název systému BIOS, někteří výrobci zde udávají pouze znovu verzi
- SerialNumber = sériové číslo stroje
- Version = verze systému BIOS, daná výrobcem

4.1.1.5 Politiky

Mezi poslední požadavky firmy Hitachi byl zisk informací o lokálních politikách. V rámci práce byla snaha najít ideální nástroj pro tento úkol, která skončila následujícím seznamem možností:

- SecEdit
- Get-GPOReport
- Get-WmiObject -Class RSOP_SecuritySettingBoolean -Namespace root\rsop\computer

Bohužel se všechny možnosti kromě první ukázaly jako možnosti limitované pro použití na systémech Windows Server a pro získávání politik doménových. To se pro potřeby Hitachi nehodilo, jelikož zdaleka ne všechny počítače, pro které je tento systém určený jsou v nějaké doméně.

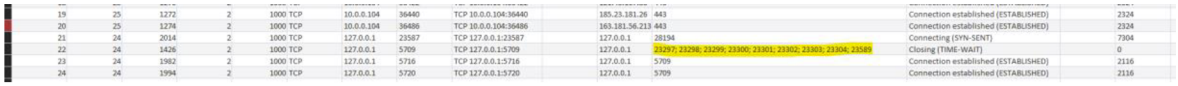
Jak se lze dočíst na portálu Microsoft Learn (JasonGerend, 2024). Secedit je nástroj příkazové řádky pro konfiguraci a analýzu bezpečnostních nastavení systému Windows porovnáním aktuální konfigurace s bezpečnostními šablonami. Jednou z klíčových funkcí seceditu je možnost exportovat bezpečnostní nastavení uložená v databázi do souboru konfigurace, což umožňuje zálohování a přenos bezpečnostních politik mezi počítači. K exportu lze specifikovat různé oblasti bezpečnosti, jako jsou politiky bezpečnosti, správa skupin, uživatelská práva a další, což umožňuje flexibilní správu bezpečnostních nastavení.

Právě té možnosti exportovat nastavení do souboru cfg bylo využito v práci, protože nelze pomocí tohoto nástroje rovnou napřímo získat daná data. Pro pospolitost práce jsem se rozhodl stejně jako u ostatních informací je ukládat do databáze, a proto jsem v rámci skriptu pro lokální politiky, přistoupil k přístupu, kdy tento soubor hned po přečtení daných informací ze systému automaticky mažu, aby nevznikal nadbytek dat.

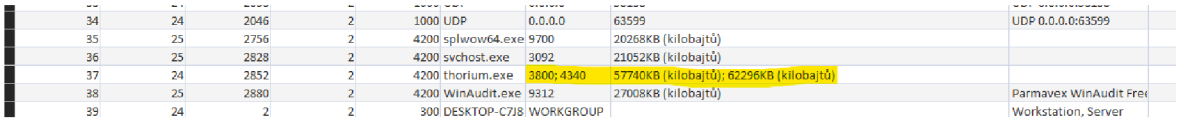
4.1.2 Skripty

Hlavní částí práce byl vývoj skriptů v PowerShellu. Tyto skripty byly navrženy tak, aby automatizovaly proces sběru dat o aktuálních nastaveních systému, za pomoci dříve zmíněných nástrojů, a jejich porovnání s předchozími stavy. Skripty se dají rozdělit do tří kategorií:

1. **Inicializace databází:** Tyto skripty (createBiosDB.ps1, createFirewallRulesDB.ps1, createLocalPoliciesDB.ps1, createWinAuditDB.ps1) realizují inicializaci databáze a vytvoření konkrétních tabulek s aktuálními konfiguracemi systému. Databáze je navržena tak, aby obsahovala podrobné informace o každém nastavení, včetně hodnot a parametrů. Další důležitou součástí těchto tabulek jsou informace, o který audit se jedná. Tyto údaje v dalších skriptech umožňují vybrat správné řádky k porovnávání.
2. **Porovnávání s databází:** Skripty jako compareBiosDB.ps1, compareFirewallRulesDB.ps1, compareLocalPoliciesDB.ps1, compareWinAuditDB.ps1 byly vyvinuty pro porovnání aktuálních nastavení s předchozími záznamy v databázi. Tímto způsobem systém identifikuje změny v konfiguraci a potenciální bezpečnostní rizika. Funguje to na principu využití údajů o auditu, které byly definovány v předchozím bodě. Díky SQL dotazu si vyberu data z posledních dvou auditů a porovnám je vůči sobě. Některá porovnání mají svoje specifika, která přispívají ke snížení počtu nalezených falešných změn a k lepší čitelnosti výsledků. Na Obrázek 12 a Obrázek 13 níže lze vidět ukázky z tabulky rozdílů, kde za pomoci agregace přes určující hodnotu v dané kategorii, u procesů jde o název a u otevřených portů o jejich adresu, dochází ke sloučení více řádků do jednoho pro zmenšení a zjednodušení výstupu.



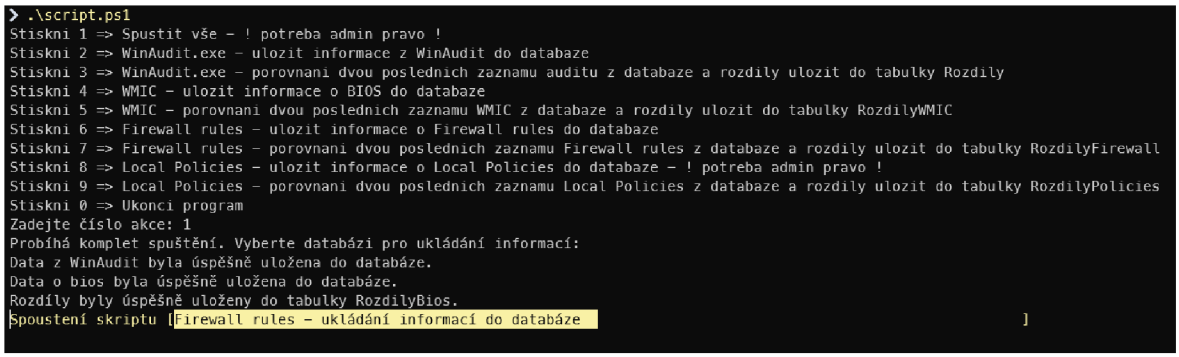
Obrázek 12: Ukázka agregace řádků v tabulce Rozdíly u portů (autor)



Obrázek 13: Ukázka agregace řádků v tabulce Rozdíly u procesů (autor)

3. **Pomocné skripty:** functions.ps1 obsahuje sadu pomocných funkcí používaných ostatními skripty pro zjednodušení a optimalizaci kódu. script.ps1 funguje jako hlavní skript pro spouštění celého procesu kontroly. Jsou v něm možnosti, jak pouštět jednotlivé části jednotlivě, nebo možnost celkové kontroly, kde byla použita funkce Write-Progress pro přehledné ukázání, jak celý skript probíhá a který ze skriptů se zrovna vykonává. Obrázek 14 níže

ukazuje, jak vypadá hlavní skript po spuštění a také jak ukazuje průběh spouštění jednotlivých skriptů pomocí Write-Progress.



Obrázek 14: Spuštění hlavního skriptu a jeho průběh (autor)

V posledních úpravách skriptů pro PowerShell jsem se zaměřil na zdokonalení flexibility a efektivity systému pro sběr a porovnání dat v oblasti systémových konfigurací. Klíčovými změnami bylo zavedení možnosti manuálního a automatického režimu ve skriptech, které se zabývají porovnáváním dat z různých auditů a databází. Tato nová funkcionalita umožňuje uživatelům větší kontrolu nad zdroji dat a způsobem porovnání, což je ideální pro situace vyžadující specifické srovnávací scénáře nebo při práci s daty z více zdrojů.

1. Flexibilní výběr databází: Skripty nyní podporují výběr mezi dvěma databázemi v manuálním režimu, což umožňuje srovnání dat z různých zdrojů nebo časových období. Tato možnost je zásadní pro detekci a analýzu změn v konfiguracích, které mohou být způsobeny aktualizacemi systému, bezpečnostními zásahy nebo neautorizovanými změnami.
2. Automatizace a zjednodušení: Automatický režim zůstává pro uživatele, kteří preferují minimalizovat interakci se skriptem a spoléhat se na standardizovaný proces sběru a analýzy dat. V tomto režimu skripty automaticky selektují relevantní data z přednastavených zdrojů a provádějí srovnání bez dalšího uživatelského zásahu.
3. Strukturalizace a organizace kódu: Všechny skripty byly refaktorovány tak, aby zahrnovaly funkce pro zpracování dat, což zlepšuje čitelnost, údržbu a opětovnou použitelnost kódu. Zahrnutí funkce pro dynamické vytváření SQL dotazů a tabulek dále zvyšuje adaptabilitu skriptů na různé databázové schémata a usnadňuje správu databází.

4.2 Průzkum doporučených nastavení CIS

Tato podkapitola je zaměřená na obsah dokumentu CIS Critical Security Controls® Version 8 (Center for Internet Security®, 2023), který obsahuje konkrétní rady, jak nastavit zabezpečení systému pro co nejlepší bezpečnost svého systému.
Dělí úrovně zabezpečení do tzv. implementačních skupin.

- IG1
    - "Podnik IG1 je malý až středně velký podnik s omezenými odbornými znalostmi v oblasti IT a kybernetické bezpečnosti, které může věnovat ochraně IT majetku a personálu. Hlavním zájmem těchto podniků je udržet provoz podniku, protože mají omezenou toleranci k výpadkům. Citlivost dat, která se snaží chránit, je nízká a týká se hlavně informací o zaměstnancích a finančních informacích. Ochranná opatření vybraná pro IG1 by měla být proveditelná s omezenými odbornými znalostmi v oblasti kybernetické bezpečnosti a jejich cílem by mělo být zmaření obecných, necílených útoků. Tato ochranná opatření budou také obvykle navržena tak, aby fungovala ve spojení s komerčním hardwarem a softwarem pro malé nebo domácí kanceláře." (Center for Internet Security®, 2023)
- IG2 (zahrnuje IG1)
    - "Podnik IG2 zaměstnává osoby odpovědné za správu a ochranu IT infrastruktury. Tyto podniky podporují více oddělení s různými rizikovými profily na základě pracovních funkcí a poslání. Malé podnikové jednotky mohou mít zátěž spojenou s dodržováním právních předpisů. Podniky IG2 často uchovávají a zpracovávají citlivé informace o klientech nebo podniku a jsou schopny odolat krátkodobému přerušení provozu. Hlavní obavou je ztráta důvěry veřejnosti, pokud dojde k narušení. Ochranná opatření vybraná pro IG2 pomáhají bezpečnostním týmům vyrovnat se s vyšší provozní složitostí. Některá ochranná opatření budou záviset na technologii podnikové úrovně a na specializovaných odborných znalostech, aby bylo možné je správně nainstalovat a nakonfigurovat." (Center for Internet Security®, 2023)
- IG3 (zahrnuje IG1 a IG2)

- “Podnik IG3 zaměstnává bezpečnostní odborníky, kteří se specializují na různé aspekty kybernetické bezpečnosti (např. řízení rizik, penetrační testování, zabezpečení aplikací). Aktiva a data IG3 obsahují citlivé informace nebo funkce, které podléhají regulačnímu dohledu a dohledu nad dodržováním předpisů. Podnik IG3 musí řešit dostupnost služeb a důvěrnost a integritu citlivých dat. Úspěšné útoky mohou způsobit značné škody na veřejném blahu. Ochranná opatření vybraná pro IG3 musí omezit cílené útoky sofistikovaného protivníka a snížit dopad útoků nultého dne.“ (Center for Internet Security®, 2023)

Nyní zde bude stručný popis jednotlivých kategorií, které si dle CIS zaslouží konkrétní zabezpečení a jejich porovnání s tím, jak jsou nebo nejsou implementovány v systému vyvinutém v rámci této práce.

4.2.1 Inventář a kontrola podnikových aktiv

Zahrnuje správu všech aktiv společnosti, jako jsou koncová zařízení, síťová zařízení a servery, a to jak fyzicky, tak virtuálně.
Co WinAudit dokáže: WinAudit může detekovat a poskytnout podrobný seznam hardwaru a softwaru na systémech Windows, což zahrnuje základní inventarizaci.
Co WinAudit nedokáže: Nezahrnuje sledování zařízení připojených virtuálně nebo vzdáleně, ani neřeší správu zařízení mimo Windows.

4.2.2 Inventář a kontrola softwarových aktiv

Zaměřuje se na správu softwaru, aby byl instalován a provozován pouze autorizovaný software, a na odhalování a zabránění instalaci neautorizovaného softwaru.
Co WinAudit dokáže: Poskytuje podrobný seznam softwarových aplikací nainstalovaných na lokálním systému.
Co WinAudit nedokáže: Nezahrnuje schopnost zjištění neautorizovaného softwaru nebo automatizaci správy softwarových záplat a aktualizací.

4.2.3 Ochrana dat

Vývoj procesů a technických opatření pro identifikaci, klasifikaci a zabezpečení manipulace s daty, jejich uchovávání a likvidace.
Co WinAudit dokáže: Identifikuje data uložená na lokálních discích.

Co WinAudit nedokáže: Neposkytuje funkce šifrování, klasifikace dat ani zásady zacházení s daty.

4.2.4 Zabezpečená konfigurace podnikových aktiv a softwaru

Zajištění bezpečné konfigurace všech podnikových aktiv a softwaru od počáteční instalace až po celý životní cyklus.
Co WinAudit dokáže: Sbírá informace o aktuálním stavu konfigurace systému.
Co WinAudit nedokáže: Neumožňuje aktivní správu nebo uplatňování zabezpečených konfigurací na vzdálených systémech.

4.2.5 Správa účtů

Procesy a nástroje pro přidělování a správu oprávnění pro uživatelské a služební účty.
Co WinAudit dokáže: Zobrazí seznam lokálních uživatelských účtů a skupin na systému.
Co WinAudit nedokáže: Nezahrnuje správu účtů ani integraci s externími správcovskými nástroji.

4.2.6 Správa přístupových práv

Vytvoření, přidělení, správa a odnětí přístupových oprávnění pro uživatelské, administrátorské a služební účty.
Co WinAudit dokáže: Poskytuje základní informace o právech lokálních uživatelských účtů.
Doplnění o SecEdit: Podrobnější výpis všech lokálních politik.
Co WinAudit nedokáže: Nezahrnuje pokročilé správce přístupu, jako je správa přístupových práv na základě rolí nebo více faktorové ověřování.

4.2.7 Trvalá správa zranitelností

Neustálé monitorování a řešení zranitelností v systémech společnosti.
Co WinAudit dokáže: Zjistí verze operačního systému a některé aplikace, což může pomoci při identifikaci zastaralého softwaru.
Co WinAudit nedokáže: Neobsahuje nástroje pro skenování zranitelností nebo automatizovanou správu záplat.

4.2.8 Správa protokolů auditu

Zaznamenávání a správa protokolů auditu, které umožňují detekci a reakci na bezpečnostní incidenty.

Co WinAudit dokáže: Sbírá základní systémové protokoly.

Co WinAudit nedokáže: Nezahrnuje pokročilé možnosti správy protokolů nebo integraci s externími systémy pro správu protokolů.

4.2.9 Ochrana e-mailů a webových prohlížečů

Opatření pro zabezpečení e-mailové komunikace a webového prohlížení proti malwaru a phishingovým útokům.

Co WinAudit dokáže: Identifikuje nainstalované webové prohlížeče.

Co WinAudit nedokáže: Nezahrnuje ochranu proti hrozbám z e-mailů nebo webových prohlížečů, jako je blokování škodlivých příloh nebo URL.

4.2.10 Obrana proti malwaru

Implementace a správa opatření na ochranu před malwarovými hrozbami.

Co WinAudit dokáže: Zjistí antivirové programy nainstalované na systému.

Co WinAudit nedokáže: Nezahrnuje aktivní monitorování nebo odstraňování malwaru.

4.2.11 Obnova dat

Zajištění schopnosti společnosti rychle a efektivně obnovit data po bezpečnostním incidentu.

Co WinAudit dokáže: Identifikuje existenci zálohovacího softwaru.

Co WinAudit nedokáže: Neprovádí zálohování ani obnovu dat.

4.2.12 Správa síťové infrastruktury

Správa a bezpečnost síťové infrastruktury, včetně zařízení a komunikačních kanálů.

Co WinAudit dokáže: Zjišťuje základní síťové konfigurace a statistiky.

Co WinAudit nedokáže: Neumožňuje správu síťové infrastruktury nebo sledování síťového provozu.

4.2.13 Monitorování a obrana sítě

Aktivní monitorování a obrana sítě pro detekci a reakci na potenciální hrozby.

Co WinAudit dokáže: Sbírá základní informace o síti a připojeních.

Doplnění o pravidla firewallu: Podrobnější výpis všech pravidel firewallu.

Co WinAudit nedokáže: Neobsahuje nástroje pro hloubkovou analýzu síťového provozu nebo detekci hrozeb v reálném čase.

4.2.14 Školení a zvyšování bezpečnostního povědomí

Vzdělávání zaměstnanců o bezpečnostních hrozbách a osvědčených postupech.
Co WinAudit dokáže: Nezahrnuje funkce související s tímto kontrolním bodem.
Co WinAudit nedokáže: Nezahrnuje školicí moduly nebo nástroje pro zvyšování bezpečnostního povědomí.

4.2.15 Správa poskytovatelů služeb

Řízení bezpečnostních rizik spojených s externími poskytovateli služeb.
Co WinAudit dokáže: Nezahrnuje funkce související s tímto kontrolním bodem.
Co WinAudit nedokáže: Nezahrnuje správu poskytovatelů služeb ani hodnocení bezpečnostních rizik.

4.2.16 Bezpečnost aplikací

Zabezpečení aplikací používaných v podnikovém prostředí.
Co WinAudit dokáže: Nezahrnuje funkce související s tímto kontrolním bodem.
Co WinAudit nedokáže: Nezahrnuje nástroje pro testování bezpečnosti aplikací nebo revize kódu.

4.2.17 Řízení incidentů

Příprava a reakce na bezpečnostní incidenty pro minimalizaci jejich dopadu.
Co WinAudit dokáže: Nezahrnuje funkce související s tímto kontrolním bodem.
Co WinAudit nedokáže: Nezahrnuje nástroje pro řízení incidentů, sledování incidentů nebo forenzní analýzu.

4.2.18 Testování penetračními testy

Pravidelné testování bezpečnostních opatření prostřednictvím simulovaných útoků za účelem identifikace a řešení zranitelností.
Co WinAudit dokáže: Nezahrnuje funkce související s tímto kontrolním bodem.
Co WinAudit nedokáže: Nezahrnuje nástroje pro penetrační testování nebo hodnocení bezpečnosti.

4.2.19 Závěrečná doporučení

Na konci této kapitoly bude uvedeno několik doporučení, které mohou pomoci v oblastech, kde kontrola za pomoci systému z této práce nedokáže příliš pomoci.

Ochrana dat pomocí šifrování:

Použití BitLocker: V rámci Windows, lze aktivovat BitLocker pro šifrování celého disku. Toto šifrování zabraňuje neoprávněnému přístupu k datům, pokud by došlo ke ztrátě nebo krádeži zařízení.
Šifrování souborů a složek: Pro důležité soubory nebo citlivá data lze použít nástroje jako VeraCrypt pro šifrování jednotlivých souborů a složek.

Bezpečnost aplikací a vývoj softwaru:

Bezpečnostní revize kódu: Pravidelně provádět bezpečnostní revize a statickou analýzu kódu, aby byly odhaleny potenciální slabiny před nasazením aplikace.
Ochrana webových aplikací: Použití Web Application Firewall (WAF) pro ochranu vašich webových aplikací před běžnými útoky, jako jsou SQL injection a cross-site scripting (XSS).

Řízení incidentů a odpovědi:

Plán řízení incidentů: Vypracujte a pravidelně aktualizujte plán řízení bezpečnostních incidentů, který zahrnuje postupy pro identifikaci, reakci a zotavení z bezpečnostních incidentů.
Nástroje pro detekci a reakci na incidenty (EDR): Zvažte implementaci řešení EDR (Endpoint Detection and Response), které poskytuje pokročilé sledování a reakční schopnosti pro identifikaci podezřelých aktivit na koncových bodech.

Bezpečnostní školení a povědomí:

Pravidelné školení zaměstnanců: Organizujte pravidelná školení o bezpečnostních hrozbách a osvědčených postupech, aby byli zaměstnanci informováni a mohli lépe rozpoznat phishingové útoky a další sociálně inženýrské taktiky.
Simulace phishingových útoků: Pravidelně testujte své zaměstnance pomocí simulovaných phishingových kampaní, aby byli lépe připraveni na skutečné hrozby.

Segmentace sítě: Použijte segmentaci sítě pro oddělení kritických aktiv od ostatních částí sítě, čímž snížíte riziko šíření hrozeb.
Pokročilá detekce hrozeb: Zvažte použití systémů pro detekci a prevenci průniku (IDS/IPS) pro monitorování a reakci na podezřelé síťové aktivity.

4.3 Průzkum výsledků CIS-CAT® Pro Assessor

Díky spolupráci s firmou Hitachi byla možnost si vyzkoušet licencovaný nástroj od společnosti CIS, který provádí různě důkladné kontroly dle zadaných parametrů. Jelikož jsem testoval pouze na domácím desktopovém počítači, který funguje v rámci celé sítě prakticky jako jediný přístroj, zvolil jsem kontrolu nejnižšího stupně zabezpečení IG1, viz jejich definice výše. Kompletní výsledky této kontroly lze najít ve dvou formátech (txt a html) jako Přílohu č. 2 - Odkaz na adresář kontroly bezpečnostních nastavení na GitHubu. Zároveň je kontrolovaný stroj a jeho systém Windows 11 specificky upravený na rychlost a efektivitu práce, spíše než na zabezpečení. Rychlé shrnutí formou screenshotu webové stránky přikládám na Obrázek 15 níže.
Stručný přehled výsledků, hlavně těch negativních s odůvodněním, proč je použito dané nastavení:

1. Uživatelská kontrola a přístup:

Nedostatečné nastavení politik hesel, jako je historie hesel, minimální délka hesla a komplexita hesel. To může usnadnit neoprávněný přístup k účtům.
Na svém desktopovém počítači, jakožto člověk žijící sám, žádné heslo nastavené nemám, takže politiky s ním spojené jsou stejně irelevantní.

2. Ochrana účtů:

Slabé nastavení zabezpečení pro blokování účtů, což zahrnuje nastavení pro trvání blokace účtu a prahové hodnoty pro neúspěšné pokusy o přihlášení. Tyto politiky jsou klíčové pro ochranu proti útokům hrubou silou.
Stejné odůvodnění jako předchozí bod, bez hesla nemůže dojít k neplatnému přihlášení.

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Account Policies	2	8	0	0	1	0	2.0	10.0	20%
1.1 Password Policy	2	5	0	0	0	0	2.0	7.0	29%
1.2 Account Lockout Policy	0	3	0	0	1	0	0.0	3.0	0%
2 Local Policies	59	39	0	0	1	0	59.0	98.0	60%
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	32	29	0	0	1	0	32.0	61.0	52%
2.3.1 Accounts	2	3	0	0	0	0	2.0	5.0	40%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	0	0	0	0	0	0.0	0.0	0%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	1	6	0	0	0	0	1.0	7.0	14%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	0	2.0	5.0	40%
2.3.10 Network access	9	3	0	0	0	0	9.0	12.0	75%
2.3.11 Network security	2	9	0	0	1	0	2.0	11.0	18%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	5	3	0	0	0	0	5.0	8.0	62%
3 Event Log	0	0	0	0	0	0	0.0	0.0	0%
4 Restricted Groups	0	0	0	0	0	0	0.0	0.0	0%
5 System Services	10	10	0	0	0	0	10.0	20.0	50%
6 Registry	0	0	0	0	0	0	0.0	0.0	0%
7 File System	0	0	0	0	0	0	0.0	0.0	0%
8 Wired Network (IEEE 802.3) Policies	0	0	0	0	0	0	0.0	0.0	0%
9 Windows Defender Firewall with Advanced Security (formerly Windows Firewall with Advanced Security)	0	23	0	0	0	0	0.0	23.0	0%
9.1 Domain Profile	0	7	0	0	0	0	0.0	7.0	0%
9.2 Private Profile	0	7	0	0	0	0	0.0	7.0	0%
9.3 Public Profile	0	9	0	0	0	0	0.0	9.0	0%
10 Network List Manager Policies	0	0	0	0	0	0	0.0	0.0	0%
11 Wireless Network (IEEE 802.11) Policies	0	0	0	0	0	0	0.0	0.0	0%
12 Public Key Policies	0	0	0	0	0	0	0.0	0.0	0%
13 Software Restriction Policies	0	0	0	0	0	0	0.0	0.0	0%
14 Network Access Protection NAP Client Configuration	0	0	0	0	0	0	0.0	0.0	0%
15 Application Control Policies	0	0	0	0	0	0	0.0	0.0	0%
16 IP Security Policies	0	0	0	0	0	0	0.0	0.0	0%
17 Advanced Audit Policy Configuration	9	18	0	0	0	0	9.0	27.0	33%
17.1 Account Logon	0	1	0	0	0	0	0.0	1.0	0%
17.2 Account Management	1	2	0	0	0	0	1.0	3.0	33%
17.3 Detailed Tracking	0	2	0	0	0	0	0.0	2.0	0%
17.4 DS Access	0	0	0	0	0	0	0.0	0.0	0%
17.5 Logon/Logoff	3	3	0	0	0	0	3.0	6.0	50%
17.6 Object Access	0	4	0	0	0	0	0.0	4.0	0%
17.7 Policy Change	2	3	0	0	0	0	2.0	5.0	40%
17.8 Privilege Use	0	1	0	0	0	0	0.0	1.0	0%
17.9 System	3	2	0	0	0	0	3.0	5.0	60%

Obrázek 15: Výstup nástroje Assessor (Autor)

3. Síťová bezpečnost:

Nedostatečné omezení NTLM a auditace příchozího NTLM provozu, což zvyšuje riziko útoků založených na prolomení autentizačních protokolů.

Slabé nastavení pro přístup k síťovým zdrojům, včetně nedostatečné ochrany před anonymním přístupem a konfigurace firewallu.

Chybné nastavení se týká primárně sítě LAN, na kterou by se neměl mít kdo připojit v tomto případě.

4. Servisy Windows

Bylo spuštěno několik zbytečných servis, které jsou defaultně spuštěny OS Windows, i přes snahu optimalizovat systém již před touto kontrolou.
Zde jsem plně poslechl doporučení a všechny přebytečné servisy vypnul.

5. Nastavení brány firewall

V rámci výsledků jsou ukázány všechny části brány firewall jako vypnuté, což ovšem není pravda a ani zbytek výsledků v této části neodpovídá reálnému stavu v systému. Nevím, jestli to bylo způsobeno nějakým specifickým nastavením mého systému, ale tyto nastavení jsou správně, ne tak, jak ukazuje nástroj CIS.

6. Advanced Audit Policy Configuration

Account Logon: Většina nastavení auditování účtů pro ověření přihlášení selhala, což znamená, že nejsou sledovány úspěšné ani neúspěšné pokusy o přihlášení, jelikož jsou všechny pokusy o přihlášení automaticky úspěšné, tak to nemá smysl sledovat.
Account Management: Auditování správy aplikací a uživatelských účtů neprobíhá správně, pouze správa bezpečnostních skupin je nastavena korektně.
Object Access: Nedostatečné auditování přístupu k objektům, jako jsou sdílené soubory a odnímatelná média. Jsem jediný s přístupem do sítě i k PC, nemělo by dojít k žádnému nečekanému přístupu.

5 Výsledky a závěr

Tato práce úspěšně demonstrovala vývoj a implementaci automatizovaného systému pro kontrolu bezpečnostních nastavení systémů založených na platformě Windows, ve spolupráci s firmou Hitachi. Hlavní cíle práce byly splněny tím, že byl vytvořen systém, který efektivně detekuje a dokumentuje změny v bezpečnostních nastaveních, což minimalizuje riziko lidské chyby a zvyšuje celkovou kybernetickou bezpečnost organizace. Průběh práce odhalil několik klíčových poznatků, zejména význam pravidelné aktualizace a monitorování systémových nastavení v reakci na neustále se vyvíjející kybernetické hrozby.

Teoretická část práce poskytuje komplexní přehled o základech kybernetické bezpečnosti, který je zásadní pro pochopení a řešení bezpečnostních výzev spojených s průmyslovými řídicími systémy, jako je MicroSCADA. V této sekci byl podán historický kontext vývoje kybernetických hrozeb a obranných strategií, které formují současný stav kybernetické bezpečnosti. Dále byly zkoumány teoretické principy, modely a standardy, které jsou základem pro současné bezpečnostní praxe.

Praktická část diplomové práce byla zaměřena na vývoj automatizovaného systému pro kontrolu bezpečnostních nastavení systémů založených na platformě Windows, který byla snaha realizovat s využitím nástrojů, jež jsou integrovány přímo do prostředí Windows. Důležitým aspektem implementace byla integrace automatizovaného systému do stávající korporátní infrastruktury společnosti Hitachi. Skripty byly přizpůsobeny tak, aby kompatibilně spolupracovaly s ostatními bezpečnostními nástroji a systémy používanými ve firmě. Proto byl pro audit systému vybrán již firmou používaný nástroj WinAudit a pro ukládání dat databáze Microsoft Access. Pro zisk dalších informací v rámci systému již byly vybrány pouze rutiny a programy, implementované přímo Microsoftem jako součást OS Windows.

Pro dosažení efektivity a integrace s Windows prostředím byl pro vývoj skriptů zvolen jazyk PowerShell. Tato volba umožnila využít pokročilé funkce pro správu systémových nastavení a konfigurací, což výrazně zlepšilo schopnost systému identifikovat kritické změny a potenciální bezpečnostní rizika. Skripty PowerShellu jsou klíčové pro extrakci a porovnání aktuálních nastavení s předchozími stavy, což usnadňuje rychlou identifikaci neautorizovaných nebo podezřelých změn.

Jednou z možných cest rozvoje této práce by mohlo být rozšíření o robustnější kontrolu nastavení v rámci BIOS, ta by mohla být provedena specifickými nástroji od výrobců základních desek, které určují i jak jejich BIOS funguje. Toto rozšíření by ale bylo velmi

obtížné kvůli vysokému počtu výrobců hardwaru a tím pádem i vysokému počtu různých systémů BIOS. Dalším problémem by bylo řešení licencí nástrojů těchto výrobců.

Další možnosti zkoumání by mohly zahrnovat rozšíření systému na jiné operační systémy, jako například různé distribuce Linux, které jsou velmi vhodné k využití jako servery, nebo jeho adaptace pro specifické průmyslové aplikace, což by mohlo výrazně rozšířit jeho aplikovatelnost a užitečnost. Navazující práce by mohly také prozkoumat vliv nově vznikajících technologií, jako je umělá inteligence, na zlepšení automatizovaných bezpečnostních kontrol.

6 Seznam použité literatury

Alam, S. (2024). *Cybersecurity: Past, Present and Future* (arXiv:2207.01227). arXiv. https://doi.org/10.48550/arXiv.2207.01227

Aptien. (2023, December 15). *Co je CIA triáda informační bezpečnosti | Informační bezpečnost | Aptien*. https://aptien.com/cs/kb/articles/what-is-cia-triad

AV-ATLAS, T. I. I.-S. (2024). *AV-ATLAS - Malware & PUA*. AV-ATLAS - Malware & PUA. https://portal.av-atlas.org/malware

Bhagwani, V., & Balasinorwala, S. (2023, August 2). CYBER SECURITY. *IJSREM*. https://ijsrem.com/download/cyber-security-6/

Boura, M. (2022). *Zabezpečení certifikátů Eliptických křivek*.

Center for Internet Security®. (2023, August). *CIS Controls*. CIS. https://www.cisecurity.org/controls/

Choi, S.-K., Yang, C.-H., & Kwak, J. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. *KSII Transactions on Internet and Information Systems*, *12*(2), 906–918.

Cloudflare, Inc. (2024). *What is a WAF? | Web Application Firewall explained*. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

cs.theastrologypage.com. (2024, April). *Co je antivirový software? - Definice z techopedie - Bezpečnostní 2024*. Icy Science. https://cs.theastrologypage.com/anti-virus-software

Dewri, R., Poolsappasit, N., Ray, I., & Whitley, D. (2007). *Optimal security hardening using multi-objective optimization on attack tree models of networks*. 204–213. https://doi.org/10.1145/1315245.1315272

Fard, M. F., Sahraei-Ardakani, M., Ou, G., & Liu, M. (2022). Targeted Hardening of Electric Distribution System for Enhanced Resilience against Earthquakes. *2022*

IEEE 31st International Symposium on Industrial Electronics (ISIE), 870–875. https://doi.org/10.1109/ISIE51582.2022.9831593

Hitachi Energy. (2022, October 21). *MicroSCADA X | Hitachi Energy*. https://www.hitachienergy.com/products-and-solutions/scada/microscada-x

JasonGerend. (2024, February 7). *Windows 11 and Windows Server 2022*. https://learn.microsoft.com/en-us/powershell/windows/get-started?view=windowsserver2022-ps

Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 20:1-20:34. https://doi.org/10.1145/3372823

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE*, *104*(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235

Parmavex Services. (2014). *WinAudit*. https://winaudit18.rssing.com/chan-66076478/all_p5.html

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing (5th Edition)* (5th ed.). Prentice Hall Press.

Python Software Foundation. (2024, April 14). *difflib—Helpers for computing deltas*. Python Documentation. https://docs.python.org/3/library/difflib.html

Security.org Team. (2023, February 22). 2023 Antivirus Market Annual Report. *Security.Org*. https://www.security.org/antivirus/antivirus-consumer-report-annual/

Smith, J., Pereyda, J., & Gammel, D. (2016). Cybersecurity best practices for creating resilient control systems. *2016 Resilience Week (RWS)*, 62–66. https://doi.org/10.1109/RWEEK.2016.7573308

Tarhan, K. (2023). Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies. *Przegląd Strategiczny*, 393–414. https://doi.org/10.14746/ps.2022.1.23

Ujjwal Rao. (2023). Overview of Cyber Security. *International Journal of Advanced Research in Science, Communication and Technology*, 47–51. https://doi.org/10.48175/IJARSCT-9470

Zscaler™. (2024). *What Is the Purdue Model for ICS Security? | Zscaler*. https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

7 Přílohy

7.1 Odkaz na adresář práce na GitHubu

https://github.com/bourama1/DiplProg

7.2 Odkaz na adresář kontroly bezpečnostních nastavení na GitHubu

https://github.com/bourama1/DiplReports

8 Zadání práce z IS (eVŠKP)

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2023/2024

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Matěj Boura**
Osobní číslo:	**I2200595**
Adresa:	Družstevní 803, Nový Bydžov, 50401 Nový Bydžov, Česká republika
Téma práce:	Systém pravidelné kontroly bezpečnostních nastavení řídicího systému MicroSCADA
Téma práce anglicky:	Regular control of safety settings of the MicroSCADA control system
Jazyk práce:	Čeština
Vedoucí práce:	doc. Ing. Vladimír Soběslav, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Základní bezpečnostní opatření zahrnují různá bezpečnostní nastavení operačních systémů (nastavení v registrech, lokální nebo globální politiky, firewall atd.) i samotného HW počítačů (BIOS atd.). Cílem je navrhnout a odzkoušet systém, kterým by bylo možno pravidelně (např. jednou do roka) porovnat skutečná nastavení s původními (zjisti, zda nedošlo ke změně bezpečnostních nastavení obsluhou apod.). Předpokládáme, že některé kontroly bude možné automatizovat a některé budou "ruční".
Dále se práce věnuje teoretické části, která poskytuje komplexní přehled o základech kyberbezpečnosti, s důrazem na její význam pro řídicí systémy v průmyslových aplikacích a také podorobně rozebírá problematika kybernetických hrozeb vztahujících se k řídicím systémům, včetně historických příkladů, které ilustrují potenciální dopady těchto hrozeb na průmyslové a infrastrukturní operace.
Osnova:

1. Úvod
2. Cíl a metodika práce
3. Kybernetická bezpečnost průmyslových systémů
4. Systém pravidelné kontroly s využitím nástrojů CIS
5. Výsledky a závěr

Seznam doporučené literatury:

1. Alam, S. (2024). *Cybersecurity: Past, Present and Future* (arXiv:2207.01227). arXiv. https://doi.org/10.48550/arXiv.2207.01227
2. Bhagwani, V., & Balasinorwala, S. (2023, August 2). CYBER SECURITY. *IJSREM*. https://ijsrem.com/download/cyber-security-6/
3. Boura, M. (2022). *Zabezpečení certifikátů Eliptických křivek*.
4. Center for Internet Security®. (2023, August). *CIS Controls*. CIS. https://www.cisecurity.org/controls/
5. Choi, S.-K., Yang, C.-H., & Kwak, J. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. *KSII Transactions on Internet and Information Systems*, *12*(2), 906–918.
6. Cloudflare, Inc. (2024). *What is a WAF? | Web Application Firewall explained*. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/
7. Dewri, R., Poolsappasit, N., Ray, I., & Whitley, D. (2007). *Optimal security hardening using multi-objective optimization on attack tree models of networks*. 204–213. https://doi.org/10.1145/1315245.1315272
8. Fard, M. F., Sahraei-Ardakani, M., Ou, G., & Liu, M. (2022). Targeted Hardening of Electric Distribution System for Enhanced Resilience against Earthquakes. *2022 IEEE 31st International Symposium on Industrial Electronics (ISIE)*, 870–875. https://doi.org/10.1109/ISIE51582.2022.9831593
9. Hitachi Energy. (2022, October 21). *MicroSCADA X | Hitachi Energy*. https://www.hitachienergy.com/products-and-solutions/scada/microscada-x
10. JasonGerend. (2024, February 7). *Windows 11 and Windows Server 2022*. https://learn.microsoft.com/en-us/powershell/windows/get-started?view=windowsserver2022-ps
11. Kaloudi, N., & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 20:1-20:34. https://doi.org/10.1145/3372823

12. Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348
13. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE*, *104*(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235
14. Parmavex Services. (2014). *WinAudit*. https://winaudit18.rssing.com/chan-66076478/all_p5.html
15. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing (5th Edition)* (5th ed.). Prentice Hall Press.
16. Python Software Foundation. (2024, April 14). *difflib—Helpers for computing deltas*. Python Documentation. https://docs.python.org/3/library/difflib.html
17. Security.org Team. (2023, February 22). 2023 Antivirus Market Annual Report. *Security.Org*. https://www.security.org/antivirus/antivirus-consumer-report-annual/
18. Smith, J., Pereyda, J., & Gammel, D. (2016). Cybersecurity best practices for creating resilient control systems. *2016 Resilience Week (RWS)*, 62–66. https://doi.org/10.1109/RWEEK.2016.7573308
19. Tarhan, K. (2023). Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies. *Przegląd Strategiczny*, 393–414. https://doi.org/10.14746/ps.2022.1.23
20. Ujjwal Rao. (2023). Overview of Cyber Security. *International Journal of Advanced Research in Science, Communication and Technology*, 47–51. https://doi.org/10.48175/IJARSCT-9470

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: