VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

METODIKA PENETRAČNÍHO TESTOVÁNÍ V PRŮMYSLOVÝCH ŘÍDÍCÍCH SYSTÉMECH

METHODOLOGY OF PENTESTING IN INDUSTRIAL CONTROL SYSTEMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Patrik Slabý**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Patrik Slabý**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2021/22
Studijní program:	Informační management

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

Metodika penetračního testování v průmyslových řídících systémech

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrh řešení a přínos práce
Závěr

Cíle, kterých má být dosaženo:

Vytvoření metodiky penetračního testování v průmyslových řídících systémech.

Základní literární prameny:

BODUNGEN, Clint E., Bryan L. SINGER, Aaron SHBEEB, Stephen HILT a Kyle WILHOIT. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. New York: McGraw-Hill Education, 2017. ISBN 978-1-25-958971-3.

JORDÁN Vilém a Viktor ONDRÁK. INFRASTRUKTURA KOMUNIKAČNÍCH SYSTÉMŮ II. Kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-2145-240-4.

JORDÁN Vilém a Viktor ONDRÁK. INFRASTRUKTURA KOMUNIKAČNÍCH SYSTÉMŮ III. Integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-2145-241-1.

KNAPP, Eric D. a Joel LANGILL. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. London: Syngress, 2015. ISBN 978-0-12-420114-9.

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

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato diplomová práce se zaobírá návrhem metodiky penetračního testování průmyslových řídících systémů. Záměrem práce je přiblížit problematiku těchto systémů, jež mají zcela jiné priority než systémy informačních technologií a na základě těchto parametrů poté navrhnout postup a pravidla, kterými by se měly subjekty podílející se na testech řídit. Absence metodiky pro takto specifické prostředí ovlivňující kybernetický i fyzický prostor může mít katastrofální dopady. Teoretická část se věnuje základním pojmům a terminologii důležité pro informační a kybernetickou bezpečnost, operační technologie a penetrační testy. Vlastní návrh poté obsahuje popis jednotlivých kroků metodiky penetračního testování pro průmyslové řídící systémy.

Klíčová slova

operační technologie, průmyslové řídící systémy, penetrační testování, metodika penetračního testování

Abstract

This diploma thesis deals with the design of a methodology for penetration testing of industrial control systems. This work aims to approach the issue of these systems, which has completely different priorities than information technology systems, and based on these parameters to then design a procedure and rules that should be followed by the subjects participating in the tests. The absence of a methodology for such a specific environment affecting cyberspace and physical space can have catastrophic consequences. The theoretical part deals with basic concepts and terminology important for information and cyber security, operational technologies, and penetration tests. The design then contains a description of the individual steps of the penetration testing methodology for industrial control systems.

Key words

operational technologies, industrial control systems, penetration testing, methodology of penetration testing

Bibliografické citace

SLABÝ, Patrik. *Metodika penetračního testování v průmyslových řídících systémech* [online]. Brno, 2022 [cit. 2022-05-08]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/143237. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 8. května 2022

……

podpis studenta

Poděkování

Touto cestou chci poděkovat svému vedoucímu práce Ing. Petru Sedlákovi, nejen za vedení diplomové práce, ale i za cenné informace, rady a zkušenosti předávané v průběhu celého studia. Velice si vážím také jeho ochoty vždy pomoci. Dále chci poděkovat mému oponentovi RNDr. Mgr. Ing. Lukáši Petrovi a za podporu při studiu své rodině, přátelům a kolegům.

OBSAH

ÚVOD

Dvacet let trvá si vybudovat reputaci. A pár okamžiků kybernetického útoku ji může celou zničit.

Globální stav kybernetické kriminality je na vzestupu. Její dokumentace probíhá v široké škále a můžeme si tak jednotlivé útoky promítat v reálném čase na našich obrazovkách. Subjekty, používající pro náplň svých pracovních povinností výpočetní techniku, jsou nuceni zvyšovat bezpečnostní povědomí u svých zaměstnanců. Odborníci vydávají nové doporučení, normy nebo směrnice. Dá se tvrdit, že máme všechny podstatné aspekty, které jsou potřebné pro zajištění bezpečnosti osob, firem i společnosti. Problémem se stává jejich implementace, kdy dochází k selhání mezi tranzitem popisu cílového stavu a reálného stavu. Což má za následek vznik bezpečnostních mezer umožňujících zacílení jakékoliv organizace vedoucí k možnému vytvoření bezpečnostního incidentu. Předpokladem k naplnění škody je tedy u útočníka pouze dostatek financí a času.

Musíme si počátečně uvědomit jednu skutečnost – hrdinové musejí vyhrát vždy, zatímco padouchům stačí vyhrát pouze jednou. Do role hrdiny můžeme adaptovat subjekty snažící se naplňovat své stanovené vize, mise a cíle pro zajištění uspokojení svých zákazníků, ať již produkty nebo službami. Padouši jsou poté narušitelé této činnosti snažící se tento proces kompromitovat s cílem oslabení daného subjektu, vidiny finanční odměny nebo prosazování svého názoru kriminální činností.

Možnost útoku na aktiva subjektu se tedy snažíme omezit na co možná nejmenší míru. Efektivní obranná činnost je však vždy náročnější než činnost útočná s cílem poškodit. Proto k celkovému zlepšení úrovně kybernetické bezpečnosti využíváme činností obou. A nejlépe jejich kombinaci. Pro simulaci reálného útoku je využíváno penetračních testů v různém rozsahu a zaměření. Zatímco v oblasti informačních technologií je jejich využití běžnou součástí již řádku let, do operačních technologií se testy zařazují teprve nedlouho.

Operační technologie a jejich penetrační testování s sebou nesou nová úskalí, jež je potřeba regulovat a řídit. Oproti penetračnímu testu informačních technologií, je v případě nekorektního testování u operačního prostředí možné ohrozit zdraví osob a způsobit velké škody na majetku objednatele penetračního testu. Prioritou je, a vždy bude, zajistit dostupnost daného průmyslového řídícího systému pro poskytování jeho základní služby se značným důrazem na bezpečnost celého procesu testování.

Největším podnětem pro provádění testů průmyslových řídících systémů se stal v roce 2010 Stuxnet, poukazující na staronové problémy. Od tohoto data byl spuštěn globální výzkum na úrovni zabezpečení těchto systémů. Odhalil problémy s nezabezpečenou komunikací na úrovni protokolů, jednoduché zajištění nedostupnosti systémů či pevné kódování hesel v paměti. Využívání zastaralých operačních systémů, vzhledem k životnosti v řádech desetiletí, není také ničím neobvyklým.

Na základě zmíněných skutečností vznikne v rámci této práce metodika penetračního testování průmyslových řídích systémů, definující veškeré činnosti potřebné k zajištění v tomto prostředí. Bude navržen koncept úrovňového testování, dle kterého se může objednatel řešení řídit s možností využití nástrojů dodavatelem pro jednotlivé činnosti. Celá práce je koncipována jako mezioborové řešení s názvem PENTICS.

„Umění války nás učí nedoufat, že nepřítel nepřijde, ale spoléhat se na to, že jsme připraveni ho přivítat; nedoufat, že nezaútočí, ale spoléhat se, že jsme svá postavení učinili nedobytnými.“

— Sun Tzu

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Zprvu by se mohl zdát rozdíl mezi informačními a operačními technologiemi zanedbatelný. Opak je ovšem pravdou, a ne jinak tomu je s přístupem k penetračnímu testování těchto prostředí.

Cílem této práce je vytvoření metodiky penetračního testování průmyslových řídících systémů, která bude definována na mezioborové úrovni.

Vyhotovená metodika PENTICS by měla obsahovat postup a případné návodné ukázky provádění jednotlivých částí, jakožto i doporučení použití nástrojů. Subjekty by se na základě metodiky měly být schopny řídit a postupovat v celém průběhu testování, a tak dojít k bezpečnému zvládnutí celého procesu penetračního testování průmyslových řídících systémů bez ohrožení osob a majetku.

V mnoha případech jsou celky řízené průmyslovými řídícími systémy určeny jako kritická infrastruktura státu. Z toho důvodu je v rámci teoretické práce popsána legislativní problematika týkající se kybernetické bezpečnosti, audit kybernetické bezpečnosti a instituce v České republice, které mohou být zainteresovány při řešení bezpečnosti kritické infrastruktury státu. Je také nutné vyčlenit si rozdíl mezi kybernetickou a informační bezpečností, protože se jednotlivé pojmy často zaměňují nebo spojují dohromady. Představeny budou samotné průmyslové řídící systémy, normy, které se na ně vztahují a koncept penetračního testování.

Analytická část se zabývá analýzou současného stavu vztahu povinnosti penetračního testování z hlediska zákon a popis motivu pro tvorbu nové metodiky penetračního testování. Bude prezentován problém s průmyslovými řídícími systémy v rámci ukázky dostupnosti těchto systémů z veřejně dostupné sítě, jejich zabezpečení nebo historie útoků. Zmíní se i problematika penetračního testování těchto systémů.

Na základě analytické části bude poté koncipován samotný návrh metodiky penetračního testování průmyslových řídících systémů PENTICS. Zde bude navržena koncepce úrovňového testování, dle které se budou moci jednotlivé subjekty zainteresované při penetračním testování řídit a postupovat.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V rámci části teoretických východisek práce se budu zaobírat popisem pojmů a jejich představením. Jednotlivé části by měly poukázat na propojení průmyslových řídících systémů a vlivu na život celé společnosti. Nejdříve budou představeny legislativní požadavky, které se týkají České republiky. Rozeberu také rozdíl mezi kybernetickou a informační bezpečností, nebo vysvětlím, co znamená audit kybernetické bezpečnosti. Zaměřím se také na instituce zaobírající se kybernetickou bezpečností v České republice a následně vymezím teoretický základ pro pochopení informačních technologií, technologií operačních a z nich konkrétně průmyslových řídících systémů.

1.1 Legislativa

V České republice se kybernetickou a informační bezpečností zabývá zákon č. 181/2014 Sb., novela zákona o kybernetické bezpečnosti a o změně souvisejících zákonů, zákon č.205/2017 Sb., novela zákona o kybernetické bezpečnosti, směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 a opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS) a vyhláška č.82/2018 Sb., o kybernetické bezpečnosti (1).

1.1.1 Zákon č.181/2014., o kybernetické bezpečnosti a o změně souvisejících zákonů

Návrh zákona o kybernetické bezpečnosti (ZKB) byl předložen ještě pod taktovkou Národního bezpečnostního úřadu (NBÚ) a vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015. Je transpozicí směrnice NIS a upravuje „*práva a povinnosti osob, jakož i pravomoc a působnost orgánů a veřejné moci v oblasti kybernetické bezpečnosti*“ (1).

Hlavními cíli zákona jsou:

- definovat základní úroveň bezpečnostních opatření,
- detekce kybernetických bezpečnostních incidentů,
- hlášení kybernetických bezpečnostních incidentů,
- systém opatření k reakci na kybernetické bezpečnostní incidenty
- a další (1).

Zákon o kybernetické bezpečnosti je závazný celkem pro 7 subjektů, jež jsou definovány v § 3 ZKB. Jedná se o následující:

- poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací,
- orgán nebo osoba zajišťující významnou síť,
- správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury (KII),
- správce a provozovatel významného informačního systému (VIS),
- provozovatel základních služby nebo správce a provozovatel informačního systému základní služby (PZS),
- poskytovatel digitální služby (PDS),
- orgán veřejné moci využívající služeb poskytovatelů cloud computingu (2).

1.1.2 Vyhláška 82/2018 Sb., o kybernetické bezpečnosti

Aktuální vyhláška č. 82/2018 Sb. byla vydaná Národním úřadem pro kybernetickou bezpečnost (NÚKIB) s platností od 21. května 2018. Zapracovává Směrnici NIS a nahradila předchozí vyhlášku č. 316/2014 Sb., o kybernetické bezpečnosti. Upravuje tak:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického incidentu,
- náležitosti oznámení a provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob a likvidace dat, provozních údajů, informací a jejich kopií (stanoveno bodem g, který se přidal s aktualizací vyhlášky) (1).

Jedním z nejpodstatnějších bodů vyhlášky je hlášení kybernetického bezpečnostního incidentu, což může být provedeno elektronickou formou, nebo v listinné podobě pomocí formuláře (pouze v případech, kdy nelze využít elektronickou komunikaci). V případě využití elektronické formy se využívá formuláře zveřejněného na stránkách Úřadu, e-mailu na adresu elektronické pošty Úřadu (výhradně určená pro příjem hlášení kybernetických bezpečnostních incidentů), datovou zprávou do datové pošty Úřadu nebo prostřednictvím datového rozhraní (1, 3).

Kategorizace kybernetického bezpečnostního incidentu dle VKB:

- Kategorie III – velmi významný kybernetický bezpečnostní incident,
- Kategorie II – významný kybernetický bezpečnostní incident,
- Kategorie I – méně významný kybernetický bezpečnostní incident (1).

1.1.3 Směrnice NIS

Směrnice NIS, celým názvem směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Cílem této směrnice je „*harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu*“ (3). Část povinností, které směrnice NIS ukládá, jsou řešeny již v ZKB. Právě na základě této směrnice byly přidány 2 subjekty – provozovatel základních služeb a poskytovatel digitálních služeb (3,4)

Poskytovatelem digitálních služeb je jakákoli osoba poskytující digitální službu (on-line tržiště, internetový vyhledávač, službu cloud computingu) (4).

Provozovatel základní služby může být veřejný nebo soukromý subjekt a je tak alternativou KII. Základní službou chápeme službu, která je závislá na elektronických komunikačních sítích nebo informačních systémech. Pokud by došlo k narušení služby, tak by mohlo dojít k významnému dopadu na zabezpečení společenských nebo ekonomických činnosti v energetice, dopravě, bankovnictví, infrastruktuře finančních trhů, zdravotnictví, vodním hospodářství, digitální infrastruktuře a chemickém průmyslu (4).

1.2 Kybernetická a informační bezpečnost

V názvosloví kybernetická a informační bezpečnost má mnoho odborníků nesrovnalosti. Někteří se dokonce domnívají, že jsou tyto pojmy synonymem, ačkoli tomu tak není. Kybernetická a informační bezpečnost se liší především jejich perimetrem.

Kybernetická bezpečnost je bezpečnost zabývající se celým kybernetickým prostorem. Přičemž kybernetickým prostorem rozumíme prostředí, ve kterém se zpracovávají, vyměňují a vytváří informace. Je tvořený informačními systémy, službami a komunikačními sítěmi. Kybernetická bezpečnost zahrnuje právní, organizační, technické a vzdělávací prostředky, směřující k ochraně kybernetického prostoru (3, 4).

Informační bezpečnost, používá se také bezpečnost informací, se poté zabývá celou organizací – fyzickou, personální, organizační i komunikační bezpečností. Je zastřešena řadou norem ISO/IEC 27000 a informační bezpečnost řeší konkrétně norma ISO/IEC 270002. Ta definuje úkol zajištění CIA triády, tedy:

- dostupnost,
- integrita,
- důvěrnost (3, 4, 5, 6).

Mimo jiné má zabezpečit ochranu aktiv před poškozením, krádeží nebo přírodní katastrofou (3,4).

1.3 Audit kybernetické bezpečnosti

Audit je obecně definován jako „systematický, nezávislý a dokumentovaný proces získávání důkazů a jejich hodnocení pro stanovení rozsahu splnění požadovaných kritérií“ (3, s. 130). Cílem je zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a následně sdělit výsledky zainteresovaným zájemcům. U auditu se jedná o třístranný vztah, může být interní (organizace provádí pomocí vlastních sil) nebo externí (využití prostředků nezávislého subjektu). Externí audit slouží jako podklad pro certifikaci (3, 7).

Audit se provádí minimálně 1x ročně (dozorovaný audit) a skládá se z následujících fází:

- zahájení auditu,
- přezkoumání dokumentace,
- provádění auditu na místě,
- vyhotovení zprávy o auditu,
- dokončení auditu (3, 7).

1.4 Normalizační instituce

Normalizační instituce se zabývají mimo standardizační činnosti i standardizací bezpečnosti IT na různých úrovní. Jednotlivé instituce dělíme dle jejich působnosti na nadnárodní a světové, evropské, národní a další (3).

1.4.1 Nadnárodní a světové

Na nadnárodní a světové úrovni existuje úzká spolupráce mezi organizacemi jako je ISO, IEC nebo ITU. Jejich roli při vydávání tzv. *základních norem* si popíšeme v následujících odstavcích (3).

International Organization for Standardization (ISO)

ISO si za své poslání klade podporu rozvoje standardizačních aktivit po celém světě. Cíl přitom mají definovaný zcela jasně – zjednodušení směny zboží a služeb, spolupráce na aktivitách týkajících se intelektu, vědy, technologií a ekonomiky (3).

International Electrotechnical Comission (IEC)

Celosvětová organizace připravující vydávání mezinárodních norem pro elektrotechnické, elektronické a jim příbuzné oblasti (elektřina, magnetismus, multimédia, telekomunikace, distribuce energií, navrhování nebo bezpečnost) (3).

International Telecommunications Union (ITU)

Organizace spadající pod hierarchii OSN pomocí svých normalizačních aktivit podporuje nové technologie jako jsou mobilní technologie nebo internet. Aktuální zájem dnes směřuje ke stavebním prvkům v globální informační infrastruktuře a k tvorbě multimediálních systémů. ITU je i nadále ve vedoucí roli ve správě spekter radiové frekvence, proto i nadále zařízení (celulární telefony, letecké a námořní naváděcí systémy, vědecké výzkumné stanice, satelitní komunikace apod.) vysílají stále hladce a poskytují tak spolehlivé bezdrátové služby (3).

1.4.2 Evropské

I na evropské úrovni existuje spolupráce mezi jednotlivými institucemi, mezi které se řadí CEN, CENELEC a ETSI. Úroveň spolupráce zde vychází ze strany CENELEC, jenž spolupracuje s organizacemi CEN a ETSI (3).

Comité Européen Normalisation (CEN)

Podpora dobrovolné harmonizace technických norem v Evropě, to je přesně to, co je posláním CEN. Podporuje bezpečnost, umožňuje funkčnost výrobků, systémů a služeb. Mimo jiné má několik technických komisí s označením CEN/ISSS zabývajících se IT bezpečností (3).

Comité Européen de Normalisation Eléctrotechnique (CENELEC)

Jak bylo zmíněno na začátku, CENELEC úzce spolupracuje s organizacemi CEN a ETSI. Vytvořila dokonce nový sektor zabývající se ICT, kam jsou soustředěny aktivity spojené i s oblastí informačních a komunikačních technologií (3).

European Telecommunications Standards Institute (ETSI)

Organizace ETSI je nezisková a jejím cílem je vytváření telekomunikačních norem se zaměřením na evropské potřeby (3).

1.4.3 Národní

Národní normalizační instituce zajišťují normalizaci v oblasti informačních technologií v jednotlivých státech a většinou spadají pod organizace ISO a/nebo IEC (3).

American National Standards Institute (ANSI)

Jedná se o národní normalizační institut v USA, který sám o sobě nevytváří své národní normy. Zajišťuje spíše vývoj pomocí konsensu u jednotlivých kvalifikovaných skupin (3).

British Standard Institute (BSI)

Britský institut složený z odborníků s patřičnou kvalifikací a zkušenostmi. Ti vydávají draft (návrh) normy, který je poté podobu 60 dní dostupný veřejnosti a umožňuje tak veřejné připomínkování. Posléze proběhne posouzení jednotlivých připomínek
a publikace (3).

Deutsches Institut für Normung (DIN)

Německý institut založený na veřejné diskusi představitelů různých odvětví (průmysl, obchod, služby, věda, vláda apod.), jenž umožňuje jejich setkání a vytvoření definic pro vytvoření německé normy (3).

Český normalizační institut (ČSNI)

Nejdříve státní příspěvková organizace, aktuálně podřízená organizace pod Ministerstvem průmyslu a obchodu, zastupující naše zájmy v mezinárodních a evropských normalizačních institutech. Je právoplatným členem organizací ISO, IEC, CEN, CENELEC a dokonce ETSI. Zaměřuje se především na tvorbu českých technických norem, jejich vydávání a distribuci, poskytování informací o technických normách (3).

1.5 Instituce v ČR

V následující kapitole budou zmíněny instituce, které se zaobírají informační a kybernetickou bezpečností v rámci České republiky.

1.5.1 Národní bezpečnostní úřad (NBÚ)

Národní bezpečnostní úřad byl založen roku 1998 na základě zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Od samého počátku je postavení NBÚ stejné, jedná se o orgán výkonné moci, zařazen mezi ústřední a správní úřady. Na základě těchto skutečností není zpravodajskou službou, ani nemá pověření žádnými vyšetřovacími pravomocemi. Jeho hlavním úkolem je vydávání osvědčení (fyzické osobě nebo podnikateli) či dokladu o bezpečnostní způsobilosti (8).

Úřad se zasloužil o uzavření veřejnoprávní smlouvy se sdružením CZ.NIC o provozovateli Národním CSIRT České republiky. Před tímto úkonem bylo provozování CSIRT týmu definováno pouze na úrovni memoranda (nejdříve s Ministerstvem vnitra, posléze Národním bezpečnostním úřadem). Role Národního CSIRT ČR (CSIRT.CZ) je:

- udržování zahraničních vztahů,
- spolupráce se subjekty v rámci ČR,
- Poskytování služeb v oblasti bezpečnosti (řešení a koordinace incidentů, osvěta, proaktivní služby) (9).

1.5.2 Národní centrum kybernetické bezpečnosti (NCKB)

Součástí NBÚ bylo od roku 2011 do roku 2017 také Národní centrum kybernetické bezpečnosti (NCKB), jež vzniklo za účelem koordinace spoluprací na národní a mezinárodní úrovni při předcházení kybernetickým útokům, řešení kybernetických incidentů a dalších. Mimo jiné se zasloužilo o návrh zákona o kybernetické bezpečnosti. Od roku 2017 bylo NCKB vyčleněno z NBÚ a jeho agenda byla převzata Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) (10).

Výkonná sekce zajišťuje především:

- činnost Vládního CERT ČR (GovCERT.CZ),
- prevence před kybernetickými hrozbami,
- řešení a koordinace kybernetických bezpečnostních incidentů,
- výzkum a vývoj v oblasti kybernetické bezpečnosti a další (10).

1.5.3 Národní útvar pro kybernetickou a informační bezpečnost (NÚKIB)

NÚKIB je „*ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany*“ (11). Byl zaveden na základě novely zákona o kybernetické bezpečnosti 1. srpna 2017 a vykonává činnosti v rámci kybernetické bezpečnosti – vydávání opatření, ochrana utajovaných informací, kryptografická ochrana. Mimo jiné obstarává problematiku s družicovým systémem Galileo (11).

1.5.4 Bezpečnostní informační služba (BIS)

Zpravodajská instituce českého státu, působící uvnitř území. Její fungování je upraveno zákonem č. 154/1994 Sb., o Bezpečnostní informační službě a je řízena a kontrolována vládou České republiky. BIS se v rámci svých aktivit zabývá také jevy a aktivitami ovlivňující bezpečnostní zájmy ČR nebo hrozby pro komunikační infrastrukturu a její uživatele z hlediska kybernetické bezpečnosti. Řeší tak nejrůznější druhy elektronických útoků s dopadem na chráněné zájmy ČR nebo prověřuje různá internetová fóra, kde dochází k nelegálnímu obchodu v kyberprostoru (12).

1.5.5 Národní centrum kybernetických operací (NCKO)

Na základě stanoveného úkolu pro vybudování a posilování schopnosti kybernetické obrany v rámci Národní strategie kybernetické bezpečnosti pro období 2015–2020 vybudovalo Vojenské zpravodajství (VZ), jakožto odpovědný subjekt za zajištění kybernetické obrany, Národní centrum kybernetických operací. Úkolem NCKO je vybudování účinného systému obrany v kybernetickém prostoru. Obranou se zde myslí *„souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším*

napadením" (13). Oproti kybernetické bezpečnosti se obrana liší v typu a intenzitě útoku a s tím spojenými reagujícími opatřeními. Legislativně řeší otázky kybernetické obrany novela zákona č. 289/2005 Sb., o Vojenském zpravodajství, která tak odpovídá na to, jak se VZ podílí na zajištění, jak probíhá detekce kybernetických útoků nebo aktivní zásah (13).

1.5.6 Velitelství informačních a kybernetických sil (VeKySIO)

Armáda České republiky (AČR) je hlavní složkou ozbrojených sil České republiky spadající pod Ministerstvo obrany České republiky. Dle úrovně velení se dělí na úroveň:

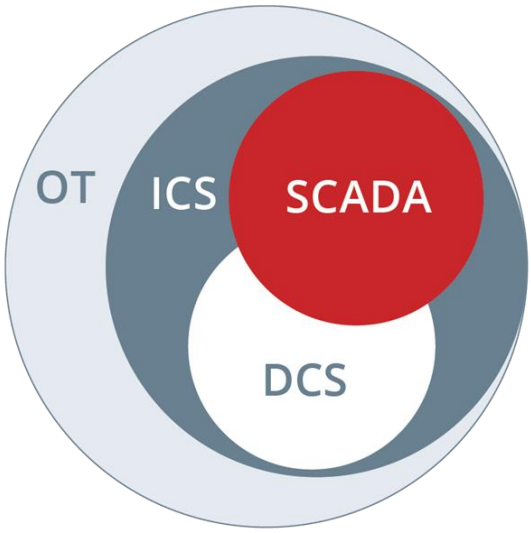
- strategickou,
- operační,
- taktickou (14).

Do taktické úrovně velení přibyly, kromě již zaběhlých pozemních, vzdušných a speciálních sil, také síly teritoriální a kybernetické. Stalo se tomu tak 1. července 2019 s definovanou počáteční operační schopností od počátku roku 2020. Proto bylo od 1.ledna 2020 vyčleněno z organizační struktury Pozemních sil 103. Centrum CIMIC/PSYOPS a bylo zařazené do podřízenosti VeKySIO s názvem Skupina informačních a kybernetických sil (SkIKS). Mimo této skupiny je v podřízenosti zmiňovaného velitelství také Centrum CIRC (Computer Incident Response Capability). CIRC má za úkol *„proaktivní identifikace kybernetických bezpečnostních hrozeb a incidentů pomocí nepřetržitého monitoringu důležitých segmentů datových sítí resortu MO, a jejich následná analýza, vyhodnocování a reportování relevantním partnerům"* (15). Dále připravuje protiopatření v procesu rychlé reakce, spolupracuje s odbornými orgány při šetření kybernetických bezpečnostních incidentů apod. (16).

VeKySIO působí nezávisle, společně nebo v součinnosti s dalšími druhy sil a Vojenským zpravodajstvím. V rámci jeho schopností je celé spektrum operací v kybernetickém prostoru, to i informační a psychologické operace nebo civilně-vojenská spolupráce (16).

1.6 Operační technologie

Operační technologie (OT) *„zahrnuje širokou škálu programovatelných systémů nebo zařízení, které interagují s fyzickým prostředím (nebo spravují zařízení, která interagují s fyzickým prostředím). Tyto systémy/zařízení detekují nebo způsobují přímou změnu prostřednictvím monitorování a/nebo řízení zařízení, procesů a událostí“* (17). OT je nadřazenou množinou pro průmyslové řídící systémy, systémy správy budov, dopravní systémy nebo systémy monitorování a měření fyzického prostředí. Velice zjednodušeně můžeme tvrdit, že OT zajišťuje dodání každodenních služeb, které jsou považovány jako za samozřejmost. Mezi ně můžeme zařadit dodávku elektřiny nebo čistou tekoucí vodu z kohoutku (18).

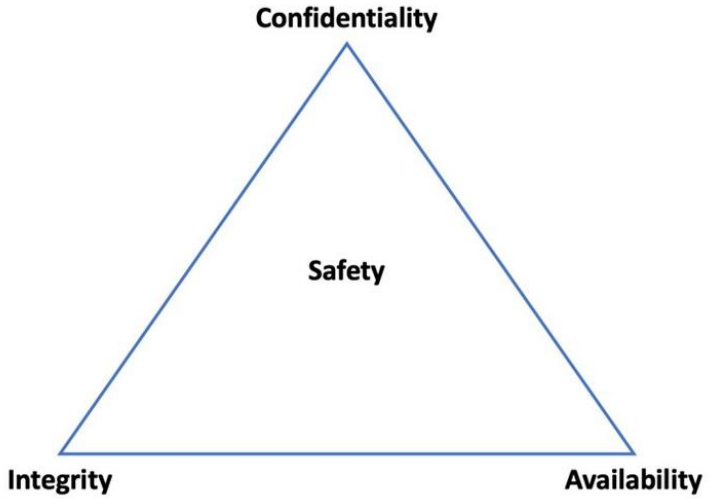


Obrázek 1: Členění OT (Zdroj: 18)

1.7 OT vs IT

Pojem operačních technologií jsme si tedy již jasně vydefinovali. Ovšem stále není definován rozdíl mezi operačními technologiemi a technologiemi informačními. Prvním bodem, na který se v rozdílu lze podívat je jejich určení. Zatímco informační technologie, jak již z názvu napovídá, slouží ke zpracování informací jako takových. Naproti tomu primárním účelem operačních technologií je využívání fyzického vybavení (4).

Další rozdíl je patrný z CIA triády – důvěrnost, integrita a dostupnost. Obecně se toto pořadí definuje jako prioritní pro informační technologie. V rámci operačních technologií se CIA triáda obrací a na prvním místě máme dostupnost, poté integritu a následovně důvěrnost. Důvod je zcela jasný. Operační technologie řídí například i automobily a je mnohem podstatnější, aby při autonehodě ve správný okamžik zafungovaly bezpečnostní prvky a vystřelil airbag. Skutečnost, že si data přečte například i řídící jednotka dveří, se tak stává zanedbatelnou. Navíc bychom se u operačních technologií měli zaměřit primárně na bezpečnost a vytvořit tak SAIC požadavky na předpoklad bezpečnosti OT/ICS (4).



Obrázek 2: Vylepšená CIA triáda – CIAS (Zdroj: 19)

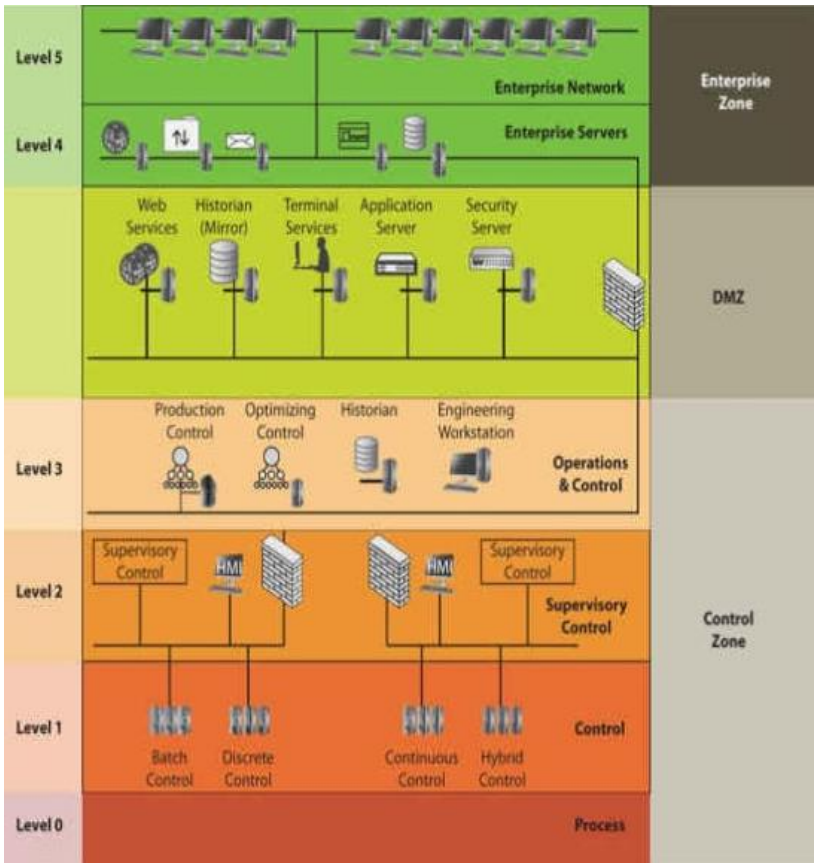
1.8 Průmyslové řídící systémy

ICS (z angl. Industrial Control Systems) jsou hlavním segmentem operačních technologií a zároveň zastřešujícím pojmem pro systémy SCADA a DCS. Slouží k monitorování a ovládání průmyslových procesů, kterými mohou být:

- dopravníkové pásy v dolech,
- spotřeba elektrické energie v energetické síti,
- ventily v plynovodech,
- vibrace na turbíně apod. (18).

Tyto systémy bývají v častých případech určeny jako kritické s nutností vysoké dostupnosti. Při nezajištění jejich zabezpečení je v přímém ohrožení zdraví osob a jejich okolí. Bavíme se zde o situacích jako je únik nebezpečných látek nebo uvolnění mechanických součástek. Na základě těchto skutečností vzniklo v rámci segmentu OT/ICS mnoho nových norem, které se zabývají průmyslovou bezpečností. Speciálně kybernetickou bezpečností v průmyslových řídících systémech se zabývá ISA/IEC 62443 (dříve ISA-99), NIST SP 800-82 nebo ISA-95 (20).

Popis závislostí a spoluprací mezi jednotlivými hlavními komponenty ve většině ICS je definován v rámci Referenčního modelu Purdue (Purdue model) a slouží tak pro širokou veřejnost jako vstupní bod pro seznámení se s OT prostředím. Tento model byl přijmu ISA-99, aktuálně ISA/IEC 62443, a dělí síť na 7 úrovní a 3 logické celky – podniková zóna, DMZ (demilitarizovaná zóna) a kontrolní zóna (20).



Obrázek 3: Purdue referenční model pro ICS (Zdroj: 20, str. 16)

V rámci jednotlivých úrovní je poté dělení následující:

- **Úroveň 5 (Podniková zóna) –** Systémy na podnikové síti jsou většinou pro více zařízení nebo závodů. Přebírají data z podřízených systémů v jednotlivých lokalitách a ty používají k jejich vyhodnocování a poskytování dál. Není součástí ICS, ovšem na konektivitu s nimi spoléhá, jelikož z ní získává data.
- **Úroveň 4 (Místo obchodu a logistiky) –** Oblast, kde se nacházejí veškeré systémy IT, jež podporují výrobní procesy v dané lokalitě. Přebírají data z podnikových systémů a ty dále distribuuje na OT nebo ICS. Příkladem systémů na této úrovni je databázový server, aplikační server, souborový server apod.
- **Průmyslová demilitarizovaná zóna (IDMZ) –** Zóna pro sdílení informací mezi IT a OT umožňuje bezpečně propojit tyto sítě s různými bezpečnostními požadavky. IDMZ přidává další vrstvu oddělení a kontroly. Zabraňuje přímé komunikaci mezi těmito sítěmi s odlišnými požadavky. Navíc díky ní nejsou systémy v nižších vrstvách přímo vystaveny útokům či kompromitaci. Její součástí jsou například proxy servery, databázové replikační servery, doménové kontroléry nebo terminálové servery (jump servery). DMZ je nejkritičtější částí, co se týká zabezpečení a z toho důvodu by se na ni mělo brát zvýšené pozornosti.
- **Úroveň 3 (Místo výroby a řízení operací) -** První úroveň v OT části, jež typicky slouží k dozoru nad OT sítí. Část, kde mohou operátoři na operátorských stanicích sledovat a monitorovat procesní události a zasahovat do nich nebo reagovat na upozornění/události. Lze si ji představit jako centralizovaný velín s HMI, kde jsou procesy z celého závodu. Nalezneme zde databázové servery, souborové servery, inženýrské pracovní stanice serverů HMI atd.

- **Úroveň 2 (Oblast dohledového řízení) –** Většina funkcionalit stejná jako na úrovni 3 s rozdílem v jejich rozsahu. Oblast dohledového řízení se zaměřuje pouze na menší část z celého systému. Konkrétní části jsou zde monitorovány a ovládány pomocí HMI systémů. Operují zde PLC (dozorčí charakter funkcionality), inženýrské stanice nebo HMI (samostatné/systémový klient)
- **Úroveň 1 (Základní ovládání) –** Místo všech ovládacích zařízení. Mají na starosti operace jako otevírání ventilů či startování motorů. Najdeme zde PLC, VFD, PID.
- **Úroveň 0 (Fyzické procesy) –** Nejnižší úroveň, kde je místo skutečných procesních zařízení, jež jsou řízeny a monitorovány z vyšších úrovní. Tato zařízení jsou souhrnně označována jako EUC (z angl. Equipment Under Control), jedná se o motory, pumpy, snímače nebo ventily. Na úrovni 0 se také nacházejí IED (z angl. Intelligent Electronic Devices) (20, 21).

1.8.1 Typy architektur

V dřívějších dobách se dělila architektura průmyslových řídících systémů na DCS a SCADA systémy (PLC není v tomto případě bráno jako systém). Oba typy měly svá specifika, ovšem v dnešní době, kdy se technologie vyvíjejí, je velice náročné jednoznačně určit jejich typ. Oba systémy dokážou monitorování a ovládání výrobních a průmyslových zařízení. Obsahují aplikace a nástroje pro celou škálu operací nad automatizovanými procesy. A navíc, jsou všestranné, jelikož jedna stanice může mít funkcionality pro vícero typů osob a činností (22).

V následujících řádcích si popíšeme největší rozdíly, které zde najdeme.

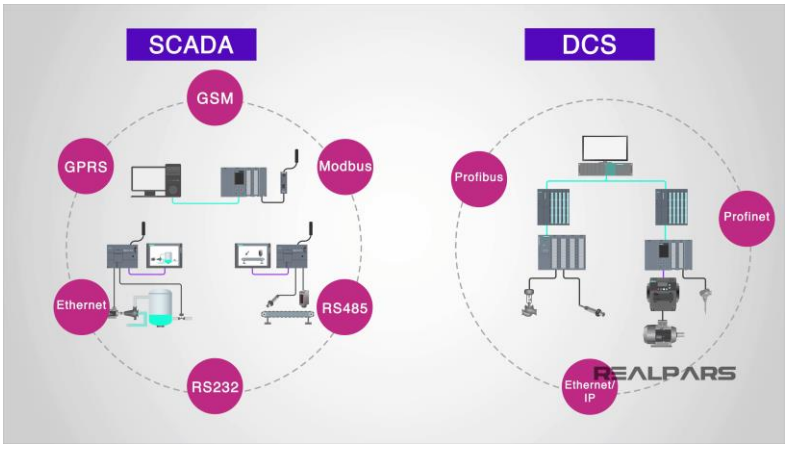
DCS

DCS (z angl. distributed control systém) má značnou výhodu v integrovaném softwaru operátorského rozhraní, kdy nemusí být pro každé zařízení specifický program pro jeho správu. Možná i proto měly DCS integrované předdefinované funkce, které stačilo pouze přizpůsobit a nasadit do potřebného prostředí. Za tuto výhodu ovšem

platí daní v podobě delší doby zpracování. Oproti SCADA systémům je bezpečnější, nikoli drasticky. Navíc se jedná o uzavřenou architekturu, tzn. nelze využít zařízení jiných dodavatelů (23).

SCADA

SCADA, zkratka pro Supervisory Control and Data Acquisition, je systém s otevřenou architekturou, u něhož můžeme kombinovat komponenty od různých dodavatelů. Některé značky podporují zvýšenou kompatibilitu mezi svými zařízeními, ve většině případů tomu tak ale není. Navíc na obsluhu každého typu zařízení je potřebný specifický software. Na druhou stranu je lepší pro časové citlivé procesy. Obsahuje však PLC a RTU, které je potřebné vždy od základu naprogramovat. Oproti DCS má větší škálu komunikačních protokolů, kterých může být využito (23).



Obrázek 4: DCS vs SCADA (Zdroj: 23)

1.8.2 Komponenty

ICS sítě mají své specifické řídící komponenty, které můžeme rozdělit do dvou skupin – servery a kontroléry. Servery dělíme dle jejich funkcionalit na řídící, DCS/SCADA server, data historian a vstupně výstupní server. Více si je přiblížíme v následujících odstavcích (24).

Řídící server

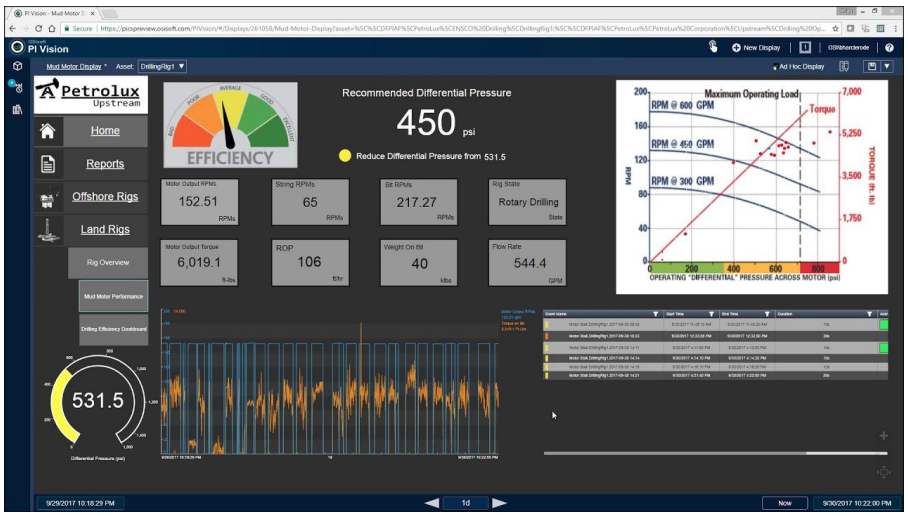
Je řídícím serverem komunikujícím s podřízenými jednotkami na úrovni výrobních procesů. Spojuje je ICS síť pomocí kontrolního řídícího softwaru. (4, 24).

SCADA server (MTU)

SCADA server, jinak používaná také terminologie MTU (z angl. Master Terminal Unit), pracuje jako hlavní server v ICS síti, přičemž PLC a RTU jsou v síti podřízenými. Provádí dohled nad výrobními procesy (4, 24).

Data historian

Specializovaný softwarový systém shromažďující informace o všech procesech (bodové hodnoty, upozornění atd.) z průmyslových systémů a zařízení, které ukládá do centrální databáze. Existují řešení proprietární (ABB, Areva, Emerson, GE) i třetích stran (Aspen Technologies, Canary Labs, OSIsoft). Posbíraná data slouží k analýzám a statistikám procesů v ICS. Jedná se o „prémiový“ cíl útoku, proto by měla být zvýšená pozornost při jeho zabezpečení (4, 22).



Obrázek 5: OSIsoft PI Vision ukázka (Zdroj: 25)

Input/output server (I/O server)

Shromažďuje, ukládá a poskytuje přístup k procesním informacím z PLC, RTU a IED. Operátoři jej mohou využít k interakci s HMI a řídícím serverem. Na straně kontrolérů již na základě funkcionalit jednotlivé prvky nedělíme, jelikož se jedná o specifické prvky (22).

HMI

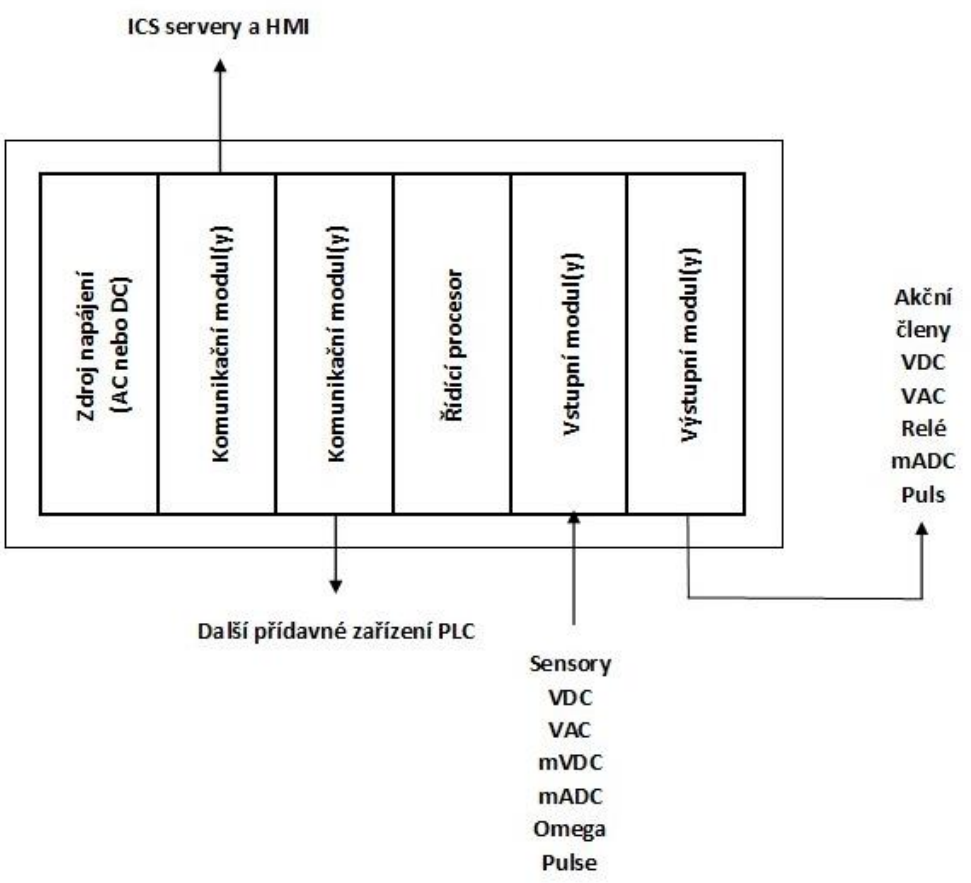
HMI (z angl. Homan-machine interface) je prostředkem interakce s PLC, RTU a IED pro operátory. Nahrazuje fyzické přepínače, ciferníky a další elektrická zařízení grafickým rozhraním, které reprezentuje digitální kontroléry. Umožňuje tak operátorům spustit nebo zastavit cykly, upravit nebo nastavit body a vykonat další funkce potřebné pro interakci řídících procesů (22).

Obecně je vyráběno ve dvou provedeních, první založeno na moderních OS (Windows 7, 8, 10), kdy dokáže provádět různé funkce. Druhý typ kombinuje zodolněný průmyslový počítač, dotykovou obrazovku a je montován přímo jako panel. Navíc je zde OS z rodiny Windows Embedded (CE, XP, 7, 8, Compact), takže ho je nutné programovat separátním počítačem se speciálním softwarem (22).

PLC

PLC (z angl. Programmable logic controller) je speciálním průmyslovým počítačem, používaným k automatizaci výrobních procesů. Bylo vyvinuto, aby v moderní době nahradilo elektromechanické relé. Je specifické fyzickým zodolněním oproti klasickým PC, jenž známe. Navíc nepoužívá komerční operační systémy. Principiálně je založeno na speciálních aplikačních programech automaticky generujících výstup na základě specifického vstupu. Pro jejich programování se využívá 5 programovacích jazyků – LD (z angl. Ladder Diagram), SFC (z angl. Sequential Function Charts), FBD (z angl. Function Block Diagram), ST (z angl. Structured Text), IL (z angl. Instruction List). Jednotlivé programovací jazyky jsou definovány v IEC-61131-3 (22).

Velmi jednoduché PLC mohou být nazývány PLR (z angl. programmable logic relays), programovatelné logické relé. Mnoho typů zařízení je specifických pro určité typy průmyslových použití, ve všech případech ale pracují v reálném čase (22).



Obrázek 6: Komponenty PLC (Zdroj: Vlastní zpracování dle 22, str. 60)

RTU

RTU (z angl. Remote terminal unit), polní zařízení vybavené bezdrátovým a drátovým rozhraním, které podporuje sběr, monitoring a řízení dat. Je řízeno mikroprocesorem, který dostává příkazy a odesílá data zpět do centrální monitorovací stanice. Vzhledem k jeho názvu je jasné jeho spojení se vzdáleným ovládání – pomocí modemu, mobilního datového připojení, rádiově nebo jinými způsoby. Jsou většinou instalovány na ne příliš dostupných místech, kde na ně působí vnější vlivy jako jsou teplota, vlhkost či zvěř (22).

Funkcionalita RTU a PLC se v dosti případech překrývá. V případě, kdy má RTU integrovanou programovou logiku a kontrolní funkce, může docházek záměně za dálkově ovládané PLC skombinované s integrovaným telekomunikačním vybavením (22).

IED

IED (z angl. Intelligent electronic device) je inteligentní elektronické zařízení naplňující požadavky na různorodé fyzické a logické potřeby v průmyslovém prostředí. Zcela zjednodušeně se jedná o sensory/akční členy, které jsou „inteligentní“ nebo „chytré“ či dokonce „smart“, jak je v dnešní době oblíbené používat. Pro nás to znamená, že jsou schopny sbírat data z okolního prostředí, předávat je dalším zařízením a provádět místní zpracování a řízení (22).

Aktuálně se ovšem již na základě popisu PLC, RTU a IED jednotlivé komponenty slévají do kupy. Ono tomu tak ovšem v některých případech reálně je, existují totiž zařízení, které oplývají schopností měření, diagnostiky, vzdáleného ovládání a telekomunikace v rámci jednoho celku, a dokonce podporují několik programovacích jazyků zároveň. Pro oddělení těchto pojmů budeme považovat IED za zařízení podporující *specifickou* funkcí v rámci celého kontrolního systému a PLC s RTU k obecném užití (22, 24).

Nebuďme nyní však na omylu, že jsme si představili kompletní spektrum aktiv v průmyslových řídících systémech. V rámci průmyslové sítě se mohou nacházet také tiskárny, přístupové systémy (čtečky karet) nebo méně překvapivé Active Directory a časové servery. Zrovna časové servery jsou v rámci průmyslových řídících systému dosti citlivým tématem, vzhled k řízení v reálném čase, kdy je nutné zajistit synchronizaci času mezi jednotlivými systémy a jejich periferiemi (4, 22, 24).

Všechna zařízení mají nějaké typy zranitelností, proto je potřebné tímto způsobem přistupovat k celé problematice. I na první pohled zcela neškodné zařízení by mělo být posouzeno z hlediska bezpečnostních slabin.

1.8.3 Systémové operace

Úkolem komponentů zmiňovaných v předešlých odstavcích je vytvořit a automatizovat určitou průmyslovou operaci, např. generování elektrické energie nebo vytvoření produktu. Typická průmyslová operace je složena z několika vrstev naprogramované logiky tak, aby manipulovala s mechanickými prvky v pořadí, jenž bude mít za výsledek automatizaci procesu. A právě řídící smyčky (angl. control loops) se zasluhují o automatizaci jednotlivých specifických funkcí v rámci procesu automatizace (22).

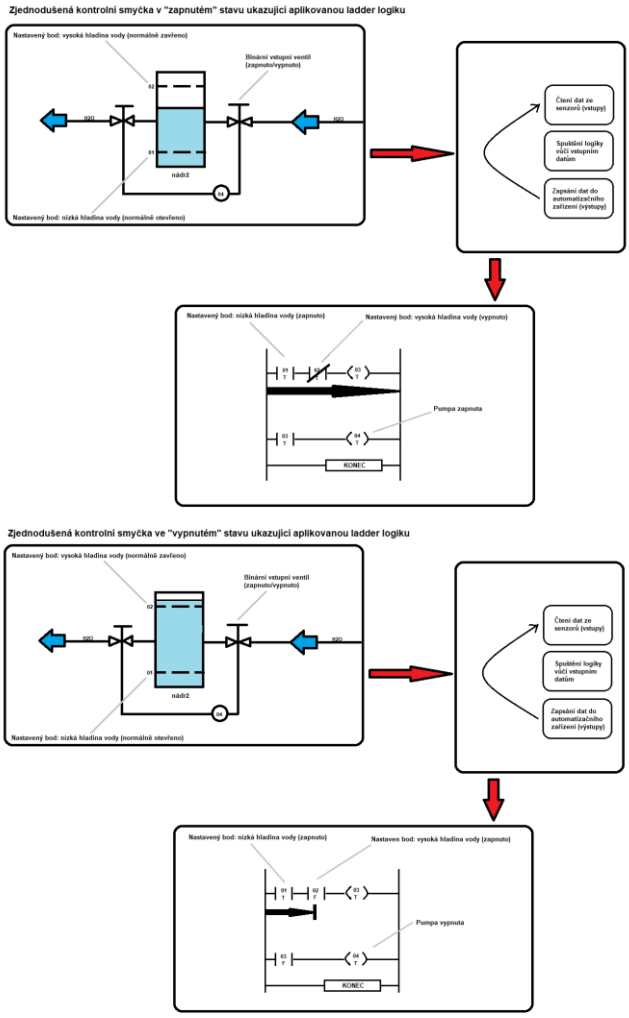
Řídící smyčky

Řídící prvky jsou programovány specifickou logikou nazývající se řídící smyčka (z angl. control loop). Termín *smyčka* je odvozený od pojmu *ladder logic*, tedy logiky plošně používané v těchto systémech. Pro představu funkčnosti – PLC prochází cyklicky svými různými vstupy, aplikuje logiku kódu na úpravu výstupů a poté znovu začne skenovat vstupy (22). V programování můžeme tuto smyčku přirovnat k nekonečnému cyklu jakým má v jazyce C++ syntaxi:

```
#include <stdio.h>
int main()
{
    while (1)
    {
        //nekonečně opakující se část kódu
    }

}
```

Samozřejmě kód řídících systémů není v tomto programovacím jazyce psán, slouží pouze k ilustrativnímu příkladu. Kód v rámci řídící smyčky může vypadat například následovně:



Obrázek 7: Kód řídící smyčky (Zdroj: Vlastní zpracování dle 22, str. 71)

Řídící procesy

Řídící proces je obecný pojem používaný pro definování větších automatizovaných procesů v průmyslových operacích. Ku příkladu taková výroba plastového výrobku si projde čtyřmi fázemi – uzavření vstřikovací formy, plnění formy a dotlak, chlazení a plastifikace, otevření vstřikovací formy a odformování výrobku. Každá fáze může být definována jako řídící proces tvořený z jedné i více řídících smyček. S jednotlivými procesy lze většinou interagovat pomocí HMI, to předává grafický přehled z jedné nebo více řídících smyček umožňující tak komunikaci s podřazenými kontroléry (PLC, RTU) a to až na úroveň vyčtení dat ze senzorů (22).

Smyčky zpětné vazby

Každý automatizovaný proces musí spoléhat na určitou úroveň zpětné vazby jak mezi řídícími smyčkami, tak řídícími smyčkami/procesy a operátorem. Zpětná vazba je zde poskytována přímo z HMI pro kontrolu specifického procesu. Může být decentralizovaná i centralizovaná mezi různými procesy. Jedná se tedy o proces, v kterém jsou výstupy ze systému vraceny zpět a používány jako vstupy (22).

Produkční informační management

Centralizovaný management pro průmyslové řídící systémy je provozován pomocí jednoho nebo více systémů data historianů, které provádějí historizaci. Tedy proces převodu dat z prostředí řízeném v reálném čase automatizovaných procesů a jejich ukládání v průběhu času. Na historizované data se používají analytické nástroje – SPC (Statical Process Control) a SQC (Statistical Quality Control) (22).

Podnikový informační management

Provozní monitoring a analýzy jsou využívány managementem pro ladění operací, zlepšení efektivity, minimalizaci nákladů a maximalizaci zisku. Proto je nutné replikace dat provozních/operačních na data podniková dostupná v podnikové síti. Problémem je jejich přenos. K dohledovým datům je možné přistupovat pomocí HMI nebo data historian klientu. A oba typy přístupu mají své výzvy k zabezpečení – problematika identit, komunikačních pravidel, čí vlivu na procesy (týká se pouze HMI) (22).

1.8.4 Hrozby

S tužbou vlastníků aktiv získat benefity konvergence IT a OT se náhle do popředí začaly dostávat hrozby pro řídící systémy, které v odpojených, rozumějte ostrovních, systémech byly z velké části ignorovány. Ale pouhou konvergencí konektivity to teprve začíná (20).

Mnoho systémů totiž používá zastaralé operační systémy, na které nejsou aplikovány záplaty (z angl. patch), což znamená tisíce neošetřených zranitelností. V běžných IT systémech by již dávno tyto patche byly aplikovány a bylo znemožněno

jejich zneužití na základě exploitů. V OT tomu tak ale není. Běžný patch nebo update může mít negativní vliv na chování těchto zařízení i sítě, proto se odkládají na plánované odstávky, kde se tyto servisní úkony provádějí (20).

Navíc ICS zařízení, protokoly a aplikace nebyly nikdy vyvíjeny s prioritou bezpečnosti. Co považujeme v IT za standard, zde může způsobit reset nebo úplné selhání ICS zařízení. K tomu si můžeme přidat, že ICS aplikace a protokoly byly původně vyvinuty bez autentizačních mechanismů, šifrování a dalších běžných praktik kybernetické bezpečnosti (20).

Poslední podstatnou hrozbou je nedostatečná znalost IT dovedností uvnitř prostředí ICS. Setkávají se zde celkem 3 oblasti – IT, elektrotechnika a automatizace. Proto v mnoha případech dochází k chybám při údržbě, nastavení nebo hardeningu (20).

1.8.5 Dopady kompromitace

Všichni tedy chápeme, že se pohybujeme v prostředí, kde jsou chemické reakce, vysoké teploty, velký tlak a mechanické komponenty, které mohou způsobit dopad na bezpečnost, zdraví a lidské blaho. Jaké tedy mohou být následky kompromitace? Obecně se jedná o:

- katastrofální bezpečnostní selhání,
- uvolnění nebezpečných látek do okolí,
- zastavení výroby,
- regulační pokuty
- a ztrátu veřejné důvěry (20).

1.8.6 Metody útoků

Existuje spousta metod, jak zaútočit na identifikovaný cíl. Ať už to je útok typu MitM, DoS, útok přehráním a mnoho dalších metod, jež jsou v ICS síti velmi efektivní. Některé z nich si ve zkratce popíšeme (20, 22).

MitM

Man in the middle je typ útoku, kde je útočník mezi komunikujícími zařízeními a odposlouchává síťový provoz. Reálně je útočník takovou spojkou obou zařízení, kdy rozhoduje, co přepošle, a tak může modifikovat posílaná data. Problémem je zde nutnost získání důvěryhodnosti u obou zařízení. Aplikace v ICS je komplikovaná kvůli komunikaci zařízení pomocí *sessions*, jenž jsou navázány a udržovány po dlouhou periodu času (20, 22).

DoS

Denial of service způsobuje nedostupnost služby/prostředku. Jako u většiny případů by tento typ útoku v IT odvětví nezpůsobil nijak výrazné škody, šlo by například pouze o zpomalení načítání webové stránky. My jsme ale v oblasti mechanických čas a kouzel, kde zákony IT neplatí. Při tomto vektoru útoku dojde ke ztrátě kontroly (LoC – Loss of Control), kdy se fyzický proces přepne do „bezpečného“ stavu, vypne se. Na úrovni HMI se bavíme o ztrátě přehledu (LoV – Loss of View), který v případě nedostupnosti výrobních řídích dat, většinou vede k zastavení procesu a jeho obnově. Krásným příkladem je legendární Ping smrti (angl. Ping of death). Ten má v příkazovém řádku následující syntaxi: `ping -s 65535 <IP adresa>` (20, 22).

Útok přehráním

Na první pohled jednoduchý vektor útoku se zaměřuje na zopakování požadovaného procesu na základě odchycených paketů a jejich opětovného použití. To je možné díky přenášené řídící komunikaci v plaint textu, tedy nezašifrované podobě (22).

Kompromitace HMI

Nejjednodušší způsob, jak získat neoprávněné řízení a ovládání, je využít schopností HMI. Nejefektivnější je to skrz rozhraní konzole využitím instalace vzdáleného přístupu, čímž dojde ke kompromitaci. K tomu se využívá Metasploit framework a pro získání vzdáleného přístupu poté Meterpreter shell (k instalaci vzdáleného VNC serveru). Tak se lze dostat přímo do rozhraní HMI,

zde není již potřeba přímá znalost mechanismů na pozadí, jelikož je umožněno ovládání pomocí grafického rozhraní (22).

Kompromitace inženýrské stanice

Téměř identické mechanismy jako u kompromitace HMI pomocí Meterpreter payloudů. Rozdílem zde je rozsah, na jakém poté může útočník škodit. HMI má většinou omezenou funkcionalitu, zatímco inženýrská stanice (EWS) obsahuje také speciální nástroje sloužící k modifikaci a manipulaci s ICS zařízení jako je PLC. Plus se na EWS mnohokrát vyskytuje uložená dokumentace o řídícím systému týkajících se designu, konfigurace a provozu závodu. Čímž se stává mnohem více ceněným cílem (22).

Reálně se poté setkáváme se smíšenými útoky, kombinující více expoitů a zranitelností na více cílů. Jedná se útoky, který využívají různé techniky a nástroje na získání přístupu do sítě, obejití zabezpečení a poté získání přístupu do průmyslové části sítě, kdy se teprve nyní může snažit o kompromitaci nebo další exploitaci. Sofistikovanost útoku byla povýšena Stuxnetem, jenž se dokázal specificky chovat v různých prostředích. Dále tento koncept pak povýšil Skywiper, známý také jako Flame (22).

1.9 Průmyslové sítě

V rámci této diplomové práce je průmyslovou sítí myšlena jakákoliv sít, podporující propojení komunikace mezi zařízeními vytvářejících nebo podporující průmyslové řídící systémy.

1.9.1 Požadavky na design a architekturu

Na první pohled není design technologicky o moc odlišnější než v IT, většina komunikace na drátové i bezdrátové úrovni je založena na Ethernetu a IP (někde lze stále vidět sériovou komunikaci pomocí RS 232/422/485). Ovšem zde všechny podobnosti končí. Průmyslová síť je designovaná primárně na dostupnost, proto se používají protokoly operující v reálném čase, přenos dat pomocí UDP a sítě odolné proti chybám propojující koncové zařízení a servery. Design je odvozen právě od odlišných požadavků na funkčnost síťové architektury, viz. Tabulka 1: Požadavky na sítě.

Tabulka 1: Požadavky na sítě (Vlastní zpracování dle 22, str. 88)

Funkce	Provozní síť (oblast řízení a procesů)	Provozní síť (oblast dohledová)	Podniková síť
Opera v reálném čase	Kritická	Vysoká	Nejlepší možný
Spolehlivost/ Odolnost	Kritická	Vysoká	Nejlepší možný
Šířka pásma	Nízká	Střední	Vysoká
Relace	Málo, explicitně definováno	Málo	Mnoho
Latence	Nízká, konzistentní	Nízká, konzistentní	N/A, znovuzaslání povoleno
Síť	Sériová, Ethernet	Ethernet	Ethernet
Protokoly	Real-time, proprietální	Téměř real-rime, otevřené	Nejsou real-time, otevřené

A nyní máme dilema. Vysoká dostupnost vyžaduje kruhovou nebo mesh topologii a operativnost v reálném čase s nízkou latencí na druhou stranu minimální switching a routing. Právě tyto požadavky diktují, jak bude vypadat design a architektura sítě. To může vést k potřebě speciálního síťového vybavení kompatibilního s výše uvedeným, a tak dosažení potřebné funkcionality. Další, co určuje design jsou používané průmyslové protokoly (22).

Při aplikaci switchingu a routingu do sítě s mnoha subnety, dáváme vždy přednost switchingu. Routing využíváme pouze u komunikace překonávající funkční hranice. Využitím L3 switche místo kombinace několika zařízení pracujících na L2 a L3 poté dokážeme zlepšit výkon sítě a ušetřit několik hopů. Využíváme STP (z angl. Spanning Tree Protocol) eliminující smyčky a dynamické routování. Pro komplexní a sofistikovaný design lze využít VSRP (z angl. Virtual Switch Redundancy Protocol) a VRRP (z angl. Virtual Router Redundancy Protocol). Při ponoření hlouběji do oblasti řídícího prostředí se využívá řada otevřených nebo proprietárních protokolů, které mohou mít nativní podobu nebo být přizpůsobené k přenosu přes Ethernet. Například síť fieldbus používá dvouvodičovou konektivitu závislou na tzv. couplerech (tap) a terminátorech.

Specifické oblasti průmyslových sítí si vyžadují jedinečné požadavky na design a využití specifické topologie (22).

1.9.2 Typické topologie

Mezi jednotlivé topologie využívané v průmyslových sítích řadíme topologii typu:

- sběrnice,
- mesh,
- bezdrátový mesh,
- hvězda,
- větev nebo strom,
- a kruh (22).

Nikdy není použita pouze jedna topologie a jedná se o kombinaci výše zmíněných. Topologie sítě výrazně ovlivňuje možnosti segmentace sítě. Ku příkladu je dual-homing připojující jedno zařízení do dvou a více sítí zároveň. Ani při nastavení ACL (angl. access control list), implementaci IDS a aplikačního firewallu tak nemusíme zabránit útočníkovi v obejití těchto zabezpečovacích mechanismů. To je potřeba brát v potaz a nejlépe se některým topologiím, pokud to situace umožňuje, zcela vyhnout. Musíme tedy dobře a podrobně porozumět výhodám i nevýhodám jednotlivých topologií a dále pak správně segmentovat síť na všech úrovních (22).

1.9.3 Protokoly

K pochopení, jak funguje průmyslová síť je potřebné porozumět alespoň na základní úrovni komunikační protokoly, které se zde využívají a proč se zde využívají. Vzhledem k požadavkům, jaké zde musíme naplnit na komunikaci v reálném čase, chybí základní funkce, jež by mohly snížit efektivnost. Což znamená absenci i takových „drobností“ jako je autentizace a šifrování. Mnoho protokolů navíc prošlo, nazvěme to modernizací, aby mohli pracovat na Ethernetu a IP (angl. Internet Protocol). Dodavatelé tak mohou využívat komerční technologie. Tato modernizace má za následek jejich vysokou zranitelnost vůči kybernetickým útokům. Pojďme si tedy jednotlivé protokoly představit. Pro jejich představení jsou rozděleny do tří kategorií – fieldbus, průmyslový ethernet a backend (22).

Fieldbus Protokoly

Na přelomu tohoto tisíciletí byla vydána IEC 61784 definující celkem 9 protokolů (FOUNDATION Fieldbus, CIP, PROFIBUS/PROFINET, P-NET, WorldFIP, INTERBUS, CC-Link, HART a SERCOS). Některé z nich si popíšeme:

- **Modicon Communication Bus (Modbus)**, protokol představený v roce 1979 založený na principu žádost/odpověď pracující na 7 vrstvě OSI modelu původně pro implementaci na RS-232C nebo RS-485. Má definované 3 PDU (angl. Protocol data units) – Modbus Request, Modbus Response, Modbus Exceptional Response. Obecný datový rámec je složený z adresy, funkčního kódu, dat a kontroly chyby. V průběhu let vzniklo několik jeho variant – Modbus RTU a ASCII (podpora binárního a ASCII přenosu), Modbus TCP (podpora IP), Modbus+ (podpora propojení sběrnic pomocí techniky předávání tokenu). Využívá se mezi PLC a HMI nebo hlavním/řídícím PLC a podřízenými zařízeními. Chybí zde autentizace, šifrování, kontrolní součet a je náchylný na DoS útoky.
- **Distributed Network Protocol (DNP3)**, protokol podobný jako Modbus. Motivem jeho vývinu bylo mít spolehlivý protokol v prostředí elektro průmyslu, kde je vysoká míra EFI (z angl, electromagnetic interference), elektromagnetického rušení. DNP3 přidává kontrolní součet a vytváří unikátní klíč pro relaci, primárně ovšem se zaměřením na integritu dat, nikoli jejich zabezpečení. Můžeme tedy využít stejné metody jako u Modbusu a navíc doplnit manipulaci synchronizace času, potlačení alarmů a další.
- **Process Fieldbus (PROFIBUS)**, je master/slave protokol podporující užití více master uzlů pomocí předávání tokenu (pokud má master token, tak komunikuje se slave). Chybí zde autentizace na mnoho funkcionalit, díky spoofingu lze dosáhnout imitace master uzlu, a tak získat možnost konfigurovat slave.

- **Industrial Ethernet**, je termínem referujícím na adaptaci IEEE 802.3 Ethernet standardu do průmyslových automatizačních řešení pracujících v reálném čase. Z toho důvodu jsou všechny níže zmíněné protokoly spadající do této kategorie náchylné na jakékoliv zranitelnosti Ethernetu. Spadají sem tedy:
  - **Ethernet Industrial Protocol (Ethernet/IP)**
  - **PROFINET**
  - **EtherCAT**
  - **Ethernet POWERLINK**
  - **SECOS III**
- a další, např. **HART**, **CIP**, **S7comms** nebo **BACnet** (22).

Backendové protokoly

- **OLE for Process Control (OPC)**, není průmyslovým protokolem, ale sérií standardizačních specifikací pro usnadnění integrace různých forem dat na systémech od různých dodavatelů. Funguje jako klinet/server, kde klient volá lokální proces, ten se ale spouští vzdálené na serveru, což se nazývá vzdálené volání procedury, RPC (z angl. remote procedure call).
- **Inter-Control Center Communications Protocol**, slouží ke komunikaci mezi kontrolními centry v energetice. Je zařazen do kategorie backend, jelikož jeho design počítal s využitím v rámci obousměrné komunikace WAN mezi kontrolním centrem, elektrárnou, rozvodnou a dalšími částmi (22).

1.10 Standardy a regulace

I v průmyslové systémy mají své standardy a regulace. Některé z nich nejsou pro Českou republiku nijak závazné, ovšem v oblastech hardeningu a požadavků na dodávky pro kritickou infrastrukturu se aktuálně zdají být západní regulace propracovanější, proto nebude od věci některé z nich závěrem zmínit.

1.10.1 ISO/IEC 27000

Řada norem zabývající se bezpečností informací řídící se stejnou strukturou a pravidly. Celkové obsahuje více jak třicet norem, z nichž jádro tvoří osm z nich:

- ISO 27000 – definice pojmů a slovník s terminologií,
- ISO 27001 – norma, která se týká ISMS,
- ISO 27002 – souhrn nejlepších praktik pro bezpečnost informací,
- ISO 27003 – příručka pro návrh a zavedení ISMS,
- ISO 27004 – měření,
- ISO 27005 – řízení rizik bezpečnosti informací,
- ISO 27006 – požadavky na orgány provádějící audit a certifikaci ISMS,
- ISO 27007 – doporučení k provádění auditů (3).

Nejzajímavějším je pro nás ISO 27002, dříve publikované jako ISO 17799. Sice nepředává rady, jak zabezpečit specifické prostředí průmyslových řídících systémů, ale je namapována přímo na národní bezpečnostní standardy (ZoK, VoK). V roce 2017 dále vyšla standardizace technického reportu z roku 2013. Je označený jako ISO/IEC 27019:2017 a zaměřuje se na kontroly bezpečnosti informací pro energetický průmysl. Původní technický report (TR27019:2013) vycházel z požadavků NERC CIP a celkem rozšiřoval o 42 oblastí, které nebyly v ISO/IEC 27002 (22).

1.10.2 ISA/IEC-62443

Série standardů rozdělená do 4 skupin zaměřujících se na širokou škálu témat potřebných pro implementaci bezpečnosti průmyslových automatizačních a dohledových systémů (IACS, z angl. Industrial Automation and Control System). Jednotlivé skupiny jsou následující:

- IEC 62443-1 – General,
- IEC 62443-2 – Policies and procedures,
- IEC 62443-3 – Systém,
- IEC 62443-4 – Component (22).

První skupina se zabývá standardizací pojmů a zajištění konzistence referencí, metrik a modelů. Skládá se ze 4 dokumentů, přičemž nejzajímavějším je ten s označením 62443-1-3, jelikož definuje právě jednotlivé metriky, jež jsou velice nápomocné v kvantifikace dodržování bezpečnostních praktik pro IACS (22).

Skupina dvě se poté zaměřuje se svými 4 dokumenty na potřebná pravidla a postupy vytváření efektivního IACS bezpečnostního programu. Z této skupiny pochází první vydaný standard z celé série a to 62443-2-1 definující požadavky na systém řízení bezpečnosti pro IACS. Dále je definovaný patch management v rámci průmyslové architektury (62443-2-3) a požadavky na certifikaci IACS dodavatelů (62443-2-3) (22).

Třetí skupina, 62443-3 cílí na technologie kybernetické bezpečnosti – obsahuje dokumenty s dostupnými technologiemi, posudky a metodiky návrhu. Nesmíme zapomenout na bezpečnostní požadavky (22).

Poslední skupina, 62443-4, má na starosti bezpečný vývoj komponent a obsahuje detailní požadavky na vytvoření SDLC (z angl. Secure Development Lifecycle) pro IACS (22).

1.10.3 NIST SP 800-82

Poprvé publikována v květnu 2013, obsahuje doporučení pro bezpečnost, management, procesní a technické kontroly vedoucí ke zlepšení bezpečnosti řídících systémů. Aktuálně NIST přichystal již návrh třetí revize a vyhlíží se oficiální vydání do poloviny roku 2022. (22).

Mimo jiné pod taktovkou NIST vzniká také framework pro zlepšování kybernetické bezpečnosti kritické infrastruktury, ten je dostupný z odkazu: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

1.10.4 Další

Mezi další standardy a regulace jsem přidal NERC CIP a CFATS. Jedná se o čistě americké záležitosti, ovšem stojí za zmínku.

NERC CIP

Z amerického NERC CIP bychom si měli vzít příklad minimálně ve vysokých sankcích při nedodržování požadavků na bezpečnost kritické infrastruktury. Je uplatnitelný pouze v Severní Americe pro energetický průmysl a doplňuje řadu dalších standardů s kterými je v souladu. Vzhledem k uplatnění v této oblasti, kde se používá distribuovaný kontrolní systém je relevantní také pro další provozovatele průmyslových sítí (22).

CFATS

Protiteroristické standardy chemického zařízení (z angl. Chemical Facility Anti-Terrorism Standards) definují RBPS (angl. Risk-based Performance Standards), kde jsou různé návrhy pro zabezpečení systémů pro chemické zařízení (22).

Mezi další poté patří NEI 08-09 (Plán kybernetické bezpečnosti pro jaderný reaktor), API 1164 (Zabezpečení SCADA pro potrubní systémy ropy a plynu), SG-CG/M490 (Zabezpečení rozvodné soustavy v EU) a ENISA s několika publikacemi (20, 22).

1.11 Penetrační testování

Nejlepším způsobem, jak ověřit míru zranitelnosti systému proti neoprávněnému průniku, je penetrační testování. Za použití specializovaných nástrojů se zkouší proniknout různými vektory do všech možných částí testovaného aktiva, a to jak zvenčí, tak zevnitř. Na základě těchto pokusů lze odhalit zranitelnosti (slabá místa). Penetrační testování tak tvoří podstatnou část bezpečnostní analýzy (3).

1.11.1 Typy

Provádí se v několika variantách dle rozsahu znalostí prostředí – black box, white box a grey box.

Black box

V tomto případě se jedná o penetrační test, kdy má tester minimum či vůbec žádné znalostí o prostředí, které bude testovat. Jedná se simulaci reálného útoku, kdy se snažíme

imitovat perspektivu útočníka, jenž si musí zjišťovat všechny informace. Tento druh testu je proto velkým rizikem, a to zvlášť v prostředí ICS. Doporučené, v některých případech i regulované, je provádět tyto testy pouze na testovacím/vývojovém prostředí (7, 20).

White box

Znalost prostředí je na úrovni maxima předaných a dostupných informací (prostředí, systémy, informace o společnosti, IP adresy, operační systémy, aplikace nebo dokonce zdrojové kódy). Tímto způsobem lze docílit získání více informací z penetračního testu než u Black boxu a následně tak lépe zabezpečit náš systém. V rámci ICS i White box může způsobit škody, doporučuje se tak testovat na testovacím/vývojovém prostředí (7, 20).

Grey box

Smícháním černé a bílé vznikne šedá barva. Průnikem Black boxu a white boxu vznikl grey box. V reálném prostředí v mnoha případech nelze zjistit informace o systému 1:1, stejně tak není dobré zůstávat testu bez žádných znalostí, a to už jen kvůli nastavení restrikcí, co se nesmí v průběhu testu provádět. V rámci ICS je schůzka mezi testery a lokalitním týmem důležitá pro vymezení restrikcí a nastavení cílů pro penetrační test (ne vždy se musí jednat o celý systém, lze testovat pouze jeho dílčí část) (7, 20).

1.11.2 Příprava

Příprava penetračního testu může být různorodá, vždy záleží na jeho cíli. Prvním krokem je tedy počáteční ustanovení, které vydefinuje jeho cíle. Jakým způsobem se bude testování provádět (black/white/grey box), vymezení restrikcí a pravidel pro testování, předání dokumentací, dohoda o mlčenlivosti, zvolení časového prostoru, předání kontaktních údajů pro potřeby komunikace v průběhu testování a další. Na základě těchto dat lze poté vytvořit počáteční sběr dat formou OSINT a doplnění tak jednotlivých informací. V rámci přípravy by neměla být vynechána část ze strany testerů, kdy se pro nový test (myšleno zakázku) vytváří čistá instalace penetračních prostředků (7, 20).

1.11.3 Testování

Fáze testování se provádí na základě stanov určených v přípravné fázi. Penetrační testy by vždy měly být prováděny pouze oprávněnými osobami, které mají dostatečný počet zkušeností a znají principy testovaného prostředí. Kroky, u kterých nelze predikovat chování systému by měly být konzultovány s určenou kontaktní osobou (7, 20).

1.11.4 Reporting

Při testování se běžně provádí logování vlastních aktivit, pro zjednodušení poslední fáze penetračních testů, kterou je vytvoření závěrečné zprávy. Ta slouží k hodnocení celého procesu testů. Jsou zde definovány kroky, jakými bylo postupováno, úskalí, na které testeři narazili a hlavní částí jsou zjištěné zranitelnosti a rizika. V rámci reportingu by neměla chybět ani doporučení, jakým způsobem systém zabezpečit proti zjištěné zranitelnosti (7, 20).

2 ANALÝZA PROBLÉMU A SOUČASNÉHO STAVU

V aktuální situaci je obecně problematika penetračního testování řešena legislativně velmi okrajově. Pokud již řešena je, tak se nejedná o vynucované provedení tohoto typu testu. Což je zvláštní, když se jedná o jednu z nejvíce efektivních metod, jak zjistit bezpečnostní nedostatky. Díky správnému výstupu v podobě reportu posléze poskytuje nutné a rychlé kroky k jejich nápravě. Na základě toho bude zhodnoceno pokrytí penetračního testování a důvod tvorby metodiky.

Penetrační testování průmyslových řídících systémů má své úskalí, a to především v oblasti jejich zabezpečení. Implementace běžných mechanismů ze světa informačních technologií nelze do operačních technologií přenést tak snadno. V některých případech to nelze vůbec, a proto je dobré se o této problematice zmínit. Jednotlivé problémy totiž mohou vést k vystavení těchto systémů do veřejně dostupné sítě – internet. Takové případy a širší souvislosti, v čem tkví problém, budou prezentovány na třech případových studiích. Že se nejedná o nestandardní situaci, se dá poznat na již vzniklých incidentech, které budou popsány a zanalyzovány. Zbylé kapitoly budou věnovány problematice penetračního testování ICS a možným vhodným nástrojům, které se ke specifickým činnostem dají použít.

2.1 Pokrytí penetračního testování

Penetrační testování je řešeno v rámci zákonných povinností velmi okrajově. Vezměme v potaz nejdříve povinnosti, které se vztahují na české subjekty nebo subjekty podnikající na území České republiky. Na ty se vztahuje ZKB a VKB. Penetrační testování je poté zmíněno pouze ve VKB § 11 odst. 3 (Řízení změn), jež dále odkazuje na postup podle § 25 odst. 1 (Aplikační bezpečnost). Uskutečnění testu je určeno pro povinné osoby uvedené v § 3 písm. c), d) a f) zákona a dále přiměřeně pro povinnou osobu v § 3 písm. e). Test je prováděn při uvedení informačního a komunikačního systému do provozu nebo v souvislosti s významnou změnou uvedenou v § 11 odst. 3 (27, 28).

Dále se penetračním testováním zaobírá Obecné nařízení o ochraně osobních údajů (ONOOÚ), které se dotklo všech organizací účinkujících na evropském trhu. Široké veřejnosti je známější pod zkratkou GDPR. ONOOÚ článkem 32, odst. 1 písm. d) ukládá povinnost správcům a zpracovatelům zajistit úroveň zabezpečení včetně procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Obecně je doporučeno penetrační testy provádět na pravidelné periodické bázi, např. 1 ročně (29).

ISO/IEC 27001 penetrační testování nedefinuje přímo, protože přílohou A.12 Operační bezpečnost - A.12.6 Správa technických zranitelností definuje prevenci exploitace technických zranitelností. Kontrola A.12.6.1 Management technických zranitelností pak říká, že organizace musí získat informace o technických zranitelnostech informačních systémů včas. Tento bod je z hlediska standardu naplněn při kontrole zranitelností a organizace tedy ví, že její systémy jsou zranitelné vůči určitým zranitelnostem. Doporučuje se však, aby organizace kromě splnění požadavků kontroly A.12.6.1 provedla i penetrační testování, tím získá lepší přehled kvantifikace možných škod v případě úspěšné kompromitace systému (30).

Podobně tomu je i u Směrnice o bezpečnosti sítí a informací (NIS). Ani zde nenajdeme přímou zmínku o penetračním testování, ovšem k naplnění cílů A (Řízení bezpečnostních rizik) a B (Ochrana proti kybernetickým útokům) je test nezbytný (31).

Pokud tuto kapitolu shrneme, ve většině případů není penetrační testování legislativně vynucováno až na výjimečně případy. V rámci standardů a norem se nacházejí pouze doporučení, a to pouze na úrovni informačních technologií, nikoli operačních technologií a průmyslových řídících systémů.

Je potřebné doplnit, že mnoho osob se mylně domnívá, že technická kontrola je synonymem pro penetrační testování či naopak. Opak je ovšem pravdou. Technická kontrola se skládá z automatického a manuálního testu zjištění konfigurace jednotlivých prvků systému, jeho programového vybavení, využívání služeb a dalšího. Technická kontrola se oproti penetračnímu testování liší v neinvazivním přístupu testování. Součástí penetračního testu jsou i aktivity zahrnuté do auditu rizik, ovšem za účelem další invazivní činnosti pro laterální pohyb nebo využití nového vektoru útoku.

2.2 Tvorba metodiky

V současné době neexistuje adekvátní či vůbec jednotná metodika pro penetrační testování průmyslových řídících systémů. Aktuálně nejpopulárnější publikace, jakými jsou OSSTMM, OWASP, NIST nebo ISSAF, se této specifické oblasti nijak nedotýkají, a tak vzniká prostor pro vznik nové metodiky. Z tohoto důvodu zpracovávám tuto diplomovou práci, která by v budoucnu mohla sloužit jako inspirace pro jednotný návrh řešení. Pro vlastní návrh řešení budou použity poznatky autora z prostředí průmyslových řídících systémů, odborné publikace a aktuální metodiky, které mohou pomoci ve strukturalizaci vstupních a závěrečných ustanovení.

Hned na začátek musíme definovat skutečnost nemožnosti přenesení metodiky nebo rámce pro testy IT na oblast OT (nadmnožina ICS). Již plytkou analýzou těchto oblastí lze zjistit jiná prioritizace požadavků v rámci CIA triády – dostupnost, integrita a důvěrnost. Na straně jedné stojí systémy informačních technologií s nejvyššími požadavky na důvěrnost, na straně druhé průmyslové systémy a potřeba maximální dostupnosti. Proto je tato metodika strukturována do pěti částí, které umožňují zahrnutí všech oblastí pro úspěšně a bezpečné vykonání penetračního testu průmyslových řídích systémů. Jedná se o mezioborové řešení, tedy nejsou zde definovány konkrétní postupy pro různé typy odvětví typu energetika, chemický průmysl, výrobní linky atd.

2.3 Úskalí ICS

Úskalí je na úrovni ICS hned několik. Ty hlavní bude definovány a popsány v následujících bodech:

- vystavení do internetu,
- slabá segregace,
- defaultní nastavení,
- zranitelnosti v protokolech a aplikacích.

Do nedávna byla největší výhodou průmyslových řídících systémů jejich kompletní separace od ostatních systémů. Jednalo se tak o ostrovní systémy. Geniální metodu zabezpečení. Jedná so o odpojení průmyslové sítě od sítě podnikové a od internetu, tím je vytvořena nepřekonatelná bariéra k jejich dosažení. Aktuální konvergence OT a IT

ovšem tuto výhodu celkově smazala. Potřeba digitalizace, trendy v oblasti Průmyslu 4.0 nebo IIoT nutí organizace k propojení těchto systémů s veřejně dostupnou sítí, kde se stávají náchylnými. Závažnost takto vystavených systémů bude prezentována v kapitole 2.4 Dostupnost ICS z internetu a na reálných případech tak bude možné pozorovat vzniklá rizika.

Slabá segregace OT a IT částí je dalším častým problémem, vedoucím ke kompromitaci ICS. Špatně definované zóny k připojení do průmyslové sítě umožňují snadné dosažení na citlivá průmyslová zařízení. Daný problém se dá vyřešit pomocí udržení bezpečnostních zón a vydefinování jasných bodů konektivity mezi těmito systémy.

Na mnoho zranitelností byly vydané patche nebo aktualizace firmwaru. Průmyslové řídící systémy ovšem v mnoha případech operují v nepřetržitém režimu. Upgrade na novější verzi firmwaru může způsobit výpadek. A náhradní zařízení jsou navíc kromě programové logiky nastaveny do defaultního nastavení. Při nahrazení komponent tak máme v systému zařízení bez aplikovaných bezpečnostních politik. Pokud ho samozřejmě daná společnost má. Stav její absence není ojedinělý.

Protokoly používané v ICS nebyly původně vyvíjeny s prioritou na bezpečnost, ale na práci v reálném čase. Od vývoje těchto protokolů nedošlo ke změně. Například MODBUS používá komunikaci v prostém textu, nemá ani správnou autorizaci. To může vést ke změně v programovém kódu nebo vypnutí zařízení. Na úrovni aplikací se potkáme s náchylností na zranitelnosti manipulace parametrů, SQL nebo CMD Injection. Absence šifrování může vést k odchycení přihlašovacích údajů. Přebrání relace je další možností útoku.

Celkové bezpečnosti nenapomáhá ani fakt nedostatku bezpečnostního povědomí. Útoky phishingu, spear-phishingu a sociálního inženýrství přidávají na obrátkách. Jedno kliknutí tak může způsobit kompromitaci počítače, díky kterému pak lze pomocí laterálních pohybů kompromitovat i část s průmyslovými řídícími systémy.

Posledním bodem je pak mnohdy zastaralá technologie. ICS jsou budovány s dlouhou dobou návratnosti v desítkách let. V průběhu času tak dochází k částečným modernizacím udržující systém v provozu. Takový systém je za 10 let neaktuální a nevycházejí na ně nové patche ani aktualizace. Stává se tak mnohem snadnějším cílem pro útok.

2.4 Dostupnost ICS z internetu

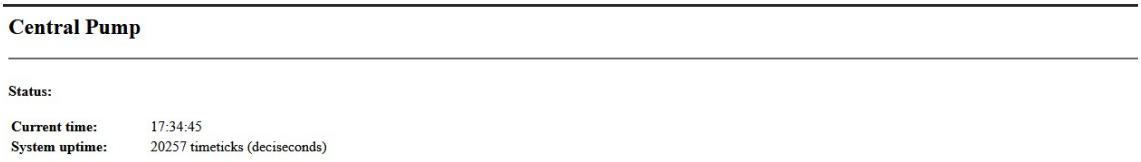
Dlouhou řadu let byla výhodou ICS jejich nedostupnost z internetu. Proč výhodou? Díky absenci některých stěžejních zabezpečovacích mechanismů by byly ve veřejně dostupném internetu snadným terčem útočníků. Takto se jednalo o ostrovní systémy spravované oprávněnými osobami lokálně, tedy uvnitř fyzického perimetru. Tím se nevyvrací možnost vektoru fyzického útoku, alespoň je ovšem minimalizována pravděpodobnost vektoru útoku z veřejně dostupné sítě. Od dob počátku implementace průmyslových řídících systémů došlo k potřebě decentralizace a digitalizace. Tyto dvě významné změny mají za následek vystavení průmyslových řídících systémů veřejnému prostoru. A to buď cíleně nebo neúmyslně.

S detekcí průmyslových řídících systémů vystavených do internetu částečně pomáhá nejznámější placený vyhledávač Shodan. Shodan vznikl za účelem shromažďování informací o všech zařízeních připojených přímo k internetu. Od roku 2010 shromažďuje data také o ICS se svým ICS radarem. Proč tedy pomáhá pouze částečně? Jedná se o dvousečnou zbraň, která lze použít jak k odstranění chyb zabezpečení na straně provozovatele, tak k ulehčení nalezení vektoru útoku pro útočníka.

Jednotlivé případy, které mohou navést k zneužití si odprezentujeme pomocí tří případových studií.

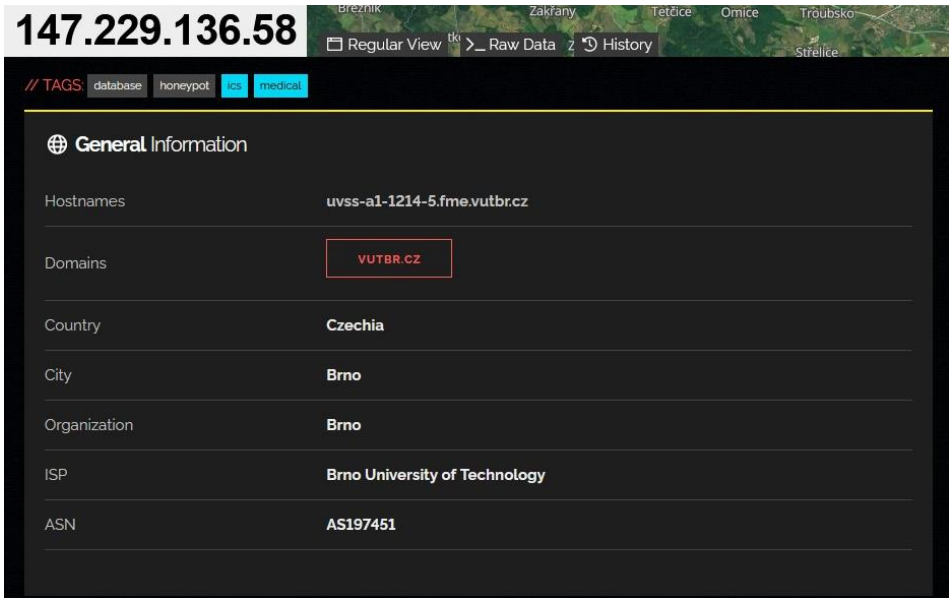
Případová studie I – VUT

Při průzkumu dostupných systémů na veřejném rozsahu VUT Shodan odhalil honeypot. Jenom pro upřesnění, k vyhledání takového zařízení stačí pouze vydefinovat správně tři slova a výsledkem může být webový portál na Obrázku 8: Webové rozhraní VUT Honeypot.



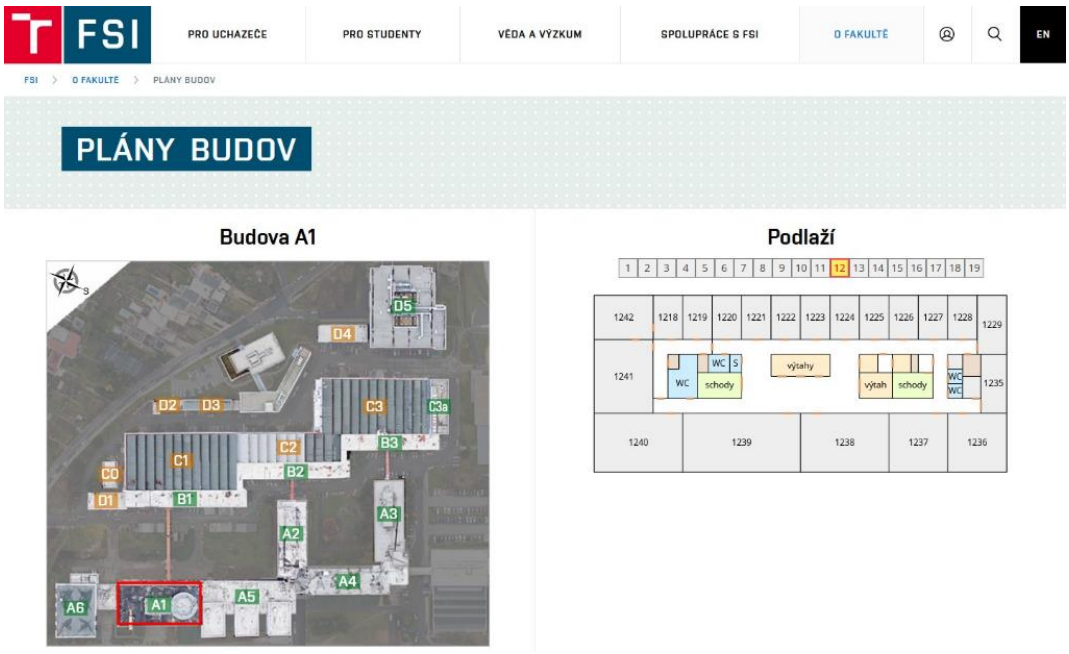
Obrázek 8: Webové rozhraní VUT Honeypot (Zdroj: Vlastní zpracování)

Jedná se o webový portál prezentující se jako centrální pumpa/čerpadlo, kde je definován její stav, aktuální čas a doba běhu systému (nejspíše pro zjištění času uplynulého od posledního útoku). Jak vypadá takový honeypot v Shodanu se lze podívat na Obrázku 9: Shodan – VUT Honeypot.



Obrázek 9: Shodan – VUT Honeypot (Zdroj: Vlastní zpracování)

Jedná se o výstřižek, u kterého chybí na pravé straně vyobrazené otevřené všechny porty. Na první pohled tedy nejde o nic zajímavého. Přeci jen, dostupných honeypotů se v internetu vyskytuje spousta. Ovšem vždy je potřebné zvažovat všechny aspekty, které na dostupném zařízení můžeme vypozorovat. Z názvu hostname můžeme usuzovat jeho lokaci v místnosti 1214, budovy A1, Fakulty strojního inženýrství VUT. Pokud v této fázi pomineme fakt, že se jedná o honeypot a jednalo by se o reálný cíl, který se nám nedaří kompromitovat v kyberprostoru, tak nám tyto informace mohou být užitečné pro jeho kompromitaci v off-line prostředí – tedy pomocí sociálního inženýrství. Největším problémem sociálního inženýrství je většinou neznalost prostředí, kam vstupujeme. I tento problém může být téměř eliminován pomocí zpravodajství z otevřených zdrojů (OSINT). Při vyhledání „vut uvss“ zjistíme, že uvss je nejspíše zkratkou pro *Ústav výrobních strojů, systémů a robotiky* na jejichž portálu se dají zobrazit zaměstnanci s jejich kancelářemi. Po prokliku na kancelář se dokonce zobrazí plány budovy a podlaží.



Obrázek 10: VUT FSI – Plány budov (Zdroj: 32)

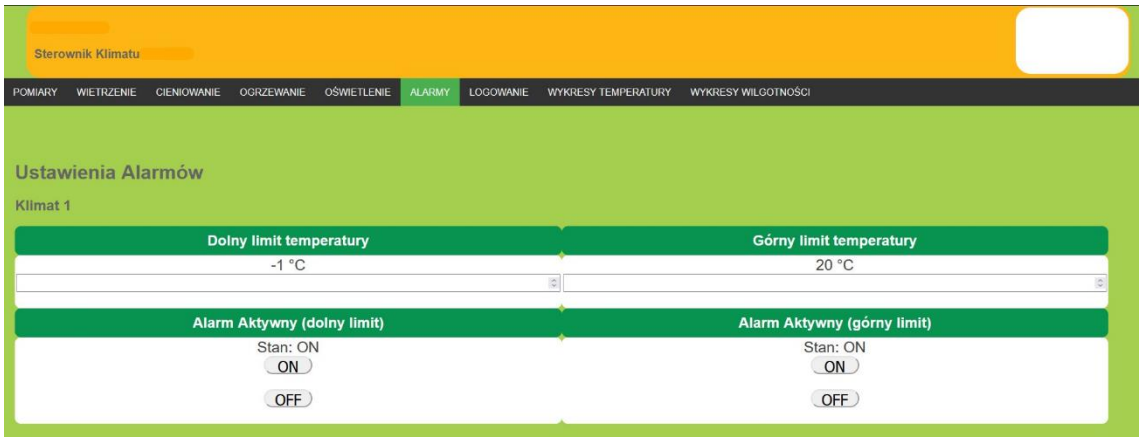
Zde zjišťujeme, že na 12. patře budovy A1 se místnost s označením 1214 nenachází. Ale nachází se zde místnost s označením 1241, kde by se potenciálně zařízení mohlo nacházet. Navíc se jedná o místnost pro kterou není registrován žádný zaměstnanec fakulty. Nelze popírat, že se v této případové studii pohybujeme ve velmi teoretické rovině. Proto se v další případové studii, kde bude využito Google Dorkingu, podíváme na to, že i takovéto informace se dají dohledat z reálného systému

Případová studie II – Polsko

S malými vynaloženými náklady tedy dokážeme vyhledat mnoho informace o veřejně dostupných průmyslových řídících systémech. Otázkou je, zdali se tohoto dá docílit i bez nutnosti vkladu peněžních prostředků. Odpověď je ano. K získání dat může posloužit i obyčejný Google Search. Následující technika je pojmenována Google hacking nebo také Google dorking a zahrnuje použití pokročilých operátorů ve vyhledávači k nalezení konkrétních chyb. Za touto metodou stojí americký počítačový bezpečnostní expert Johny Long, který je znám pod přezdívkou j0hnny nebo j0hnnyhax. V průběhu let se shromáždilo i mnoho variant, jak takto odhalit průmyslové řídící systémy. Jakým způsobem tyto systémy vyhledávat, bude uvedeno v metodice PENTICS samotné. Zde si ukážeme pouze případovou studii, kde se zaměřuji na zařízení Siemens s webovým rozhraním.

Případová studie II je z Polska a bude prezentovat odhalený systém ovladače klimatizace a osvětlení prostor společnosti, která se zabývá rostlinnými školkami. Webové rozhraní pro ovládání využívá platformy Simaticu S7-1200. Pro nastavení parametrů teploty nebo osvětlení tedy stačí překonat pouze přihlášení v rámci této stránky. K zobrazení veškerých dat nám ale nic nebrání. Zcela bezpochyby se jedná o zásadní chybu architekta tohoto systému, která by mohla podnik, jenž je na stabilních teplotách závislý, i zlikvidovat.

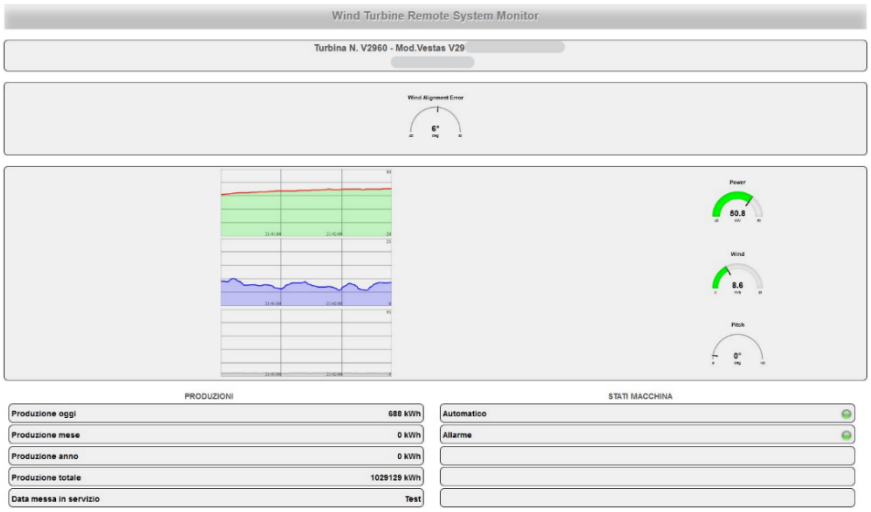
Webové rozhraní si lze prohlédnou na Obrázku 11: Webové rozhraní SIMATIC S7 – Polsko nacházející se na další stránce.



Obrázek 11: Webové rozhraní SIMATIC S7 – Polsko (Zdroj: Vlastní zpracování)

Případová studie III – Itálie

Ještě více podivuhodným se stal nález vzdáleného monitoringu větrné turbíny, který nám poskytuje aktuální data. Jedná se o větrnou turbínu Vestas V29 s jmenovitým výkonem 225.0 kW, jenž je pod správou italského výrobce elektrické energie. Z Obrázku 12: Webové rozhraní SIMATIC S7 - Itálie můžeme vyčíst aktuální výkon, který je 52,6 kW, rychlost 8,6 m/s nebo že od začátku spuštění tohoto „testovacího“ prostředí bylo vyrobeno 1029131 kWh. Po prokliku na stránky dodavatele zjistíme, že je tato větrná turbína v provozu od roku 2009. Jedná se pouze o technologická data, která nijak neohrožují výrobu jejich zpřístupněním. Vždy ale musíme zvažovat širší kontext, kterého se veškeré informace týkají.



Obrázek 12: Webové rozhraní SIMATIC S7 – Itálie (Zdroj: Vlastní zpracování)

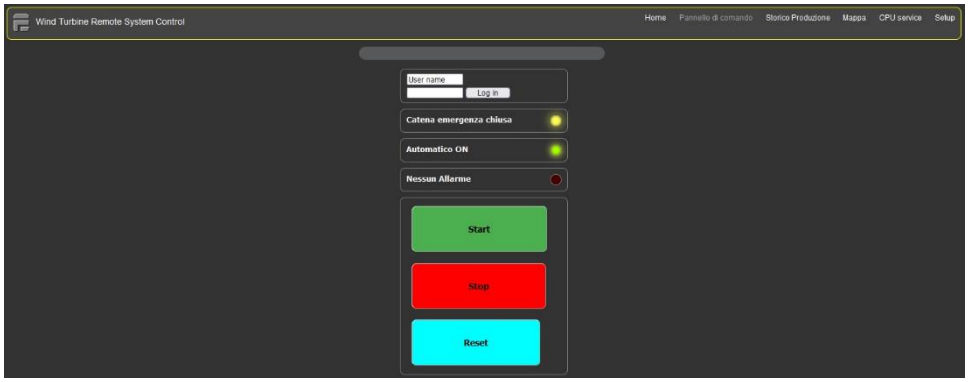
Na stránkách výrobce lze totiž nají informace o normě, dle které své větrné turbíny upgraduje, nejen pro vzdálený monitoring, ale také vzdálené ovládání. Tyto informace a informace od vendora postačí k zjištění informací vedoucích ke spouštěči motorů Siemens ET 200SP.

Obrázek 13: Spouštěč motorů Siemens ET 200SP – Itálie (Zdroj: Vlastní zpracování)

Zde se stačí proklikat skrz menu na uživatelsky definované stránky, kde je již vzdálené ovládání systému. Zde nalezneme hned několik částí k zobrazení. První je všeobecný přehled s podrobnými technologickými daty.

Obrázek 14: Webové rozhraní ET 200SP – Itálie (Zdroj: Vlastní zpracování)

Dále se můžeme přepnout do kontrolního panelu, kde je login interface. Po přihlášení přechází ovládání řízení turbíny do manuálního režimu a můžeme tak daný motor na větrné elektrárně vypnout nebo zapnout.

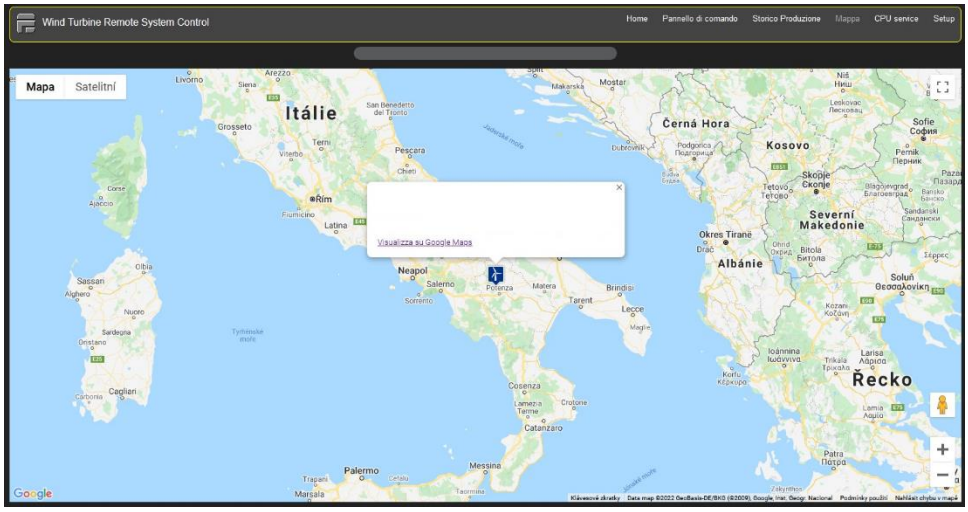


Obrázek 15: Webové rozhraní ET 200SP, manuální ovládání – Itálie (Zdroj: Vlastní zpracování)

K zobrazení je také historie výroby. Tato větrná turbína vyrábí například od roku 2019.

Obrázek 16: Webové rozhraní ET200SP, technologická data – Itálie (Zdroj: Vlastní zpracování)

A v záložce mapa je dokonce zaznamenána její fyzická poloha.



Obrázek 17: Webové rozhraní ET200SP, mapa – Itálie (Zdroj: Vlastní zpracování)

V posledních dvou částech je poté služba CPU, jež odkazuje na login interface do modulu ET 200SP. Nejzajímavější je poslední část s názvem Setup, tedy nastavení. Tato část je rozdělena do 3 kategorií – vítr, generátor a hydraulický systém. Je nutno zmínit, že italský dodavatel zde doplnil informativní upozornění: „*POZOR! Nesprávné nastavení některých parametrů by mohlo ohrozit výkon stroje. Manipulaci doporučuje pouze kvalifikovaný personál*“.

Obrázek 18: Webové rozhraní ET 200SP, parametry – Itálie (Zdroj: Vlastní zpracování)

Mnohem smutnější než nalezení takovýchto systémů ve veřejné síti, je proces hlášení takovéhoto nálezu. V případě dostupných větrných turbín v Itálii došlo dvakrát k upozornění dodavatele řešení v rozmezí 2 měsíců. Bez reakce. Pro nahlášení nastalé situace italskému CSIRTu je nutné mít speciální placený e-mail, u kterého je potřebné se prokázat občanským průkazem. Proto přešlo řešení pod český NÚKIB, který potřebné záležitosti předal na mezinárodní úrovni jednotlivým státům.

2.5 Historie a analýza incidentů na ICS

Četnost útoků na průmyslové systémy není taková, jakož tomu je v segmentu IT, ovšem výjimkou také nejsou. Největší přelom nastal v roce 2010, ovšem kořeny sahají mnohem hlouběji.

Prapůvodce incidentů

Za prapůvodce, kdy se dá mluvit o incidentu, můžeme zmínit Marconiho hacknutí bezdrátové komunikace. Stalo se tak v roce 1903, kdy se italský rozhlasový průkopník, Guglielmo Marconi, připravoval k prezentaci dálkové bezdrátové komunikace pomocí morseova kódu. A to na vzdálenost více jak 300 mil. Před tím, než prezentace vůbec započala se rozeznělo klikání morseova kódu, které po přeložení znělo:

> *Rats, rats, rats, rats.*
> *There was a young fellow of Italy,*
> *Who diddled the public quite prettily* (33).

Za tímto skutkem stál britský hudební mág Nevil Maskelyne, který chtěl vyvrátit tvrzení Marconiho, že bezdrátový telegram může posílat zprávy bezpečně. Tím se také stal nejspíše prvním osobou, která veřejně oznámila zranitelnost v rámci moderních technologií (33).

Čistírna odpadních vod Maroochy Shire

Píše se březen roku 2000 a oblast Maroochy Shire (Queensland, Australie) se potýká s problémy na novém systému odpadních vod. Problém spočívá v selhání komunikace s čerpací stanicí odpadních vod pomocí radiofrekvenčních signálů. Čerpadla navíc nefungovala korektně a alarm, který měl upozornit systémové inženýry při chybě nefungoval podle očekávání. Jeden z inženýrů při monitoringu zjistil, že do signálů někdo úmyslně zasahuje a způsobuje tak tyto problémy. Na základě tohoto byl najat tým specialistů a byla kontaktována policie (34).

Po roce, v dubnu 2001, byl dopaden Vitek Bode, u kterého byl nalezen notebook a speciální SCADA vybavení. K ovládání až 150 čerpacích stanic používal obyčejný radiový vysílač. V průběhu 3 měsíců vypustil miliony galonů neupravené odpadní vody do vodních cest a lokálních parků. Motivem měla být odplata za jeho odmítnutí na pracovní pozici u rady města Maroochy. Je to jeden z případů, kdy útok na ICS dospěl k fyzickým škodám. Tento případ je výjimečný dopadením, a dokonce odsouzením útočníka. Navíc poukázal na 4 skutečnosti:

- Je velmi náročné se bránit před útoky „insiderů“, tj. osob uvnitř společnosti nebo přístupem do ní
- Radiokomunikace používaná ve SCADA systémech je obecně nezabezpečená a špatně nakonfigurovaná
- SCADA systémy by měly být zabezpečeny zároveň pomocí fyzických a logických ovládacích prvků
- SCADA systémy musí zaznamenávat připojení a příkazy všech zařízení, především těch, které obsahují připojení k nebo ze vzdálených míst (34).

Gruzínská válka

Při gruzínské válce vybouchlo turecké potrubí, stalo se tak roku 2008 a v prvních okamžicích to bylo považováno za kybernetický útok. Na základě analýzy SANS ICS týmu toto tvrzení bylo rozporováno, protože nebylo dostatek potřebných dat, které by toto tvrzení potvrdilo nebo odvrátilo. Je to ovšem krásný příklad, kdy se selhání průmyslového systému svádí na kybernetický útok. Nebo naopak. Popírat se nikoli nedá fakt využívání kybernetických útoků v průběhu této války ze strany Ruska (35).

Rusko bylo první, které připustilo nasazení taktiky kybernetické války. To v tomto případě zahrnovalo narušení elektrické sítě a vyřazení systému včasného varování. Což mělo za následek nemožnost komunikace obyvatelstva při vtrhnutí ruských vojsk (35).

Stuxnet

Nejznámější z nejznámějších. I tak se dá hovořit o malwaru z roku 2010. Jednalo se o nejvíce sofistikovaný útok, který mířil specificky na ICS a spouštěl se automaticky pouze tehdy, když měl potřebná data. Nehrozilo tak prozrazení. Stuxnet měl za cíl zničení íránského programu na obohacování uranu v Natanzu. Konkrétně mířil na zničení odstředivek. Jednalo se o utajovaný projekt zpravodajských agentur americké a izraelské vlády pod krycím názvem „Operace Olympijské Hry“. A opravdu se tak stalo, pomocí Struxnetu bylo zničeno kolem 1000 těchto odstředivek. Ovšem mimo ně bylo infikováno také dalších 200 000 zařízení (36, 37).

Největším silou Stuxnetu byla jeho schopnost vlastní replikace a šíření se skrz různé systémy. Není se čemu divit, když využíval 4 zero days exploity. Navíc využíval digitální certifikát, který byl ukraden ze dvou odlišných taiwanských společností. Stal se tedy při instalaci pro počítačové systémy důvěryhodným. Mimo jiné byl také téměř nevystopovatelný, jelikož schovával své binární soubory pomocí Windows rootkitu. Funkcionalita tohoto malwaru byla modifikace PLC kódu pomocí rootkitu na PLC zařízeních značky Siemens. Škodlivý kód modifikoval data posílaná z PLC do HMI, a tak nebylo možné odhalit vadná data, které PLC reálně zpracovávalo. Zajímavostí také je způsob, jakým byl Stuxnet programován. Nejednalo se o kód psaný na linuxové distribuci, ale na platformě Microsoft Windows. Dokonce existuje tvrzení o existenci více verzí tohoto malwaru. Prozrazení tohoto projektu a infikace dalších zařízení mimo původní cíl opera v prostředí Natanzu padá nejspíše na hlavu izraelských tajných služeb, konkrétně Jednotky 8200, které jedna z verzí při testování unikla (36, 37).

Co si z tohoto vzít? Dobře sponzorovaný sofistikovaný zdroj dokáže vyvinout a napadnou jakýkoliv systém. Proto je podstatná schopnost obnovy z kybernetického útoku.

Night Dragon

Taktiky, techniky a procedury (TTPs), které cílily ropné, energetické a petrochemické společnosti. Útok zasáhl minimálně 71 organizací a cílil na shromažďování dat. Mimo jiné i ze SCADA systémů. Night Dragon využíval od roku 2006 do roku 2011 jednoduché, ale účinné techniky – sociální inženýrství, spear-phishing, exploiatace známých Microsoft Windows zranitelností a kompromitace Microsoft Active Directory. Tyto ne příliš sofistikované techniky kromě sbírání dat od těchto společností mohli přejít ke vzdálenému ovládání HMI (38).

Night Dragon je důkazem možnosti kompromitace společností pomocí ne příliš sofistikovaných, ale účinných, metod.

Shamoon – Saudi Aramcoa a RasGas

Dne 15.srpna 2012 destruktivní malware zaútočil na počítačové systémy firmy Saudi Aramco, největší energetickou společnost na světě. Datum bylo zvoleno cíleně, jelikož všech 55 000 zaměstnanců Saudi Aramco zůstalo doma, aby se připravili na oslavu jednoho z největších islámských svátků – Lailat al Qadr. Po spuštění malwaru bylo přepsáno na 30 000 počítačů. Jediné, co na počítači zbylo, byla hořící americká vlajka. Shamoon byl malware, který se zaměřoval na kradení dat a obsahoval také destruktivní modul. Ten přepisoval Mater Boot Record (MBR), tabulku oddílů a většinu dokumentů s náhodnými daty. Po tomto zásahu již nejdou data obnovit. Dvanáct dní později Shamoon malware napadl katarskou plynařskou společnost RasGas. RasGas je jednou z největších společností na světě se zkapalněným zemním plynem. Není známo, že by malware měl přímý dopad na ICS nebo SCADA systémy Saudi Aramco nebo RasGasu (39).

Přehrada u New Yorku

Důkaz toho, proč nevystavovat SCADA systémy do internetu. V roce 2013 se k malé přehradě Bowman dostali íránští hackeři. Nikoli fyzicky, ale v kyberprostoru. Bowmanská přehrada je používána pro kontrolu přílivu vody při bouři. Její SCADA systém byl v době útoku připojen do internetu pomocí mobilního modemu. A to i kvůli probíhající údržbě, kdy nebyla možná její kontrola, ale pouze sledování monitoringu.

Většina odborníků se shodla, že se nejspíše nejednalo o cílený útok, ale o využití příležitosti snadného cíle. (40)

Technické detaily vniknutí do systému bowmanské přehrady nejsou známy, jelikož je tento prvek kritickou infrastrukturou (KI).

Havex

RAT (remote access trojan) malware ze stejné dílny jako o Dragonfly/Energetic Bear nebo BlackEnergy. První výskyt v roce 2013, v roce 2016 byl spjat se skupinou GRIZZLEY STEPPE, která byla součástí RIS (ruská civilní a vojenskou zpravodajská službou) (41).

Havex dokáže komunikovat s C2 (command-and-control) serverem, který umí nasazovat modulární paylody. Jeden z analyzovaných paylodů enumeroval všechna připojená síťová zařízení používající klasickou verzi DCOM (Distributed Component Object Model) standardu OPC (Open Platform Communications) k získání informací o připojených ICS zařízeních a jiných zdrojích v síti (41).

Havexův specifický paylod zaměřený na kontrolní systémy shromažďoval informace o serveru, včetně CLSID, názvu serveru, ID programu, verze OPC, informace o vendorovi, stavu provozu a dalších. Ovšem tento typ útoku nebyl bez chyb. Na mnohých OPC platformách způsoboval výpadky, což způsobovalo DoS (Denial of Service) efekt na zařízení, která na OPC komunikaci byla závislá (41).

Německá ocelárna

Útok na nespecifikovanou německou ocelárnu byl zaznamenán v prosinci 2014 pomocí spear-phishingu a sociálního inženýrství. Tím útočníci získali přístup do firemní sítě, odkud si propracovali cestu do sítě technologické. Zde způsobili mnohonásobné selhání individuálních řídících systémů zabraňujících výbuchu pece jejím odstavením, což vedlo k masivním škodám ocelárny. Schopnosti útočníka byly popsány jako „velmi pokročilé“. Útočníci měli širokou znalost jak v IT bezpečnosti, tak detailní znalost ICS a procesu výroby železa (43).

Obrázek 19: Pec na železo (Zdroj: 43)

BlackEnergy

Kampaň probíhající od roku 2011. Zaznamenána ovšem až v roce 2014 a připsána RIS skupině – GRIZZLEY STEPPE. Cílem byly HMI různých výrobců – GE Cimplicity, Advantech/Broadwin WebAccess a Siemens WinCC (44)

Malware BlackEnergy je modulární, a ne všechny funkcionality jsou vždy spouštěny na všech zařízeních. Typickým útokem byla infekce, která hledala jakékoliv namapované síťové složky a odnímatelná média, jež můžou vykonat laterální pohyb s infikovaným prostředím (44).

Dragonfly/Energetic Bear

Další kampaní, která probíhala pod skupinou GRIZZLEY STEPPE byl Dragonfly/Energetic Bear. Primárně využíval Havex malware, sekundárně poté Karagany RAT. Záznamy o útocích jsou z USA, Turecka a Švýcarska. Mělo se jednat o poslední fázi kampaně, kdy se měli útočníci snažit o získání přístupu do sítě (45).

Ukrajinská distribuční síť

První známý útok na elektrickou síť byl právě na Ukrajině v roce 2015. O dodávku elektrické energie přišlo bezmála 230 000 lidí kvůli odstavení 30 rozvoden. SCADA vybavení bylo vyřazeno z provozu a obnovení dodávky muselo být dokončeno ručně. Pozdější vyšetřování ukázalo využití BlackEnergy malwaru v makru dokumentu Microsoft Excel. Tento dokument byl do korporátní sítě doručen pomocí spear-phishipng e-mailů. Jednalo se o vztyčený prst pro všechny subjekty, které byly zařazený do kritické komunikační infrastruktury, zdali jsou opravdu dostatečně zabezpečeni (46).

K dalšímu útoku na ukrajinskou distribuční síť došlo začátkem roku 2022 při invazi ruských vojsk. Byly použity stejné techniky, jak v letech 2015 i 2016. Za útokem by měla stát ruská jednotka 74455 (Sandworm) (46).

Vodárenská společnost „Kemuri“

Kemuri je pouze fiktivní název vodárenské společnosti, jejíž problémy byly prezentovány v roce 2016 společností Verizon Security Solutions. Útočníci zde získali přístup ke korporátní síti pomocí SQL injection a phishingu. Pomocí různých kroků došli k získání přístupu na AS400 server, odkud již nebyl problém ovládat SCADA systém pro vodní okruhy. V tomto systému upravili množství chemikálií ovlivňujících kvalitu vody tak, aby se obnova dodávky vody prodloužila (47).

Obrázek 20: Čistička vody (Zdroj: 48)

Podstatné je zmínit že chabá architektura sítě a ICS vystavené do internetu jsou snadným cílem, který může mít dopad na velké množství lidí a jejich zdraví.

CRASHOVERRIDE

Jeden z nejzajímavějších incidentů po Stuxnetu, odehrávající se o 7 let později, tj. koncem roku 2017. Jeho využití v rámci útoku na Ukrajině potvrdila firma Dragon Security ve spolupráci se slovenským ESETem. CRASHOVERRIDE je také znám pod názvem "Industroyer". Způsobil velké škody, které měly za následek výpadek rozvodné elektrické sítě. Dle výzkumných agentur se jednalo o malwar, který byl cílený pouze na elektrické sítě. Čtvrtý, který se zaměřoval specificky na průmyslové systémy (po Stuxnetu, BlackEnergy-2, Havex). A po Sruxnetu druhý malware, který měl za cil narušení fyzických průmyslových procesů. Zajímavý je také poznatek, že CRASHOVERRIDE neměl za cíl špionáž nebo sběr dat jako u většiny předešlých, ale jeho jediným motivem bylo způsobení výpadku (49).

Správně bychom jej ovšem neměli nazývat malwarem, nýbrž malware frameworkem a hned vysvětlím proč. CRASHOVERRIDE v sobě má zabudované moduly pro IEC 101, IEC 104, IEC 61850 a OPC. Je navrhnut, aby umožnil navíc i přidání dalších payloadů, jakým muže být DNP3, ale podobné využití nebylo doposud potvrzeno. Mimo jiné obsahoval také nonICS moduly pro smazání souborů nebo deaktivaci procesů na běžícím systému, čímž je dosažená větší efektivita při útoku. Moduly při útoku vynucuji otevření přerušovačů okruhu na RTU, které poté uzavřou do nekonečné smyčky. Tím je docílení stálého otevření, a to i v případě pokusu o převzetí na manuální řízení (49).

Existují obavy, kdy by mohl tento malware framework způsobit výpadky delší než hodiny. Výpadek by mohl trvat i dny, pokud by se útočníci zaměřili na více cílů zároveň. Muselo by se tedy jednat o koordinovaný útok. Nic takového není nemožné, dokonce můžeme říct dosti možné, ovšem ne triviální (49).

Tento případ je opět ukázkou toho, že s dostatečnými finančními prostředky a motivem lze způsobit fyzické narušení průmyslových řídících systému, které mají vliv na obyvatele různých zemí.

Německé větrné turbíny

Větrné turbíny v oblastech bez pokrytí mobilní sítí využívají k ovládání a vzdálenému monitoringu satelitní komunikaci. V případě německých větrných turbín o celkovém výkonu 11 GW tomu není jinak. Specifiky pak využívají komunikaci přes KA-Sat u které došlo k výpadku spojení 31. března. Nedošlo zde přímo k útoku na řídící systémy, ale na zmiňovaný satelit KA-Sat. Ten je využíván také k pro vojenské komunikační služby americké armády. Zdá se tak, že výpadek konektivity k větrným farmám byl vedlejší škodou útoku na vojenský cíl. Zprvu byl odhad postižení na 3000 větrných turbín, posléze došlo ke korekci na 5800 celkově zasažených turbín. Při výpadku ztrácí operátoři možnost kontroly a regulace, přičemž větrná turbína přechází do provozního módu autopilota (50).

2.6 Problematika penetračního testování ICS

Jak bylo zmíněno již v kapitole 2.2 Tvorba metodiky, k penetračním testům ICS nelze přistupovat stejným způsobem jako se přistupuje k systémovému testování podnikového IT. V době 5-7 let nazpět bylo moderní snahou přesvědčovat vlastníky průmyslových systémů o opaku – implementace IT řešení lze provádět i v ICS, tedy i penetračního testování. Nikdo se nechtěl bavit o výzvách, které jsou v rámci ICS čeleny. Na přelomu století byl ovšem představen koncept CIA triády, především pro certifikaci CISSP (Certified Information Systems Security Profesional). Záměr byl jasný, nastínit tři hlavní oblasti informační bezpečnosti:

- Confidentiality - důvěrnost
- Integrity - integrita
- Availability - dostupnost

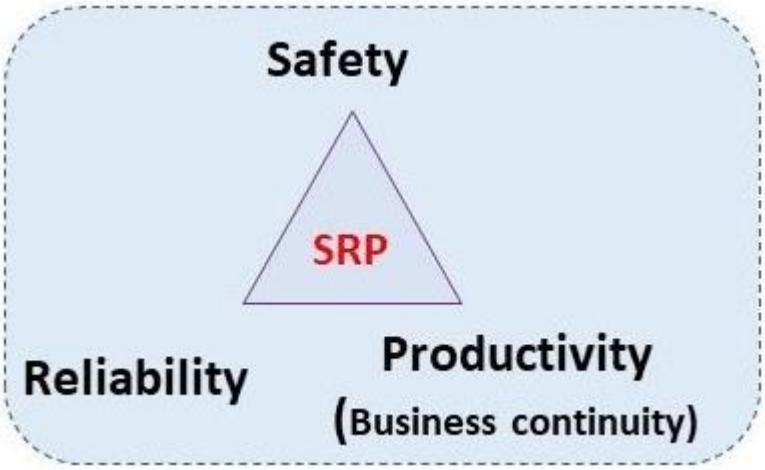
Doposud se neví, zdali bylo toto pořadí dle priorit prezentováno takto naschvál, ovšem v průběhu času je priorita v rámci IT prezentována výše zmíněným způsobem.

Od této části se ovšem cesty s ICS dělí. Primární funkcí ICS je spravování a ovládání procesů vybavení, jakým mohou být pumpy, ventily a další prvky, které jsou provozovány v bezpečnostních systémech, jaderných nebo elektrických zařízeních, rafineriích atd. Mnoho z těchto systémů je provozováno k udržování kritické výroby

a bezpečnostních procesů. Pokud dojde k nedostupnosti těchto systémů, firmy mohou ztratit obrovské množství produkce a lidé se mohou vážně zranit. Navíc jsou tyto systémy klasifikovány jako systémy s vysokou dostupností. Což znamená udržení dostupnosti na úrovni minimálně 99,999 procent. A proto se zde priority v konceptu CIA triády mění a dostupnost je na vrcholu:

- Availability - dostupnost
- Integrity - integrita
- Confidentiality - důvěrnost

Největší důraz je tedy na dostupnost ICS zařízení, hned poté následuje kvalita posílaných a přijímaných dat. Špatný příkaz poslaný na takové zařízení, může způsobit jeho výpadek. Důvěrnost je v tomto případě téměř zanedbatelná. Proto se v dnešní době v rámci OT začíná mluvit o tzv. **SRP triádě** – Safety (bezpečnost), Reliability (spolehlivost) a Productivity (produktivita). Ani tento přístup ovšem není dokonalým a osobně se přikláním k rozšíření CIA triády o S a zachování priorit pro OT systémy. To znamená, že nám vzniká SAIC zaměřující se primárně na bezpečnost, která je vyhodnocována pro všechny další body CIA triády individuálně (51).



Obrázek 21: SRP triáda (Zdroj: 51)

Průmyslové systémy nebyly vyvinuty s ohledem na bezpečnost, viz. Kapitola *2.3 Zabezpečení ICS*. Mezi problémy penetračního testování ICS musíme zahrnout následující body:

- **Nízký výpočetní výkon –** Systémy pracují s vestaveným procesorem, takže může dojít ke snadnému přetížení, které způsobí například zamrznutí, reset, chyby, ztrátu síťové komunikace nebo dokonce ztrátu vlastní konfigurace.
- **Špatné zacházení s protokolovým zásobníkem –** Problematika zpracování síťového provozu, který tato zařízení neočekávají je obtížná. Stejně jako u předešlého bodu, může dojít ke stejným scénářům v případě kdy je na ně zaslán nadrozměrný nebo deformovaný paket, nemluvě o problému s jinými protokoly.
- **Použití zastaralých systémů –** Mnoho průmyslových systémů obsahuje stále zastaralé systémy, jakými je Windows XP nebo dokonce Windows NT a Windows 95. EOF pro tyto systémy je 20 a více let, ovšem klasické problémy (modrá obrazovka smrti) jsou přítomné stále.
- **Síť s malou šířkou pásma –** Ve většině ICS sítí se využívá komunikace s malou šířkou pásma přenosu. To je způsobeno i již výše zmiňovanými zastaralými systémy. Při velkém nebo neočekávaném síťovém provozu či DoS útoku, může nastat výpadek komunikace se zařízením nebo celkové přerušení spojení s ním. Takový výpadek může každopádně způsobit i správně vytvořený příkaz ping.

Vysoká úroveň síťového provozu může způsobit latence, které nejsou akceptovatelné.

Pro shrnutí – aktivní penetrační testování, skenování zranitelností anebo dokonce pouze jednoduché skenování sítě, jaký využívá například Nmap, může způsobit problémy, které byly již zmíněny. Pokud je tedy obava o dostupnost produkční sítě, potom by mělo být veškeré aktivní skenování a testování prováděno v testovacích nebo vývojových prostředcích. (20, str.112)

2.7 Vhodné nástroje a vybavení

Ač se může zdát aktuální propast mezi informačními a operačními technologiemi nekonečná, v rámci nástrojů a vybavení nejsou od sebe tyto technologie příliš daleko. Samozřejmě zde svá specifika najdeme, především na úrovni 3 a níže v Purdue referenčním modelu pro ICS, ovšem jedná se například o využití jiných modulů, pro již zaběhlé nástroje nebo vybavení pro penetrační testování informačních technologií. Zaběhlé nástroje se omezují spíše na úrovni jejich způsobu použití.

Kromě klasického hardwarového vybavení v podobě notebooku může penetrační tester použít další užitečná zařízení doplňující jeho celkovou vybavenost. Za zmínku stojí Raspberry Pi, Alfa, Rubber Ducky, BashBunny nebo HackRF One. Mimo tyto zmíněné prvky lze využit specializované stavby HW prostředků pro konkrétní účely průmyslového prostředí uložené do zodolněného racku, který tak lze snadno přemístit na lokalitu, kde probíhá testování. Veřejně dostupné jsou i nástroje přímo od dodavatelů, jako tomu je u Siemensu. Ten poskytuje adapter pro připojení notebooku k PLC SIMATIC S7.

Obrázek 22: HackRF One (Zdoj: 52)

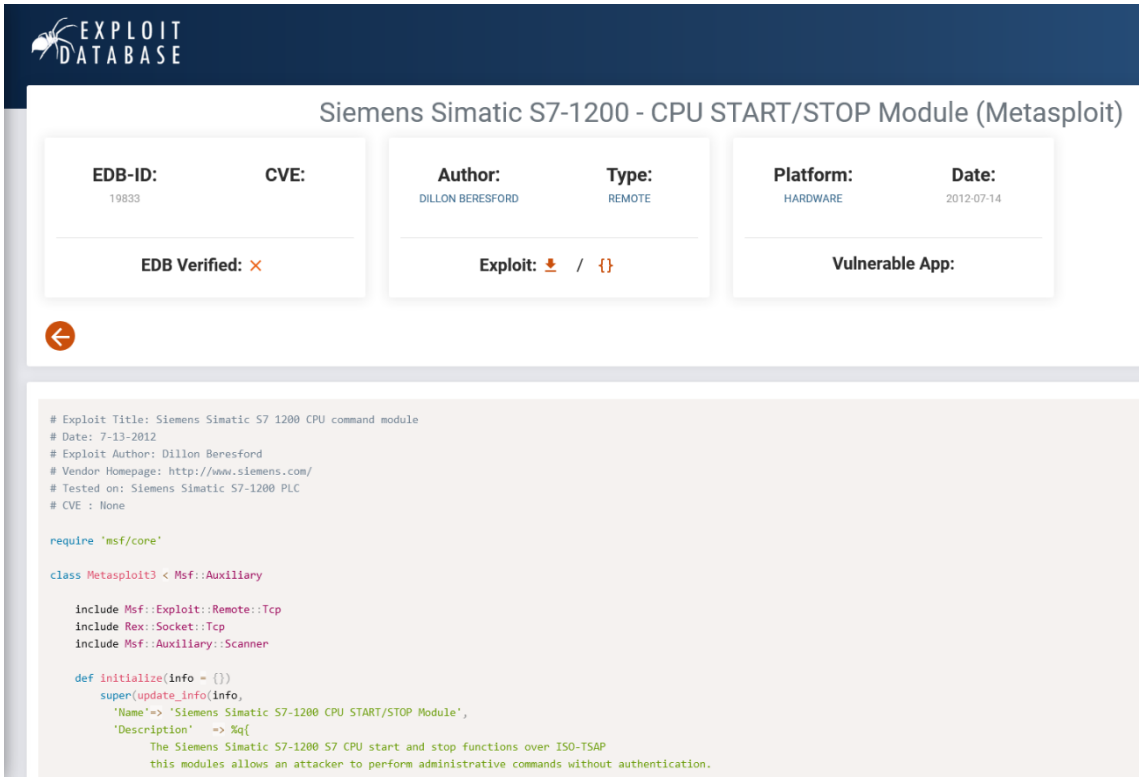
Existuje spousta nástrojů a softwaru, které lze implementovat do existujících operačních systémů. Takový proces je velmi časově náročný a je tak lepší využít již existujících Linuxových distribucí určených pro dané účely penetračního testování. Ty lze instalovat na železo, virtualizovat nebo je spouštět v cloudu. Nejadekvátnější metodou pro použití v průmyslových řídících systémech je jejich virtualizace. Nejrozšířenějším operačním systémem je Kali Linux a ParrotOS. Specificky vyvinutou distribucí pro průmyslové řídící systémy je operační systém ControlThingsPlatform, který vznikl z projektu SamuraiSTFU.

Obrázek 23: Kali Linux Intro (Zdroj: 53)

Nástroje používajíce se k testování se mohou dělit na proprietární (nástroj, u kterých je potřebné vlastnit placenou licenci či spoléhat na důvěryhodnost vydavatele) a nástroje zdarma (dle filozofie free open-source software, kdy je zdrojový kód volně dostupný veřejnosti. Pro testování sítě je možné využívat nástrojů:

- Nessus
- Nmap
- Wireshark.

Léty ověřený framework Metasploit slouží k vývoji a spouštění exploitů vůči cíli. Jeho moduly mohou být doplněny o SCADA specifické exploitace různých vendorů – BACnet, General Electric, Moxa, Schneider Electric nebo Siemens. Pro dva zmíněné je dostupný například exploit pro CPU STOP, viz. Obrázek 24: Exploit DB – Simatic S7-1200 CPU START/STOP Module. Další exploity lze získat ze stránek *exploit-db.com* nebo si je můžeme sami naprogramovat.



Obrázek 24: Exploit DB – Simatic S7-1200 CPU START/STOP Module (Zdroj: 54)

Na lámání hesel existují nástroje pro platformu Windows Ophcrack a pro Linux Hashcat, John the Ripper, Hydra nebo Medusa. Při potřebě testu bezdrátových sítí je k dispozici aircrack-ng a hackrf.

Mnohdy je jedinou možností průniku využití fyzického sociálního inženýrství, kde jsou dostupné nástroje pro odemčení zámků (lockpick). Velmi efektivní, zvláště v průmyslovém prostředí, se jeví kombinace helmy, reflexní vesty a žebříku. Mnohdy dojde k vpuštění do objektu samotnými zaměstnanci, kteří se v dobré víře snaží pomoci. Proto i takové vybavení může být, a je součástí vybavení penetračního testera.

3 VLASTNÍ NÁVRH ŘEŠENÍ

Vlastní návrh řešení je obsažen v příloze nazvané PENTICS, kde jsou jednotlivé části popsány podrobně. V rámci hlavního těla dokumentu diplomové práce bude popsán především obsah jednotlivých kapitol s definicí jejich významu v navržené metodice. Mimo jiné v hlavním dokumentu bude popsána celková struktura pomocí grafického znázornění metodiky penetračního testování průmyslových řídících systémů. Celá metodika je koncipována jako mezioborové řešení, a proto neuvádí konkrétní případy využití jednotlivých nástrojů a pouze jejich využití omezuje na úrovni, které zainteresované subjekty v rámci procesu testování budou rozumět. Proces testování by měl probíhat jako komplexně řízená činnost mezi oběma subjekty pro zajištění ochrany majetku, osob a zdraví.

Obrázek 25: PENTICS (Zdroj: Vlastní zpracování)

PENTICS je rozdělen celkem na šest částí. Jednotlivé části pokrývají testování od začátku definované prvotním setkáním objednatele a dodavatele, přes samotný proces testování, až po finální reportování. Složení je proto následující:

1. Počáteční ustanovení
2. Modelování hrozeb
3. Průzkum a získávání informací
4. Externí testování
5. Interní testování
6. Reportování

Postup samotného testování je tak možné vidět zjednodušeně v rámci jednotlivých kapitol pomocí grafu, jednotlivé části jsou v metodice penetračního testu dále segmentovány na menší podmnožiny popsané v metodice.

3.1 Počáteční ustanovení

První část definující počáteční ustanovení pokrývá body před započetím penetračního testování, kdy dochází ke schůzce mezi objednatelem a dodavatelem a vymezuje se rozsah, cíle, komunikační kanály, řešení incidentů a pravidla testování. V rozsahu je definována koncepce úrovňového testování, které je možné definovat na jednotlivé metody, využívané při testování. V rámci počátečního ustanovení postupuje dle Grafu 1: PENTICS – Počáteční ustanovení.

V rámci inicializační schůzky se stanoví rozsah penetračního testu, který vytyčuje jeho hranice, čímž je předejito problémům s nenaplněním cílů či dokonce problémům právním. Je nutné definovat, co vše bude testováno, jakým způsobem, rozsah daného způsobu a povolené metody, tj. zmiňované vymezení hranic. V rámci rozsahu a následného dotazníku by měl pomoci vést schůzku dodavatel na základě svých zkušeností. Samotný rozsah také obsahuje pomocný dotazník definující nutné minimum pro získání informací mezi subjektem objednatele a dodavatele. Okruhy těchto otázek jsou vymezeny na obecné otázky, otázky zaměřené na ICS, otázky zaměřené na fyzický perimetr, otázky zaměřené na sociální inženýrství, otázky pro manažery a otázky pro systémové inženýry. Dotazník je součástí vstupních dat do rozsahu. Obsahové informace rozsahu poté vstupními daty pro stanovení cílů.

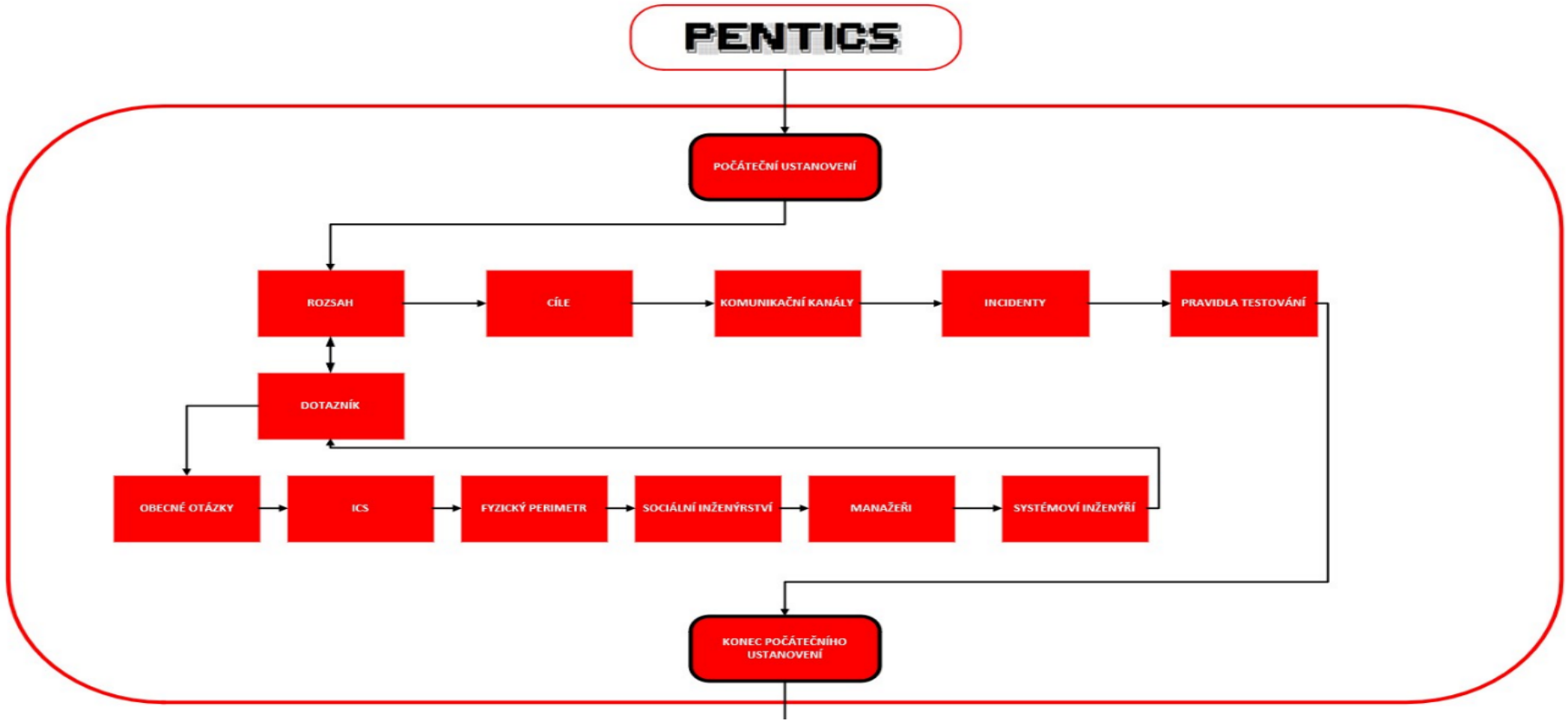
Každý prováděný penetrační test by měl být orientován na cíl. Nastavení cíle a klíčových bodů splnění vede k jasnému zjištění naplnění požadavků objednatele. Ten by měl být schopen definovat primární a sekundární cíl. Kdy primární cíl je definován jako množina zaměřená s cílem splnit např. zákonné požadavky, požadavky ze standardu nebo certifikace. Sekundární cíl je zaměřen na technologii samotnou ve znění požadavků na otestování konkrétních systémů nebo systémových celků.

V případě nastání nenadálé nebo neočekávané události je nutné mít stanoveny komunikační kanály mezi objednatelem a dodavatelem. Komunikační kanál je jasně definován a komunikace funguje na předem domluvené časové frekvenci nebo vykonané akci. Minimální rozsah nastavení výše uvedených parametrů je povinný pro hlášení bezpečnostních incidentů, a to prostřednictvím nouzového kontaktu jak ze strany dodavatele, tak objednatele.

Při penetračním testování dochází k testu samotného procesu hlášení incidentů, v kterém jsou zainteresovány strany neinformované o průběhu testu. Jen tak a pouze se dá ověřit procesní účinnost na dané úrovni. Informovanost o testu by měla být držena na principu nutného minima. Informované osoby budou mít k dispozici data o čase vykonávání testu, jeho rozsahu a musí být začleněni do komunikace reportování průběhu testu.

Pravidla testování doplňují rozsah testování o podmínky, jakými mají být testované prostředky objednatele testovány. Pravidla zahrnují:

- Časový plán
- Nakládání s daty
- Zakázané činnosti
- Právní aspekty
- Způsob reportován



Graf 1: PENTICS – Počáteční ustanovení (Zdroj: Vlastní zpracování)

3.2 Průzkum a získávání informací

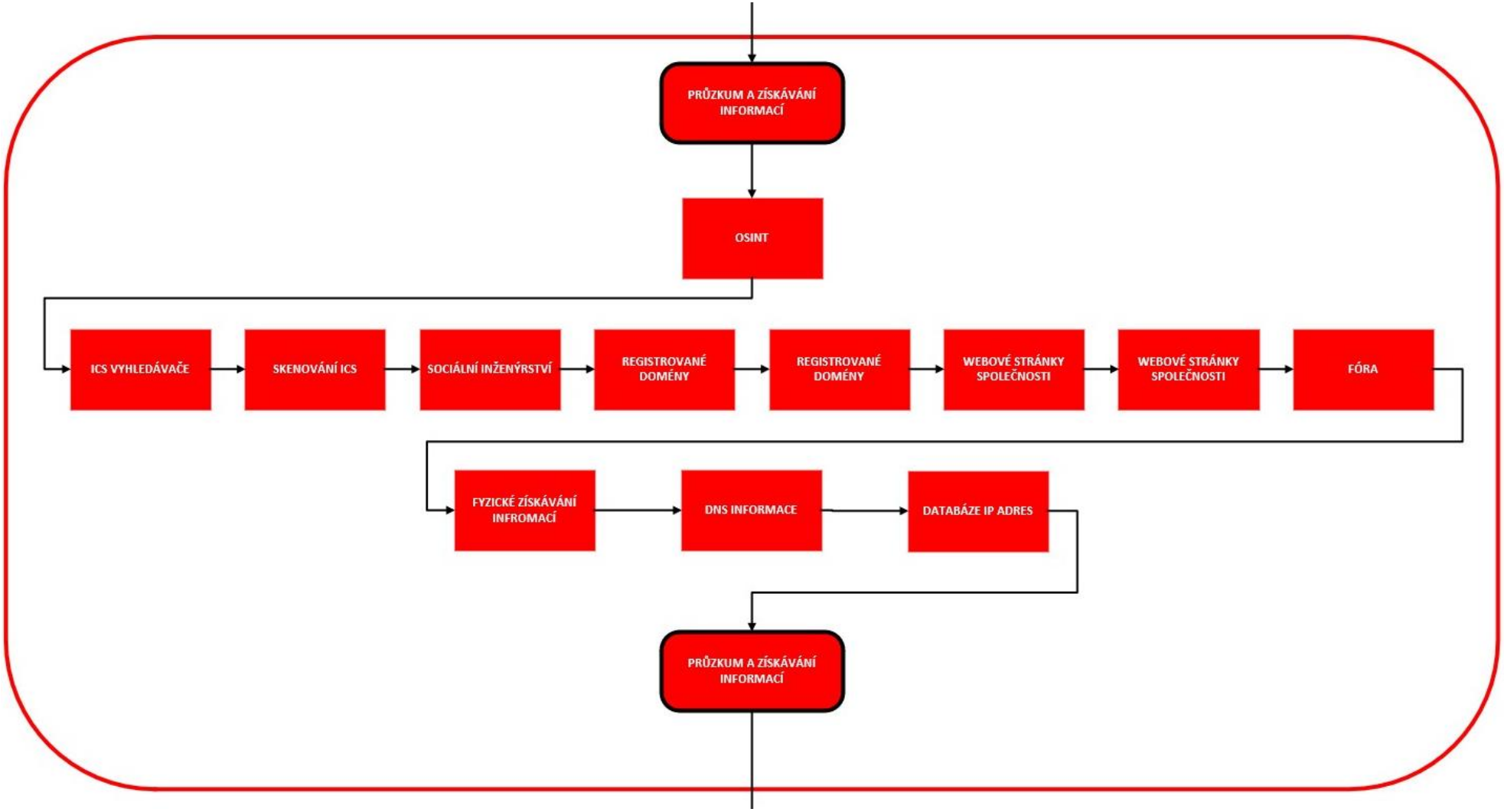
První aktivní částí penetračního testu je průzkum získávání informací. Účelem kapitoly je poskytnutí myšlenkového procesu, návodných rad a postupů pro provádění průzkumu proti stanovenému cíli. Při správném využití lze docílit vytvoření vysoce strategického plánu. Rozsah penetračního testu je ovšem určujícím parametrem pro omezení definovaná časem, úsilím, přístupem k informacím a dalšími. Jedná se o průzkum proti cíli, za účelem získat co nejvíce informací, jenž lze využít během fáze externího testování. Čím více relevantních informací je schopen dodavatel (pentester) získat během této fáze, tím bude možné využít více vektorů útoku ve fázích následujících.

Stěžejním bodem je získávání informací pomocí OSINT (z angl. Open Source Intelligence), což je forma shromažďování zpravodajských informací z veřejně dostupných zdrojů a jejich analýzy za účelem získání použitelných informací. Ty vedou k zjištění vstupních bodů (fyzické, elektronické, lidské) do organizace. Ve většině případů objednatel a jeho zaměstnanci nezohledňuje informace, které o sobě zveřejňují jako stěžejní pro útočníka, v tomto případě dodavatele (pentestera). Navíc je mylné mínění, že OT/ICS systémy jsou izolovaný od okolního prostředí nebo veřejné sítě.

Ve stanovách provádění získávání informací by mělo být na počátku stanoveno:

- Identifikace a cíl
- Limitace
- Délka testu
- Cíl testu

Dovednosti a techniky pro získání informací o ICS se nijak výrazně neliší od jiných penetračních testů a obsahují informace o objednateli, IP rozsahy a URL adresy spojené s cílem. Stěžejním je pro tuto část metoda získávání informací z veřejných zdrojů – OSINT. V rámci průzkumu a získávání informací postupujeme dle Graf 2: PENTICS – Průzkum a získávání informací.

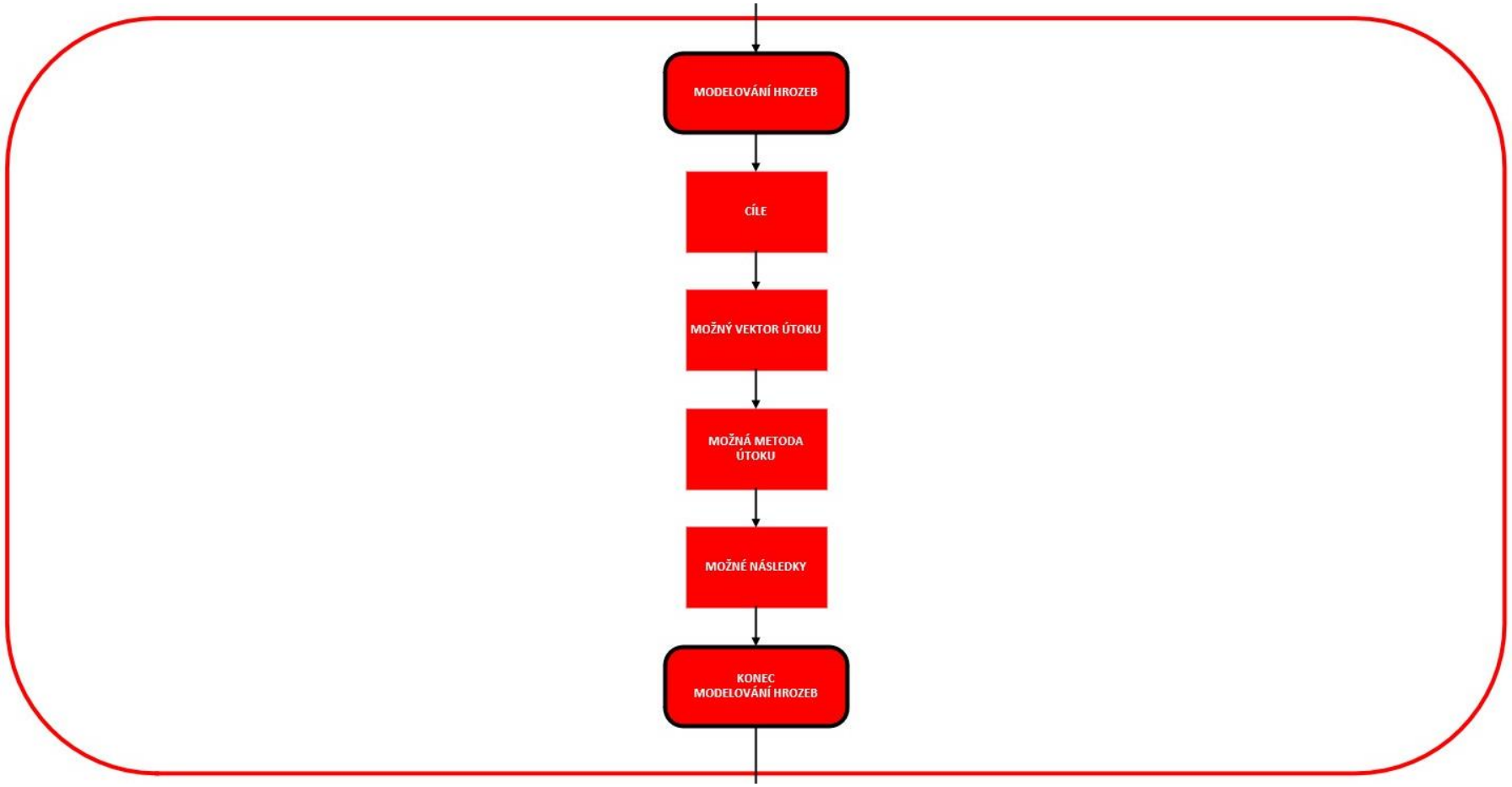


Graf 2: PENTICS – Průzkum a získávání informací (Zdroj: Vlastní zpracování)

3.3 Modelování hrozeb

Tato část definuje přístup k modelování hrozeb, který je vyžadován pro správné provedení penetračního testování. Není zde použit konkrétní model, ale je vyžadováno, aby byl použitý model konzistentní a v průběhu času se neměnil, v případě reprezentace hrozeb, jejich schopnosti, kvalifikace a organizace. A to především z důvodu možnosti opakovaného použití při budoucím testu se stejnými výstupy a možností porovnání.

Metodika se zaměřuje na modelování hrozeb z pohledu možnosti napadení cíle v průmyslovém prostředí. V rámci tabulky *Tabulka 5: Modelování hrozeb ICS* byly shrnuty nejčastější cíle s možným vektorem útoku, metodou daného útoku a možnými následky. Díky tomu je možné lépe prezentovat možná rizika a velikost daného rizika v případě kompromitace. Tabulka slouží jako vzor pro vstupní data na úrovni doplňkového modelu. V rámci Modelování hrozeb postupujeme dle Graf 3: PENTICS – Modelování hrozeb.



Graf 3: PENTICS – Modelování hrozeb (Zdroj: Vlastní zpracování)

3.4 Externí testování

Externí penetrační testování je hodnocení bezpečnosti perimetru objednatele. Prvním cílem externího testování je nalezení způsobu, jak daný perimetr kompromitovat a získat tak přístup do interní sítě. Část tohoto testování by měla být plně řízena mezi dodavatel a objednatelem řešení. Dodavatel musí komunikovat s objednatelem ve stanoveném rozsahu. Minimálně však při následujících třech milnících:

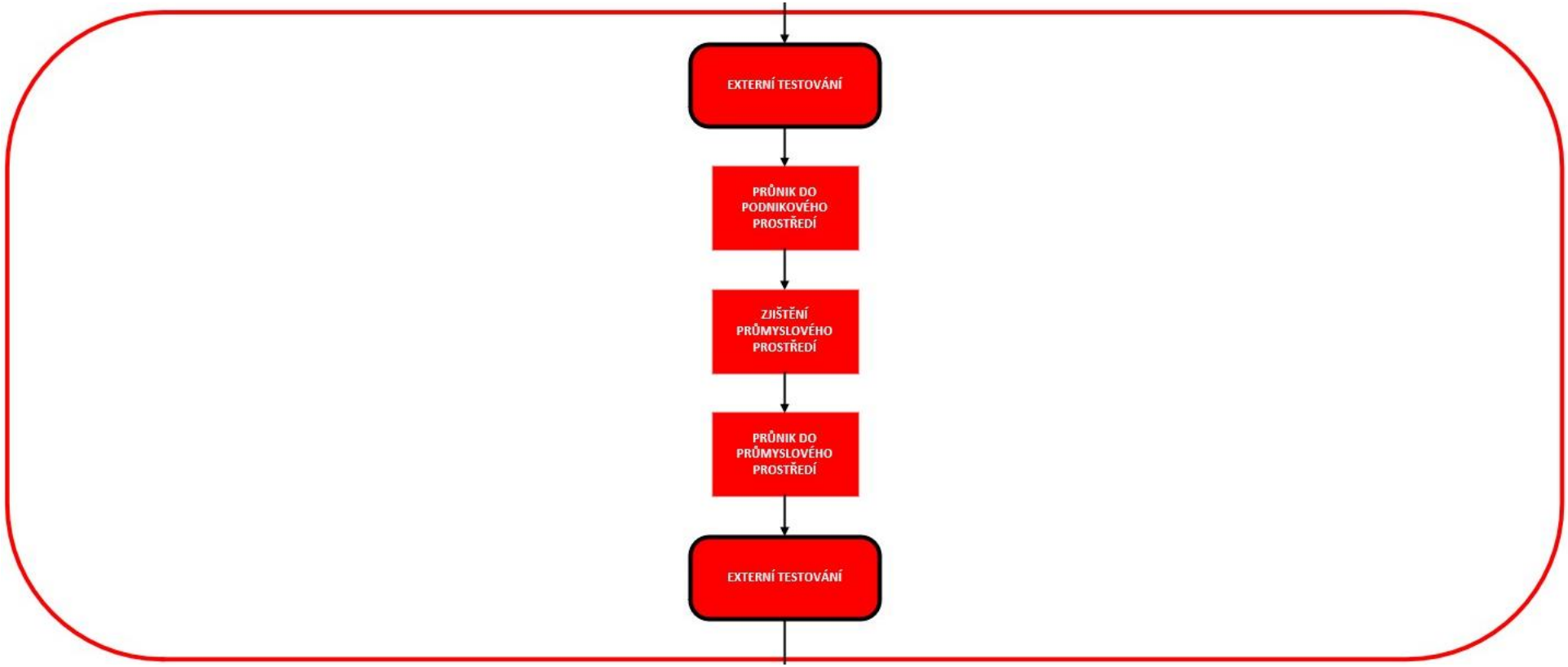
1. Průnik do podnikové sítě
2. Zjištění průmyslové sítě
3. Průnik do průmyslové sítě

V případě úspěšného naplnění třetího milníku, průnik do průmyslové sítě, dochází k ukončení části externího testování a přechází se na část interního testování. Při využívání metod fyzického průniku do prostředí je stanoven příznak určující úspěšné naplnění dílčích milníků následovně:

1. Průnik do podnikového prostředí
2. Zjištění průmyslového prostředí
3. Průnik do průmyslového prostředí

Pozn.: Průmyslovým prostředím je prostředí umožňující manipulaci s průmyslovými řídícími systémy. Nikoli obecné fyzické prostředí určené pro výrobu.

V rámci průzkumu a získávání informací postupujeme dle Graf 4: PENTICS – Externí testování.

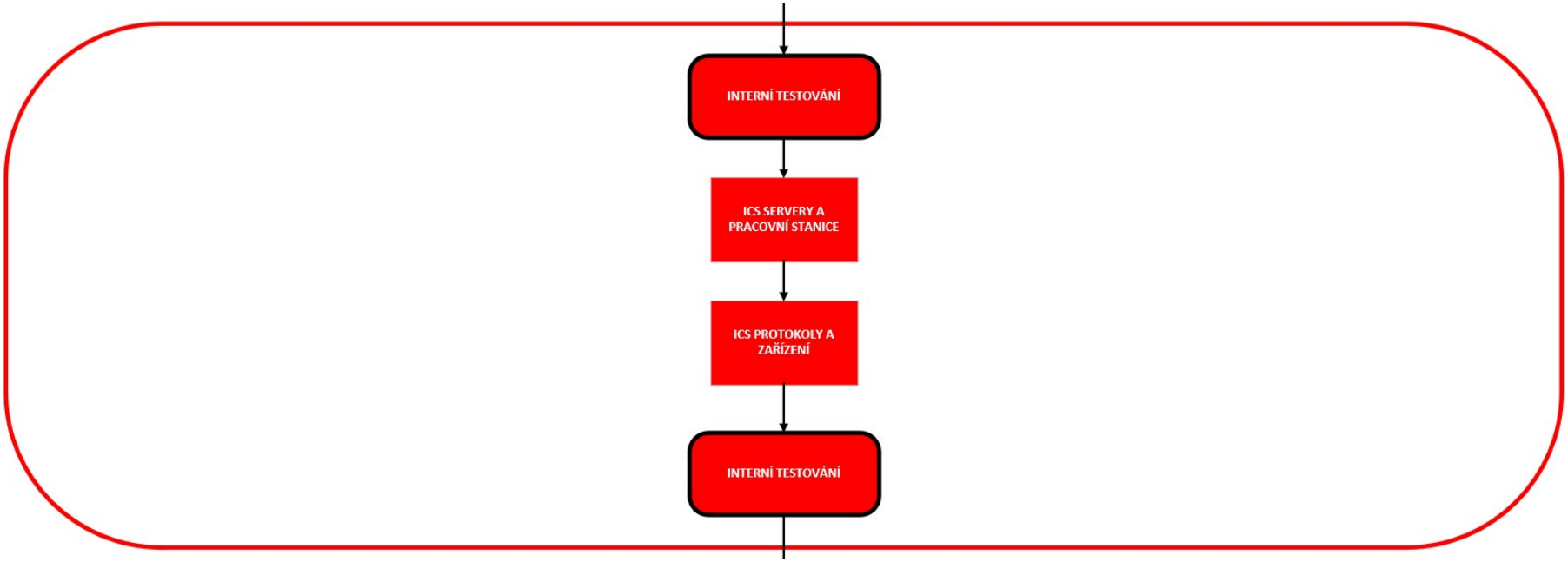


Graf 4: PENTICS – Externí testování (Zdroj: Vlastní zpracování)

3.5 Interní testování

Interní penetrační testování je proces probíhající za neustálé spolupráce dodavatele a objednatelem penetračního testu. Průběh testu je po celou dobu diskutován a umožňuje tak bezpečné dosažení cíle. Testování probíhá výhradně fyzicky na lokalitě. Dále je pro tuto sekci objednatel omezován v rámci používání a způsobu používání penetračních nástrojů na rozsah neohrožující zdraví osob a majetku objednatele, a to dle referenční koncepce úrovňového testování. Tato část testování se doporučuje provádět na virtualizovaném prostředí, umožňující tak využití celého spektra metod testování průmyslových řídících systémů. Proces interního testování se dělí na testování ICS serverů/pracovních stanic a ICS protokoly/zařízení.

V rámci Interního testování postupujeme dle Graf 4: PENTICS – Interní testování.

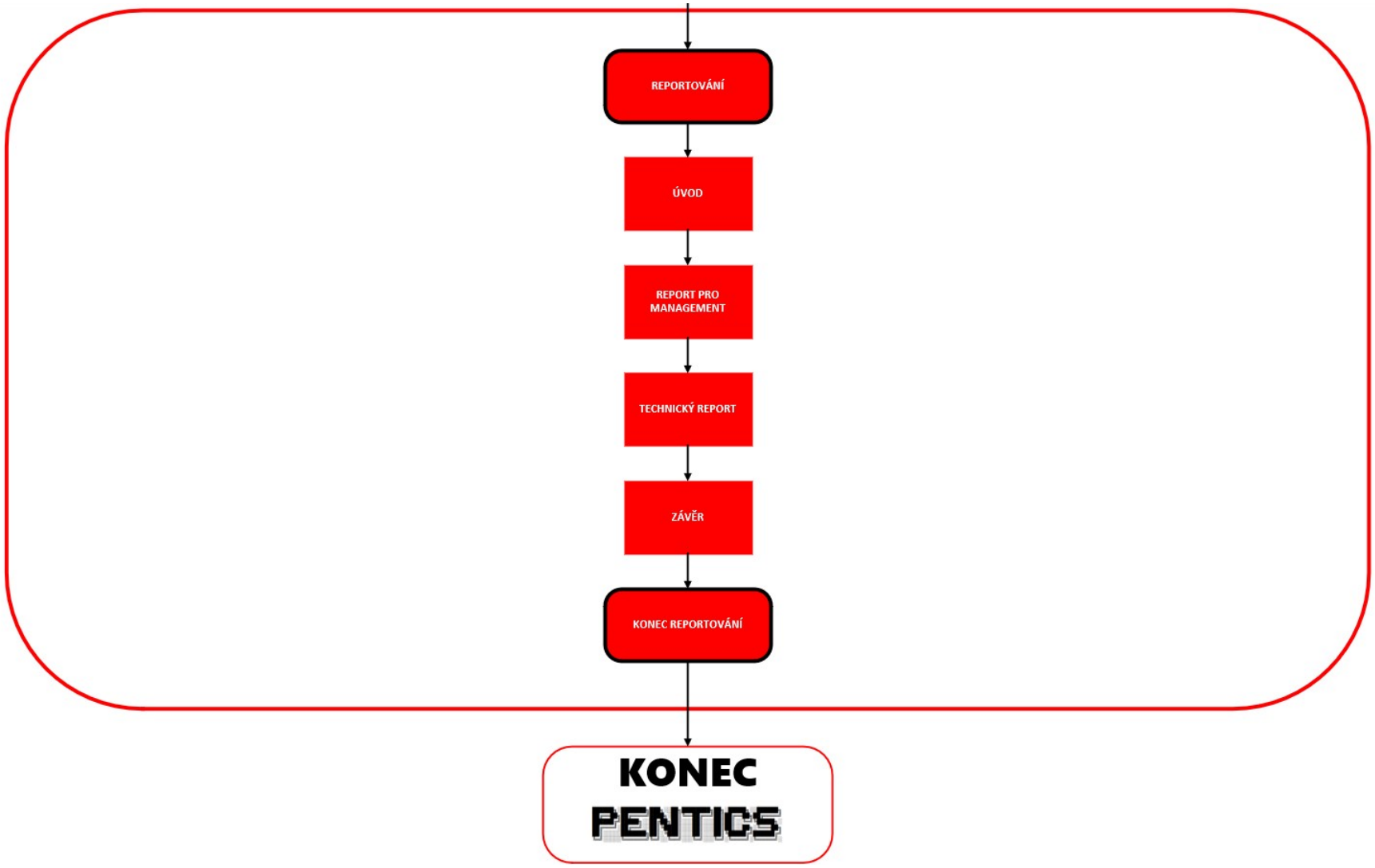


Graf 5: PENTICS – Interní testování (Zdroj: Vlastní zpracování)

3.6 Reportování

Tato část dokumentu definuje základní kritéria pro reportování výsledků penetračního testování. Reportování obsahuje dvě základní části specificky zaměřené na předložení výsledků managmentu objednatele a část popisující technické aspekty prováděného testování vedoucí k pochopení celkového postupu prováděného dodavatelem. Report slouží také jako důkaz dodavatele o provedení testu u objednatele. Sken zranitelností nelze považovat jako plnohodnotný report sloužící k předání informací objednateli. Dále je doporučeno na počátku stanovit tabulku revizí a distribučního listu.

V rámci reportování postupujeme dle Graf 5: PENTICS – Reportování.



Graf 6: PENTICS – Reportování (Zdroj: Vlastní zpracování)

3.7 Ekonomické zhodnocení a přínos práce

V rámci návrhové části, která je obsažena v samostatném dokumentu PENTICS, jsem vytvořil z aktuálně dostupných dat nejspíše první mezioborovou metodiku penetračního testování se zaměřením na průmyslové řídící systémy.

Abychom si samotný přínos diplomové práce mohli uvědomit, je nejdříve nutné vyčíslit hodnotu diplomové práce z hlediska jejího vzniku, tedy nákladů na tvorbu. Na metodice PENTICS bylo při její tvorbě stráveno 80 hodin práce. Přičemž sazbu za člověkoden jsem stanovil na 8 000 Kč, tedy 1000 Kč/hod při standardním přepočtu. Výsledná cena práce na metodice dosahuje 80 000 Kč. Vybavení potřebné pro provedení testu má hodnotu 450 000 Kč. Náklady spojené s provedením testu by měly vždy zahrnovat alespoň účel a rozsah testování, počet IP adres, úroveň dovedností penetračního testera, velikost společnosti, oblast podnikání nebo fyzickou lokaci, kde se test bude odehrávat. Vzhledem ke specifičnosti prostředí je cena takového testu v rozmezí 500 000 Kč až 5 000 000 Kč. Odůvodnit cenu si můžeme pomocí modelu ROSI. Zkratka ROSI vychází z anglického Return on Security Investment, tedy Návratnost investic do zabezpečení. Náhodná společnost může zvažovat investici do provedení pravidelného penetračního testu na roční bázi. V průběhu roku se setkala se 3 útoky na průmyslové řídící systémy (ARO – roční míra výskytu). Každý útok stál společnost zhruba 2 400 000 Kč v datech a produktivitě (SLE – očekávaná jednorázová ztráta). Za rok tedy celkem 7 200 000 Kč (ALE – očekávaná roční ztráta). Provedením penetračního testu se předpokládá zabránění 80 % útoků (MR – míra zmírnění). Náklady na provedení testu jsou 1 500 000 Kč (C – náklady). Na základě modelu ROSI, který vyšel ROSI = 284 %, se jeví volba pravidelného testování jako nákladově efektivní řešení. Náklady kybernetického incidentu při útoku na ICS totiž zahrnují drastické snížení produktivity, ztrátu dat, obavy z prostojů, pokuty, vysoké náklady na nápravu a vliv na společnost. Narušení SAIC triády není dobré brát na lehkou váhu a všechny aspekty je potřebné vždy zvážit.

Hlavním přínosem zpracované metodiky PENTICS je na prvním místě jednoznačně bezpečnost. Zabezpečení zdraví, osob a majetku společnosti, která bude chtít penetrační test dle metodiky provádět. Historicky nastalo již mnoho případů, kdy při neproprietárním testování průmyslových řídících systémů došlo nejen ke škodám na majetku, ale také na zdraví osob. Metodika PENTICS nezajišťuje stoprocentní bezpečnost při průběhu testu, ovšem zajišťuje řízený proces, který aproximuje celou hodnotu nebezpečí téměř k nule. Jednotlivé části má objednatel řešení možnost modifikovat, s čímž ovšem přijímá riziko na svoji stranu. V rámci metodiky byl navíc stanoven nový úrovňový koncept testování, který celému procesu ještě více napomáhá.

Bezpečnostní přínos se nevztahuje pouze na proces testování, ale také na společnost jako celek. Mnoho jednotlivců si neuvědomuje skutečnost, že průmyslové řídící systémy ovládají svět. Ať se jedná o semafory, automatizační linky nebo elektrárny. Výpadek takového systému může znamenat stav ohrožení. Díky metodice lze bezpečně odhalit reálně zneužitelné zranitelnosti, odhalit špatné konfigurace, ověřit skutečnost, že systém je efektivně a účelně zabezpečen nebo pomoci s dokončením dokumentace. Metodika tak přispívá celkovému zlepšení úrovně provádění testů se zaměřením na průmyslové řídící systémy.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout mezioborové řešení metodiky penetračního testování průmyslových řídících systémů podle které by se mohly subjekty v daných odvětvích orientovat a řídit. S růstem útoků na operační technologie budou nároky na jejich zabezpečení růst a tím pádem se bude zvyšovat i tlak na jejich testování, které je potřebné řídit dle specifik odvětví.

Pro vytvoření metodiky samotné je nutné vymezit teoretické základy, o nějž se lze opřít. V rámci širšího kontextu byly popsány aktuální legislativa, normalizační instituce nebo subjekty, které se v rámci České republiky zaobírají bezpečností z hlediska informační a/nebo kybernetické bezpečnosti. Pro pochopení problematiky je vysvětlen také teoretický základ operačních technologií, průmyslových sítí nebo penetračního testování. Nelze opomenout rozdíl mezi operačními a informačními technologiemi, jelikož se jedná o primární důvod vytváření této metodiky.

V rámci analýzy současného stavu došlo k zamření na pokrytí penetračního testování z hlediska zákona, standardů a certifikací. Je zde také odůvodněna tvorba nové metodiky, problémy se zabezpečením ICS. V rámci diplomové práce byla provedena šetření, která dala podklad pro vytvoření tří případových studií poukazující na problematiku z reálného světa. Tyto případové studie mají poukázat na jednoduchost možnosti provedení útoku. Analyzovány jsou i toky historické. Závěrem je analyzována problematika testování ICS a vhodné nástroje.

Samotné navrhované řešení je poté definováno v příloze, kde je samotná metodika s názvem PENTICS. Ta se dělí do pěti částí, které řeší proces penetračního testování od prvního setkání zainteresovaných subjektů až po konečné reportování. Jednotlivé části jsou popsány a definovány do takové hloubky, kdy je možné je mezioborově využit. Metodika nemá za cíl vytvořit pracovní postup penetračního testování.

Na základě vydefinovaných cílů práce došlo k jejich splnění. Metodika PENTICS poskytuje ucelenou oporu pro zainteresované subjekty mezioborových řešení. V budoucnu dojde k jejímu rozvoji na úrovni oborových řešení.

SEZNAM POUŽITÝCH ZDROJŮ

(1) Aktuální legislativa. Národní centrum kybernetické bezpečnosti [online]. [cit. 2021-09-20]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

(2) Povinné osoby. Národní centrum kybernetické bezpečnosti [online]. [cit. 2021-09-20]. Dostupné z: *https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/povinne-osoby/*

(3) ONDRÁK Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

(4) SEDLÁK, P. Management průmyslových řešení. [přednáška]. Brno: VUT, Fakulta podnikatelská, 2021.

(5) JORDÁN Vilém a Viktor ONDRÁK. INFRASTRUKTURA KOMUNIKAČNÍCH SYSTÉMŮ II. Kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-2145-240-4.

(6) JORDÁN Vilém a Viktor ONDRÁK. INFRASTRUKTURA KOMUNIKAČNÍCH SYSTÉMŮ III. Integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-2145-241-1.

(7) SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

(8) NBÚ: O nás [online]. [cit. 2022-05-01]. Dostupné z: *https://www.nbu.cz/cs/o-nas/955-o-nas/*

(9) CSIRT: O nás [online]. [cit. 2022-05-01]. Dostupné z: *https://csirt.cz/cs/o-nas/*

(10) GovCERT: O nás [online]. [cit. 2022-05-01]. Dostupné z: *https://www.govcert.cz/*

(11) NÚKIB: O NÚKIB [online]. [cit. 2022-05-01]. Dostupné z: *https://www.nukib.cz/cs/o-nukib/*

(12) BIS: Kybernetická bezpečnost [online]. [cit. 2022-05-01]. Dostupné z: *https://www.bis.cz/kyberneticka-bezpecnost/*

(13) NCKO: Kybernetická obrana [online]. [cit. 2022-05-01]. Dostupné z: *https://www.vzcr.cz/kyberneticka-obrana-46*

(14) AČR [online]. [cit. 2022-05-01]. Dostupné z: *https://acr.army.cz/*

(15) AČR: CIRC [online]. [cit. 2022-05-01]. Dostupné z: *https://circ.army.cz/*

(16) AČR: Velitelství kybernetických sil a informačních operací [online]. [cit. 2022-05-01]. Dostupné z: *https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/*

(17) CSRC: Operational Technology Security [online]. [cit. 2022-05-01]. Dostupné z: *https://csrc.nist.gov/Projects/operational-technology-security*

(18) What's the Difference Between OT, ICS, SCADA and DCS? [online]. [cit. 2022-05-01]. Dostupné z: *https://csrc.nist.gov/Projects/operational-technology-security*

(19) An Improved CIA Triad: The CIAS Triad [online]. [cit. 2022-05-01]. Dostupné z: *https://and-sanford.medium.com/an-improved-cia-triad-the-cias-triad-6bc17825f1e7*

(20) BODUNGEN, Clint E., Bryan L. SINGER, Aaron SHBEEB, Stephen HILT a Kyle WILHOIT. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. New York: McGraw-Hill Education, 2017. ISBN 978-1-25-958971-3.

(21) ACKERMAN, Pascal. Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Birmingham: Packt Publishing, 2017. ISBN 978-1-78839-515-1.

(22) KNAPP, Eric D. a Joel LANGILL. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. London: Syngress, 2015. ISBN 978-0-12-420114-9.

(23) DCS vs SCADA [online]. [cit. 2022-05-01]. Dostupné z: *https://realpars.com/dcs-vs-scada/*

(24) ICS components [online]. [cit. 2022-05-01]. Dostupné z: https://resources.infosecinstitute.com/topic/ics-components/

(25) OSIsoft PI Vision Demo: Mud Motor Performance [online]. [cit. 2022-05-01]. Dostupné z: *https://www.youtube.com/watch?v=pC-dTFQ1Imw*

(26) ACKERMAN, Pascal. Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment. Second edition. Birmingham: Packt Publishing, 2021. ISBN 978-1-80020-209-2.

(27) Zákon č. 205/2017 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické

bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony ze dne 7. června 2017.

(28) Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat ze dne 21. května 2018.

(29) Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016.

(30) Penetration Testing for ISO 27001 Control A.12.6.1 [online]. [cit. 2022-05-03]. Dostupné z: *https://www.breachlock.com/penetration-testing-for-iso-27001-control-a-12-6-1/*

(31) NIS Directive & NIS Regulations [online]. [cit. 2022-05-03]. Dostupné z: *https://www.redscan.com/services/nis-directive-and-nis-regulations/*

(32) VUT FSI: Plány budov [online]. [cit. 2022-05-03]. Dostupné z: *https://www.fme.vutbr.cz/fakulta/planek/A1/12*

(33) Origin Of Wireless Security: The Marconi Radio Hack Of 1903 [online]. [cit. 2022-05-03]. Dostupné z: *https://hackaday.com/2017/03/02/great-hacks-of-history-the-marconi-radio-hack-1903/*

(34) SAYFAYN, Nabil a Stuart MADNICK. Cybersafety Analysis of the Maroochy Shire Sewage Spill. Cambridge, 2017. Massachusetts Institute of Technology.

(35) Georgia-Russia conflict (2008) [online]. [cit. 2022-05-03]. Dostupné z: *https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008)*

(36) Stuxnet analysis by Langner [online]. [cit. 2022-05-03]. Dostupné z: *https://www.langner.com/stuxnet/*

(37) Stuxnet Malware Analysis Paper [online]. [cit. 2022-05-03]. Dostupné z: *https://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper*

(38) Global Energy Cyberattacks: “Night Dragon” [online]. 2011 [cit. 2022-05-03]. Dostupné z: *https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf*

(39) Shamoon computer virus variant is lead suspect in hack on oil firm Saipem [online]. [cit. 2022-05-03]. Dostupné z: *https://www.reuters.com/article/cyber-shamoon-idUSL1N1YH0QC*

(40) Throwback Attack: How the modest Bowman Avenue Dam became the target of Iranian hackers [online]. [cit. 2022-05-03]. Dostupné z: *https://www.industrialcybersecuritypulse.com/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/*

(41) Dragonfly/Havex Reference Material [online]. [cit. 2022-05-03]. Dostupné z: *https://scadahacker.com/resources/havex.html*

(42) Steel mill in Germany (2014) [online]. [cit. 2022-05-03]. Dostupné z: *https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_(2014)*

(43) Decarbonising the iron and steel industry [online]. [cit. 2022-05-03]. Dostupné z: *https://www.man-es.com/process-industry/applications/iron-steel*

(44) BlackEnergy: Five Things to Know about the Crimeware Turned Cyberwarfare Tool [online]. [cit. 2022-05-03]. Dostupné z: *https://www.hypr.com/blackenergy/*

(45) Group: Dragonfly, Energetic Bear, ... [online]. [cit. 2022-05-03]. Dostupné z: *https://collaborate.mitre.org/attackics/index.php/Group/G0002*

(46) Russian hackers tried to bring down Ukraine's power grid to help the invasion [online]. [cit. 2022-05-03]. Dostupné z: (46) *https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/*

(47) Throwback Attack: Kemuri Water Company attack puts critical infrastructure at risk [online]. [cit. 2022-05-03]. Dostupné z: *https://www.industrialcybersecuritypulse.com/throwback-attack-kemuri-water-company-attack-puts-critical-infrastructure-at-risk/*

(48) Hackers hijacking water treatment plant controls shows how easily civilians could be poisoned [online]. [cit. 2022-05-03]. Dostupné z: *https://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266*

(49) CRASHOVERRIDE: The Malware That Attacks Power Grids [online]. [cit. 2022-05-03]. Dostupné z: https://www.recordedfuture.com/crashoverride-malware-overview/

(50) Satellite cyber attack paralyzes 11GW of German wind turbines [online]. [cit. 2022-05-03]. Dostupné z: *https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/*

(51) SRP Triad -Best for ICS Cyber Security [online]. [cit. 2022-05-03]. Dostupné z: https://www.linkedin.com/pulse/srp-triad-best-ics-cyber-security-daniel-ehrenreich/

(52) HackRF One [online]. [cit. 2022-05-03]. Dostupné z: *https://greatscottgadgets.com/hackrf/one/*

(53) Kali Slide Intro [online]. [cit. 2022-05-03]. Dostupné z: *https://gitlab.com/kalilinux/documentation/graphic-resources/-/blob/master/slide-deck/kali-slide-00-intro.png*

(54) Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit) [online]. [cit. 2022-05-03]. Dostupné z: *https://www.exploit-db.com/exploits/19833*

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

ACL	Access control list
AČR	Armáda České republiky
BIS	Bezpečnostní informační služba
C2	command-and-control
C2	command-and-control
CIA	Důvěrnost – integrita – dostupnost
CIRC	Computer Incident Response Capability
CISSP	Certified Information Systems Security Profesional
DCS	Distribuovaný řídící systém
DMZ	Demilitarizovaná zóna
DoS	Denial of Service
EFI	electromagnetic interference
EWS	Inženýrská stanice
EWS	Inženýrská stanice
FBD	Function Block Diagram
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
IACS	Industrial Automation and Control System
ICS	Průmyslové řídící systémy
IDMZ	Průmyslová demilitarizovaná zóna
IED	Intelligent electronic device
IL	Instruction List
ISSAF	Information Systém Security Assessment Framework
KII	Kritická informační infrastruktura
LD	Ladder Diagram
LoC	Loss of Control
LoV	Lost of View
MitM	Man in the Middle
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NCKO	Národní centrum kybernetických operací

NIST	National Institute of Standards and Technoogy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ONOOÚ	Obecné nařízení o ochraně osobních údajů
OPC	OLE for Process Control
OS	Operační systém
OSINT	Open Source Intelligence
OSSTMM	Open Source Security Testing Methodology Manual
OT	Operační technologie
OWASP	Open Web Appliacation Security Project
PDS	Provozovatel digitální služby
PLC	Programmable Logic Controller
PLR	Programmable Logic Relays
PZS	Provozovatel základní služby
RAT	Remote Access trojan
RPC	Remote Procedure Call
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDLC	Secure Development Lifecycle
SFC	Sequential Function Charts
SkIKS	Skupina informačních a kybernetických sil
SPC	Statical Process Control
SQC	Statical Quality Control
ST	Structured Text
VeKySIO	Velitelství informačních a kybernetických sil
VFD	Variable-frequence drive
VIS	Významný informační systém
VoK	Vyhláška o kybernetické bezpečnosti
VUT	Vysoké učení technické Brno
VZ	Vojenské zpravodajství
ZKB	Zákon o kybernetické bezpečnosti
ZoK	Zákon o kybernetické bezpečnosti

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ