Aplikovaná kybernetická bezpečnost

Bc. Tomáš Hájek

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Tomáš Hájek**
Osobní číslo:	**L21269**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Aplikovaná kybernetická bezpečnost**

Zásady pro vypracování

1. Proveďte rešerši dostupných zdrojů týkající se problematiky kybernetické bezpečnosti ve vztahu k vybranému subjektu.
2. Proveďte analýzu současného stavu kybernetické bezpečnosti vybraného subjektu.
3. Navrhněte opatření pro zlepšení současného stavu kybernetické bezpečnosti vybraného subjektu.
4. Aplikujte navržená opatření a vhodně je prezentujte.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.
2. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
3. SANTOS, Henrique M. D. *Cybersecurity: A Practical Engineering Approach*. Boca Raton: CRC Press, 2022. ISBN 978-0--367-25242-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 28. 4. 2023

Jméno a příjmení studenta: Bc. Tomáš Hájek

.....
podpis studenta

ABSTRAKT

Diplomová práce pojednává o kybernetické bezpečnosti vybrané obchodní společnosti. Teoretická část je zaměřena především na definici kyberprostoru a kybernetické bezpečnosti se zhodnocením aktuálního stavu v České republice. Následuje popis vybraných kybernetických a jiných bezpečnostních hrozeb. Poté je tato část, s ohledem na část praktickou, zakončena popisem chráněných aktiv, včetně popisu jejich zabezpečení právě na úseku kybernetické bezpečnosti. Praktická část obsahuje popis vybrané obchodní společnosti, včetně jejich konkrétních chráněných aktiv. Následuje samotné posouzení kybernetických rizik vybrané společnosti, na které navazuje aplikace konkrétních opatření. Závěrem je prostřednictvím příslušných softwarů vyhodnocena účinnost aplikovaných opatření.

Klíčová slova: kybernetická bezpečnost, chráněná aktiva, posouzení rizik, metoda FMEA, aplikace kybernetických opatření

ABSTRACT

The diploma thesis deals with the cyber security of a selected business company. The theoretical part focuses mainly on the definition of cyberspace and cybersecurity with an assessment of the current state of the art in the Czech Republic. This is followed by a description of selected cyber and other security threats. Then, with regard to the practical part, this part ends with a description of protected assets, including a description of their security in the field of cyber security. The practical part contains a description of the selected business company, including their specific protected assets. This is followed by the actual cyber risk assessment of the selected company, followed by the application of specific measures. Finally, the effectiveness of the applied measures is evaluated using appropriate softwares.

Keywords: cybersecurity, protected assets, risk assessment, FMEA method, application of cyber measures

Děkuji vedoucímu diplomové práce Ing. Petru Svobodovi, Ph.D., a určenému konzultantovi Ing. Pavlu Valáškovi, kteří mi poskytli věcné rady i podněty a především mi věnovali svůj čas. Poděkování dále patři majiteli společnosti, který mi umožnil provést analýzu jeho informační infrastruktury a po vzájemné domluvě aplikovat z analýzy plynoucí konkrétní opatření. V neposlední řadě patří poděkování i mému zaměstnavateli.

Závěrem chci poděkovat všem členům své rodiny, kteří mi během studia poskytli podporu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Ze statistik Policie České republiky a několika posledních zpráv o stavu kybernetické bezpečnosti České republiky jasně vyplývá, že kybernetické útoky a obecně kriminalita páchaná v kyberprostoru mají vzrůstající tendenci. Tento trend v kombinaci se zkušenostmi autora diplomové práce v oblasti správy informačních technologií byl jednoznačným důvodem výběru tohoto tématu diplomové práce.

Cílem samotné diplomové práce, respektive jejího autora, je vhodně prezentovat problematiku kybernetické bezpečnosti vybrané obchodní společnosti, včetně popisu a vyhodnocení účinnosti konkrétních aplikovaných opatření plynoucích z provedené analýzy rizik metodou FMEA.

Teoretická část práce bude rozdělena do tří kapitol. První z nich bude věnována teorii kybernetické bezpečnosti. Konkrétně se bude jednat o definici kyberprostoru a kybernetické bezpečnosti, k níž autor kromě odborných publikací využije i zjištěných závěrů své původní bakalářské práce Kybernetická bezpečnost vybrané obce. Tato kapitola bude následně uzavřena vyhodnocením aktuálního stavu kybernetické bezpečnosti České republiky s ohledem na státem vydané podklady. Cílem druhé kapitoly teoretické části bude popsat konkrétní vybrané kybernetické a jiné bezpečnostní hrozby, mimo jiné s ohledem na poslední platnou Zprávu o stavu kybernetické bezpečnosti České republiky. Naopak cílem nebude, jak je již zřejmé, detailní popis všech současných kybernetických hrozeb. Třetí kapitola definuje vybraná chráněná aktiva v oblasti kybernetické bezpečnosti včetně popisu jejich zabezpečení s ohledem na současné nejmodernější praktiky a doporučení.

Praktická část práce bude stěžejní a z velké části splní výše stanovený cíl autora. Úvodní kapitola popíše vybranou obchodní společnost. Nebude chybět situační nákres areálu, popis a půdorysy budov tvořících tento areál. Na toto naváže popis provozované lokální sítě, včetně koncových prvků ICT. Druhá kapitola praktické části práce splní úlohu identifikace možných kybernetických hrozeb. Ty budou následně ohodnoceny a sestaveny v registr kybernetických hrozeb dané společnosti rozdělený na sedm dílčích úseků. V této kapitole budou vymezeny i úseky možných hrozeb, které nebudou identifikovány, neboť nejsou předmětem cíle diplomové práce. Výše vytvořený registr kybernetických hrozeb následně poslouží jako vstup k analýze a hodnocení rizik metodou FMEA, respektive sedmi dílčích analýz touto metodou. Předposlední kapitola praktické části práce vyčíslí finanční nároky na

aplikaci z analýzy plynoucích opatření. Následně tato kapitola přejde k podrobnému popisu aplikace těchto opatření.

Po aplikaci kybernetických opatření budou vyčísleny reálné, tedy konečné náklady. Závěrem bude vyhodnocena účinnost autorem práce aplikovaných kybernetických opatření. K tomuto vyhodnocení budou využity vybrané softwarové nástroje v podobě desktopových aplikací, vulnerability testů a jiných online nástrojů.

I. TEORETICKÁ ČÁST

1 TEORIE KYBERNETICKÉ BEZPEČNOSTI

Cílem této kapitoly je čtenáři prezentovat problematiku kybernetické bezpečnosti s ohledem na její postavení a současný stav v České republice. Předtím je však nutné definovat pojem kyberprostoru, který představuje stěžejní místo, kde se kybernetická bezpečnost realizuje.

1.1 Kyberprostor

Drtivá většina odborných publikací zabývajících se problematikou kybernetické bezpečnosti a bezpečností obecně, stejně tak jako autorova původní bakalářská práce (2021), úvodem zmiňuje vizionářskou definici kyberprostoru Williama Gibsona. Tu tento americko-kanadský spisovatel uvedl ve svém díle Neuromancer již v roce 1983 a ani zde nesmí tato definice kyberprostoru chybět. Její znění je následující:

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat…“ (Gibson, 1983)

Gibsonův kyberprostor je pak možné dle Jirovského (2007) navštívit přímým propojením lidského mozku s počítačem, přičemž toto propojení představuje jistou fikci. Sám autor diplomové práce k problematice kyberprostoru dříve ve své bakalářské práci (2021) uvedl, že se jedná o:

„Fikci, která nemá žádného vlastníka, neexistují zde žádné hranice, tento svět je volně přístupný, plný informací, bohužel i dezinformací a ve své podstatě tu neplatí žádná pravidla.“ (Hájek, 2021)

Tuto definici pak velmi vhodně doplňuje odborná publikace CyberCrime, kde její autor uvádí, že:

„Kyberprostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném.“ (Kolouch, 2016)

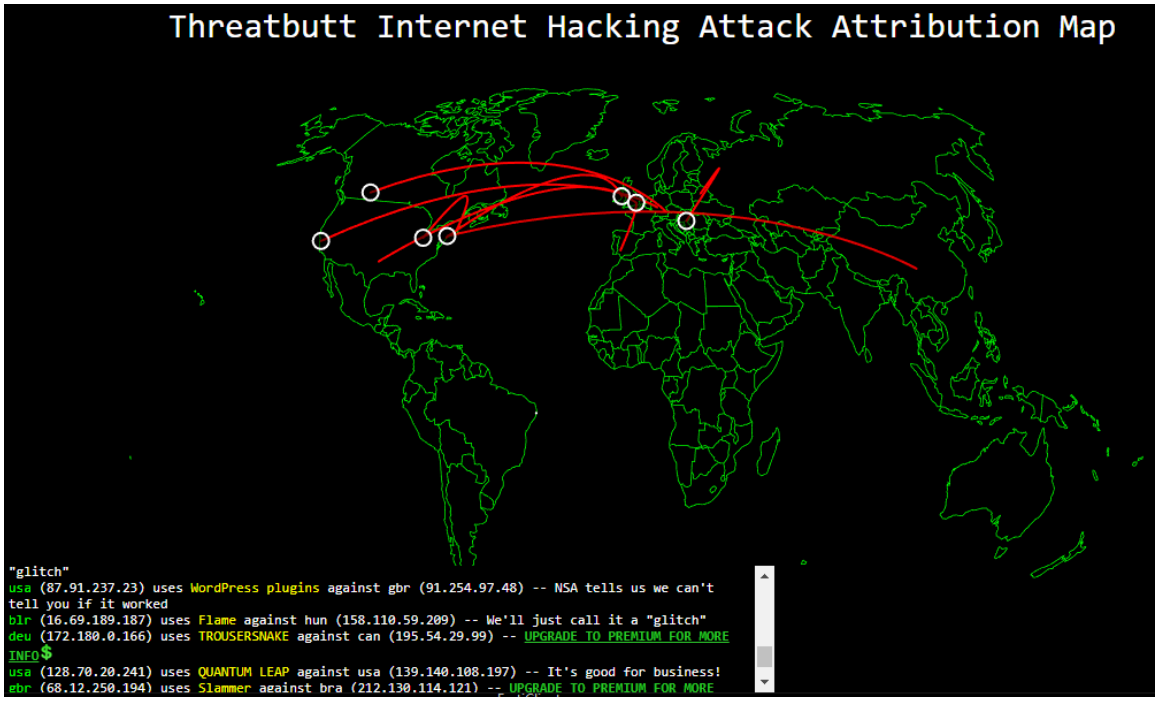
Zde se již odborné publikace rozchází. Některé nejprve definují Internet a definici kyberprostoru k němu pak pouze přirovnají. S tím však autor diplomové práce nesouhlasí a v podstatě nesouhlasil již ve své bakalářské práci (2021). S ohledem na provoz lokálních sítí, které nejsou součástí celosvětové sítě Internet, se nabízí otázka, zda je tedy kyberprostorů několik. Jiné zdroje, zejména ty zahraniční, oproti tomu srovnávají různé

definice napříč mnoha publikacemi a judikaturou. Naštěstí v České republice je od 1. ledna 2015 účinný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Autoři tohoto stěžejní zákona v oblasti kybernetické bezpečnosti pak konkrétně v § 2 přišli s vlastní definicí kyberprostoru v následujícím znění:

„… digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“ (Česko, 2014)

S touto definicí lze bez větších výtek souhlasit. Důležité je však ještě kyberprostor rozdělit na hmotnou a nehmotnou část, což z uvedené zákonné definice nevyplývá. Nehmotnou část lze opět přirovnat k již zmíněné fikci, zatímco hmotnou část tvoří prvky ICT (Hájek, 2021). V kyberprostoru probíhá v reálném čase několik různorodých kybernetických útoků za sekundu. To lze čtenáři prezentovat prostřednictvím obrázků z webových služeb, které neustále monitorují kybernetické útoky v celosvětové síti Internet.

Obrázek 1 Mapa kybernetických útoků v reálném čase (Cyberthreat Real-Time Map, 2021)



Obrázek 2 Mapa internetových hackerských útoků v reálném čase (Threatbutt Internet Hacking Attack Attribution Map, 2023)

Dle autora diplomové práce právě kybernetické útoky z velké části zhmotňují onu fikci. Bez ohledu na to, zda se jedná například o DoS útok či podvodný e-mail, je tato fikce zhmotněna prostřednictvím lidského útočníka a následně škod, které kybernetický útok napáchá na prvcích ICT, lidských obětech či jiných materiálních a finančních statcích. Zde nastupuje na řadu dnes neustále omílaná kybernetická bezpečnost.

1.2 Kybernetická bezpečnost

Již v autorově bakalářské práci (2021) se zdálo logické hledat definici kybernetické bezpečnosti či její východisko v judikatuře. Zde opět nastupuje již zmíněný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zákon č. 205/2017 Sb., 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, případně zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Bohužel tyto stěžejní zákony pojem kybernetické bezpečnosti nedefinují (Hájek, 2021).

Na řadu tedy přicházejí dokumenty vydávané ústředním správním orgánem v oblasti kybernetické bezpečnosti, Národním úřadem pro kybernetickou a informační bezpečnost.

Tento úřad pravidelně vydává několik dokumentů. Za zmínku stojí Zpráva o stavu kybernetické bezpečnosti České republiky a Národní strategie kybernetické bezpečnosti České republiky. Konkrétně Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 definuje kybernetickou bezpečnost takto:

„Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“ (Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, 2015)

K této definici již jednou autor diplomové práce ve své původní bakalářské práci uvedl, že s ní nesouhlasí a jeho stanovisko stále trvá. Důvodem je fakt, že se tato definice vztahuje pouze na území České republiky a zapomíná na prvky ICT, které nejsou součástí výše definovaného kyberprostoru (Hájek, 2021). S ohledem na definici kybernetické bezpečnosti uvedenou ve Výkladovém slovníku kybernetické bezpečnosti v následujícím znění:

„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“ (Jirásek, Novák a Požár, 2013)

lze nesouhlasné stanovisko autora diplomové práce mimo jiné opřít i o odbornou publikaci CyberSecurity. V té její autoři k výše uvedené definici z Výkladového slovníku kybernetické bezpečnosti uvádějí, že:

„Tato definice je relativně přesná, avšak její omezení pouze na kyberprostor může být zavádějící, neboť kybernetickou bezpečnost lze aplikovat i na prvky ICT, které nejsou zapojeny do kyberprostoru…“ (Kolouch, Bašta et al., 2019)

Ve své původní bakalářské práci (2021) autor této diplomové práce k problematice kybernetické bezpečnosti závěrem prezentoval definici kybernetické bezpečnosti z výše zmíněné publikace CyberSecurity. Od té doby prošel další odborné publikace, kdy lze příkladem uvést velmi aktuální publikaci Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru (2021). Autoři této odborné publikace, stejně jako řada jiných, převzali výše citovanou definici kybernetické bezpečnosti z Výkladového slovníku kybernetické bezpečnosti a dále s ní nepracovali.

Nezbývá tedy než opět prezentovat definici z odborné publikace CyberSecurity, ke které autor diplomové práce již ve své bakalářské práci (2021) neměl žádné výhrady. Jeho

stanovisko dosud trvá. Níže uvedenou definici stále považuje za věcnou, úplnou a aktuální (Hájek, 2021).

„Kybernetickou bezpečnost je možné vymezit jako:

- *souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších ICT, aplikací, dat a uživatelů,*
- *schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.*

Kybernetická bezpečnost je realizována jak v rámci kyberprostoru, tak mimo něj.“ (Kolouch, Bašta et al., 2019)

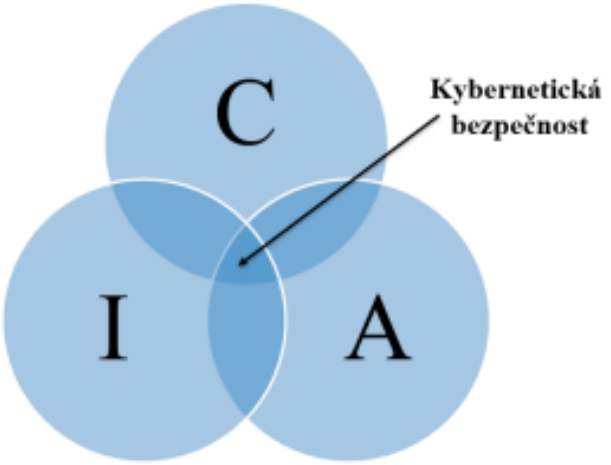
Po uvedení čtenáře do problematiky kybernetické bezpečnosti je nutné dále definovat triády kybernetické bezpečnosti. Těch existuje celá řada a díky nim se kybernetická bezpečnost aplikuje v praxi. Pravděpodobně nejznámější je Triáda CIA, často rozšiřována na model známý jako Parkerian Hexad, nebo lidé, technologie a procesy.

1.2.1 Triáda CIA

Legislativní ukotvení této triády vychází z ustanovení § 5 písm. e) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. V tomto ustanovení se zavádí opatření na ochranu utajovaných informací, přičemž cílem je zajistit jejich důvěrnost, integritu a ochranu (Česko, 2005). Název této triády je pak převzat z počátečních písmen anglického překladu (Confidentiality, Integrity, Availability). Autoři odborných publikací následně k jednotlivým prvkům této triády dodávají:

a) Důvěrnost představuje skutečnost, kdy k chráněným aktivům mohou přistupovat výhradně oprávněné (autorizované) osoby. Příkladem uvádějí klasifikaci informací dle výše zmíněného zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti (Kolouch, Bašta et al., 2019).
b) Integritu (celistvost) pro změnu autoři aktualizovaného Výkladového slovníku kybernetické bezpečnosti (2015) definují jako vlastnost, respektive jistotu, že jsou data původní a nebylo s nimi tedy manipulováno (Jirásek, Novák a Požár, 2015).

c) Dostupnost závěrem znamená *„vlastnost přístupnosti a použitelnosti na žádost oprávněné entity“* (Jirásek, Novák a Požár, 2015).



Obrázek 3 Vztah Triády CIA a kybernetické bezpečnosti (Kolouch, Bašta et al., 2019)

Odborná literatura tuto triádu dále rozšiřuje, neboť ji mnoho autorů považuje v praxi za nedostatečnou. Nejznámější je pak již výše zmíněný model Parkerian Hexad, jehož autor Donn B. Parker rozšířil původní triádu o:

a) držení či získání kontroly nad systémem neoprávněnou osobou,

b) narušení pravosti, kdy se neoprávněné aktivum vydává za oprávněné,

c) užitečnost získaných dat, kdy je nutné brát ohled na zašifrovaná data, která neoprávněná osoba nemůže dešifrovat (Pender-Bey).

Obrázek 4 Parkerian Hexad (Kolouch, Bašta et al., 2019)

1.2.2 Lidé, technologie a procesy

Nejvýznamnějšími prvky kybernetické bezpečnosti jsou lidé. Bohužel právě oni představují v oblasti bezpečnosti ten nejslabší článek, čehož v současné době využívají převážně sociální inženýři (Kolouch, Bašta et al., 2019), neboť jak uvádí Schneier (2000): *„Na stroje útočí jen amatéři; profesionálové se zaměřují na lidi.“*

Druhou oblast pak představují technologie, respektive technologická zařízení (prvky ICT). Tyto prvky poskytují uživatelům služby a v neposlední řadě zajišťují bezpečnost chráněných aktiv. Je nesmírně důležité, aby tato zařízení byla provozována a udržována stále aktuální.

Lidi (uživatele) a technologie závěrem spojují procesy. Ty umožňují oprávněným osobám ony technologie využívat. Příkladem lze uvést hned několik procesů:

a) hardwarová a softwarová aktualizace technologií,

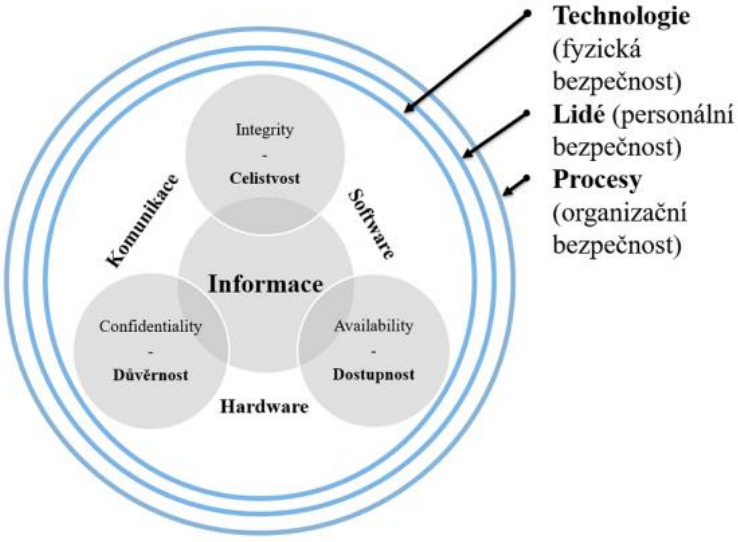
b) správa uživatelských rolí,

c) řízení kybernetických rizik,

d) testování zabezpečení, penetrační testování nebo

e) simulace a reakce na kybernetické a jiné útoky.

Ve vztahu ke kybernetické bezpečnosti je pak velmi důležité, aby každá organizace cílila na kvalitní výběr a systém vzdělávání v oblasti lidských zdrojů, zejména pak administrátorů (Kolouch, Bašta et al., 2019; Sedlák a Konečný, 2021).

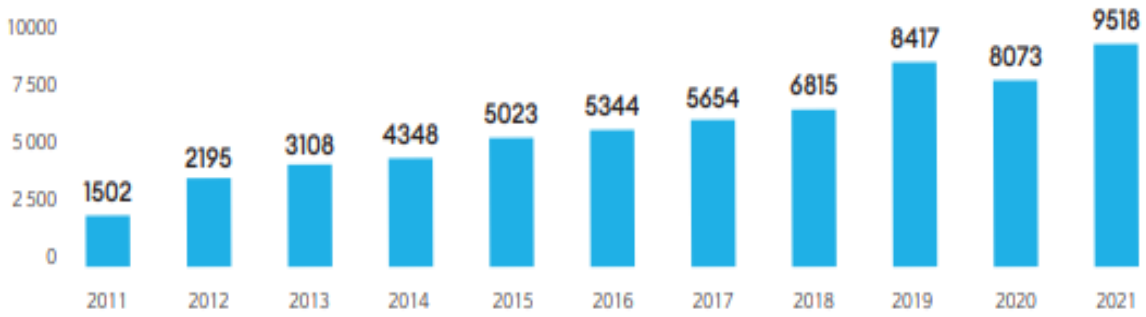


Obrázek 5 Triáda CIA rozšířená o lidi, technologie a procesy (Kolouch, Bašta et al., 2019).

1.3 Aktuální stav kybernetické bezpečnosti v České republice

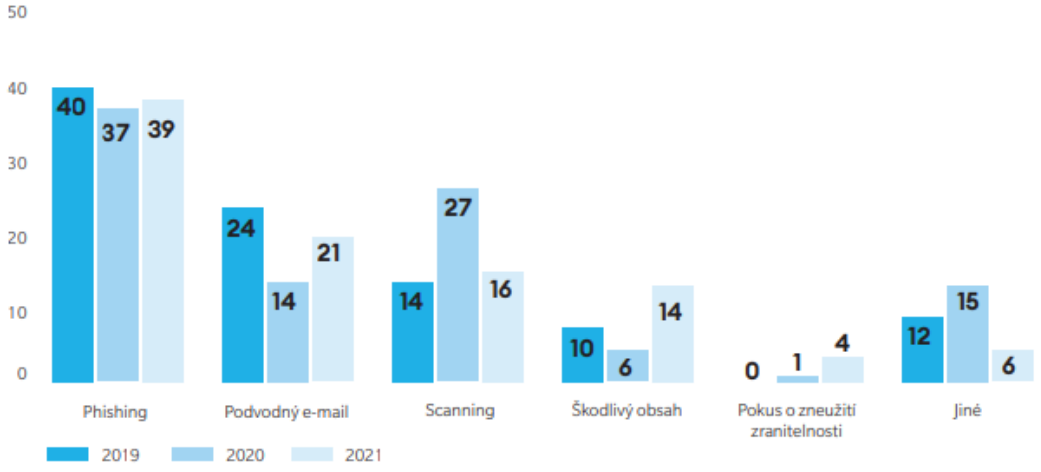
Aktuální stav kybernetické bezpečnosti v České republice je poměrně snadné zhodnotit. Jak již bylo v této kapitole zmíněno. Národní úřad pro kybernetickou a informační bezpečnost pravidelně v měsíci červnu vydává zprávu o stavu kybernetické bezpečnosti České republiky za uplynulý rok. Poslední zpráva o stavu kybernetické bezpečnosti je tedy s ohledem na časový harmonogram tvorby diplomové práce z roku 2021.

Stejně jako Zpráva o stavu kybernetické bezpečnosti České republiky z roku 2020, i ta poslední (2021) uvádí, že počet škodlivých kybernetických aktivit meziročně stoupl a dochází k nim na celém území našeho státu. V roce 2020 se konkrétně jednalo o 468 incidentů, zatímco v roce 2021 jich bylo hlášeno 476. O tomto nárůstu svědčí i statistiky Policie České republiky prezentované ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2021 (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021; Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022).

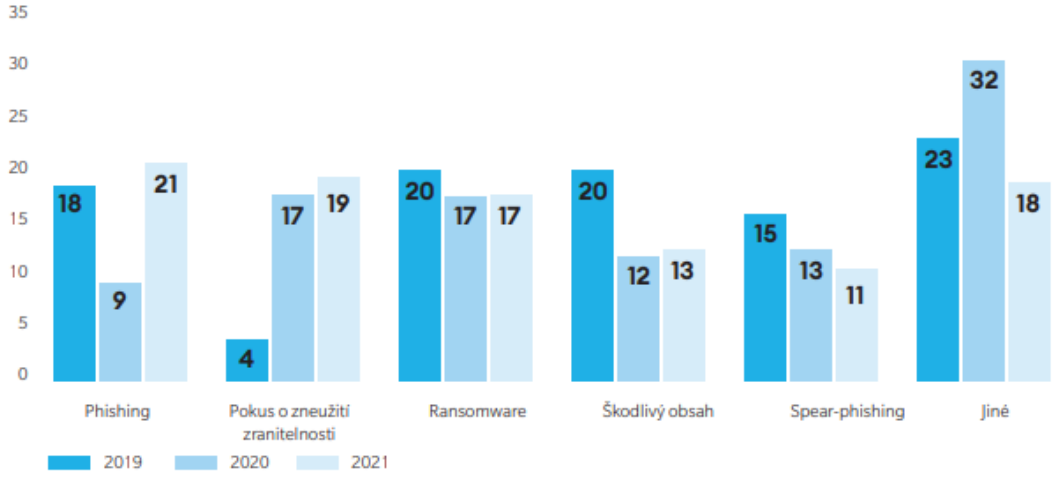


Obrázek 6 Vyšetřované kyberkriminální případy v ČR mezi lety 2011 a 2021 (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)

Z poslední vydané zprávy dále jasně vyplývá, že nejčastějšími typy útoků byly v roce 2021 phishing, podvodné e-maily a scanning (skenování sítí). V předminulém roce (2020) tomuto žebříčku dominoval především spam, opět následovaný phishingem a scanningem. Nejzávažnějším útokem, který zasáhl i české zdravotnictví, byl ransomware (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021; Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022).

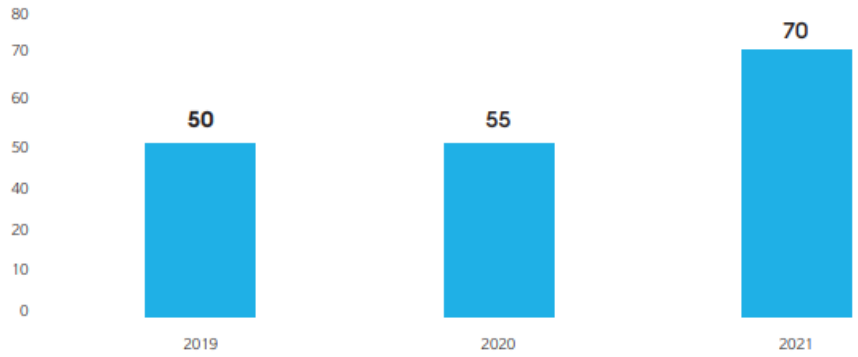


Obrázek 7 Nejčastější typy kybernetických útoků v letech 2019–2021 (%) (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)

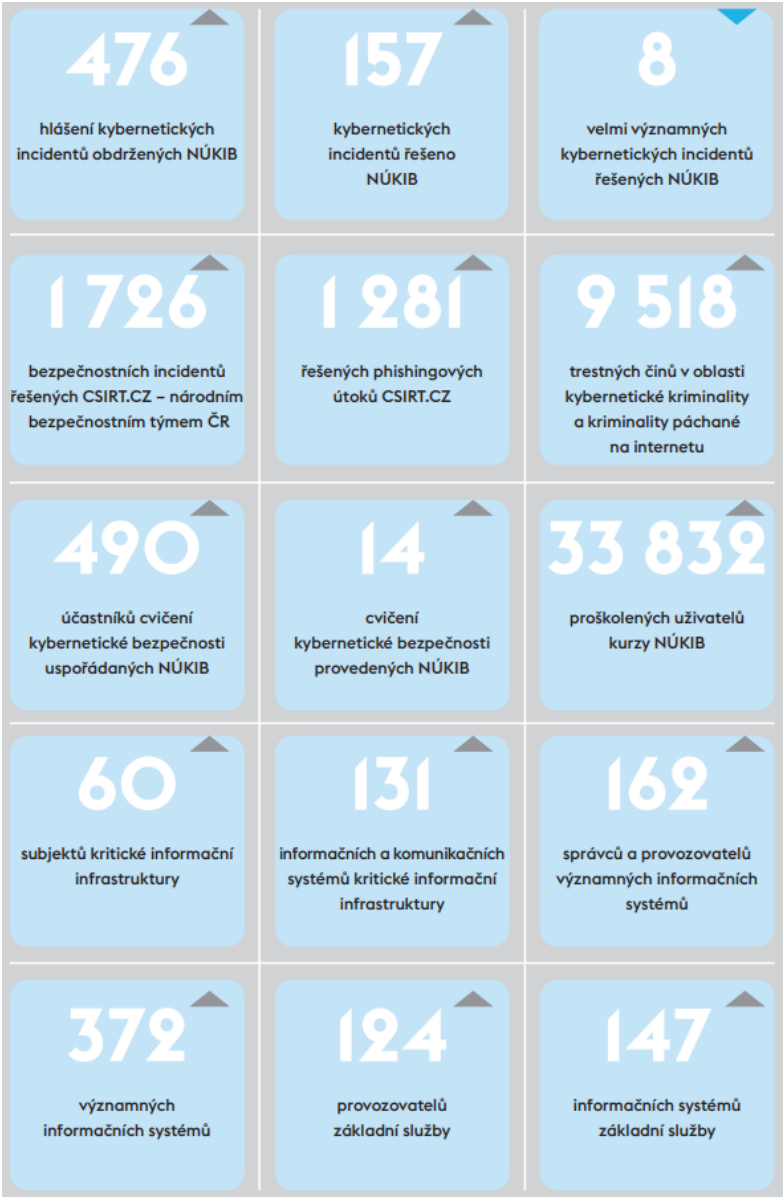


Obrázek 8 Nejzávažnější typy kybernetických útoků v letech 2019–2021 (%) (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)

Cílem kybernetických útoků jsou pak dlouhodobě subjekty kritické infrastruktury (KI) a jejich cílem je narušit výše definovanou Triádu CIA, zejména pak dostupnost veřejných služeb (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022).



Obrázek 9 Podíl kybernetických útoků omezujících dostupnost KI v letech 2019–2021 (%) (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)



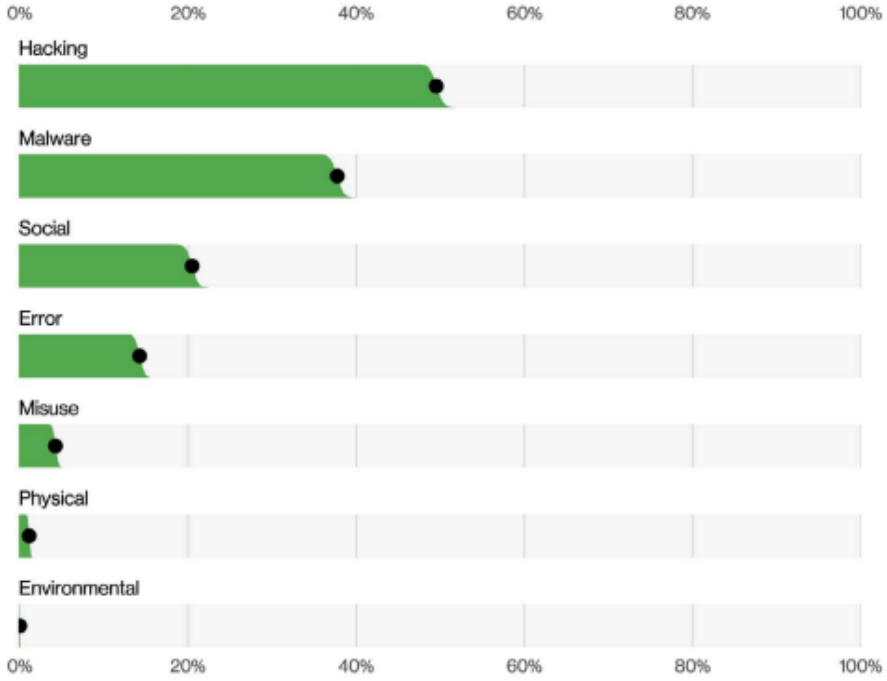
Obrázek 10 Kybernetická bezpečnost ČR za rok 2021 v datech (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)

Dle Sedláka a Konečného (2021) je prostředkem zajištění kybernetické bezpečnosti Národní strategie kybernetické bezpečnosti České republiky na období let 2021 až 2025, která účinně reaguje na současné i budoucí výzvy kyberprostoru. Mimo to pak zavádí Odolnou společnost 4.0, která se především zaměřuje na vzdělávání, osvětu a rozšiřování počtu expertů v oblasti kybernetické bezpečnosti.

2 KYBERNETICKÉ A JINÉ BEZPEČNOSTNÍ HROZBY

Předmětem této kapitoly je popis kybernetických a jiných hrozeb, které v současné době bezprostředně ohrožují chráněná aktiva vybrané obchodní společnosti. To vše s ohledem na praktickou část diplomové práce. Nejedná se tedy o kompletní výčet všech známých kybernetických a jiných hrozeb.

Při samotném výběru konkrétních hrozeb autor diplomové práce zohlednil světové statistiky. Důvodem je, že kyberprostor nezná hranic a v praktické části analyzovaná společnost může být napadena odkudkoli a jakkoli.

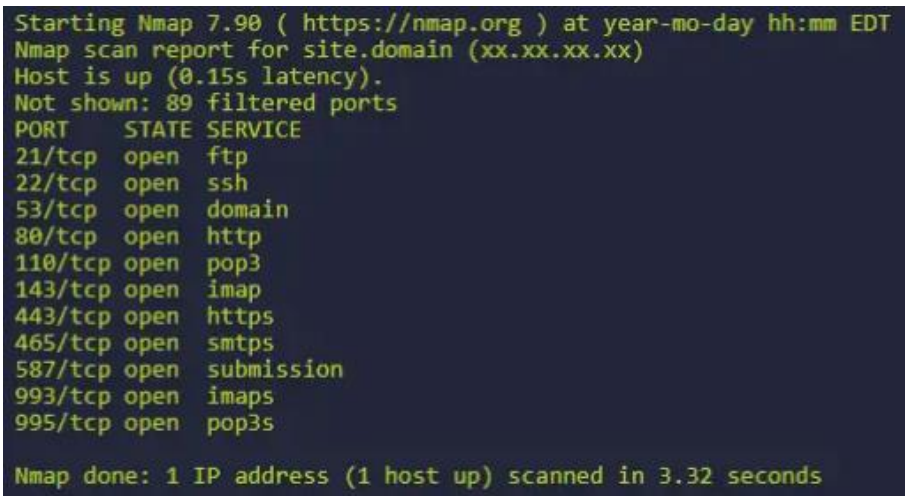


Obrázek 11 Světový podíl konkrétních hrozeb za rok 2022 (Widup et al., 2022)

2.1 Hacking, cracking

Dle Jirovského (2007) byl s příchodem prvních počítačů hackerem označován technicky zdatný jedinec. Následoval rozmach nejrůznějších technologií a začaly se objevovat první hackerské skupiny. Ty zpočátku pouze sdílely konkrétní zjištěná hesla, následně se je však začaly snažit prolamovat a posléze vznikly speciální hackerské nástroje. Jako hacker je v dnešní době chápán zpravidla člověk, který využívá zjištěných zranitelností ke zvýšení bezpečnosti chráněných aktiv a jeho činnost úzce souvisí s penetračním testováním. Oproti tomu cracker využívá těchto bezpečnostních děr k páchání nelegální činnosti, zpravidla za

účelem vlastního obohacení (Sedlák a Konečný, 2021). Zde autor diplomové práce považuje za nutné dodat, že tyto dva pojmy se v praxi rozlišují zcela výjimečně. Příkladem lze uvést českou státní správu, která v oficiálně vydávaných dokumentech zavádí obecný pojem hacktivisté. Ať už čtenář tuto aktivitu nazve jakkoli, důležité je zmínit, že tato není sama o sobě škodlivá. Výhradně zde záleží na tom, k čemu hacktivista zjištěné bezpečnostní nedostatky využije (zneužije). Sám autor diplomové práce používá různý software k analýze síťového provozu (Wireshark, Nmap a další online vulnerability testy) za účelem vyhodnocení aplikovaných bezpečnostních opatření. Výjimkou není ani použití těchto nástrojů v praktické části diplomové práce k onomu vyhodnocení aplikovaných kybernetických opatření.



Obrázek 12 Nmap report (Nmap Online, 2023)

Dlouhodobým monitorováním této problematiky ze strany autora diplomové práce lze dílčím závěrem prezentovat jeho osobní názor: nejúspěšnějšími hackery a bohužel i crackery jsou vývojáři antivirových programů.

2.2 Vybraný malware

Úvodem autor diplomové práce čtenáři zdůrazňuje, že trojský kůň není malware, jak je často v médiích prezentováno. Trojský kůň je pouze způsob, jakým se konkrétní malware infiltruje do chráněného aktiva. Konkrétní způsoby infiltrace malwaru pak lze dle Krále (2015) shrnout takto:

a) trojský kůň,

b) virus,

c) červ (worm) nebo

d) bot a botnet.

Malware jako takový pak lze charakterizovat jako škodlivý program, jehož cílem je získat přístup k citlivým informacím oběti nebo naopak tento přístup znemožnit, například zašifrováním dat (Wilson, 2021). Vzhledem k praktickému zaměření této diplomové práce s důrazem na aplikaci doporučených opatření nepovažuje její autor za podstatné specifikovat konkrétní rozdíly ve výše uvedených způsobech infiltrace malwaru. Níže však popíše vybraný malware s ohledem na nejzávažnější typy kybernetických útoků v letech 2019–2021 uvedené ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2021.

Phishing a spear-phishing

Phishing je (nejenom) metoda podvodných e-mailů v kombinaci s využitím praktik sociálního inženýrství, jejichž cílem je zmást oběť a vylákat z ní, zpravidla citlivé, údaje. V praxi se jedná většinou o uživatelské jméno a heslo do konkrétních informačních systémů, kdy lze příkladem uvést bankovní aplikaci. Samotný podvodný e-mail vypadá velmi věrohodně a odkazuje na podvodné stránky, které od oběti vyžadují zadání zmíněných údajů. Tyto údaje jsou ihned útočníkem zneužity (Král, 2015; Sedlák a Konečný, 2021). Momentálně se drží v popředí techniky vishing a smishing, kdy se útočník snaží z obětí vylákat citlivé údaje prostřednictvím podvodného telefonátu či SMS zprávy.

Spear-phishing je oproti phishingu vyspělejší, tváří se důvěryhodněji a je mnohem těžší ho odhalit. V praxi není zasílán hromadně, ale pouze konkrétní osobě, neobsahuje chyby a je doručen ze známé e-mailové adresy (Šulc, 2018).

Pokus o zneužití zranitelností

Zneužití zranitelností úzce souvisí s backdoor programy, které umožňují útočníkům bez vědomí uživatele přistupovat k chráněným aktivům (Král, 2015). Dle NÚKIB bylo v roce 2021 konkrétně zneužito zranitelností ProxyLogon, ProxyShell a Log4Shell (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022). K těmto zranitelnostem autor diplomové práce dodává, že se v podstatě jedná o bezpečnostní chyby služby Microsoft Exchange zajišťující příjem a odesílání e-mailů.

Ransomware

Výhružky, vydírání či požadování výkupného od zranitelného cíle, tak lze jednoduše charakterizovat tento typ malwaru (Sedlák a Konečný, 2021). Nejčastěji se jedná

o smyšlenou výzvu k zaplacení pokuty nebo obdobného poplatku. V krajním případě se jedná o zašifrování dat na pevném disku, přičemž útočník požaduje finanční odměnu za jejich dešifrování. Samotné dešifrování však nelze zaručit (Král, 2015). Šulc (2018) dále doplňuje, že na chráněná aktiva se tento malware dostává při návštěvě jakéhokoliv webu zobrazujícího reklamu, přičemž největší riziko hrozí OS Windows.

Škodlivý obsah

Škodlivý obsah představuje sám o sobě veškerý malware. Ze zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021 však vyplývá, že její tvůrci škodlivým obsahem měli na mysli konkrétně výše popsaný ransomware a dále dialer a spyware, které k průniku využily metod trojského koně, virusu i červu. Král (2015) pak spyware definuje jako špionážní program sledující činnost oběti za účelem získání přihlašovacích údajů ke konkrétním informačním službám, zatímco dialer v dnešní době přesměrovává vytáčená telefonní čísla na linky s vysokými sazbami.

2.3 Sociální inženýrství a jiné podvodné aktivity

Sociální inženýrství lze obecně charakterizovat jako podvodnou techniku využívající kombinaci jiných podvodných technik, jako je například zmíněný phishing. Santos (2022) k této praktice uvádí, že je přímo zaměřena na organizační procesy a pracovní postupy organizace, čímž přímo cílí na konkrétní uživatele. Wilson (2021) dodává, že 63 % úspěšných kybernetických útoků pochází z interních zdrojů dané organizace, zpravidla nevědomky provedených novými zaměstnanci. Mimo to ve své odborné publikaci popisuje příklad sociálního inženýrství, který tuto techniku dle autora diplomové práce dokonale objasňuje:

Útočník (sociotechnik) zacílí na zaměstnance, který pravidelně vynechává školení na téma kybernetické bezpečnosti. Z falešné e-mailové adresy, vydávající se za IT technika organizace, zašle zaměstnanci odkaz na nutnou „aktualizaci“ systému. Zaměstnanec neznaje tyto praktiky v dobré víře „aktualizaci“ nainstaluje. Tímto způsobem dojde k prolomení první vrstvy (lidé) a škodlivý kód se začne šířit celou interní sítí (Wilson, 2021).

Z příkladu pana Wilsona jasně vyplývá, že sociální inženýři nemají oproti hacktivistům potřebné technické znalosti, pouze manipulují jedním z prvků výše definované triády, lidmi. Závěrem se nabízí uvedení citátu:

„Dějiny sociálního inženýrství jsou dějiny lidské hlouposti a slabin lidského vnímání – vlastností, které jsou po celou historii lidstva dnes a denně zneužívány.“ (Jirovský, 2007)

2.4 SQL injection

Ačkoli ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021 není tento typ útoku známý, autor diplomové práce ho považuje za nutný charakterizovat. Důvodem je praktická analýza organizací provozované webové aplikace, kdy jsou zpracovávaná data ukládána prostřednictvím MS-SQL databáze. Ze strany autora diplomové práce je samotné definování principů SQL injection útoku složité, neboť pochopení této problematiky vyžaduje od čtenáře hlubší znalosti programování, alespoň na úrovní dotazování se do SQL databáze.

Podstatou útoku SQL injection je napadení databázové vrstvy aplikace vložením vlastního kódu do neošetřeného vstupu prezentační vrstvy aplikace (Hranický, 2023). Tyto útoky lze obecně dělit dle více kategorií, což není dále pro účely této diplomové práce podstatné. Pro hlubší pochopení problematiky čtenářem je níže uveden příklad SQL injection útoku:

1) Předpokládejme následující URL adresu odkazující na e-shop s kategorií slevy.

```
https://e-shop.cz/products?category=Slevy
```

Obrázek 13 Původní URL adresa (Hranický, 2023)

2) Prezenční vrstva aplikace odešle databázové vrstvě dotaz v níže uvedeném tvaru.

```
SELECT *
FROM products
WHERE category = 'Slevy'
```

Obrázek 14 Dotaz do SQL databáze (Hranický, 2023)

3) Útočník může URL adresu upravit dle obrázku níže.

```
https://e-shop.cz/products?category=Slevy' UNION SELECT username, password FROM users--
```

Obrázek 15 Pozměněná URL adresa (Hranický, 2023)

4) Databázová vrstva spustí do SQL databáze následující dotaz.

```
SELECT *
FROM products
WHERE category = 'Slevy'
UNION SELECT username, password
FROM users --
```

Obrázek 16 Škodlivý dotaz do SQL databáze (Hranický, 2023)

5) Výsledkem takto upraveného dotazu ze strany útočníka je kromě zobrazení zlevněných produktů i zobrazení všech uživatelských jmen a hesel zákazníků uložených v SQL databázi (Hranický, 2023).

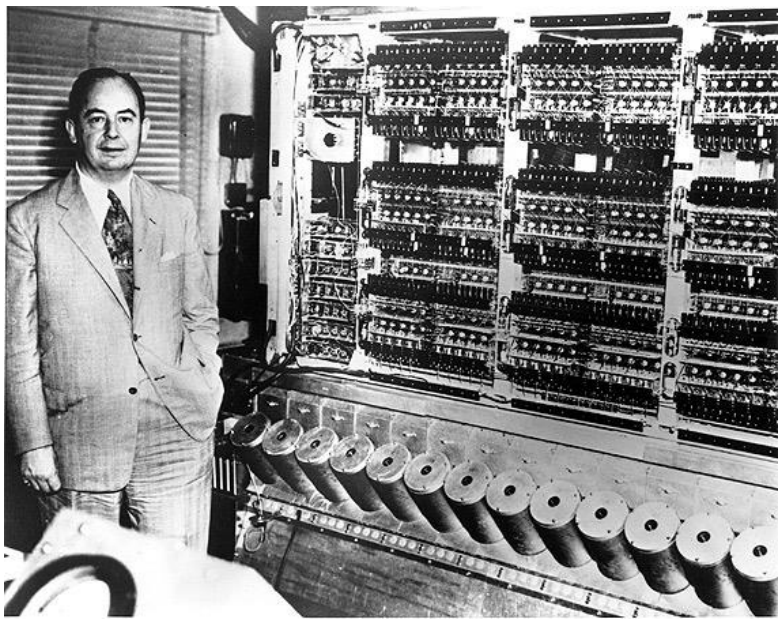
Jak již plyne z příkladu, cílem tohoto útoku je přistoupit k citlivým údajům, které neměly být prezenční vrstvou aplikace vůbec zobrazeny. Výjimkou není útok, který pozmění strukturu databáze, upraví data ve svůj prospěch nebo celou databázi rovnou smaže.

3 CHRÁNĚNÁ AKTIVA A TEORIE JEJICH ZABEZPEČENÍ

Cílem této kapitoly je popsat chráněná aktiva analyzovaná v praktické části diplomové práce. Konkrétně sem patří počítač, rozdělený na hardware a software, počítačová síť, router a firewall, data, databáze a síťová datová uložiště.

3.1 Počítač (pracovní stanice)

Obecné definice počítačů zpravidla mluví o stroji, který je schopen automaticky provádět výpočty. Smejkal (2018) ve své odborné publikaci uvádí, že první pomůckou pro výpočty byl starověký abakus, tj. kuličkové počítadlo. Za vynálezce prvního mechanického počítače je ovšem považován až anglický strojní inženýr Charles Babbage, který na počátku 19. století vytvořil koncept programovatelného počítače (Computer, 2023). Avšak první plnohodnotný počítač navrhl až v roce 1936 Alan Turing, konkrétně ve své seminární práci On Computable Numbers, with an Application to the Entscheidungsproblem. Turing tento stroj nazval Universal Computing Machine a dokázal, že je schopný vypočítat jakoukoli vypočitatelnou sekvenci (Turing, 1936). Následoval rok 1945 a matematik John von Neumann přišel s prvním počítačem (EDVAC), který byl schopen uložit program, čímž položil základy dodnes využívané von Neumannovy architektury (Smejkal, 2018).



Obrázek 17 EDVAC (History of Computers, 2023)

Uplynula řada let a počítače prošly velkou proměnou, která mimo jiné nabízí vysoký výpočetní výkon a malé rozměry. Pro účely této diplomové práce dále postačí dnešní

moderní počítače rozdělit na hardware (technické vybavení) a software (programové vybavení).

Obrázek 18 Dnešní mikropočítač (Raspberry Pi 4 Model B - 8GB RAM, 2023)

3.1.1 Hardware

Bez ohledu na rozměry je každá pracovní stanice sestavena z různých komponent, odborně nazývaných hardware. Tyto komponenty se pak liší v závislosti na druhu pracovní stanice. Mezi ty nejzákladnější druhy patří server, stolní počítač, notebook a dnes velmi oblíbené mikropočítače. Samotné komponenty jsou tvořeny zpravidla ze základní desky, alespoň jednoho procesoru (CPU), pevného disku (HDD, častěji SSD) a operační paměti (RAM). Napájení těchto fyzických součástí zajišťuje napájecí zdroj, o chlazení se nejčastěji starají ventilátory a vše je, s výjimkou mikropočítačů, uloženo v počítačové skříni. Bez těchto základních komponent nemůže dnešní počítač tvořit funkční celek, což nevylučuje osazení základní desky dalšími speciálními kartami (grafická, zvuková, síťová aj.). Samotnou kapitolu představují periferní zařízení, která nemají na počítač provozní vliv. Rozdělit je lze na vstupní a výstupní. Prakticky sem patří monitor, klávesnice, myš, ale i tiskárna nebo reproduktory. Cílem těchto zařízení je zrychlit, případně usnadnit uživateli počítače jeho práci (Smejkal, 2018).

3.1.2 Software

Software představuje programové vybavení počítače, jehož cílem je zabezpečit komunikaci mezi jednotlivými prvky hardware, počítačem samotným a uživatelem (Smejkal, 2018).

Vůbec na nejnižší úrovni tohoto programového vybavení je firmware, v počítači známý jako BIOS, dnes již mnohem častěji rozhraní UEFI. Úkolem tohoto firmware, uloženého ve stálé paměti základní desky, je při startu počítače nakonfigurovat připojený hardware a zavést, respektive spustit operační systém nainstalovaný na pevném disku. Operační systém pak tvoří druhou pomyslnou vrstvu software. Třetí vrstva je tvořena aplikačním software, kam patří veškeré programy umožňující uživateli pracovní stanice vykonávat nějakou činnost. Mezi nejznámější operační systémy patří Windows, MacOS a Linux, kdy v praktické části diplomové práce jsou aplikována opatření pouze na operačním systému Windows. Do aplikačního software lze zařadit textové a tabulkové editory, počítačové hry, antivirové programy nebo programy zajišťující připojení k technologii VPN na straně klienta.

3.1.3 Teorie zabezpečení pracovní stanice

Z praktického pohledu této diplomové práce mají pracovní stanice obrovský význam, neboť z velké části představují chráněná aktiva, na která jsou aplikována opatření plynoucí z provedené analýzy kybernetických rizik. V této podkapitole jsou shrnuty nejdůležitější aspekty zajišťující kybernetickou bezpečnost pracovních stanic s operačním systémem Windows, jejich cílem je samozřejmě zajistit důvěrnost, integritu a dostupnost dat. Na straně často opomíjeného zabezpečení hardware se jmenovitě jedná o:

a) fyzické znepřístupnění pracovní stanice cizím osobám (možnost zaplombovat přístup k hardware),

b) fyzickou ochranu pracovní stanice před prachem, vlhkem, otřesy aj.,

c) pravidelnou fyzickou kontrolu a čištění hardware,

d) využívání pouze certifikovaného hardware,

e) aplikaci hardwarového šifrování.

Na straně software je pak důležité zajistit:

a) heslem chráněný vstup do BIOS/UEFI,

b) aktivní funkci Secure Boot,

c) deaktivovanou možnost bootovat z externích zařízení,

d) aktivní nástroj (službu) BitLocker a

e) nainstalovaný antivirový program s aktivním firewallem.

Nejdůležitější je pak zajistit uživatelem pracovní stanice:

a) používání pouze legálního software,

b) pravidelné aktualizování firmware, operačního systému a aplikací,

c) zabezpečení uživatelských účtů silnými hesly,

d) běžnou činnost vykonávat prostřednictvím uživatelských účtů ve skupině users,

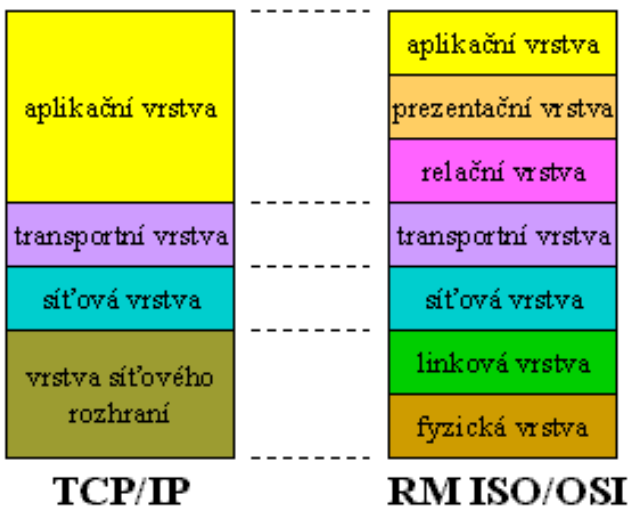
e) používání bezpečných komunikačních protokolů HTTPS a SSH v kombinaci s VPN,

f) pravidelnou zálohu dat a

g) maximální opatrnost a obezřetnost (Anon, 2018; Kopecký, 2019).

3.2 Počítačová síť

Počítačovou síť lze definovat jako spojení alespoň dvou pracovních stanic, které mezi sebou navážou vzájemnou komunikaci. V praxi se nejedná pouze o pracovní stanice, ale o jakákoli zařízení podporující sadu protokolů TCP/IP (Transmission Control Protocol/Internet Protocol). Počítačová síť pak představuje soubor technických a softwarových prostředků, které zprostředkovávají výměnu informací mezi výše popsanými zařízeními (Smejkal, 2018). Samotná architektura TCP/IP je členěna do čtyř vrstev, které jsou znázorněny na obrázku níže včetně porovnání s referenčním komunikačním modelem ISO/OSI.



Obrázek 19 Architektura TCP/IP (Peterka, 2015)

Pro účely této diplomové práce postačí dále doplnit, že vzájemná komunikace síťových zařízení mezi jednotlivými vrstvami probíhá shora dolů. Aplikační vrstva, která je přímo

využívána aplikacemi (protokoly HTTP, SMTP, FTP a další), na základě žádosti o spojení s jiným síťovým zařízením zašle požadavek ke spojení transportní vrstvě. Transportní vrstva pak prostřednictvím síťové vrstvy zajistí samotný spolehlivý přenos dat vzdálenému zařízení v síti, včetně kontroly jeho doručení (Horák, 2003; Endorf, Schultz a Mellander, 2005). Výhodou protokolu TCP/IP je jeho implementace ve všech operačních systémech a díky tomu je využíván k vzájemné komunikaci zařízení v nejznámější celosvětové síti Internet (Smejkal, 2018). Nevýhodou je využívání jeho slabin k provádění kybernetických útoků. To je zapříčiněno faktem, že v době vzniku tohoto protokolu (1983) nekladli jeho tvůrci dostatečný důraz na bezpečnost. Nepředpokládali totiž tak masivní rozšíření Internetu (Jirovský, 2007).

Aby vzájemná komunikace mezi jednotlivými síťovými zařízeními mohla probíhat, musí být tato zařízení v síti jednoznačně identifikovatelná. K tomu slouží IP adresa (IPv4, IPv6). Bohužel mnoho odborných publikací pojednávajících o počítačových sítí tvrdí, že IP adresa musí být v síti jedinečná. Z toho může čtenář usoudit, že každé zařízení v Internetu má unikátní IP adresu. To ovšem s ohledem na rozlehlost této sítě a omezený počet IP adres není pravda (IPv4 již byly vyčerpány, jejich celkový počet je přes 4 mld.).

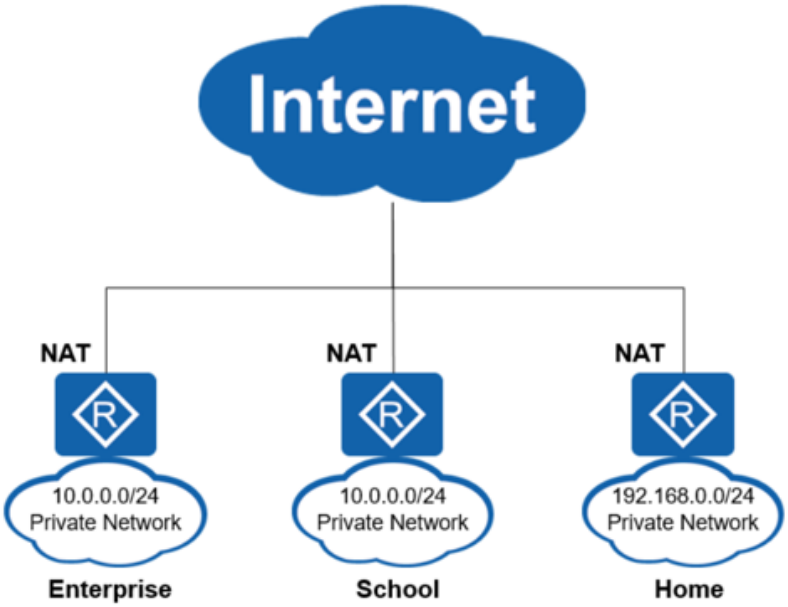
V praxi se tento problém obchází přepisem zdrojové nebo cílové IP adresy, respektive skrytím celé lokální sítě za jednu IP adresu. K tomu je využíván NAT (Network Address Translation). Podmínka jedinečnosti IP adresy pak samozřejmě musí platit jen na úrovni lokální sítě, ale nikoli v rámci celého Internetu. NAT je dnes zpravidla implementován ve firmware každého routeru a z hlediska bezpečnosti nabízí jasné výhody:

a) útočník nezná strukturu lokální sítě,

b) nemůže navázat spojení s konkrétní pracovní stanicí a

c) je schopen odpovídat jen na výzvy z lokální sítě.

V praxi však tyto výhody neznamenají, že jsou uživatelé lokální sítě chráněni před kybernetickými útoky (Krčmář, 2007).

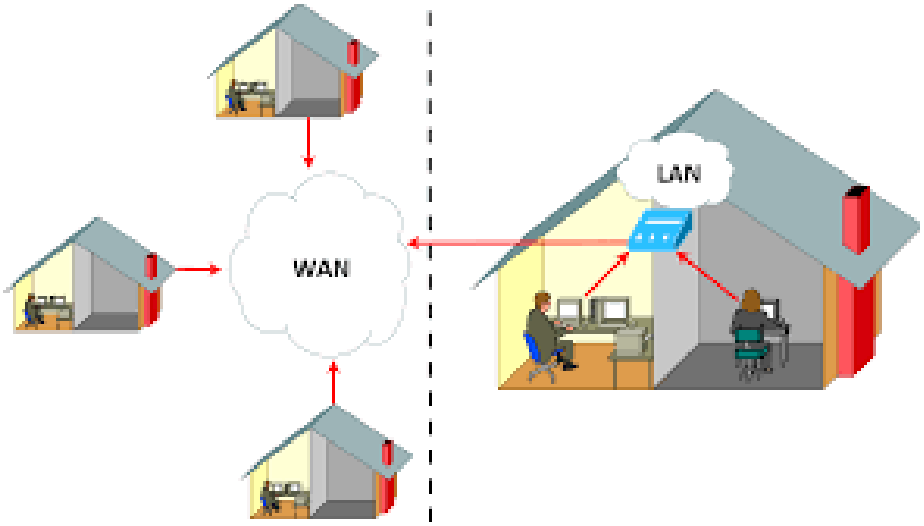


Obrázek 20 NAT (Introduction to Different Types of NAT, 2022)

Samotný provoz počítačových sítí je však mnohem, mnohem komplikovanější. Nehledě na to je lze dále dělit dle několika kategorií. Pro účely této diplomové práce, zejména pak pro její praktickou část, budou počítačové sítě rozčleněny pouze dle jejich rozlehlosti, přenosového média a typu propojení. Zvlášť bude popsána technologie VPN mající dnes zásadní podíl na kybernetické bezpečnosti mnoha chráněných aktiv. Taktéž pojednání o počítačových sítích výše je pro další potřebu považováno za dostatečné.

3.2.1 Dělení počítačových sítí dle jejich rozlehlosti

Počítačové sítě lze dle rozlehlosti rozdělit na lokální sítě (LAN), metropolitní sítě (MAN) a rozsáhlé sítě (WAN), které předchozí dvě spojují. Toto dělení je však díky technologickému pokroku spíše učebnicový příklad, neboť hranice mezi uvedenými sítěmi přestávají být zřetelné (Smejkal, 2018). V praxi se pak většinou počítačové sítě dělí pouze na internet (WAN) a intranet (LAN), který je od WAN sítě oddělen routerem, v případě vyšších nároků na bezpečnost firewallem (oba prvky však mají již implementovaný NAT). Jak tedy z předchozí věty vyplývá, nejznámější celosvětová síť Internet je tvořena obrovským počtem LAN rozmístěných po celém světě. Tyto LAN pak mají (případně nemají) za jasně stanovených podmínek k Internetu přístup.



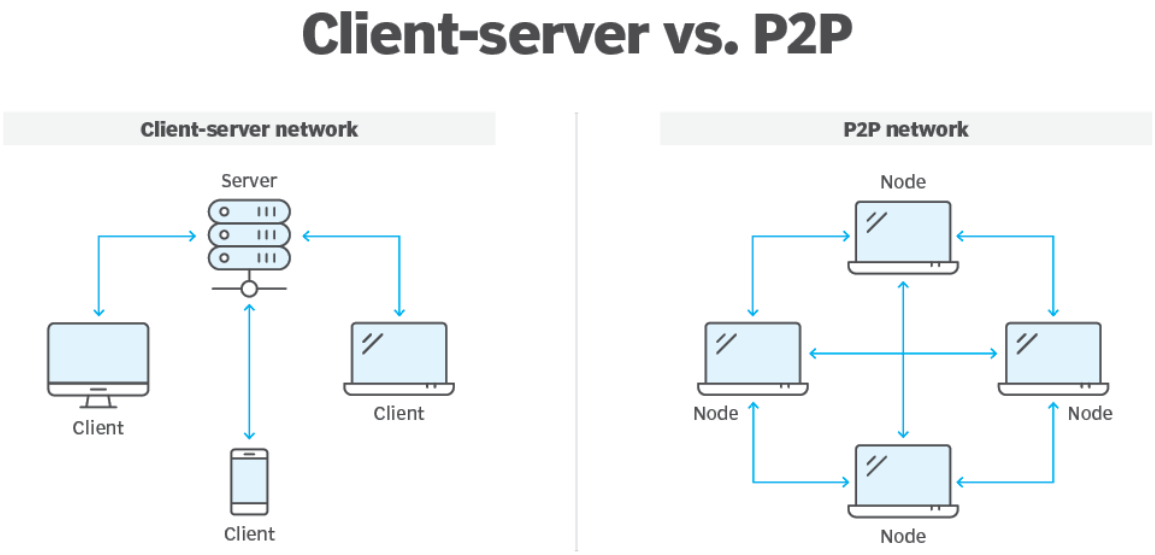
Obrázek 21 Vztah mezi WAN a LAN (What do LAN, WAN, and SD-WAN mean?, 2016)

3.2.2 Dělení počítačových sítí dle přenosového média

V každé počítačové síti musí být zajištěno fyzické spojení (komunikace) mezi jednotlivými síťovými zařízeními. Takovéto spojení je možno zajistit drátovým propojením nebo za využití bezdrátové technologie. Zvláštním případem je pak virtuální spojování označované jako VLAN. Drátové sítě lze dále kategorizovat dle použitého kabelu, nejčastěji se však jedná o kroucenou dvoulinku osazenou konektory RJ-45 a dnes již velmi často o optický kabel. Oproti tomu bezdrátové spojení lze uskutečnit za využití některé bezdrátové technologie. Nejčastěji se jedná o Wi-Fi založenou na standardu IEEE 802.11, která je součástí mnoha domácností. Výhodou jsou nízké pořizovací náklady, nevýhoda tkví v přesahu signálu mimo kontrolovaný prostor (Král, 2015). K bezdrátovému přenosu je možno využít i Bluetooth, WiMAX, mobilní sítě nebo například ZigBee.

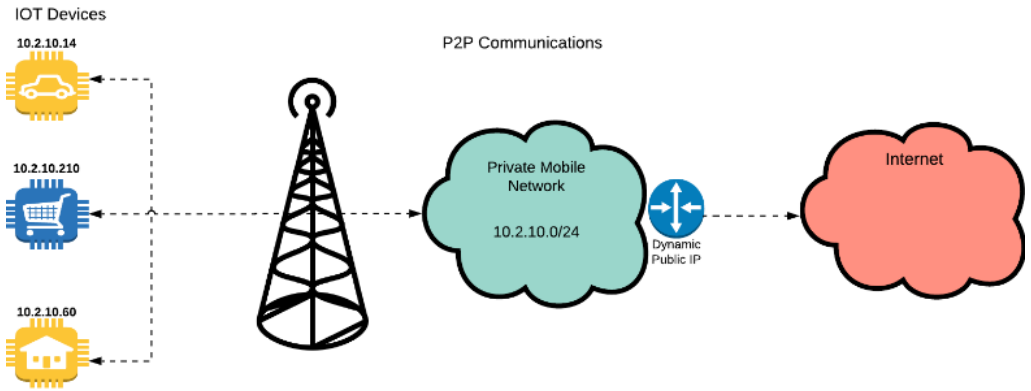
3.2.3 Dělení počítačových sítí dle typu propojení

Rozdělení počítačových sítí dle typu propojení jednotlivých síťových zařízení je možno rozčlenit do dvou kategorií. Jedná se o propojení typu klient-server a klient-klient (poměrně známé P2P sítě, z anglického peer-to-peer). Jak již z názvu vyplývá, tyto typy propojení jsou k sobě navzájem opakem. V případě propojení typu klient-server se pracovní stanice požadující nějakou službu připojují k příslušnému serveru. Z logiky věci tak lze aplikovat na tento typ propojení centralizovanou správu. Na rozdíl od decentralizovaného propojení typu klient-klient, kdy jednotlivá zařízení v síti komunikují přímo mezi sebou (Rosencrance, 2022).



Obrázek 22 Znázornění typu propojení klient-server a klient-klient (Rosencrance, 2022)

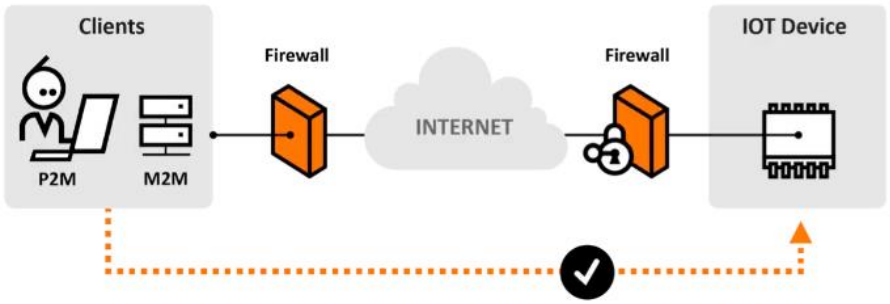
Příkladem lze uvést například chytrou kameru, tedy zařízení internetu věcí (IoT). Po jejím zakoupení zpravidla stačí provést připojení k domácí lokální síti s přístupem k internetu, nainstalovat mobilní aplikaci a sledovat živý video přenos odkudkoli na světě. Obrovskou výhodou těchto (P2P IoT) zařízení jsou nízké pořizovací náklady a možnost zprovoznění i nezkušeným uživatelem.



Obrázek 23 P2P komunikace IoT (Peer to Peer (P2P) communications for IoT, c2006-2023)

Autor diplomové práce je z pohledu kybernetické bezpečnosti vůči těmto sítím, respektive (P2P IoT) zařízením skeptický. Důvodem je, že komunikace těchto zařízení probíhá nekontrolovatelně přes NAT, zpravidla za využití portu 80 (HTTP) nebo 443 (HTTPS), na což není router (firewall) schopen reagovat, protože prostřednictvím těchto portů probíhá standardní internetová komunikace. Prvotní navázání spojení zpravidla probíhá přes server

třetí strany, učebnicové spojení klient-klient totiž v praxi existuje velmi zřídka. Většina těchto serverů je pak umístěna v Číně a je velmi obtížné monitorovat, jaká data z lokální sítě vlastně zpracovávají.

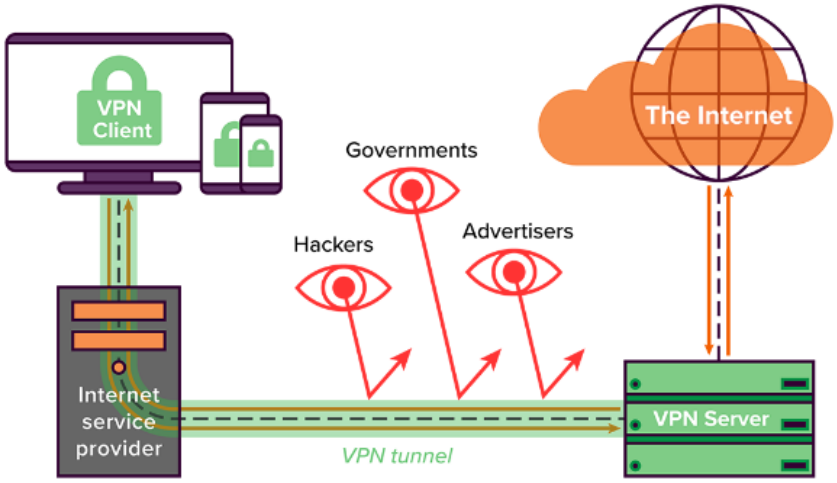


Obrázek 24 Prostupnost P2P komunikace IoT přes NAT (firewall) (A Simple Solution for End-User IoT Device Control, c2009-2023)

Mnohem bezpečnější alternativou k P2P sítím je využití připojení do lokální sítě, respektive ke konkrétním síťovým zařízením, prostřednictvím technologie VPN.

3.2.4 Virtuální privátní síť

Virtuální privátní sítě (Virtual Private Network – VPN) umožňují bezpečně propojit počítače (client-to-server) i celé lokální sítě (site-to-site) nacházející se v různých částech sítě internet. K tomuto spojení pak využívají šifrovaný tunel, kterým proudí veškerá komunikace. V praxi se VPN používá například k připojení do podnikové sítě ze vzdáleného místa, k ochraně soukromí před místním poskytovatelem internetu nebo k obcházení geografické blokace a cenzury v některých zemích (Bořánek, 2017). Mezi nevýhody VPN patří dle Bořánka (2017) snížení rychlosti připojení a s ním související vyšší latence. S ohledem na dnes nabízené komerční služby VPN a praktické zkušenosti autora diplomové práce nelze s Bořánkem v ohledu nevýhod VPN služeb souhlasit.



Obrázek 25 Zjednodušený diagram VPN (What is a VPN and how can you benefit from it?, 2020)

Vytáčený VPN tunel pak k šifrování přenášených dat využívá některý z bezpečnostních protokolů. Těch existuje celá řada. Níže jsou uvedeny ty nejvýznamnější, dva z nich jsou pak součástí praktické části diplomové práce.

PPTP (Point-to-Point Tunneling Protocol)

Jedná se o nejstarší protokol vyvinutý společností Microsoft. Výhodu jeho používání představuje rychlost komunikace, velmi snadná konfigurace a podpora všemi zařízeními. Od doby jeho prolomení ze strany NSA (2012) není považován za bezpečný a v praxi se již nepoužívá (Perunicic, 2023).

SSTP (Secure Socket Tunneling Protocol)

Rychlý a bezpečnější nástupce PPTP, taktéž vyvinutý společností Microsoft. Jeho integrace v operačním systému Windows je tedy samozřejmostí. Vyniká snadnou prostupností většiny firewallů, ale také jsou známy jeho zranitelnosti (Perunicic, 2023).

L2TP (Layer 2 Tunneling Protocol)/IPsec

Tento protokol vychází z protokolu PPTP, avšak nenabízí žádné zabezpečení. V praxi je tudíž kombinován s protokolem IPsec. V odborné komunitě se proslýchá, že byl již také prolomen NSA (Perunicic, 2023).

IKEv2 (Internet Key Exchange)/IPsec

Opět se jedná o protokol vyvinutý společností Microsoft ve spolupráci s Cisco. Je rychlejší než všechny výše uvedené protokoly (Perunicic, 2023). Tvoří součást rodiny protokolů IPsec

a momentálně nejsou prokázány žádné jeho slabiny. K provozu nevyžaduje instalaci software třetí strany (Jakubová, 2020).

OpenVPN

Nový a velmi spolehlivý protokol s otevřeným zdrojovým kódem, který podporuje mnoho bezpečnostních algoritmů. Dosud nebyly v bezpečnosti odhaleny žádné nedostatky. Hodí se i pro mobilní sítě (Perunicic, 2023; Jakubová 2020). Bohužel vyžaduje instalaci a konfiguraci software. Je široce využíván komerčními VPN službami.

WireGuard

„Extrémně rychlý VPN protokol s velmi moderním způsobem šifrování. Nabízí jednodušší, bezpečnější a efektivnější cestu použití VPN než ostatní technologie.“ (Jakubová, 2020)

WireGuard je součástí Linuxu, pro ostatní operační systémy je nutné naistalovat a nakonfigurovat potřebný software. Nejsou známy žádné jeho bezpečnostní díry (Jakubová, 2020). Tento protokol je autorem diplomové práce široce využíván. Například s vybranými modely routerů Asus, které ho podporují jak na straně klienta, tak na straně serveru, lze bez větších obtíží virtuálně spojovat celé lokální sítě napříč internetem. WireGuard je také jedním z favoritů pro praktickou aplikaci v praktické části této práce.

SSL (Secure Sockets Layer)

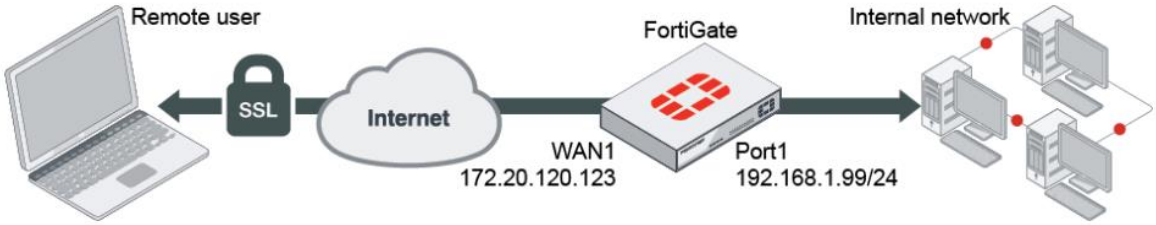
Druhým favoritem pro aplikaci v praktické části diplomové práce je SSL VPN. Zde nastává trochu zmatek. Nejedná se o zastaralý bezpečnostní protokol SSL, nýbrž o zabezpečené internetové spojení prostřednictvím protokolu TSL. Tuto VPN pak lze použít dvojím způsobem:

a) portál SSL VPN, nebo

b) tunel SSL VPN.

Portál pak klientům (myšleno uživatelům) umožňuje navázat bezpečné připojení z internetu do lokální sítě prostřednictvím webového prohlížeče. V praxi se pak jedná například o možnost využívat služeb webové aplikace podniku. Oproti tomu tunel nabízí komplexnější připojení a lze díky němu využívat i další síťové služby. Výhodou je, že SSL VPN podporují všechny moderní webové prohlížeče a samotná realizace připojení VPN je možná pouze pro již zmíněné specifické webové aplikace. Přístup do celé lokální sítě tak není nutný, což zvyšuje kybernetickou bezpečnost (What is SSL VPN?, 2023). V případě využití portálu

SSL VPN představuje jistou nevýhodu technické omezení webového prohlížeče, což lze samozřejmě obejít popsaným tunelem.



Obrázek 26 Tunel SSL VPN (SSL VPN full tunnel for remote user, 2023)

3.2.5 Teorie zabezpečení počítačových sítí

Zabezpečení počítačové sítě je nutnou podmínkou zajištění kybernetické bezpečnosti. Bohužel málokterá odborná publikace poskytuje o tomto tématu komplexní praktický přehled. Naštěstí při možnostech, které dnešní výrobci routerů či firewallů nabízejí, není z praktického hlediska zabezpečení lokální sítě nijak složité.

Bez ohledu na to, zda se jedná o drátově nebo bezdrátově řešenou síť, NAT nestačí. Nejenom s ohledem na zařízení IoT popsaná v této kapitole, která jsou schopna bez větších problému komunikovat s vnějším světem, je firewall nutný. Je známo, že některá P2P IoT zařízení jsou schopna bez vědomí uživatele odesílat konkrétní vnitřní IP adresy používané v lokální síti. Potencionální útočník tak získá ucelený přehled o zařízeních používaných ve vnitřní síti a skrze NAT se na ně dokáže připojit. Zde nastupuje zmíněný firewall. Nemusí se nutně jednat o drahý hardware. Většina moderních routerů má firewall implementovaný přímo ve firmware (Krčmář, 2007). Příkladem lze uvést routery od společnosti Asus, které kromě implementovaného firewallu nabízejí díky licenci AiProtection Pro online ochranu lokální sítě. Prakticky se pak jedná o širokou škálu služeb, jako je automatické blokování škodlivých stránek, implementovaný firewall nebo blokování infikovaných zařízení a automatické bezpečnostní aktualizace (AiProtection Plan Comparison, 2023). Zajímavé řešení pak nabízí americká společnost Fortinet, která vyvíjí firewally a antivirové programy. Konkrétně desktopové firewally FortiGate spolu s licencí FortiGuard jsou pak schopny v reálném čase zabezpečit kompletní ochranu lokální sítě a vytáčet zabezpečenou SSL VPN včetně dvoufaktorové autentizace. Toto řešení je však pro domácnosti velmi drahé.

Obrázek 27 Služby v rámci licence FortiGuard (Jarvis, 2018)

Dále je vhodné využívat virtuální sítě. Pro již několikrát zmíněná IoT a jiná chytrá zařízení, která nelze chránit antivirovým programem, je velmi příhodné vytvořit virtuální síť pouze s přístupem k internetu. Tato zařízení pak nevidí na běžně používané pracovní stanice, a nemají tak potencionálním útočníkům co odesílat. Komerčně dražší je pak veškerý provoz vnitřní sítě z a do internetu přesměrovat přes VPN vytáčenou přímo na routeru. Konkrétně s routery Asus bez problému funguje ProtonVPN nebo NordVPN za využití bezpečnostního protokolu WireGuard. Potencionální útočník tak zjistí pouze IP adresu poskytovatele konkrétní VPN služby a je mu bráněno ve sledování provozu lokální sítě.

Samostatnou kapitolu tvoří bezdrátové sítě, kde je třeba dle Krále (2015) navíc:

a) skrýt SSID (název sítě),

b) nastavit silné heslo a

c) využívat nejmodernější bezpečnostní protokol WPA2 (dnes již WPA3, pozn autora) s šifrováním AES.

d) Závěrem se nesmí zapomenout na aktivní filtrování připojených zařízení dle MAC adres (a případné vypojení DHCP serveru, pozn autora).

Zde autor diplomové práce s Králem nesouhlasí. Podle něj nepřispívá skrytí SSID ke zvýšení kybernetické bezpečnosti. Reálně pouze způsobuje automatické odpojování P2P IoT

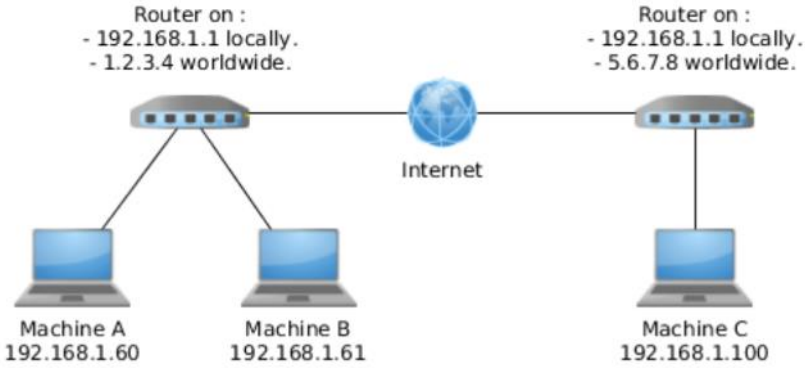
zařízení od sítě. Ta se pak bez zásahu uživatele zpravidla nedovedou k síti sama opětovně připojit.

3.3 Router a firewall

Router a firewall jsou zařízení, bez kterých je nemožné v současné době provozovat počítačovou síť. Naštěstí většina výrobců funkce obou technologií slučuje do jednoho zařízení známého jako Wi-Fi router. Ten pak umožňuje uživateli vytvořit bezdrátovou síť, zpravidla připojenou k internetu.

3.3.1 Router

Router sám o sobě představuje zařízení, které spojuje dvě a více počítačových sítí. V praxi se většinou jedná o lokální síť konkrétního uživatele (LAN) spojenou se sítí místního poskytovatele internetu (MAN či WAN). Výhodou routeru je, že všem připojeným zařízením dokáže poskytovat stejné připojení k internetu či jiné síti. Stačí tak jediná přípojka. Zařízení v místní LAN komunikující s jiným zařízením v jiné LAN, zpravidla prostřednictvím internetu, směruje veškerou komunikaci přes místní router, ten komunikaci přeposílá vzdálenému routeru a ten zase onomu vzdálenému zařízení. Díky této funkci lze mezi těmito počítačovými sítěmi jednoduše řídit provoz (Santos, 2022; What is a router?, 2023). Pro hlubší a ve smyslu bezpečnosti větší kontrolu nad síťovou komunikací mezi dvěma a více počítačovými sítěmi nastupuje firewall.

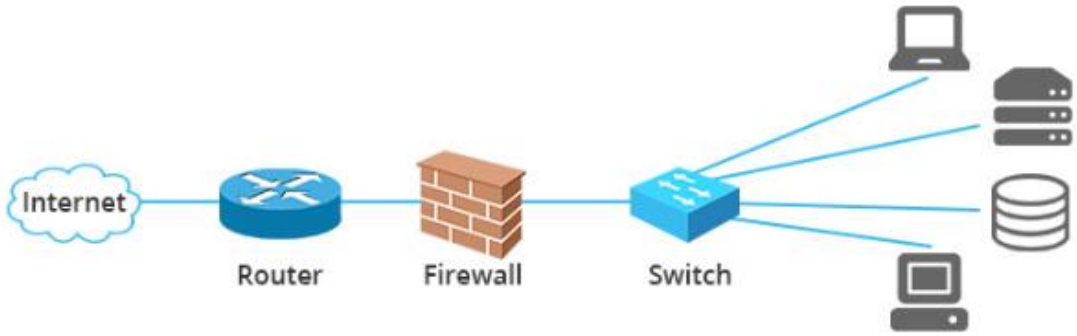


Obrázek 28 Znázornění komunikace mezi dvěma routery (Router Communication, 2023)

3.3.2 Firewall

Firewall je bezpečnostní systém, který umožňuje hloubkově analyzovat komunikaci mezi dvěma a více počítačovými sítěmi. V praxi se může jednat o softwarovou službu nebo

samostatné hardwarové zařízení. Výhodou tohoto zařízení je, že umožňuje definovat jasná pravidla komunikace mezi výše uvedenými sítěmi. Děje se tak povolením, respektive zakázáním nežádoucích TCP/UDP portů, čímž je komunikace mnohem bezpečnější (Network Switch vs Network Router vs Network Firewall, 2020; Chapman a Zwicky, 1998).



Obrázek 29 Znázornění umístění firewallu v LAN (Network Switch vs Network Router vs Network Firewall, 2020).

3.3.3 Teorie zabezpečení těchto zařízení

Většina nabízených firewallů, respektive routerů s již implementovaným firewallem umožňuje vytáčet VPN jak na straně serveru, tak klienta. Nabízí tím celou řadu v předchozí kapitole popsaných nejmodernější protokolů zabezpečení, včetně online ochrany před celou škálou kybernetických útoků. Jedinou ochranou těchto zařízení ze strany uživatele je:

a) nastavení silného hesla,

b) pravidelné aktualizace firmware a u zařízení, které to umožňují,

c) změnit výchozí uživatelské jméno (zpravidla admin) a

d) zakázat změnu konfigurace prostřednictvím připojení k bezdrátové síti (zpravidla Wi-Fi).

e) Závěrem nesmí, ve smyslu fyzické bezpečnosti, chybět fyzické znepřístupnění těchto zařízení neoprávněným osobám (Chapman a Zwicky, 1998; Santos, 2022).

3.4 Data, databáze a síťová datová uložiště

Jedním z dnešních nejcennějších aktiv podniku jsou data. U nadnárodních institucí a s ohledem na neustále se rozvíjející umělou inteligenci se stále častěji jedná o big data.

Každá data je však nutno nějak (databáze) a někam (síťová datová uložiště) ukládat (Hendl, 2021).

3.4.1 Data

Pro další potřebu této diplomové práce postačí definice dat v tomto znění:

„Reprezentace informací vhodně formalizovaná pro komunikaci, interpretaci a zpracování lidmi a automaty. Data mohou být reprezentována libovolnými řetězci znaků (čísel, příkazů, vět) uloženými na informačním nosiči…“ (Jonák, 2003)

Jak z této definice samo o sobě vyplývá, každá data je nutno nejprve nějak získat, zformátovat, uložit a zpracovat. To vše, s ohledem na dnešní nároky, v reálném čase (Hendl, 2021).

Vzhledem k praktickému zaměření této diplomové práce bude další pojednání zaměřeno na zpracovávání a ukládání výhradně elektronických dat, a to za využití databáze a síťového datového uložiště.

3.4.2 Databáze

Databázi lze obecně charakterizovat jako optimalizovaný systém uspořádaných dat, do kterého lze snadno zapisovat, upravovat již uložená data, mazat je a také jednoduše vyhledávat. V praxi nejpoužívanější jsou pak relační databáze založené na tabulkovém systému. Aby byla práce s databází optimální, je nutné používat databázový systém, někdy také nazývaný systém řízení báze dat. K těm nejpoužívanějším patří:

a) Microsoft Access,

b) Oracle,

c) SQLite,

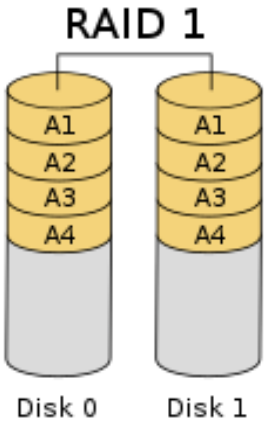
d) MySQL, nástupnická MariaDB a

e) Microsoft SQL Server používaný i ve vybrané organizaci (Hendl, 2021; Laurenčík, 2018).

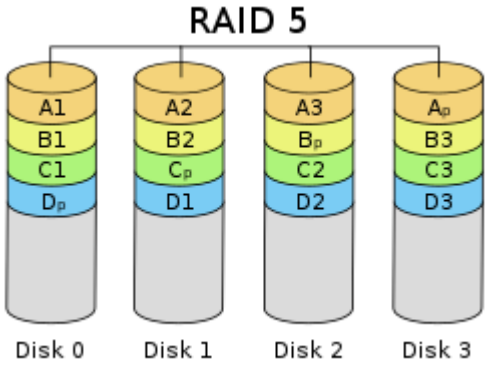
Samotná databáze je pak s mírnou nadsázkou prakticky velký soubor, se kterým některý z výše uvedených databázových systémů pracuje dle požadavků uživatele.

3.4.3 Síťové datové uložiště

Jak již z názvu vyplývá, síťová datová uložiště (NAS) jsou hardwarová zařízení umožňující ukládání a sdílení dat. K tomuto účelu jsou osazeny různorodým počtem pevných disků. Většina firmware instalovaných na těchto NAS umožňuje v kombinaci s uvedeným různorodým počtem pevných disků používat funkci RAID – vícenásobné pole nezávislých disků. Tato funkce či systém ukládání dat představuje významnou položku v samotném zabezpečení elektronických dat. Její primární funkcí je totiž ukládat data na více nezávislých disků (dle zvolené úrovně RAID), čímž je chrání před zničením a poškozením (RAID, 2023).



Obrázek 30 RAID 1 – zrcadlení (RAID, 2023)



Obrázek 31 RAID 5 (RAID, 2023)

3.4.4 Teorie zabezpečení elektronických dat

Na úseku zabezpečení elektronických dat spolu souvisejí všechny tři výše prezentované kapitoly. Chronologicky musejí být nejprve šifrována data uložená v databázi, respektive celá databáze. Databázový systém musí být udržován stále aktuální a chráněný silným

heslem, stejně jako server (operační systém), na kterém běží. Databáze pak musí být pravidelně zálohována, k čemuž lze právě využít NAS s některým typem RAID. Obecně se pak doporučuje zálohovat ve smyslu 3-2-1. To v praxi znamená neustále vytvářet tři kopie databáze, z nichž dvě jsou ukládány místně, na dvou nezávislých zařízeních a třetí kopie se ukládá mimo vyhrazené prostory (Elliott, 2021). Pravidelná aktualizace firmware NAS a fyzické zabránění přístupu neoprávněným osobám ke všem definovaným prvkům je samozřejmostí (Tuhý, 2013).

II. PRAKTICKÁ ČÁST

4 POPIS VYBRANÉ SPOLEČNOSTI A IDENTIFIKACE AKTIV

Vybraná obchodní společnost bude v této diplomové práci vystupovat pod krycím označením Taurus. Důvodem je, že si tato reálná společnost s ručením omezeným přála zůstat anonymní, což je autorem této diplomové práce respektováno. Na oplátku Taurus poskytl autorovi této diplomové práce přístup k veškerým prvkům ICT, jakožto i ke kontrole jejich vhodné konfigurace, nastavení a zabezpečení. To vše s ohledem na zákon 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), rodinu norem ISO/IEC 27000, známou jako ISMS a také s ohledem na obecné dobré praktiky v oblasti zajištění kybernetické bezpečnosti. Zde autor této diplomové práce považuje za nutné dodat, že společnost Taurus fakticky nepodléhá zákonu o kybernetické bezpečnosti a uvedená rodina norem ISO/IEC 27000, konkrétně tedy ISO/IEC 27001, nebude ve společnosti Taurus prakticky implementována. V aplikační části této diplomové práce však budou konkrétní vybraná opatření implementována právě s ohledem na výše uvedené předpisy a již zmíněné dobré praktiky v oblasti zajištění kybernetické bezpečnosti.

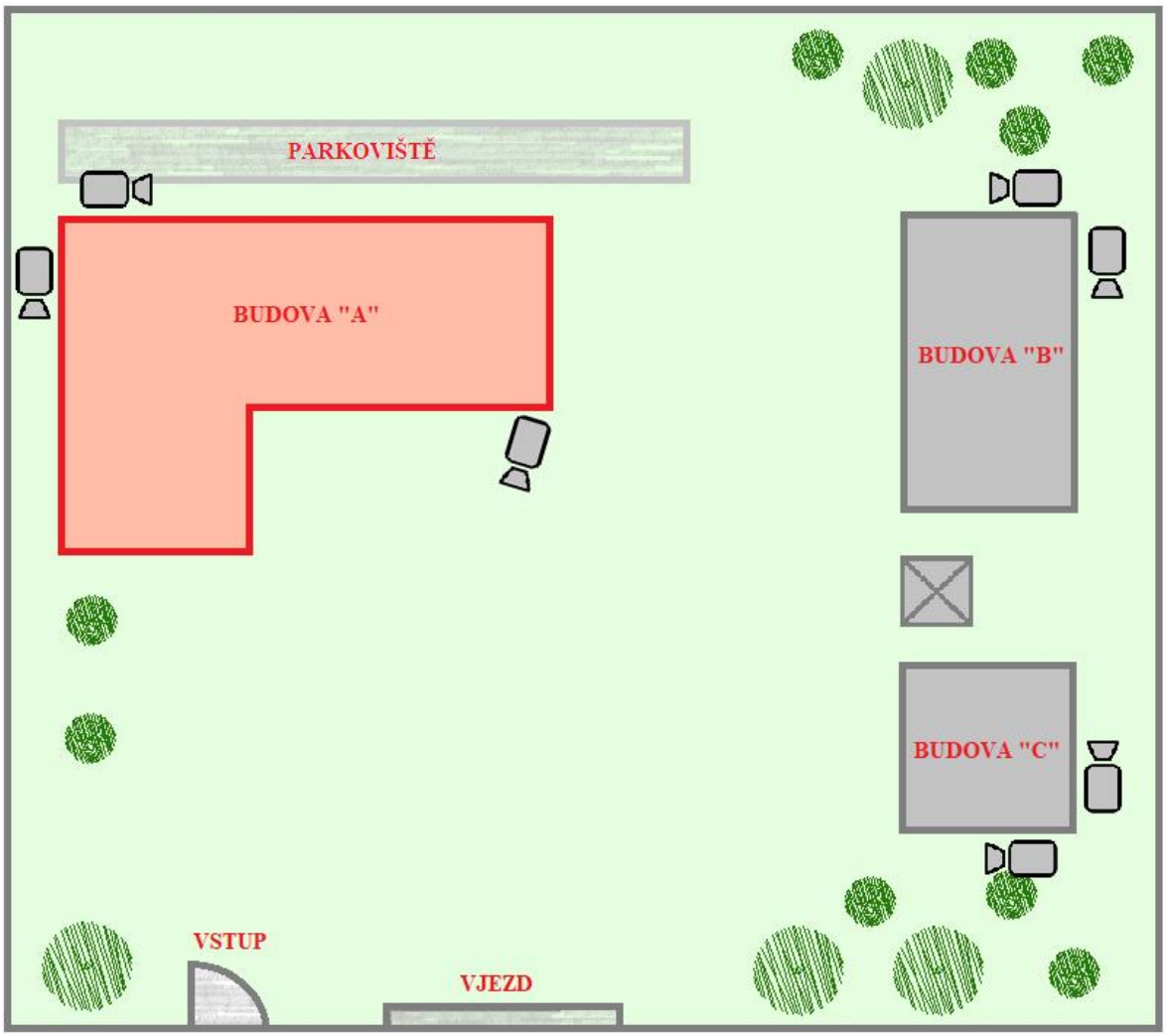
Obchodní společnost Taurus se nachází na pomezí Jihomoravského a Zlínského kraje. Její vznik je datován zápisem do Obchodního rejstříku roku 2008. Od té doby společnost sídlí ve vlastním areálu rozkládajícím se na ploše takřka 4000 m^2. Předmětem činnosti této obchodní společnosti je nákup a prodej speciálních technických zařízení. Za tímto účelem zaměstnává Taurus 28 zaměstnanců pracujících na dvě směny. Většina zaměstnanců tráví pracovní dobu mimo areál společnosti Taurus. K přístupu do firemní sítě, respektive webové aplikace, je využíváno připojení prostřednictvím technologie VPN, o čemž pojednávají podrobněji následující kapitoly, kde jsou dále identifikována zájmová chráněná aktiva, jejich potencionální zranitelnosti a stávající opatření. Bližší činnost společnosti Taurus pak s ohledem na autorem diplomové práce garantovanou bezpečnost a anonymitu, není možné zveřejnit.

Celý výše uvedený areál je oplocen drátěným pletivem o výšce 200 cm. Vstup, případně vjezd, do tohoto areálu je možný pouze dvěma způsoby. Konkrétně se jedná o uzamykatelnou vstupní branku (určenou pro pěší vstup zaměstnanců) a pojezdovou bránu (sloužící k vjezdu služebních vozidel). Vstupní branka je dále z vnější strany opatřena kulatou rozetou a klíč má pak zapůjčen každý z momentálních 28 zaměstnanců. Dálkový ovladač pro pojezdovou bránu je pak k dispozici v každém z patnácti služebních vozidel. Důležité je také zmínit, že dálkový ovladač je aktivní výhradně v pracovní době, a to každý

všední den od 7:00 do 20:00. Vjezd soukromých vozidel do areálu společnosti je zakázán, jakožto i vstup osob, které Taurus nezaměstnává.

Samotný areál popisované společnosti je pak pomyslně rozdělen na tři klíčové části (stavby). Tento je dále snímán sedmi venkovními kamerami instalovanými svépomocí a také zabezpečen Poplachovým zabezpečovacím a tísňovým systémem (PZTS) od společnosti Jablotron, trvale připojeným na Dohledové a poplachové přijímací centrum (DPPC). Tento PZTS je uzavřený celek nainstalovaný odbornou certifikovanou společností a nebude tudíž součástí praktické analýzy této diplomové práce.

Naproti vstupu či vjezdu do areálu se nachází hlavní budova, která bude dále pro účely této diplomové práce označována jako budova „A“. Na budově A jsou umístěny celkem tři venkovní kamery, které snímají jednotlivé části areálu. Vpravo vedle budovy A se nachází druhá budova, dále označována jako budova „B“, na které jsou umístěny dvě venkovní kamery. Blíže v popředí, před budovou B, se nachází třetí stavba, dále systematicky označována jako budova „C“. Na této jsou umístěny zbývající dvě venkovní kamery. Za budovou A se pak nachází parkoviště pro služební vozidla. Jako možné relaxační místo se nabízí altán stojící mezi budovou B a C. Pro lepší orientaci čtenáře je pak níže zobrazen situační nákres areálu společnosti Taurus, včetně vyobrazení již zmíněných sedmi kamer snímající tento areál.



Obrázek 32 Situační nákres areálu Taurus (Microsoft, 2022)

4.1 Popis budovy A a vnitřní fyzické bezpečnosti

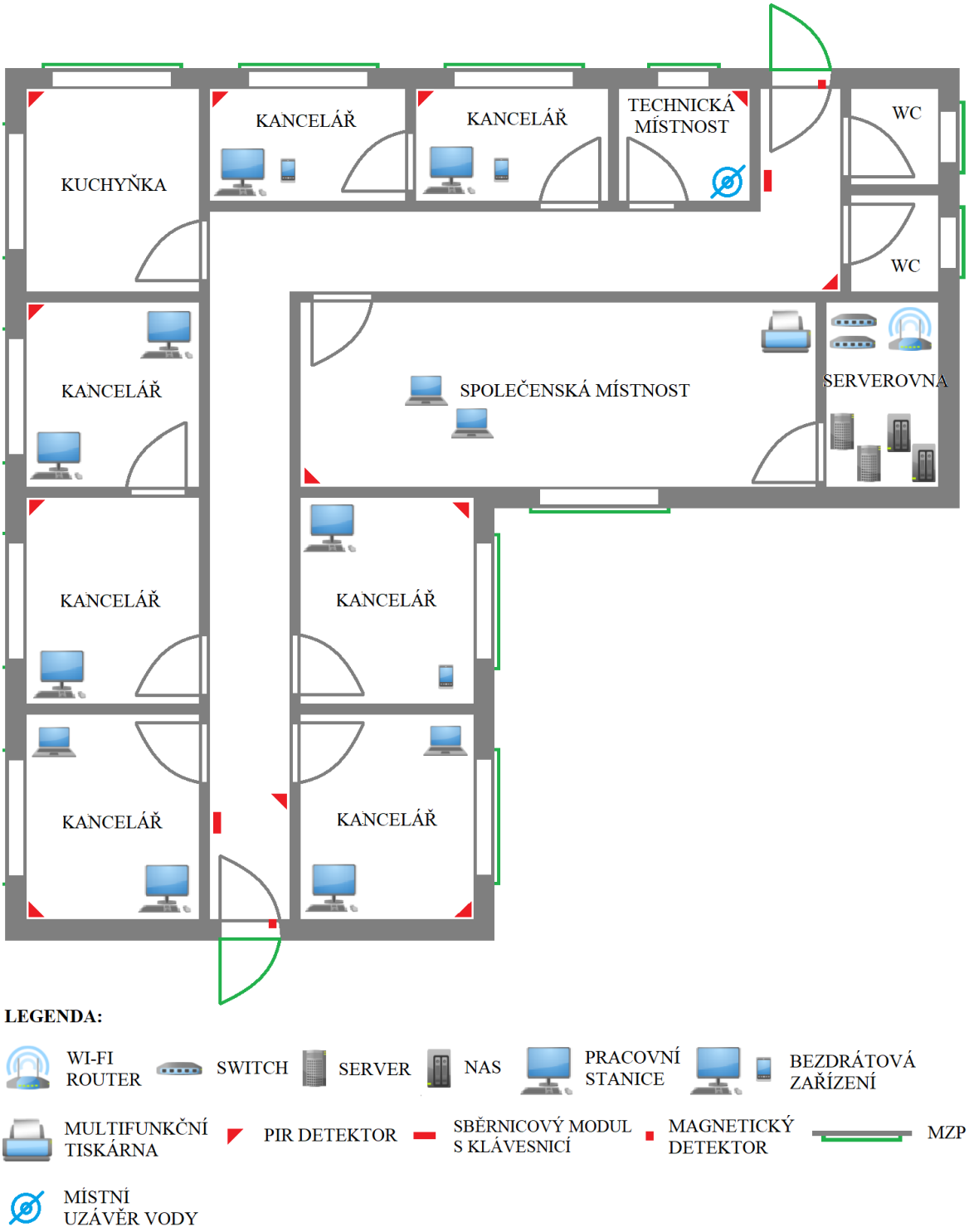
Budova A pomyslně představuje hlavní budovu popisovaného areálu. Jedná se o jednopodlažní stavbu s rovnou střechou. Uvnitř se nachází sedm kanceláří, společenská místnost, kuchyňka a technická místnost se serverovnou. Vstup je realizovaný dvěma vchodovými dveřmi, které jsou z vnější strany chráněny mechanickými zábrannými prostředky, konkrétně tedy kovovými mřížemi. Obě vchodové dveře jsou také z vnější strany osazeny klikou s kulatou rozetou. Klíče od obou vstupních dveří má k dispozici každý zaměstnanec. Všechna okna v této budově jsou také zabezpečena mechanickými zábrannými prostředky, opět, tak jako u vstupních dveří, se jedná o kovové mříže, pevně svázané s obvodovou zdí. Celá budova A je chráněna již zmíněným PZTS od společnosti Jablotron. U obou možných vstupů do budovy je umístěn sběrnicový přístupový modul s klávesnicí umožňující komunikaci s ústřednou PZTS. Celá budova A představuje ve

smyslu PZTS jednu sekci a každý zaměstnanec ji má právo obsluhovat výhradně vlastním PIN kódem. Samotná ústředna se pak nachází v serverovně a prostřednictvím lokální sítě má zajištěn přímý přístup k síti internet tak, aby bylo zajištěno spojení s DPPC. Samotné rozmístění, v tomto případě bezdrátových, PIR detektorů a dvou magnetických detektorů snímajících otevření dveří, je znázorněno níže na vytvořeném půdorysu.

Z pohledu této diplomové práce samozřejmě představuje nejdůležitější místnost serverovna. V serverovně se nachází několik prvků ICT, které budou podrobně popsány v kapitole popisující provozovanou lokální síť (LAN). Vstup do serverovny je možný pouze ze společenské místnosti jedněmi trvale uzamčenými dveřmi. Klíč má v současné době pouze majitel společnosti Taurus. Místnost serverovny nemá žádné okno. Nedílnou součástí serverovny je pak plně funkční klimatizace a samostatný elektrický jistič. Zálohu elektrické energie pro případ výpadku elektrického proudu zajišťuje komerční záložní zdroj UPS. UTP kabeláž zajišťující spojení jednotlivých prvků ICT je v serverovně a celé budově vzorově vedena v lištách, ty vyúsťují v jednotlivých kancelářích patřičným počtem síťových zásuvek. Do těchto síťových zásuvek je pak v budově A připojeno osm pracovních stanic (počítačů) a jedna síťová multifunkční tiskárna. Dle momentální potřeby zaměstnanci připojují do provozované lokální sítě i další zařízení. Zpravidla se jedná o notebooky a mobilní telefony, které ke komunikaci v síti využívají bezdrátovou technologii Wi-Fi.

Vytápění této budovy je zajištěno plynovým kotlem umístěným v technické místnosti. Jednotlivé deskové radiátory jsou pak instalovány v jednotlivých kancelářích pod okny. V technické místnosti se dále nachází osmdesátilitrový elektrický bojler zajišťující ohřev teplé vody. Tyto potencionální zdroje vody s ohledem na umístění chráněných aktiv nemohou při havárii tyto akutně ohrozit. Místní uzávěr vody se pak nachází v technické místnosti, která je všem přístupná.

Na obrázku níže, který představuje půdorys budovy A, jsou pak zakresleny výše popsané skutečnosti. Jedná se především o konkrétní rozmístění prvků ICT a komponent tvořících PZTS.



Obrázek 33 Půdorys budovy A (Microsoft, 2022)

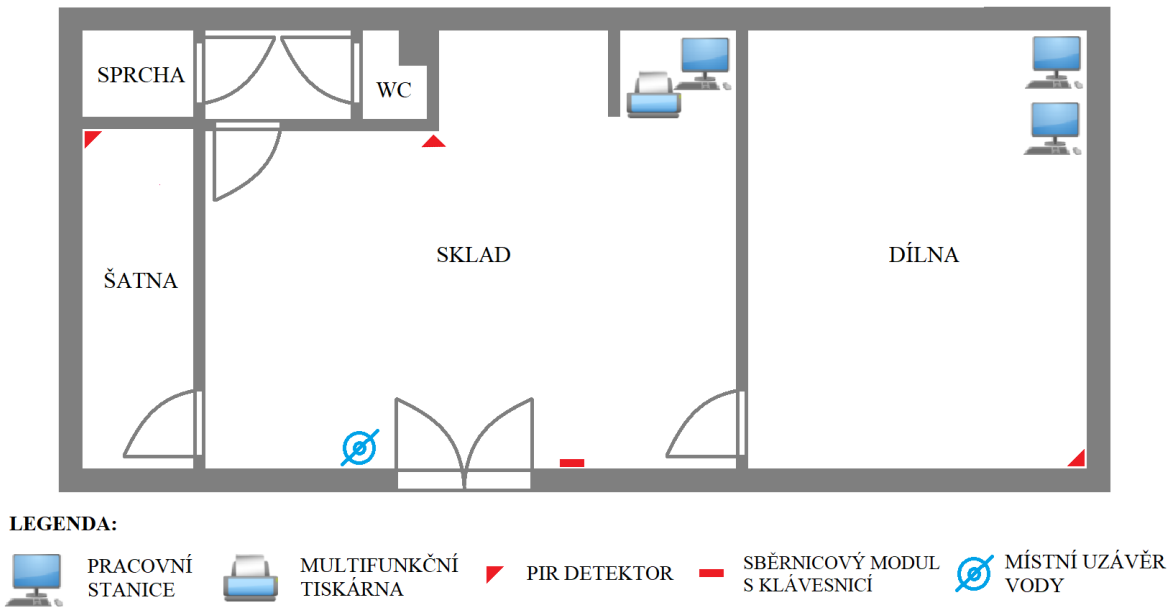
4.2 Popis budovy B a vnitřní fyzické bezpečnosti

Druhá budova v tomto areálu slouží především jako dílna, ve které jsou zpravidla opravována a testována reklamovaná zařízení. Ve smyslu PZTS představuje tato budova

druhou samostatnou sekci. Aktivace a deaktivace PZTS je opět zajišťována sběrnicovým modulem s klávesnicí, který je umístěn na zdi vpravo za jedinými vstupními dveřmi. K samotné aktivaci či deaktivaci PZTS opět slouží PIN kód zaměstnance, který má do této budovy přístup, fakticky se jedná o čtyři osoby. Na vstupních dveřích není umístěno magnetické čidlo, snímající jejich případné neoprávněné otevření. Dveře jsou však z venku osazeny klikou s kulatou rozetou. Klíč od vstupních dveří mají k dispozici pouze ony čtyři osoby. Uvnitř budovy jsou umístěny celkem tři PIR detektory snímající neoprávněný pohyb osob v těchto prostorách. Obvodová zeď budovy B neobsahuje žádné okno.

Z chráněných aktiv zájmové lokální sítě se v budově B nacházejí tři pracovní stanice a také síťová multifunkční tiskárna. Na obrázku níže jsou tato zájmová aktiva znázorněna, opět včetně PIR detektorů a sběrnicového modulu s klávesnicí.

V budově se díky sprše a toaletě nachází uzávěr vody. Vytápění je zajištěno deskovým radiátorem umístěným v šatně a chodbičce mezi sprchou a WC. Oba tyto potencionálně nežádoucí zdroje vody jsou umístěny v dostatečné vzdálenosti od chráněných aktiv, a nepředstavují tak akutní ohrožení v případě havárie.



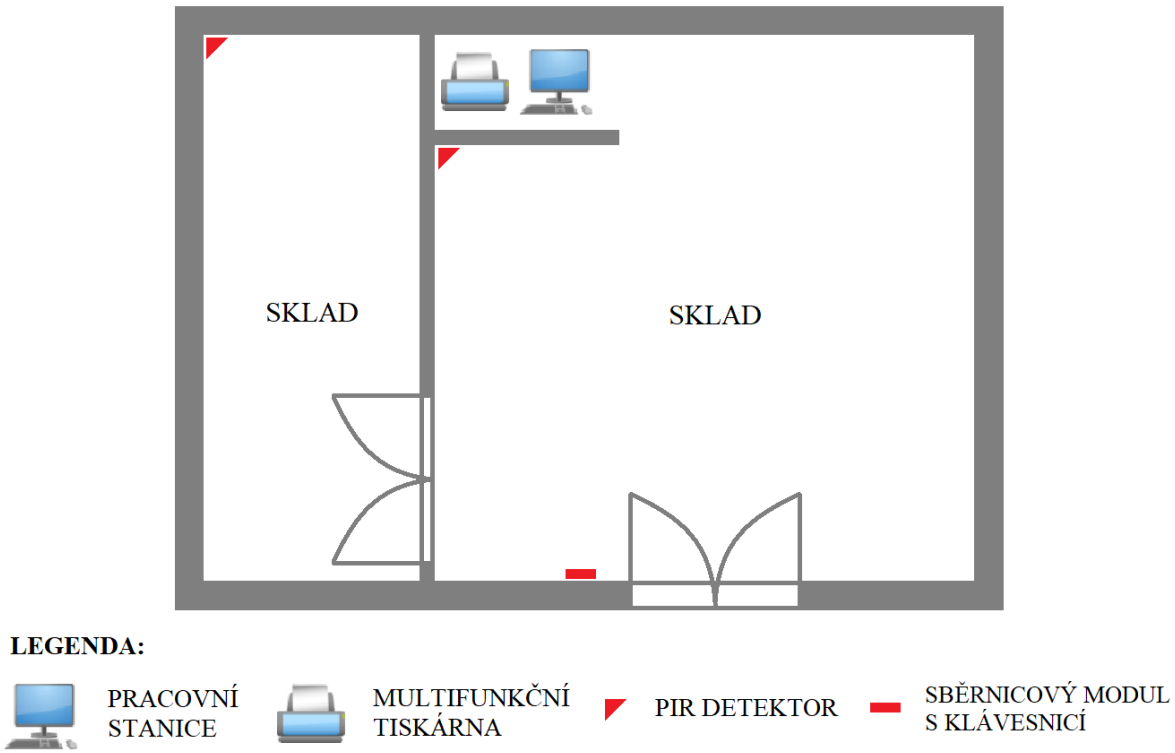
Obrázek 34 Půdorys budovy B (Microsoft, 2022)

4.3 Popis Budovy C a vnitřní fyzické bezpečnosti

Třetí a poslední sekci PZTS představuje budova C. V ní jsou umístěna zbývající dvě chráněná aktiva, která jsou součástí provozované lokální sítě. Prakticky se jedná o stolní

počítač a síťovou multifunkční tiskárnu. Budova C slouží výhradně jako sklad. Obdobně jako u výše popisované budovy B je i do této stavby realizován vstup pouze jedněmi vstupními dveřmi a v obvodové zdi není umístěno žádné okno. Na vstupních dveřích, které jsou také z vnější strany osazeny klikou s kulatou rozetou, opět chybí magnetické čidlo snímající jejich neoprávněné otevření. V prostorách jsou však instalována dvě PIR čidla a vlevo za vstupními dveřmi je umístěn sběrnicový modul s klávesnicí. Aktivace a deaktivace PZTS se opět provádí výhradně osobním PIN kódem příslušného zaměstnance. Do cylindrické vložky ve vstupních dveřích pasují stejné klíče jako do cylindrické vložky vstupních dveří budovy B. Nepřekvapí tedy, že do těchto prostor mají taktéž přístup výhradně výše zmínění čtyři zaměstnanci. Budova C není vytápěna a není zde přítomen žádný jiný potencionální zdroj vody.

Na obrázku níže jsou opět zakresleny výše popsané skutečnosti.



Obrázek 35 Půdorys budovy C (Microsoft, 2022)

4.4 Popis kamerového systému

Samostatnou kapitolu zabezpečení představuje místně provozovaný kamerový systém, který na rozdíl od PZTS bude součástí analýzy kybernetických rizik společnosti Taurus. Reálně

se jedná o poměrně běžné komerční řešení od izraelské firmy Provision ISR, které je možno instalovat svépomocí. S ohledem na uživatelskou přívětivost a plně implementovanou češtinu síťového videorekordéru (NVR) byla instalace svépomocí ze strany majitele společnosti Taurus v minulosti využita.

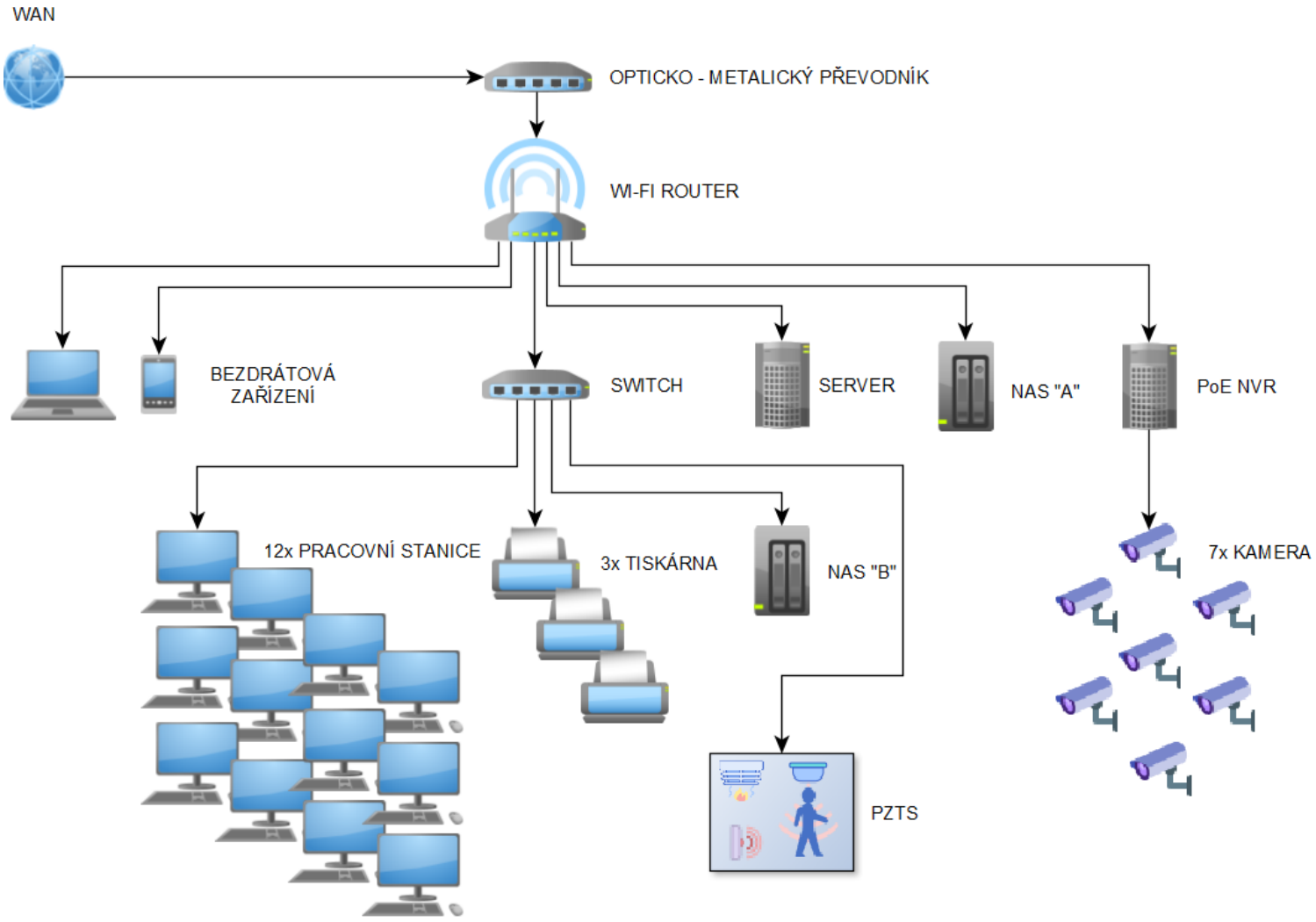
V popisovaných podmínkách společnosti Taurus je provozován model síťového videorekordéru NVR8-8200PFA. Jak pravděpodobně z modelového označení vyplývá, tento NVR umožňuje připojit až osm kamer, přičemž v předmětném areálu jich je provozováno sedm. Napájení kamer je zajištěno technologií Power over Ethernet (PoE), česky po datovém kabelu. V praxi to znamená, že každá kamera je s NVR spojena pouze jedním kabelem, konkrétně se jedná o kroucenou dvoulinku (UTP kabel), který zajišťuje jak napájení, tak přenos dat. Obrazový záznam z NVR je ukládán na HDD disk, který je osazen přímo v NVR. Odtud je dále pravidelně zálohován na síťové datové uložiště (NAS) Synology DiskStation DS218. NVR i NAS jsou nejenom ve smyslu fyzické bezpečnosti umístěny v serverovně.

Popsaný model NVR má i implementovanou detekci pohybu se zasíláním notifikací prostřednictvím mobilní aplikace od Provision ISR. V popisovaném areálu je tato funkce aktivní, konkrétně mimo pracovní dobu od 20:00 do 7:00 ve všední dny a o víkendu pak nepřetržitě. Notifikace jsou následně zasílány pouze na mobilní telefon majitele společnosti Taurus. K zajištění této funkce je NVR prostřednictvím provozované LAN neustále připojen k internetu. Datová komunikace NVR s mobilní aplikací probíhá přes P2P síť, není tak nutné mít přidělenou veřejnou statickou IP adresu a nakonfigurovaný NAT.

4.5 Popis LAN a koncových prvků ICT

Lokální síť provozovaná obchodní společností Taurus má přímý přístup k internetu, což bylo v této diplomové práci již zmíněno. Připojení k internetové síti je zajištěno optickým kabelem vyústěným v serverovně. Tento optický kabel představuje pomyslný vstup do opticko-metalického převodníku. Z tohoto převodníku již ústí UTP kabel do Wi-Fi routeru TP-Link, který reprezentuje mozek současné lokální sítě. K tomuto routeru je metalicky připojen server s operačním systémem Windows Server 2019 a již zmíněné NAS s NVR. Dále je to čtyřiadvacetiportový switch TP-Link, který zprostředkovává spojení routeru s dvanácti pracovními stanicemi (počítači), třemi síťovými multifunkčními tiskárnami, druhým NAS a již zmíněným PZTS, respektive s jeho ústřednou. Pro lepší orientaci je níže celá lokální síť graficky znázorněna a následně jsou blíže popsána zájmová chráněná aktiva,

respektive koncové prvky ICT. Závěrem je nutné dodat, že provozovaná LAN není momentálně spravována žádnou osobou.



Obrázek 36 Grafické znázornění provozované lokální sítě (yWorks, c2000-2023)

4.5.1 Wi-Fi router

V podmínkách předmětné lokální sítě je provozován Wi-Fi router TP-Link. Router má dle webových stránek výrobce nainstalovanou poslední verzi firmware. Dále je na tomto routeru aktivní VPN server za využití PPTP protokolu. Ten umožňuje vzdálené připojení k lokální síti. DHCP server je aktivní, a přiděluje tak k síti připojeným ICT prvkům automaticky IPv4 adresu, rezervační list pro DHCP službu neobsahuje žádnou vyjmutou IP adresu. Filtrování připojených zařízení dle MAC adres není aktivováno. Router má také nakonfigurovaný Port forwarding, ten umožňuje uživatelům internetu prohlížet veřejnou část webové aplikace společnosti, která běží na níže popsaném serveru. Přístup do webové aplikace a s ní související práce s daty je pak možná pouze z vnitřní lokální sítě, tedy i za využití technologie VPN. Router dále zajišťuje v budově A i bezdrátové připojení k internetu za využití bezdrátové technologie Wi-Fi a bezpečnostního protokolu WPA2.

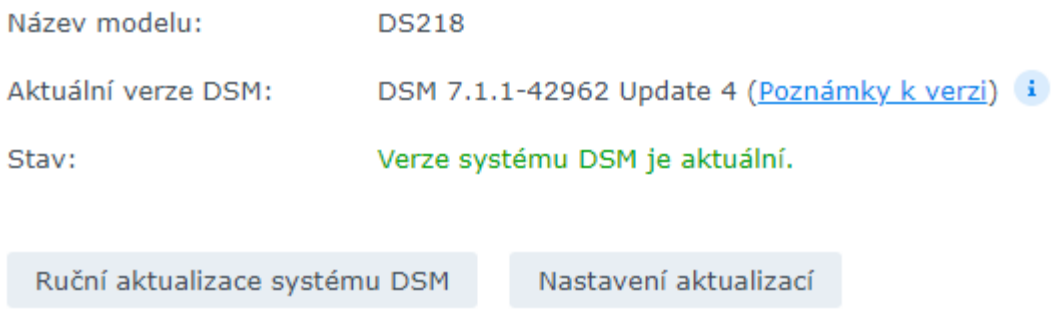
Přístup ke konfiguraci routeru je možný z lokální sítě a díky veřejné statické IP adrese i z internetu. K autentizaci je využíváno defaultní uživatelské jméno, heslo bylo změněno a splňuje obecné podmínky silného hesla. Na routeru není implementována žádná další bezpečností vrstva, jako je například demilitarizovaná zóna. Potencionální útočník tak může získat přístup ke všem prvkům ICT v lokální síti.

4.5.2 Server

Nepostradatelným zařízením je pak server Dell PowerEdge R250, osazený procesorem Intel Xeon E-2314 – 2.80 GHz 4 Core s nainstalovanou operační pamětí RAM 32 GB. Tento server zajišťuje provoz webové aplikace, která slouží ke každodennímu plnění pracovní náplně ze strany zaměstnanců. Dále zajišťuje provoz serverového softwaru Microsoft Exchange Server obsluhujícího poštovní zprávy. Operační systém běžící na tomto serveru je Windows Server 2019 a nechybí nainstalovaný antivirový program od společnosti ESET. Bootování je povoleno výhradně z vestavěného HDD disku. Přístup ke správě serveru je možný pouze přes pevně vestavěný administrátorský účet prostřednictvím Připojení ke vzdálené ploše (RDP), přístupové heslo splňuje obecné požadavky na sílu hesla. Záloha dat, konkrétně tedy SQL databáze je automaticky prováděna na síťové datové uložiště (NAS), pro účely této práce označováno jako NAS „A“.

4.5.3 Síťové datové uložiště „A“

Jak již bylo výše zmíněno, na toto NAS se automaticky pravidelně ukládají zálohy SQL databáze provozované pro správu dat webovou aplikací společnosti Taurus. Díky připojení k internetu má tento model Synology DiskStation DS218 aktuální operační systém, konkrétně DSM 7.1.1. Zařízení je osazeno dvěma HDD disky o kapacitě 4 TB, které se mezi sebou zrcadlí (RAID 1). Kapacita uložiště je využita z 15 %. Přístup je zajištěn dvěma účty. Jedná se o vestavěný účet administrátora se silným heslem a účet „zaloha“, který má povolen pouze zápis. Tento účet pak slouží k ukládání zálohy zmíněné SQL databáze. Služba QuickConnect, umožňující přístup k uložišti z internetu přes aplikaci třetí strany, není povolena.



Obrázek 37 Aktuální verze DSM síťového datového uložiště „A“ (Synology, 2023)

4.5.4 Síťové datové uložiště „B“

Operační systém DSM tohoto zařízení je také aktuální. Jedná se o stejný model Synology DiskStation DS218, jako výše uvedené. Toto datové uložiště je pak osazeno dvěma HDD disky o kapacitě 6 TB, také s nakonfigurovaným zrcadlením (RAID 1). Kapacita tohoto uložiště je pak jednak využívána k ukládání, respektive záloze obrazových záznamů z NVR a také k ukládání dat prostřednictvím osobních složek všech zaměstnanců. Přístup k NAS je tedy opět možný vestavěným účtem administrátora, účtem „kamery“ (sloužícím k záloze dat z NVR) a uživatelskými účty dle počtu zaměstnanců. Nutnost využívat silná hesla je v operačním systému DSM 7.1.1 samozřejmostí. Jednotlivé uživatelské účty zaměstnanců pak mají povolen zápis a čtení výhradně na osobní složku konkrétního zaměstnance. Služba QuickConnect je v tomto případě aktivní a využívána zaměstnanci pro vzdálený přístup k osobním složkám. Kapacita uložiště je momentálně využita z 51 %.

4.5.5 Pracovní stanice

V obchodní společnosti Taurus je k oblibě autora diplomové práce využívána unifikace. V praxi to znamená, že většina (v ideálním případě všechna) ICT zařízení jedné kategorie představují jeden a ten samý model.

Pevné pracovní stanice

V případě pevných pracovních stanic, počítačů, se jedná o modely Dell OptiPlex 3070 MT vybavené procesorem Intel Core i3 9100 Coffe Lake 4.2 GHz s instalovanou operační pamětí RAM 8 GB a SSD diskem 256 GB, kterých je v lokální síti dvanáct. Tyto modely splňují hardwarové podmínky pro instalaci operačního systému Windows 11. Díky neustálému připojení těchto počítačů k internetu je operační systém Windows 11 Pro prostřednictvím služby Windows Update nainstalován již na všech zařízeních. Antivirovou ochranu zajišťuje ESET, aktualizace virové databáze jsou automaticky stahovány z internetu. Přístup ke strojům je opět možný administrátorským účtem s poměrně slabým heslem a jedním uživatelským účtem s heslem, které obsahuje reálný název společnosti, což není vhodné. Vstup do BIOS, respektive rozhraní UEFI, není chráněn heslem. Zdroje, ze kterých lze bootovat, pak nejsou nijak omezeny. Verze rozhraní UEFI je paradoxně aktuální. Služba BitLocker umožňující šifrování disku není aktivována.

Výše popsaná zájmová chráněná aktiva, pevné pracovní stanice, jsou zaměstnanci firmy využívány zejména k práci ve společnosti provozovanou webovou aplikací. V neposlední řadě slouží k přístupu do osobních složek jednotlivých zaměstnanců. Osobní složky jsou pak v operačním systému připojeny jako síťové jednotky. S ohledem na skutečnost, že ke konkrétní pracovní stanici přistupují dva až tři zaměstnanci pod totožným uživatelským účtem, je provozované řešení přístupu k osobním složkám nevhodné.

Mobilní pracovní stanice

Používané mobilní stanice představují notebooky značky Lenovo, konkrétně se jedná o model ThinkPad E580, a mobilní telefony s datovou SIM kartou, umožňující připojení notebooků k internetu. Mobilní telefony však nebudou součástí posouzení kybernetických rizik vybrané společnosti. Počet výše uvedených notebooků je osmnáct a mají je k dispozici všichni zaměstnanci pracující převážně mimo areál společnosti Taurus. Tato zařízení jsou využívána k práci s webovou aplikací a také k přístupu do osobních složek zaměstnanců. Děje se tak za využití připojení prostřednictvím technologie VPN nebo aplikace QuickConnect. Popsané notebooky jsou osazeny procesorem Intel Core i3 8130U 2.2 GHz,

operační pamětí RAM 8 GB a SSD diskem 256 GB. Nechybí antivirová ochrana od společnosti ESET. Přístup je možný pouze jedním uživatelským účtem s rolí administrátora, tento účet je chráněn heslem. Mezi nedostatky patří přístup do BIOS, respektive rozhraní UEFI, který není chráněn heslem, možnost bootování z libovolného zařízení a neaktivní služba BitLocker.

Obrázek 38 Notebook Lenovo ThinkPad E580

4.5.6 Multifunkční tiskárny

V případě používaných tiskáren je díky jejich nedávné obměně a již zmíněné unifikaci využíváno stejných modelu. Konkrétně se jedná o tři multifunkční tiskárny Canon i-Sensys MF742Cdw, které jsou k síti připojeny UTP kabelem. Tisk a skenování dokumentů je možné provádět ze všech počítačů v síti, včetně těch, které jsou momentálně připojeny prostřednictvím technologie VPN. Firmware všech tří tiskáren je aktuální. Získání IP adresy pro konkrétní tiskárnu je nastaveno na automatický režim, tedy DHCP server. Případná administrace tiskáren není chráněna přístupovým PIN kódem.

5 IDENTIFIKACE KYBERNETICKÝCH HROZEB SPOLEČNOSTI TAURUS

K provedení analýzy a následnému hodnocení kybernetických rizik společnosti Taurus metodou FMEA je nejprve nutné této metodě jasně definovat možné vstupy. Tyto vstupy v praxi představují identifikované kybernetické hrozby. Cílem této kapitoly je tedy identifikovat možné kybernetické hrozby, konkrétně metodou brainwritingu. Takto identifikované možné kybernetické hrozby ohodnotit, respektive vyloučit ze seznamu ty, které nebudou v diplomové práci dále analyzovány, a z již ohodnoceného seznamu identifikovaných možných kybernetických hrozeb sestavit registr kybernetických hrozeb.

Pro potřebu této diplomové práce její autor metodu brainwritingu omezil na malý tým, skládající se z autora a dalších dvou kolegů z jeho zaměstnání. Na základě této metody je níže formou tabulky sestaven seznam možných identifikovaných kybernetických hrozeb společnosti Taurus. Tento seznam je pro lepší přehlednost rozčleněn na samostatné úseky:

a) fyzická bezpečnost chráněných aktiv,
b) administrace chráněných aktiv,
c) virtuální privátní síť,
d) drátová či bezdrátová lokální síť,
e) jednotlivé prvky ICT,
f) kamerový systém a
g) webová aplikace a SQL databáze.

Výše uvedené dílčí úseky jsou pak v diplomové práci jednotlivě analyzovány a hodnoceny. Návrh a aplikace opatření je opět pro přehlednost takto rozčleněna. Zde autor doplňuje, že cílem diplomové práce není identifikovat a dále analyzovat hrozby na úseku životnosti hardwaru a úmyslného i nedbalostního jednání uživatelů.

5.1 Identifikace možných hrozeb

Tabulka 1 Identifikace možných hrozeb

pořadové číslo	IDENTIFIKACE MOŽNÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
1.	povodeň	neurčena odpovědná osoba	využívání slabého (zastaralého) bezpečnostního protokolu	používání zastaralého bezpečnostního protokolu Wi-Fi	neaktuální BIOS/UEFI nebo firmware	používání defaultních přihlašovacích údajů	chybějící dvoufaktorová autentizace
2.	havárie vody	nevhodná odbornost určené osoby	neimplementovaný firewall	neaktivní filtrování bezdrátových zařízení dle MAC adres	neaktuální operační systém	využívání aplikací třetích stran	používání slabých hesel
3.	nadměrná vlhkost	nepravidelné vzdělávání určené osoby	možnost konfigurovat router přes webové rozhraní za využití veřejné statické IP adresy	aktivní DHCP server bez využití rezervačního listu	chybějící antivirový program	využívání P2P sítě	neošetřené vstupy (SQL injection)
4.	elektrický výboj	nepravidelná údržba LAN a prvků ICT	špatná delegace demilitarizovaných zón	přerušení metalického kabelu	neaktuální antivirový program	přerušení metalického kabelu	chybějící zálohování dat

pořadové číslo	IDENTIFIKACE MOŽNÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
5.	elektromagnetický výboj	nepravidelný monitoring LAN a prvků ICT	otevřené nepoužívané síťové TCP nebo UDP porty	rušení Wi-Fi signálu	nevhodná delegace přístupových účtů	chybějící záložní zdroj napájení (UPS)	chybějící šifrování databáze
6.	přepětí v elektrické síti	nepravidelné vyhodnocování logů	crackerský útok	crackerský útok	používání defaultních přístupových údajů	chybějící zálohování obrazových záznamů	chybějící šifrování (hashování) přihlašovacích údajů uživatelů
7.	nadměrná prašnost	neprovádění pravidelných aktualizací prvků ICT	infiltrace malware	infiltrace malware	používání slabých hesel		
8.	požár	nedostatečná pravidelná fyzická kontrola prvků ICT	chybějící online ochrana před kybernetickými útoky	chybějící online ochrana před kybernetickými útoky	crackerský útok		
9.	přehřátí prvků ICT			možnost konfigurovat router přes webové rozhraní za využití	infiltrace malware		

pořadové číslo	IDENTIFIKACE MOŽNÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
				veřejné statické IP adresy			
10.	neoprávněný vstup osob do serverovny			špatná delegace demilitarizovaných zón	chybějící zálohování dat		
11.	neoprávněný přístup osob k prvkům ICT			otevřené nepoužívané síťové TCP nebo UDP porty	chybějící záložní zdroj napájení (UPS)		
12.	chybějící záložní zdroj napájení (UPS)			nevhodný přístup k osobním složkám	nevhodný přístup k osobním složkám		
13.	přerušení metalického (optického) kabelu				BIOS/UEFI nechráněno heslem		
14.	chybějící zálohování dat				aktivní bootování z externích zařízení		

pořadové číslo	IDENTIFIKACE MOŽNÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
15.					neaktivní služba BitLocker		

5.2 Hodnocení možných identifikovaných hrozeb

V předchozí kapitole bylo identifikováno celkem 69 možných kybernetických hrozeb. Tyto hrozby byly pro přehlednost rozčleněny do sedmi dílčích úseků, jak již bylo úvodem této kapitoly avizováno. I přes toto rozčlenění však tvoří kybernetická bezpečnost společnosti Taurus funkční celek, proto se některé identifikované hrozby v jednotlivých dílčích úsecích navzájem překrývají a doplňují.

Po identifikaci možných hrozeb je níže ze strany autora diplomové práce provedeno jejich hodnocení. Následně jsou pro další potřebu vyloučeny hrozby, jejichž vznik je velmi nepravděpodobný, případně tyto hrozby nemohu být z objektivních důvodů v diplomové práci dále analyzovány. V tabulce níže jsou pak vyřazené možné hrozby uvedeny, včetně stručného odůvodnění.

Tabulka 2 Vyřazené možné hrozby

označení	možná hrozba	důvod vyřazení
1A	povodeň	V blízkosti areálu se nenachází žádný zdroj vody, areál společnosti Taurus je vyvýšený.
2A	havárie vody	Havárie vody se nepředpokládá, všechny prvky ICT jsou v dostatečné vzdálenosti od rozvodů vody.
3A	nadměrná vlhkost	Nadměrná vlhkost se v našich klimatických podmínkách nepředpokládá.
5A	elektromagnetický výboj	Elektromagnetický výboj se nepředpokládá, úmyslné zničení prvků ICT tímto způsobem není uvažováno.

označení	možná hrozba	důvod vyřazení
7A	nadměrná prašnost	Chybí zdroj nadměrného prachu.
2B	nevhodná odbornost určené osoby	Chráněná aktiva nejsou momentálně spravována žádnou osobou, nelze dále analyzovat.
3B	nepravidelné vzdělávání určené osoby	
3C	možnost konfigurovat router přes webové rozhraní za využití veřejné statické IP adresy	Tyto hrozby jsou dále analyzovány v dílčím úseku D.
5C	otevřené nepoužívané síťové TCP nebo UDP porty	
6C	crackerský útok	
7C	infiltrace malware	
8C	chybějící online ochrana před kybernetickými útoky	
4D	přerušení metalického kabelu	Tato hrozba je dále analyzována v dílčím úseku A.
5D	rušení Wi-Fi signálu	V okolí není provozována jiná Wi-Fi síť, úmyslné rušení se nepředpokládá.
10D	špatná delegace demilitarizovaných zón	Tato hrozba je dále analyzována na dílčím úseku C.
12D	nevhodný přístup k osobním složkám	Tato hrozba je dále analyzována na dílčím úseku E.
8E	crackerský útok	

označení	možná hrozba	důvod vyřazení
9E	infiltrace malware	Tyto hrozby jsou dále analyzovány v dílčím úseku D.
10E	chybějící zálohování dat	Tyto hrozby jsou dále analyzovány v dílčím úseku A.
11E	chybějící záložní zdroj napájení (UPS)	
4F	přerušení metalického kabelu	Tyto hrozby jsou dále analyzovány v dílčím úseku A.
5F	chybějící záložní zdroj napájení (UPS)	
6F	chybějící zálohování obrazových záznamů	
2G	používání slabých hesel	Databáze je zašifrována, nelze dále analyzovat.
3G	neošetřené vstupy (SQL injection)	
4G	chybějící zálohování dat	Tato hrozba je dále analyzována v dílčím úseku A.
6G	chybějící šifrování (hashování) přihlašovacích údajů uživatelů	Databáze je zašifrována, nelze dále analyzovat.

Na základě provedeného hodnocení možných identifikovaných kybernetických hrozeb je pro další potřebu diplomové práce, respektive pro následnou analýzu, vyřazeno celkem 27 možných hrozeb. Tabulka níže pak prezentuje registr kybernetických hrozeb, které budou v diplomové práci dále analyzovány, tedy ty, které byly výše provedeným hodnocením přijaty.

5.3 Registr kybernetických hrozeb

Tabulka 3 Registr kybernetických hrozeb

pořadové číslo	REGISTR KYBERNETICKÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
1.	elektrický výboj	neurčena odpovědná osoba	využívání slabého (zastaralého) bezpečnostního protokolu	používání zastaralého bezpečnostního protokolu Wi-Fi	neaktuální BIOS/UEFI nebo firmware	používání defaultních přihlašovacích údajů	chybějící dvoufaktorová autentizace
2.	přepětí v elektrické síti	nepravidelná údržba LAN a prvků ICT	neimplementovaný firewall	neaktivní filtrování bezdrátových zařízení dle MAC adres	neaktuální operační systém	využívání aplikací třetích stran	chybějící šifrování databáze
3.	požár	nepravidelný monitoring LAN a prvků ICT	špatná delegace demilitarizovaných zón	aktivní DHCP server bez využití rezervačního listu	chybějící antivirový program	využívání P2P sítě	
4.	přehřátí prvků ICT	nepravidelné vyhodnocování logů		crackerský útok	neaktuální antivirový program		
5.	neoprávněný vstup osob do serverovny	neprovádění pravidelných aktualizací prvků ICT		infiltrace malware	nevhodná delegace přístupových účtů		

pořadové číslo	IDENTIFIKACE MOŽNÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
6.	neoprávněný přístup osob k prvkům ICT	nedostatečná pravidelná fyzická kontrola prvků ICT		chybějící online ochrana před kybernetickými útoky	používání defaultních přístupových údajů		
7.	chybějící záložní zdroj napájení (UPS)			možnost konfigurovat router přes webové rozhraní za využití veřejné statické IP adresy	používání slabých hesel		
8.	přerušení metalického (optického) kabelu			otevřené nepoužívané síťové TCP nebo UDP porty	nevhodný přístup k osobním složkám		
9.	chybějící zálohování dat				BIOS/UEFI nechráněno heslem		

pořadové číslo	REGISTR KYBERNETICKÝCH HROZEB NA DÍLČÍM ÚSEKU						
	A. fyzická bezpečnost chráněných aktiv	**B. administrace chráněných aktiv**	**C. VPN**	**D. LAN / WLAN**	**E. prvky ICT**	**F. kamerový systém**	**G. webová aplikace a SQL databáze**
10.					aktivní bootování z externích zařízení		
11.					neaktivní služba BitLocker		

6 ANALÝZA A HODNOCENÍ KYBERNETICKÝCH RIZIK

Cílem této kapitoly je na základě výše prezentovaného registru kybernetických hrozeb provést analýzu a hodnocení kybernetických rizik. K tomu je využitá metoda FMEA rozčleněna na zmíněných sedm úseků. Z výsledků provedené analýzy je pak na základě podmínky přijatelnosti sestaveno sedm modifikovaných matic kybernetických rizik na dílčích úsecích. Takto sestavené modifikované matice kybernetických rizik jsou prezentovány níže a zobrazují ve smyslu současného stavu kybernetické bezpečnosti pouze významná a závažná rizika. Kompletní analýza kybernetických rizik metodou FMEA je samozřejmě součástí příloh.

6.1 Podmínka přijatelnosti

Podmínka přijatelnosti je dána samotnou metodou FMEA, respektive jejím rizikovým číslem vypočteným jako součin závažnosti, výskytu a odhalení příslušné hrozby. Pro další potřebu autor diplomové práce rozčlenil zjištěná rizika do tří skupin tak jako v jeho původní bakalářské práci, neboť se mu toto dělení několikrát osvědčilo. Intervaly rizikového čísla jsou pak z původní bakalářské práce zobrazeny níže formou obrázku. S výpočtem jednotlivých mezí intervalů rizikového čísla lze čtenáře opět odkázat na autorovu původní bakalářskou práci, kde je tento výpočet kompletně popsán.

Slovní hodnocení	Rizikové číslo
Zanedbatelné riziko	1 až 125
Významné riziko	126 až 613
Závažné riziko	614 až 1000

Obrázek 39 Intervaly rizikového čísla (Hájek, 2021)

Níže zpracované modifikované matice kybernetických rizik zároveň prezentují konkrétní doporučená opatření a prostřednictvím kódového označení odkazují na jejich aplikaci. Tato je následně zpracována v následující kapitole Aplikace navržených opatření.

6.2 Matice kybernetických rizik na úseku fyzické bezpečnosti chráněných aktiv

Tabulka 4 Matice kybernetických rizik na úseku fyzické bezpečnosti chráněných aktiv

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
požár	poškození prvků ICT, ztráta SW, ztráta dat	175	instalace (přidání) kouřových detektorů ke stávajícímu PZTS	autorem diplomové práce nelze aplikovat	125
neoprávněný vstup osob do serverovny	neoprávněná manipulace s prvky ICT	150	vytvoření samostatné sekce v rámci stávajícího PZTS, jasná delegace oprávnění ke vstupu jednotlivých osob		64

6.3 Matice kybernetických rizik na úseku administrace chráněných aktiv

Tabulka 5 Matice kybernetických rizik na úseku administrace chráněných aktiv

<table>
<tr><th colspan="3">SOUČASNÝ STAV</th><th colspan="3">DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ</th></tr>
<tr><th>možná chyba</th><th>možný následek chyby</th><th>rizikové číslo</th><th>doporučené opatření</th><th>aplikace doporučeného opatření</th><th>rizikové číslo</th></tr>
<tr><td>neurčena odpovědná osoba</td><td>nelze reagovat na dění v LAN</td><td>720</td><td rowspan="6">určit (zaměstnat) správce IT s vhodnou odbornou kvalifikací, vypracovat náplň práce pro tuto pozici</td><td rowspan="6">autorem diplomové práce nelze aplikovat</td><td>100</td></tr>
<tr><td>nepravidelná údržba LAN a prvků ICT</td><td>přímé ohrožení kybernetickými útoky, ztráta dat, zašifrování dat, fyzické zničení prvků ICT</td><td>700</td><td>144</td></tr>
<tr><td>nepravidelný monitoring LAN a prvků ICT</td><td rowspan="2">chybějící historická data, chybějící povědomí o dění v LAN</td><td>700</td><td>144</td></tr>
<tr><td>nepravidelné vyhodnocování logů</td><td>490</td><td>80</td></tr>
<tr><td>neprovádění pravidelných aktualizací prvků ICT</td><td>přímé ohrožení kybernetickými útoky, ztráta dat, zašifrování</td><td>250</td><td>54</td></tr>
</table>

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
nedostatečná pravidelná fyzická kontrola prvků ICT	dat, fyzické zničení prvků ICT	200			36

6.4 Matice kybernetických rizik na úseku technologie VPN

Tabulka 6 Matice kybernetických rizik na úseku technologie VPN

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
využívání slabého (zastaralého) bezpečnostního protokolu	získání přístupu do lokální sítě, přímé ohrožení kybernetický-mi útoky	700	změna využívaného protokolu, změna routeru	AO-C1	150
neimplementova-ný firewall		700	změna routeru, nebo přidání firewallu	AO-C2	100

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
špatná delegace demilitarizova-ných zón	vzdálený přístup k celé lokální síti	350	konfigurace demilitarizo-vaných zón, jasné stanovení přístupů přes technologii VPN	AO-C3	60

6.5 Matice kybernetických rizik na úseku LAN/WLAN

Tabulka 7 Matice kybernetických rizik na úseku LAN/WLAN

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
používání zastaralého bezpečnostního protokolu Wi-Fi	využití známé slabiny k průniku do sítě ze strany crackera	800	konfigurace protokolu WPA3, případně změna routeru podporujícího tento	AO-D1	180

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
			bezpečnostní protokol		
neaktivní filtrování bezdrátových zařízení dle MAC adres	nekontrolované připojení bezdrátového zařízení	320	aktivování filtrování bezdrátových zařízení dle MAC adres	AO-D2	100
aktivní DHCP server bez využití rezervačního listu	nedostupnost prvků ICT při změně IP adresy	336	aktivování rezervačního DHCP listu, vložení serveru, tiskáren, NAS a NVR	AO-D3	60
crackerský útok	zničení, nedostupnost prvků ICT, ztráta dat, zašifrování dat, ztráta SW	720	změna routeru (router s FW a online ochranou před kybernetic-kými útoky)	AO-D4	150
infiltrace malware		720			150
chybějící online ochrana před kybernetickými útoky		640			120

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
možnost konfigurovat router přes webové rozhraní za využití veřejné statické IP adresy	využití známé slabiny k průniku do sítě ze strany crackera	900			100
otevřené nepoužívané síťové TCP nebo UDP porty		720			80

6.6 Matice kybernetických rizik na úseku prvků ICT

Tabulka 8 Matice kybernetických rizik na úseku prvků ICT

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
používání defaultních	neoprávněný přístup	640	změna přihlašovacích údajů	AO-E1	125

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
přihlašovacích údajů	k prvkům ICT,				
používání slabých hesel	neoprávněná konfigurace prvků ICT	480	změna používaných hesel v souladu s podmínkami na silné heslo	AO-E2	125
nevhodný přístup k osobním složkám	neoprávněný přístup k uloženým datům	640	vzdálené připojování výhradně prostřednictvím technologie VPN, vytvoření okenní aplikace zajišťující připojení k osobní složce	AO-E3	128
BIOS/UEFI nechráněno heslem	neoprávněný přístup ke konfiguraci prvků ICT	630	zaheslování BIOS/UEFI	AO-E4	96
aktivní bootování z externích zařízení		700	deaktivování bootování z externích zařízení	AO-E5	100

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
neaktivní služba BitLocker	neoprávněný přístup k datům	700	aktivování služby BitLocker	AO-E6	100

6.7 Matice kybernetických rizik na úseku kamerového systému

Tabulka 9 Matice kybernetických rizik na úseku kamerového systému

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
používání defaultních přihlašovacích údajů	neoprávněný přístup k NVR	640	změna přihlašovacích údajů	AO-F1	125
využívání aplikací třetích stran	neoprávněný přístup k obrazovým záznamům, únik obrazových záznamů	200	přístup ke kamerovému systému výhradně prostřednictvím technologie VPN	AO-F2	80
využívání P2P sítě		175			80

6.8 Matice kybernetických rizik na úseku provozu webové aplikace a SQL databáze

Tabulka 10 Matice kybernetických rizik na úseku provozu webové aplikace a SQL databáze

SOUČASNÝ STAV			DOPORUČENÍ A APLIKACE OPATŘENÍ, STAV PO APLIKACI OPATŘENÍ		
možná chyba	**možný následek chyby**	**rizikové číslo**	**doporučené opatření**	**aplikace doporučeného opatření**	**rizikové číslo**
chybějící dvoufaktorová autentizace	neoprávněný přístup k webové aplikace	200	nasadit dvoufaktorovou autentizaci	autorem diplomové práce nelze aplikovat	125

7 APLIKACE NAVRŽENÝCH OPATŘENÍ

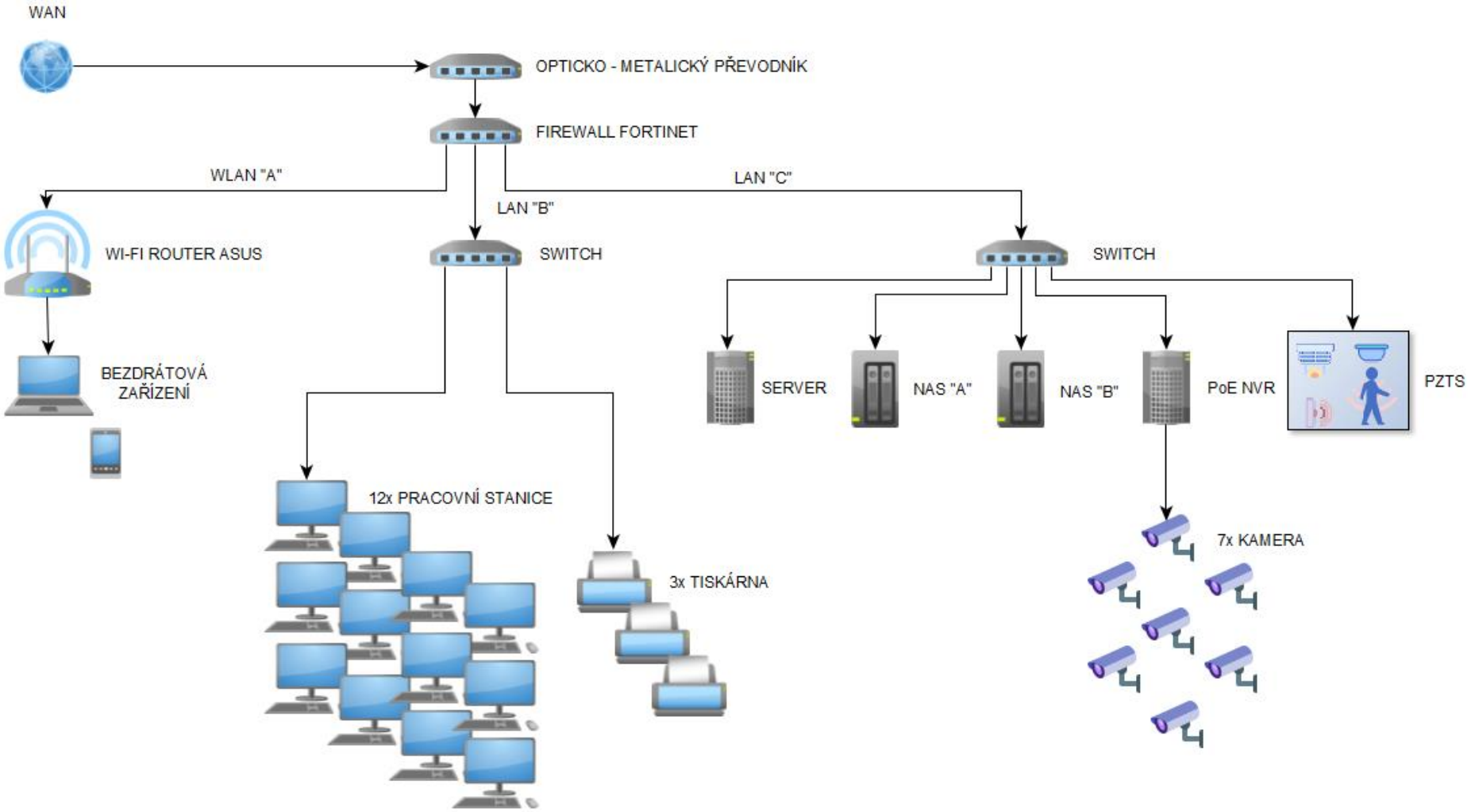
Před samotnou aplikací jednotlivých opatření je nezbytné na celou lokální síť nahlédnout jako na funkční celek. Provedenou analýzou byly zjištěny ty nejzávažnější nedostatky na úseku provozování samotné lokální sítě, která má zajištěn přístup k internetu prostřednictvím routeru, který nenabízí dostatečný způsob zabezpečení. Příkladem lze uvést chybějící bezpečnostní protokol WPA3 nutný k bezpečnému provozu Wi-Fi sítě nebo možný přístup do lokální sítě prostřednictvím technologie VPN za využívání zastaralého bezpečnostního protokolu PPTP.

K zabezpečení lokální sítě a koncových prvků ICT je tak nutné pořídit modernější zařízení. Po projednání konkrétních bezpečnostních opatření a schválení finančních prostředků ze strany majitele společnosti Taurus (viz předběžné vyčíslení nákladů) byla aplikace všech opatření odsouhlasena. V praxi se pak jedná o nákup desktopového firewallu Fortinet FortiGate FG-40F včetně licencí zajišťujících nepřetržitou online ochranu provozované sítě.

Druhou významnou položkou nákupního seznamu je pak Wi-Fi router Asus TUF-AX3000 V2. Ten byl vybrán z důvodu, že za příznivou cenu nabízí velmi slušný výkon, má implementovaný firewall, podporuje bezpečnostní protokol WPA3 a v neposlední řadě nabízí bezplatnou celoživotní licenci AiProtection. Tato licence pak obdobně jako výše zmíněná licence FortiGuard od společnosti Fortinet zvyšuje kybernetickou bezpečnost k síti připojeným zařízením. Jedná se například o implementovanou ochranu před DoS útoky a automatické blokování škodlivých webů.

Původní lokální síť je pak nejenom z bezpečnostních důvodů rozčleněna na tři samostatné lokální sítě, které mezi sebou mají jasně definovaná pravidla provozu. Z LAN (WLAN) „A“, jejímž mozkem je nově zakoupený Wi-Fi router Asus, je možné přistupovat pouze k internetu, není tak možné navázat komunikaci s LAN „B“ a „C“. Prostřednictvím VPN je zase možné přistupovat pouze do LAN „C“, a to konkrétně jen k webové aplikaci, síťovému datovému uložišti „B“ s osobními složkami zaměstnanců a kamerovému systému. Vzhledem k velmi obsáhlé konfiguraci nově zakoupených zařízení jsou níže popsána pouze dílčí nastavení plynoucí ze samotné analýzy, nikoli kompletní konfigurace firewallu a routeru.

Pro lepší orientaci čtenáře je níže graficky znázorněno nové řešení provozované lokální sítě (sítí) obchodní společnosti Taurus.



Obrázek 40 Grafické znázornění nového řešení lokální sítě (yWorks, c2000-2023)

7.1 Předběžné vyčíslení nákladů

V tabulce níže jsou hrubě vyčísleny náklady na autorem diplomové práce aplikovaná opatření. V těchto nákladech nejsou zahrnuta opatření, která není ze strany autora diplomové práce možné aplikovat. Jmenovitě se jedná o opatření na úseku fyzické bezpečnosti chráněných aktiv, kdy je nutné provést zásah do provozovaného PZTS, jakožto uzavřeného systému od společnosti Jablotron. Dále se jedná o aplikaci opatření na úseku administrace chráněných aktiv, kdy je nutné zaměstnat IT technika starajícího se o provozovanou síť. Tento personální krok byl majiteli obchodní společnosti doporučen, avšak ze strany autora diplomové práce nelze dále zabezpečit. Do třetice se jedná o nasazení dvoufaktorové autentizace do provozované webové aplikace, což může učinit pouze její vývojář. Toto doporučení bylo majiteli společnosti taktéž navrženo.

Tabulka 11 Předběžné vyčíslení nákladů

IT ÚKON, NÁKUP HW, NÁKUP SW	MINIMÁLNÍ MOŽNÁ CENA (BEZ DPH)	MAXIMÁLNÍ MOŽNÁ CENA (BEZ DPH)
Wi-Fi router Asus TUF-AX3000 v2	2 289 Kč	3 121 Kč
konfigurace routeru	bezúplatně autorem diplomové práce	
firewall Fortinet FortiGate FG-40F s licencemi FortiCare a FortiGuard Unified Threat Protection	66 383 Kč	66 383 Kč
konfigurace firewallu	bezúplatně autorem diplomové práce	
switch TP-LINK TL-SG105	364 Kč	560 Kč
UTP kabel, CAT6, 50 metrů	823 Kč	1 055 Kč
konektory RJ-45, CAT6, 50 kusů	95 Kč	115 Kč
natažení kabeláže a osazení konektorů	bezúplatně autorem diplomové práce	

IT ÚKON, NÁKUP HW, NÁKUP SW	MINIMÁLNÍ MOŽNÁ CENA (BEZ DPH)	MAXIMÁLNÍ MOŽNÁ CENA (BEZ DPH)
vytvoření okenní aplikace zajišťující připojení k osobní složce zaměstnance		
další nezbytná konfigurace ICT prvků		
Cena celkem	**69 954 Kč**	**71 234 Kč**

7.2 Aplikace opatření na úseku technologie VPN

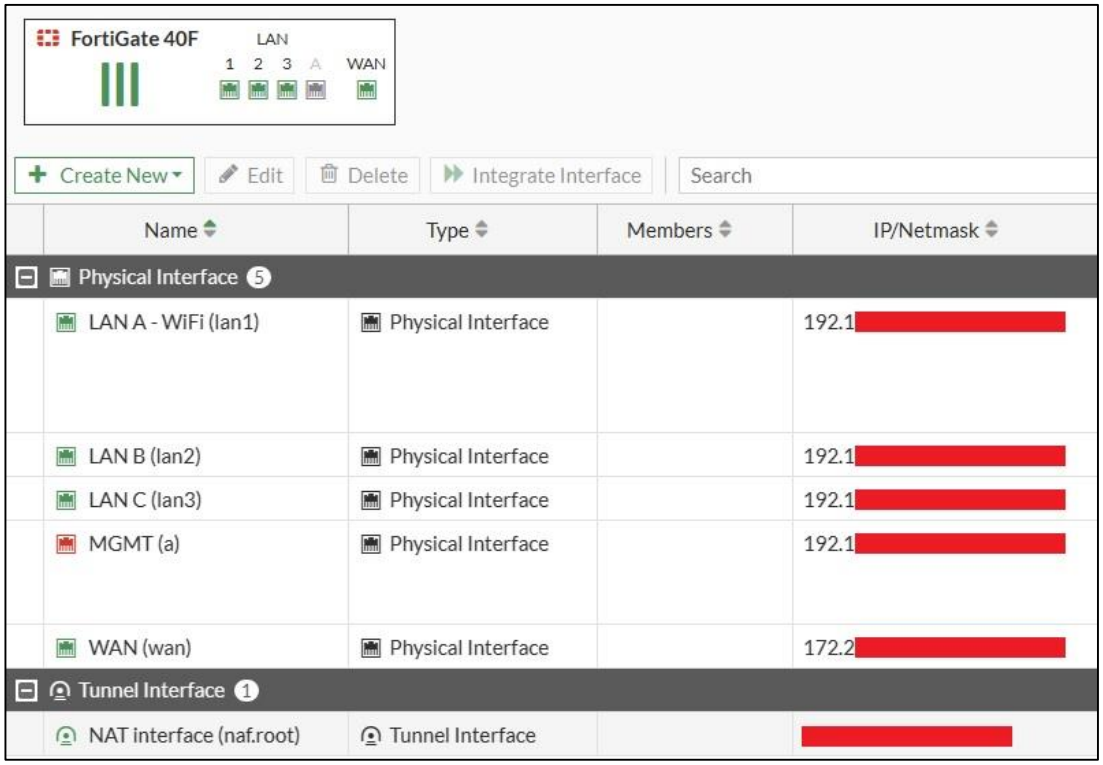
Aplikace opatření AO-C1 a AO-C2

Aplikace těchto dvou opatření spolu velmi úzce souvisí. Cílem je změnit využívaný slabý bezpečnostní protokol technologie VPN, konkrétně PPTP, a implementovat firewall. K tomuto účelu byl zakoupen desktopový firewall Fortinet FortiGate FG-40F včetně licencí zajišťujících nepřetržitou online ochranu provozované sítě. Na obrázku níže je pak zakoupený firewall již nakonfigurovaný a provozovaný.

Obrázek 41 Firewall Fortinet FortiGate FG-40F

Na port 1 je v souladu s návrhem nového řešení nakonfigurovaná LAN (WLAN) „A“, jejíž provoz zajišťuje nově zakoupený Wi-Fi router Asus. Port 2 zabezpečuje provoz „uživatelské“ LAN „B“. Tato síť pomocí na obrázku viditelného switche zajišťuje síťové

spojení dvanácti pracovních stanic a tří tiskáren. Na Port 3 předmětného firewallu je pak nakonfigurována třetí LAN (LAN „C“). V té se nachází server, na kterém běží potřebné služby, dvě síťová datová uložiště, NVR a ústředna PZTS. Do této LAN, konkrétně tedy k webové aplikaci, uložišti s osobními složkami zaměstnanců a NVR, je pak možný přístup přes nově nakonfigurovanou SSL VPN. Tunel VPN je pak vytáčený z klientské aplikace společnosti Fortinet přímo na veřejnou statickou IP adresu nově zakoupeného firewallu, kde je dále nakonfigurovaná dvoufaktorová autentizace. S ohledem na kybernetickou bezpečnost společnosti Taurus nelze v rámci těchto dvou opatření blíže popsat konkrétní konfiguraci firewallu. Na obrázku níže je výše popsaná konfigurace znázorněna. Nakonfigurované IP adresy jsou z důvodu zajištění kybernetické bezpečnosti znečitelněny.

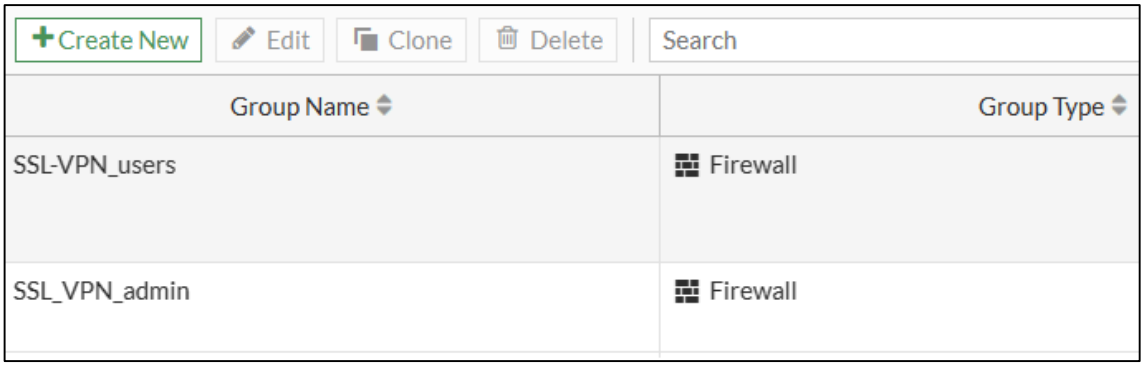


Obrázek 42 Interface na firewallu (Fortinet, 2023)

Aplikace opatření AO-C3

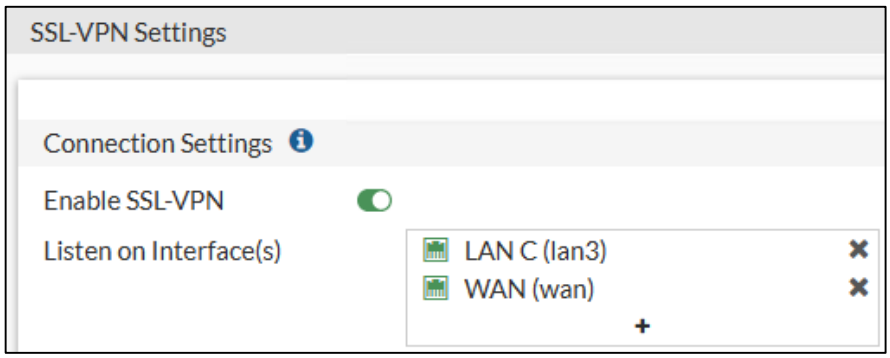
Předmětem tohoto opatření je nakonfigurování DMZ a jasné stanovení přístupů jednotlivých uživatelů přes technologii VPN do lokální sítě společnosti Taurus. K tomuto účelu autor diplomové práce vytvořil dvě uživatelské skupiny, tedy administrátory a uživatele. Tuto konfiguraci provedl v záložce User & Authentication. Výsledek je pak znázorněn na

obrázku. V téže záložce dále vytvořil uživatelské účty dle příjmení zaměstnanců společnosti Taurus a přiřadil jim členství ve skupině SSL-VPN_users.



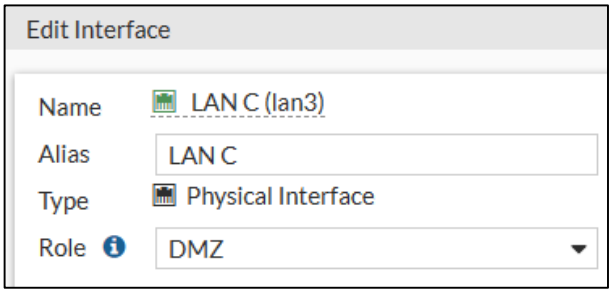
Obrázek 43 Uživatelské skupiny na firewallu (Fortinet, 2023)

V záložce VPN dále autor diplomové práce povolil přístup prostřednictvím technologie VPN pouze do LAN „C“, kde jsou umístěny pouze prvky ICT, ke kterým je vzdálený přístup nutný. K funkčnosti tohoto nastavení je nutné povolit také přístup z WAN, viz obrázek níže.



Obrázek 44 Nastavení přístupu VPN na firewallu do LAN „C“ (Fortinet, 2023)

Role DMZ pro LAN „C“ je pak nejjednodušší nastavit v záložce Network. Zde autor diplomové práce pro výše uvedenou LAN „C“ změnil roli z původní role LAN na roli DMZ.



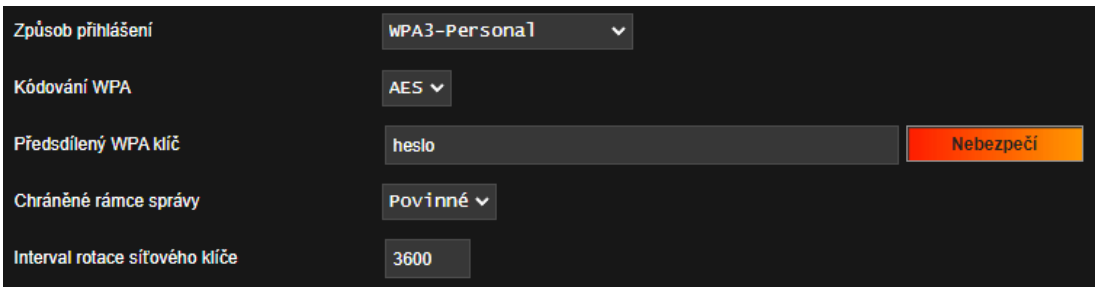
Obrázek 45 Změna role LAN na roli DMZ u LAN „C“ (Fortinet, 2023)

Zde autor diplomové práce považuje za nutné znovu zopakovat, že výše uvedená konfigurace firewallu netvoří funkční celek. Jedná se pouze o dílčí nastavení plynoucí z provedené analýzy. Kompletní konfigurace firewallu je několikanásobně krát rozsáhlejší, a tudíž zde není obsažena.

7.3 Aplikace opatření na úseku LAN/WLAN

Aplikace opatření AO-D1

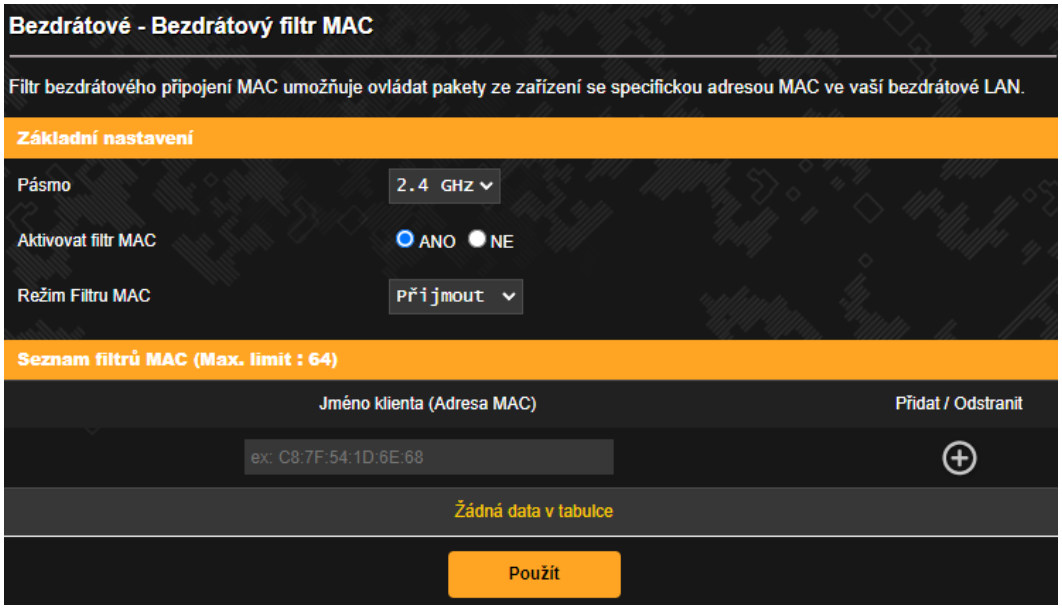
Cílem tohoto opatření je u nově zakoupeného Wi-Fi routeru Asus nakonfigurovat Wi-Fi síť za využití bezpečnostního protokolu WPA3. K tomu je nutné v konfiguraci routeru přejít do pokročilých nastavení a vybrat záložku Bezdrátové. Zde je nutné vyplnit SSID (název nové Wi-Fi sítě), jako způsob přihlášení zvolit WPA3-Personal, kódování WPA nastavit na AES, vyplnit WPA klíč (heslo k Wi-Fi síti) dle obecných zásad bezpečného hesla a povolit Smart Connect umožňující provoz Wi-Fi na 2,4 GHz i 5 GHz. Šířku pásma kanálu i kanál samotný ponechal autor diplomové práce na automatickém režimu (v okolí není provozována jiná Wi-Fi síť a nepředpokládá se tudíž rušení signálu). Dále je povolen režim Wi-Fi 6, ostatní položky jsou ponechány na výchozích hodnotách. Toto nastavení je závěrem nutné potvrdit tlačítkem Použít.



Obrázek 46 Výstřižek konfigurace Wi-Fi na Wi-Fi routeru (Asus, 2023)

Aplikace opatření AO-D2

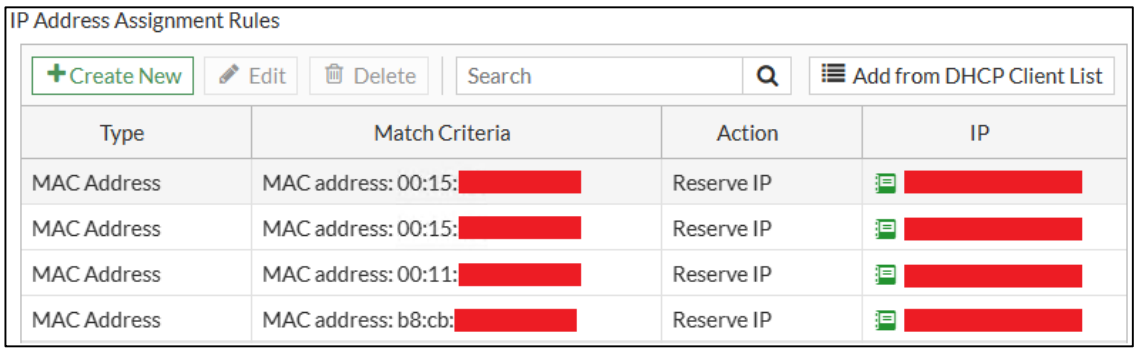
Aktivace filtrování připojených bezdrátových zařízení dle MAC adres se provádí také v záložce Bezdrátové, konkrétně v podzáložce Bezdrátový filtr MAC. Zde stačí pouze vybrat pásmo 2,4 GHz nebo 5GHz (autor diplomové práce doporučuje obě), aktivovat filtr MAC a nastavit režim filtrace na Přijmout. Následně stačí do Seznamu filtrů MAC zadat konkrétní MAC adresy, které se budou k Wi-Fi síti připojovat.



Obrázek 47 Výstřižek konfigurace filtrování připojených bezdrátových zařízení dle MAC adres na Wi-Fi routeru (Asus, 2023)

Aplikace opatření AO-D3

Pro aktivování rezervačního DHCP listu na firewallu autor diplomové práce využil záložku Interface. Zde aktivoval DHCP server a nastavil konkrétní rozsah IP adres, které lze zařízením v síti přidělit. Následně pro vybraná zařízení rezervoval konkrétní IP adresu vázanou na MAC adresu konkrétního zařízení. Na obrázku níže jsou během samotné konfigurace takto rezervovány již čtyři IP adresy. Jedná se o server, NVR a dvě NAS. Konkrétní MAC a IP adresy jsou samozřejmě znečitelněny.



Obrázek 48 Výstřižek rezervačního listu DHCP serveru na firewallu (Fortinet, 2023)

Aplikace opatření AO-D4

Toto opatření představuje změnu dosud používaného Wi-Fi routeru. Což již bylo na úseku drátové sítě aplikováno prostřednictvím opatření AO-C2. Zde byl zakoupen a autorem

diplomové práce nakonfigurován desktopový firewall Fortinet FortiGate FG-40F včetně licencí zajišťujících nepřetržitou online ochranu provozované sítě.

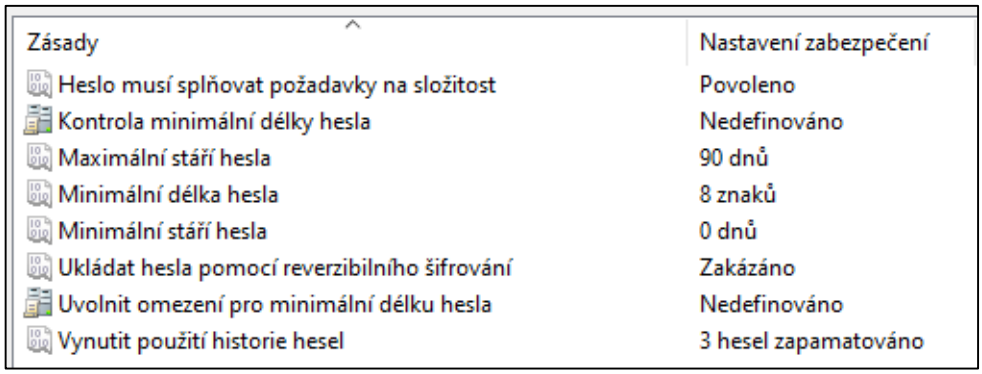
Na úseku bezdrátové sítě se pak jedná o nákup nového Wi-Fi routeru ASUS TUF-AX3000 v2 podporujícího nejmodernější bezpečnostní protokol WPA3. Samozřejmostí je online ochrana před kybernetickými útoky, o čemž bylo blíže pojednáno úvodem této kapitoly.

Obrázek 49 Router ASUS TUF-AX3000 v2

7.4 Aplikace opatření na úseku prvků ICT

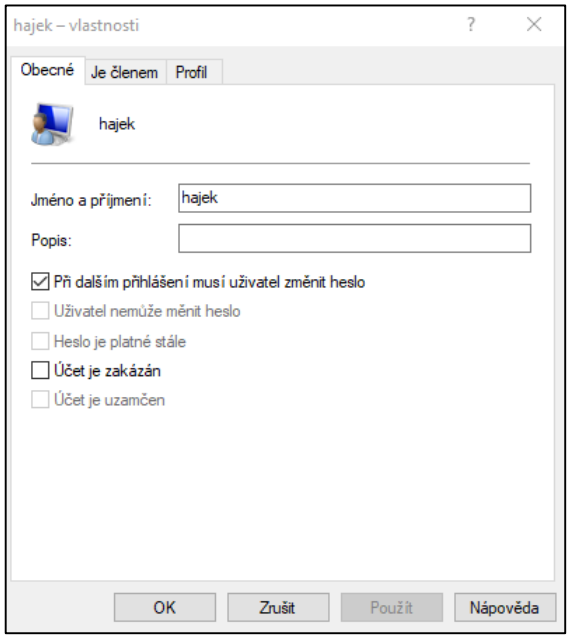
Aplikace opatření AO-E1 a AO-E2

Změnu defaultních přihlašovacích údajů, respektive v minulosti administrátorem zadaným heslem k uživatelským účtům na pracovních stanicích (pevných i mobilních), které obsahuje název společnosti, je nutné provést účtem administrátora. Nejprve je však důležité nastavit bezpečnostní politiku, která uživateli vynutí jisté bezpečnostní požadavky na heslo. Toto nastavení lze provést v Editoru zásad skupiny (gpedit.msc), zde autor diplomové práce upozorňuje, že se jedná o operační systém Windows 11. V Editoru zásad skupiny se jedná o posloupnost následujících záložek: Konfigurace počítače, Nastavení systému Windows, Nastavení zabezpečení, Zásady účtů, Zásady hesla. V Zásadách hesla se nachází celkem osm bezpečnostních politik, které lze různě nakonfigurovat. Pro účely společnosti Taurus postačí povolit bezpečnostní politiku Heslo musí splňovat požadavky na složitost, což vynutí povinnost, aby heslo obsahovalo velká i malá písmena, číslice a speciální znaky. Dále je nutné Minimální délku hesla nakonfigurovat na osm znaků a Maximální stáří hesla nastavit na 90 dnů. Co se týče historie používaných hesel, obecně se doporučuje nastavit tři.



Obrázek 50 Nastavení zásad hesla ve Windows 11 (Microsoft, 2022)

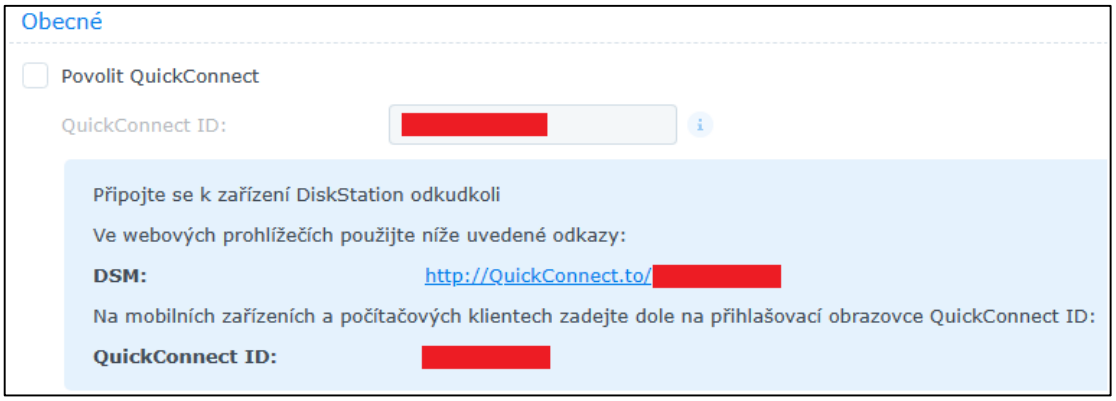
Po výše uvedené konfiguraci je dále nutné ve Správě počítače konkrétnímu uživateli vynutit změnu hesla při příštím přihlášení, čímž je aplikace těchto dvou opatření dokončena.



Obrázek 51 Vynucení změny hesla při příštím přihlášení ve Windows 11 (Microsoft, 2022)

Aplikace opatření AO-E3

Ke zvýšení účinnosti tohoto opatření nejprve autor diplomové práce v ovládacích panelech NAS Synology, v záložce Externí přístup, deaktivoval službu QuickConnect. Tato služba umožňuje prostřednictvím technologie třetí strany navázat připojení k NAS z internetu (WAN), což není s ohledem na potencionální únik informací vhodné.



Obrázek 52 Deaktivace služby QuickConnect na NAS (Synology, 2023)

Následně autor diplomové práce za využití znalostí v oblasti objektově orientovaného programování v programovacím jazyku C# naprogramoval okenní aplikaci pro OS Windows. Tato desktopová aplikace umožňuje každému zaměstnanci navázat spojení se svou osobní složkou, a to jak z lokální sítě, tak za využití připojení prostřednictvím technologie VPN z internetu. K naprogramování aplikace bylo využito vývojové prostředí Microsoft Visual Studio Community 2022 a open-source framework .NET 6.0.

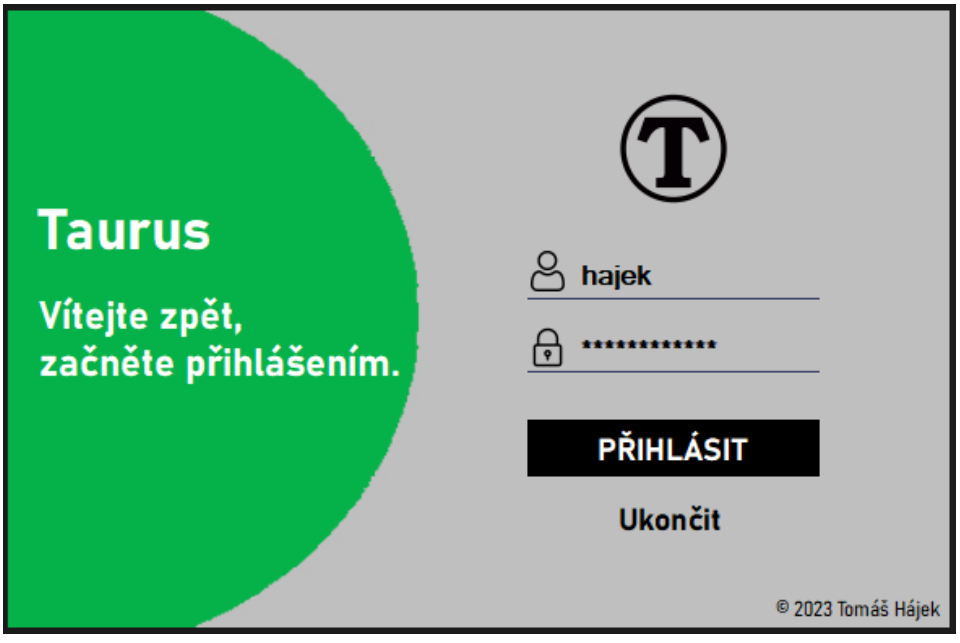
```
namespace Taurus
{
    Počet odkazů: 0
    internal class StatusServeru
    {
        Počet odkazů: 2
        public bool ServerBezi { get; private set; }

        Počet odkazů: 0
        public void OverStatusServeru()
        {
            Ping ping = new Ping();
            PingReply pingReply = ping.Send("0.0.0.0", 1500);
            if (pingReply.Status == IPStatus.Success)
            {
                ServerBezi = true;
            }
            else
            {
                ServerBezi = false;
                ChyboveHlaseni chyboveHlaseni = new ChyboveHlaseni();
            }
        }
    }
}
```

Obrázek 53 Ukázka zdrojového kódu naprogramované okenní aplikace, třída StatusServeru (Microsoft, 2022)

```
namespace Taurus
{
    Počet odkazů: 1
    class Uzivatel
    {
        Počet odkazů: 1
        public string Jmeno { get; private set; }
        Počet odkazů: 1
        public string Heslo { get; private set; }
        Počet odkazů: 1
        public string NazevOsobniSlozky { get; private set; }
        Počet odkazů: 0
        public Uzivatel(string jmeno, string heslo)
        {
            Jmeno = jmeno;
            Heslo = heslo;
            NazevOsobniSlozky = jmeno.ToLower();
        }
    }
}
```

Obrázek 54 Ukázka zdrojového kódu naprogramované okenní aplikace, třída Uzivatel (Microsoft, 2022)

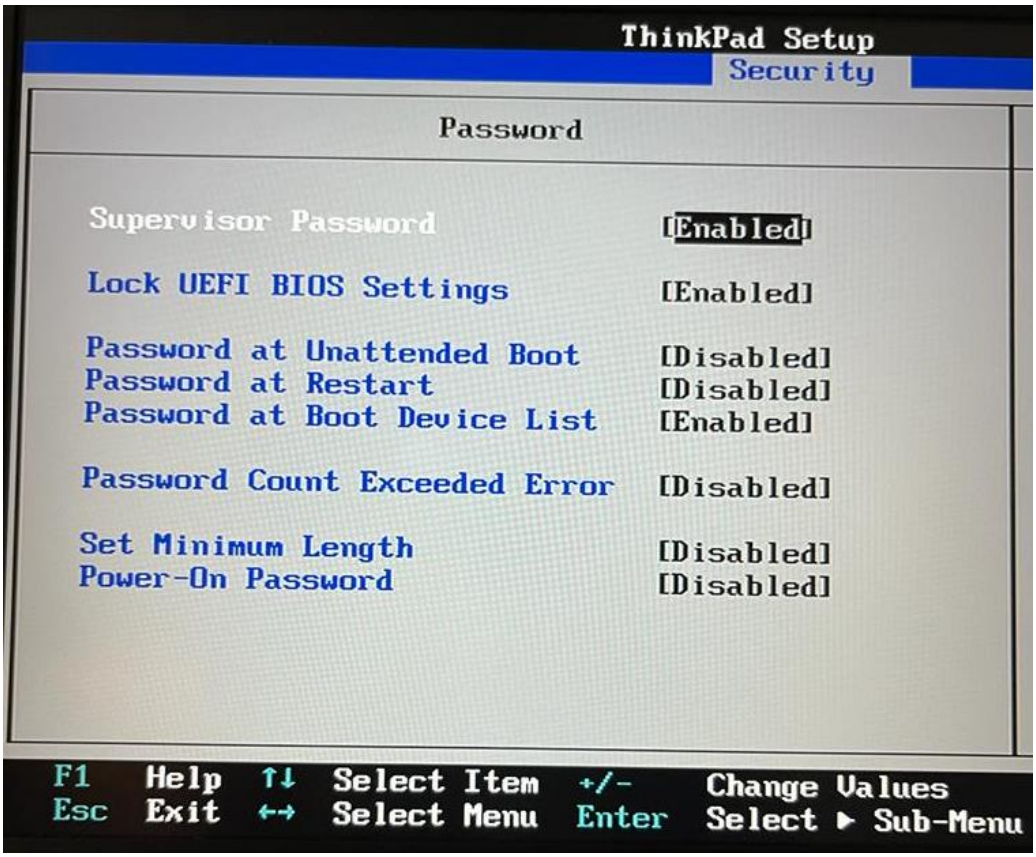
Okenní aplikace nejdříve ověří dostupnost NAS příkazem ping. V kladném případě provede validaci uživatelských vstupů a na základě správně zadaného uživatelského jména (příjmení zaměstnance) a hesla připojí uživateli osobní složku prostřednictvím Průzkumníka souborů implementovaného v OS Windows. Na obrázku níže je tato okenní aplikace zobrazena ve finální a plně funkční podobě. Reálný název společnosti i její logo bylo pro účely diplomové práce opět změněno.



Obrázek 55 Naprogramovaná okenní aplikace

Aplikace opatření AO-E4 a AO-E5

Zaheslování BIOS (v případě počítačů a notebooků společnosti Taurus již rozhraní UEFI) a deaktivování bootování z externích zařízení se konkrétně v notebooku Lenovo ThinkPad E580 provede vstupem do samotného rozhraní UEFI (klávesa F1). V rozhraní UEFI je pak možnost vytvoření a nakonfigurování vyžadování hesla při konkrétních akcích k dispozici v záložce Security.



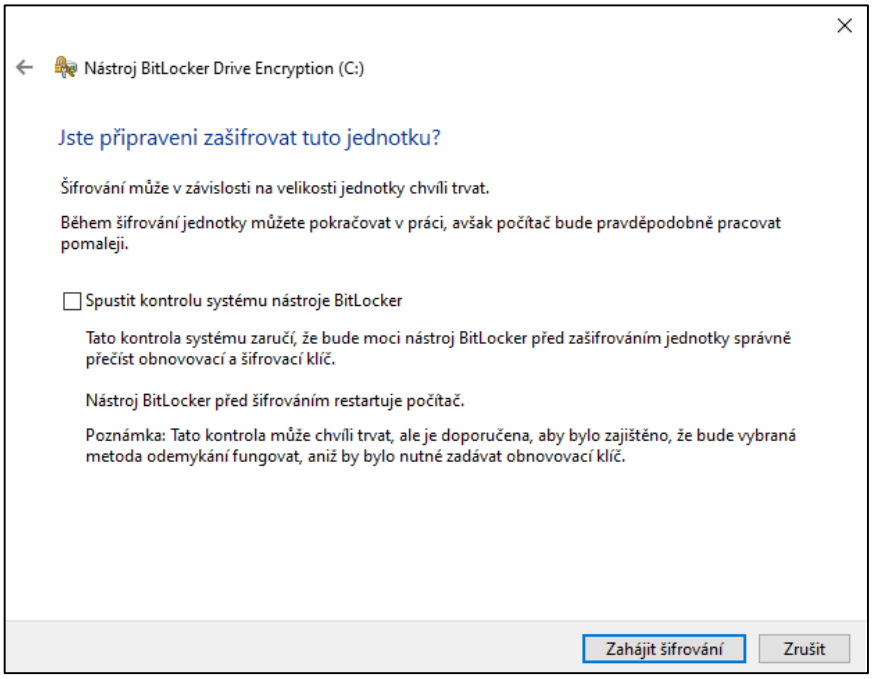
Obrázek 56 Konfigurace rozhraní UEFI v notebooku Lenovo ThinkPad E580 (Lenovo, 2023)

Zde je nutné nejprve heslo vytvořit (Supervisor Password) a pak povolit akce, při kterých má být vyžadováno. Konkrétně se jedná o akce uzamčení nastavení rozhraní UEFI a uzamčení výběru zařízení, ze kterých má být bootováno. Funkce Secure Boot je aktivní již v defaultním nastavení UEFI. Pro pevné pracovní stanice je toto nastavení obdobné.

Aplikace opatření AO-E6

Zapnutí služby BitLocker umožní šifrovat pevný disk. Při ztrátě nebo odcizení (platí hlavně u notebooků) je zvýšena pravděpodobnost, že se neoprávněná osoba nedostane k uloženým datům. K aktivování této služby je nutné otevřít Tento počítač, pravým tlačítkem myši

kliknout na systémový disk a zvolit možnost Zapnout nástroj BitLocker. Následně se provede automatická kontrola konfigurace počítače a operační systém vyzve ke zvolení možnosti zálohy obnovovacího klíče. V podmínkách společnosti Taurus autor diplomové práce zvolil možnost tisku jednotlivých obnovovacích klíčů a ty předal majiteli společnosti v obálce. V další části konfigurace autor diplomové práce zvolil možnost zašifrovat celou jednotku a režim šifrování ponechal na výchozí hodnotě. V případě více pevných disků je nutno tento postup opakovat pro každý pevný disk samostatně (pozn. autora).

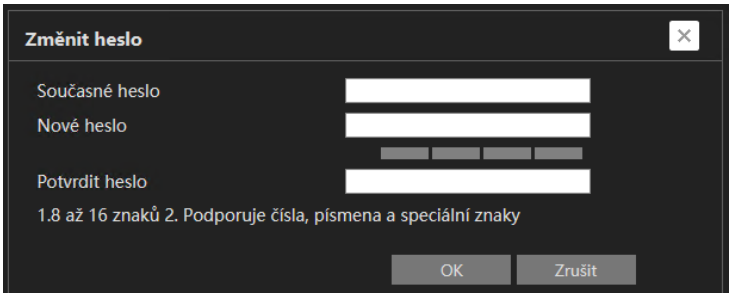


Obrázek 57 Aktivace Služby BitLocker ve Windows 11 (Microsoft, 2022)

7.5 Aplikace opatření na úseku kamerového systému

Aplikace opatření AO-F1

Změnu přístupového hesla, které bylo dosud defaultní, autor diplomové práce provedl vyplněním níže zobrazeného interaktivního okna v záložce Změnit heslo. Nově zadané heslo má dvanáct znaků tvořících velká i malá písmena, čísla a dva speciální znaky. Název defaultního administrátorského účtu jako většina zařízení toto NVR změnit nedokáže.



Obrázek 58 Změna současného hesla v NVR (Provision, 2022)

Aplikace opatření AO-F2

Toto opatření již bylo aplikováno kombinací několika výše popsaných opatření a také další konfigurací firewallu, kterou zde autor diplomové práce z bezpečnostních důvodů nemůže prezentovat. Lze však dodat, že v nastavení NVR autor diplomové práce zakázal NAT, čímž došlo k blokaci využívání aplikace výrobce sloužící k online náhledu kamer. Nově slouží k online náhledu kamer vzdálené připojení prostřednictvím aplikované technologie SSL VPN. Po navázání zabezpečeného tunelu stačí na vzdálené pracovní stanici do webového prohlížeče zadat na DHCP serveru rezervovanou IP adresu NVR. Poté zadá majitel společnosti Taurus přihlašovací údaje, čímž dojde k jeho autentizaci, a následně může kamerový systém libovolně vytěžovat.

7.6 Konečné vyčíslení nákladů

Tabulka 12 Konečné vyčíslení nákladů

IT ÚKON, NÁKUP HW, NÁKUP SW	POŘIZOVACÍ CENA (BEZ DPH)
Wi-Fi router Asus TUF-AX3000 v2	2 672 Kč
konfigurace routeru	bezúplatně autorem diplomové práce
firewall Fortinet FortiGate FG-40F s licencemi FortiCare a FortiGuard Unified Threat Protection na 5 roků	66 383 Kč
konfigurace firewallu	bezúplatně autorem diplomové práce
switch TP-LINK TL-SG105	480 Kč

IT ÚKON, NÁKUP HW, NÁKUP SW	POŘIZOVACÍ CENA (BEZ DPH)
UTP kabel, CAT6, 50 metrů	856 Kč
konektory RJ-45, CAT6, 50 kusů	98 Kč
natažení kabeláže a osazení konektorů	bezúplatně autorem diplomové práce
vytvoření okenní aplikace zajišťující připojení k osobní složce zaměstnance	
další nezbytná konfigurace ICT prvků	
Cena celkem	**70 489 Kč**

8 VYHODNOCENÍ ÚČINNOSTI KYBERNETICKÝCH OPATŘENÍ

Vyhodnotit aplikovaná opatření je velmi těžké. Tento stav je zapříčiněn zejména faktem, že hacktivisté jsou vždy o krok napřed před celou řadou nejmodernějších bezpečnostních opatření. Příkladů by šlo uvést hned několik, avšak to není cílem této kapitoly. Stejně tak jako identifikaci rizik i samotné vyhodnocení účinnosti aplikovaných opatření na úseku kybernetické bezpečnosti provádí specializované firmy prostřednictvím penetračních či obdobných testů. Cena těchto testů se pohybuje v závislosti na velikosti testované organizace v řádu desítek až stovek tisíc korun. V možnostech autora diplomové práce tedy není reálné komplexní penetrační test uskutečnit. Avšak s ohledem na možnosti internetu lze využít mimo jiné online scannery, které nabízejí vulnerability testy. Příkladem lze uvést tyto:

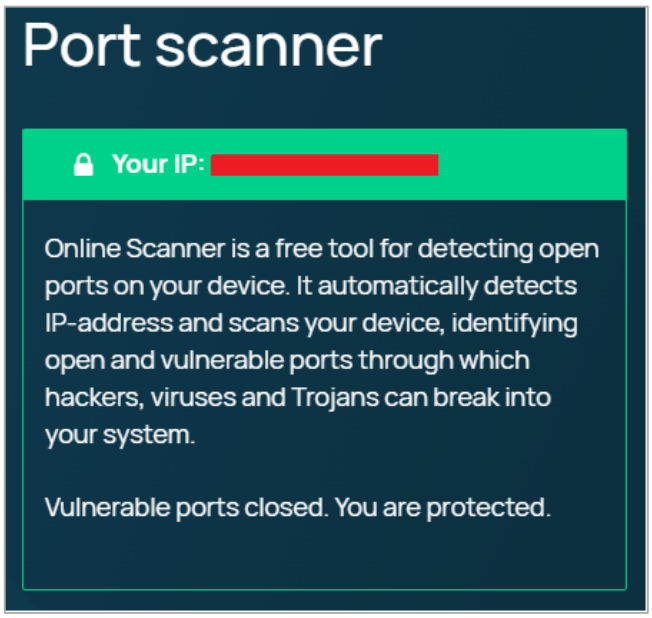
a) Pentest Tools (https://pentest-tools.com/),

b) Whoer (https://whoer.net/) nebo rozsáhlejší,

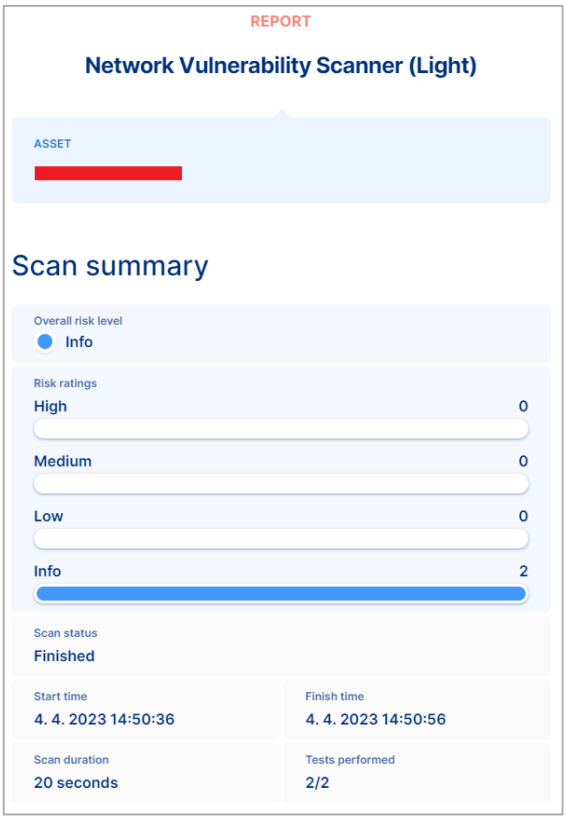
c) Integra (https://www.integra.cz/), případně desktopový,

d) Advanced IP Scanner (https://www.advanced-ip-scanner.com/) a mnoho dalších.

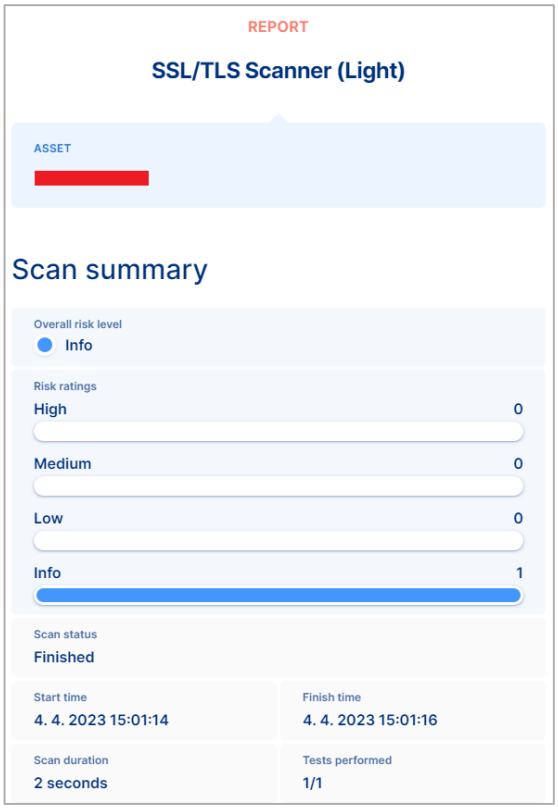
Autor diplomové práce následně výše uvedené nástroje použil k vyhodnocení účinnosti aplikovaných kybernetických opatření společnosti Taurus. Reporty vybraných testů jsou formou obrázků předloženy níže. Citlivé údaje byly opět znečitelněny.



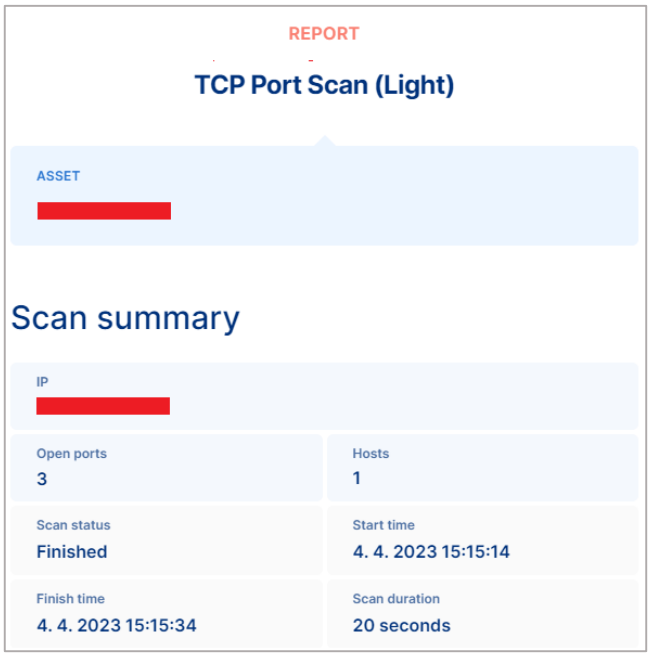
Obrázek 59 Report Port scaneru (Port scanner, c2008-2023)



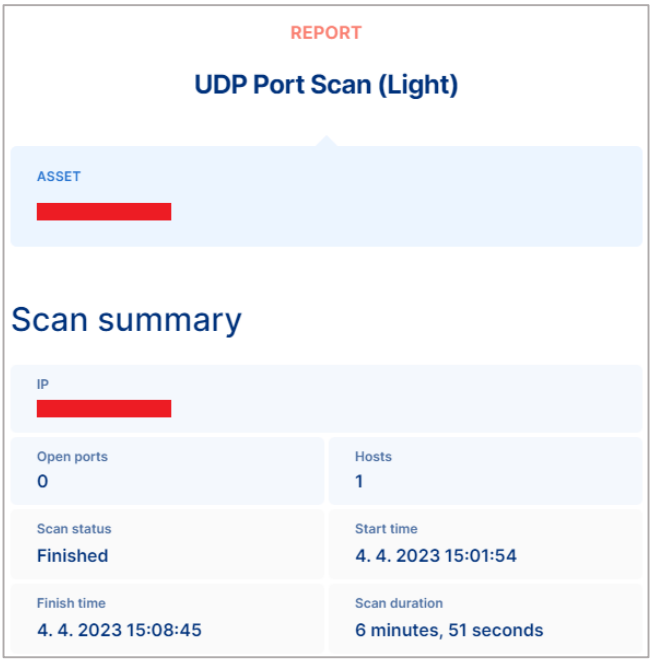
Obrázek 60 Report Network Vulnerability Scanneru (Network Vulnerability Scanner, c2013-2023)



Obrázek 61 Report SSL/TSL Scanneru (SSL/TSL Scanner, c2013-2023)



Obrázek 62 Report TCP Port Scanneru (TCP Port Scan with Nmap, c2013-2023)



Obrázek 63 Report UDP Port Scanneru (UDP Port Scan, c2013-2023)

Ačkoliv se nejednalo o kompletní penetrační testování, lze na základě výše uvedených reportů vybraných testů jednoznačně konstatovat, že aplikovaná kybernetická opatření jsou účinná. Pro doplnění autor diplomové práce uvádí, že detekované otevřené TCP porty slouží k provozu webových stránek, e-mailové komunikaci a vzdálenému připojení prostřednictvím technologie VPN.

ZÁVĚR

Cílem této diplomové práce bylo vhodně prezentovat problematiku kybernetické bezpečnosti vybrané obchodní společnosti, včetně popisu a vyhodnocení účinnosti konkrétních aplikovaných opatření. Za tímto účelem byl v první kapitole definován kyberprostor a kybernetická bezpečnost, která nemá ustálenou definici. Tento fakt byl již autorovi diplomové práce znám díky jeho původní bakalářské práci Kybernetická bezpečnost vybrané obce, kde se touto problematikou již zabýval. Díky tomu byly závěry výše uvedené bakalářské práce v této kapitole v kombinaci s další odbornou literaturou využity. Závěrem této kapitoly byl zhodnocen aktuální stav kybernetické bezpečnosti v České republice.

Druhá kapitola byla věnována definici vybraných kybernetických hrozeb s ohledem na jejich současný trend a praktickou část diplomové práce. Jmenovitě se jednalo o hacking (cracking), vybraný malware, sociální inženýrství a SQL injection. Třetí a současně poslední kapitola teoretické části diplomové práce pojednává s ohledem na praktickou část diplomové práce o konkrétních chráněných aktivech vybrané obchodní společnosti. Nechybí ani popis zabezpečení těchto zařízení s ohledem na nejmodernější techniky.

Praktická část práce je uvedena popisem vybrané obchodní společnosti. Součástí této kapitoly je i situační nákres areálu, popis a půdorysy jednotlivých budov včetně znázorněného umístění konkrétních prvků ICT, popis těchto prvků ICT i grafické znázornění provozované lokální sítě. Následující kapitola identifikuje možné kybernetické hrozby, přičemž autorem práce nejsou brány v potaz hrozby na úseku životnosti hardwaru a úmyslného i nedbalostního jednání uživatelů. Výstupem této kapitoly je registr kybernetických hrozeb rozčleněný na sedm dílčích skupin. Práce navazuje provedením analýzy a hodnocením kybernetických rizik vybrané společnosti sedmi dílčími analýzami metodou FMEA, která je přílohou této práce. V samotné práci jsou s ohledem na podmínku přijatelnosti prezentovány pouze výsledky provedené analýzy prostřednictvím matic kybernetických rizik.

Aplikační úsek praktické části práce nejprve předběžně vyčíslí náklady na aplikaci doporučených opatření a následně jsou konkrétní provedená opatření ze strany autora diplomové práce prezentována. Za připomenutí čtenáři stojí implementace firewallu zajišťujícího nepřetržitou ochranu provozované lokální sítě, konfigurace VPN

a naprogramování okenní aplikace zajišťující bezpečný přístup k osobním složkám všech zaměstnanců obchodní společnosti.

Závěrem autor diplomové práce provedl prostřednictvím vybraných softwarových nástrojů vyhodnocení účinnosti aplikovaných kybernetických opatření s kladným výsledkem.

SEZNAM POUŽITÉ LITERATURY

A Simple Solution for End-User IoT Device Control, c2009-2023. In: *Nabto* [online]. [cit. 2023-03-26]. Dostupné z: https://www.nabto.com/solution/

AiProtection Plan Comparison, 2023. In: *Asus* [online]. [cit. 2023-03-26]. Dostupné z: https://www.asus.com/content/aiprotection/

ANON, Dennis, 2018. 8 easy steps to secure your computer. In: *Privacy* [online]. [cit. 2023-03-24]. Dostupné z: https://privacy.net/how-to-secure-your-computer/

ASUS, 2023. ASUS TUF-AX3000 Firmware version 3.0.0.4.388.22525. *Asus* [software]. [cit. 2023-04-03]. Dostupné z: https://www.asus.com/networking-iot-servers/wifi-routers/asus-gaming-routers/tuf-gaming-ax3000/helpdesk_bios/?model2Name=TUF-Gaming-AX3000. Požadavky na systém: neuvedeno; velikost 45,33 MB.

BOŘÁNEK, Roman, 2017. VPN pro začátečníky: princip fungování, výhody a nevýhody. In: *Root.cz* [online]. [cit. 2023-03-25]. Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

Computer, 2023. In: *Wikipedia* [online]. [cit. 2023-03-24]. Dostupné z: https://en.wikipedia.org/wiki/Computer

Cyberthreat Real-Time Map, 2021. *Kaspersky* [online]. [cit. 2023-04-07]. Dostupné z: https://cybermap.kaspersky.com/

ČESKO, 2005. Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2014. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ELLIOTT, Jessica, 2021. What Is the 3-2-1 Backup Rule?. *CO* [online]. [cit. 2023-04-25]. Dostupné z: https://www.uschamber.com/co/run/technology/3-2-1-backup-rule

ENDORF, Carl F., Eugene SCHULTZ a Jim MELLANDER, 2005. *Detekce a prevence počítačového útoku*. Praha: Grada Publishing. ISBN 80-247-1035-8.

FORTINET, 2023. Current FortiGate version v7.0.11 build0489 (Mature). *Fortinet* [software]. [cit. 2023-03-03]. Dostupné z:

https://customersso1.fortinet.com/. Požadavky na systém: Fortinet FortiGate FG-40F; velikost neuvedeno.

GIBSON, William, 2003. Neuromancer. Ace Books. ISBN 978-0-441-56959-5

HÁJEK, Tomáš. Kybernetická bezpečnost vybrané obce [online]. Zlín, 2021 [cit. 2023-04-07]. Dostupné z: https://theses.cz/id/8igxo8/. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Pavel Valášek.

HENDL, Jan, 2021. *Big data: Věda o datech - základy a aplikace*. Praha: Grada Publishing. Průvodce (Grada). ISBN 978-80-271-3031-3.

History of Computers, 2023. *Sutori* [online]. [cit. 2023-03-24]. Dostupné z: https://www.sutori.com/en/story/history-of-computers--QwYxjjzj7bwhQKBcGXyEnqZx

HORÁK, Jaroslav, 2003. *Bezpečnost malých počítačových sítí: (praktické rady a návody)*. Praha: Grada Publishing. ISBN 80-247-0663-6.

HRANICKÝ, Jan, 2023. Lekce 2 - Technika útoku SQL injection. *ITnetwork* [online]. [cit. 2023-04-09]. Dostupné z: https://www.itnetwork.cz/php/bezpecnost/technika-utoku-sql-injection

CHAPMAN, D. Brent a Elizabeth D. ZWICKY, 1998. *Firewally - principy budování a udržování*. Praha: Computer Press. ISBN 80-722-6051-0.

Introduction to Different Types of NAT, 2022. In: *Huawei* [online]. [cit. 2023-03-25]. Dostupné z: https://forum.huawei.com/enterprise/en/introduction-to-different-types-of-nat/thread/809279-100181?page=4

JAKUBOVÁ, Veronika, 2020. Jak funguje VPN a který protokol si vybrat?. In: *MasterDC* [online]. [cit. 2023-03-25]. Dostupné z: https://www.master.cz/blog/jak-funguje-vpn-ktery-protokol-vybrat/

JARVIS, Jeannette, 2018. Fortinet Announces Enhancements to Our Security Services Portfolio. In: *Fortinet* [online]. [cit. 2023-03-25]. Dostupné z: https://www.fortinet.com/blog/business-and-technology/fortinet-announces-enhancements-to-our-security-services-portfol

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. Výkladový slovník kybernetické bezpečnosti [online]. In: . Praha: Policejní akademie ČR [cit. 2023-04-07]. Dostupné z: https://afcea.cz/wpcontent/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 3. aktualizované vyd. Praha: AFCEA, 2015, s. 69. [online]. [cit. 2023-04-07]. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing. ISBN 978-80-247-1561-2.

JONÁK, Zdeněk, 2003. Data. In: *KTD – Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. [cit. 2023-03-26]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000442&local_base=KTD

KOLOUCH, Jan, 2016. Cyber Crime. Praha: CZ.NIC. ISBN 978-80-88168-18-8.

KOLOUCH, Jan, Pavel BAŠTA et al., 2019. CyberSecurity. Praha: CZ.NIC. CZ.NIC. ISBN 978-80-88168-34-8

KOPECKÝ, Kamil, 2019. Jak zabezpečit počítač. In: *E-Bezpečí* [online]. [cit. 2023-03-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac

KRÁL, Mojmír, 2015. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing. Průvodce (Grada). ISBN 978-80-247-5453-6.

KRČMÁŘ, Petr, 2007. Proč není NAT totéž co firewall. In: *Root.cz* [online]. [cit. 2023-03-25]. Dostupné z: https://www.root.cz/clanky/proc-neni-nat-totez-co-firewall/

LAURENČÍK, Marek, 2018. *SQL: podrobný průvodce uživatele*. Praha: Grada Publishing. Průvodce (Grada). ISBN 978-80-271-0774-2.

LENOVO, 2023. UEFI BIOS 1.49. *Lenovo* [software]. [cit. 2023-03-01]. Dostupné z: https://support.lenovo.com/us/en/downloads/ds501843-bios-update-utility-bootable-cd-for-windows-10-64-bit-thinkpad-e480-e580. Požadavky na systém: Lenovo ThinkPad E580; velikost 52 MB.

MICROSOFT, 2022. Microsoft Visual Studio Community 2022. *Microsoft* [software]. [cit. 2023-03-15]. Dostupné z: https://visualstudio.microsoft.com/cs/. Požadavky na systém: Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022; velikost 21 MB.

MICROSOFT, 2022. Windows 11 verze 22H2. *Microsoft* [software]. [cit. 2023-03-03]. Dostupné z: https://www.microsoft.com/cs-cz/software-download/windows11. Požadavky na systém: Procesor 1 GHz nebo rychlejší se 2 nebo více jádry, RAM 4 GB, uložiště 64GB, rozhraní UEFI s možností zabezpečeného spouštění, TPM verze 2.0; velikost 5,2 GB.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, 2015. In: Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2023-04-07]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_20 15-2020.pdf

Network Switch vs Network Router vs Network Firewall, 2020. *FS Community* [online]. [cit. 2023-04-09]. Dostupné z: https://community.fs.com/blog/network-switch-router-firewall-why-need-all-three.html

Network Vulnerability Scanner, c2013-2023. *Pentest Tools* [online]. [cit. 2023-04-04]. Dostupné z: https://pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online-openvas

Nmap Online, 2023. *Nmap* [online]. [cit. 2023-04-08]. Dostupné z: https://nmap.online/

Peer to Peer (P2P) communications for IoT, c2006-2023. In: *OneSimCard* [online]. [cit. 2023-03-26]. Dostupné z: https://iot.onesimcard.com/Peer-to-Peer-communications-for-IoT/

PENDER-BEY, Georgie. The Parkerian Hexad: The CIA Expanded [online]. In: . [cit. 2023-04-07]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

PERUNICIC, Kristina, 2023. What VPN Protocol Should I Use? (Easy Guide - Updated 2023). In: *VPNmentor* [online]. [cit. 2023-03-25]. Dostupné z: https://www.vpnmentor.com/blog/what-vpn-protocol-should-i-use/

PETERKA, Jiří, 2015. Rodina protokolů TCP/IP. In: *EArchiv.cz* [online]. [cit. 2023-03-24]. Dostupné z: https://www.earchiv.cz/anovinky/ai1592.php3

Port scanner, c2008-2023. *Whoer* [online]. [cit. 2023-04-04]. Dostupné z: https://whoer.net/port-scanner-online

PROVISION, 2022. Latest Firmware Version - V1.4.7 - 28/11/2022. Provision [software]. [cit. 2023-03-01]. Dostupné z: https://provision-isr.com/index.php?option=com_virtuemart&view=productdetails&virtuemart_product_id=

924&virtuemart_category_id=55#/downloads. Požadavky na systém: NVR8-16400PFA; velikost 46,7 MB.

RAID, 2023. *Wikipedie* [online]. [cit. 2023-04-09]. Dostupné z: https://cs.wikipedia.org/wiki/RAID

Raspberry Pi 4 Model B - 8GB RAM, 2023. *RPishop.cz* [online]. [cit. 2023-03-24]. Dostupné z: https://rpishop.cz/raspberry-pi-4/2611-raspberry-pi-4-model-b-8gb-ram-0765756931199.html

ROSENCRANCE, Linda, 2022. DEFINITION peer-to-peer (P2P). In: *Techtarget* [online]. [cit. 2023-03-25]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/peer-to-peer

Router Communication, 2023. *Stack Overflow* [online]. [cit. 2023-04-09]. Dostupné z: https://i.stack.imgur.com/kiG8s.png

SANTOS Henrique M. D., 2022. Cybersecurity: A Practical Engineering Approach. Boca Raton: CRC Press. ISBN 978-0-367-25242-7.

SEDLÁK, Petr a Martin KONEČNÝ, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SCHNEIER, Bruce, 2000. Semantic Attacks: The Third Wave of Network Attacks. In: Schneier on Security [online]. [cit. 2023-04-07]. Dostupné z: https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

SMEJKAL, Vladimír, 2018. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-720-7.

SSL VPN full tunnel for remote user, 2023. In: *Fortinet* [online]. [cit. 2023-03-25]. Dostupné z: https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/559546/ssl-vpn-full-tunnel-for-remote-user

SSL/TSL Scanner, c2013-2023. *Pentest Tools* [online]. [cit. 2023-04-04]. Dostupné z: https://pentest-tools.com/network-vulnerability-scanning/ssl-tls-scanner

SYNOLOGY, 2023. DSM 7.1.1-42962. *Synology* [software]. [cit. 2023-03-01]. Dostupné z: https://www.synology.com/cs-cz/support/download/DS218?version=7.1#system.
Požadavky na systém: Synology DS218; velikost 50 MB.

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

TCP Port Scan with Nmap, c2013-2023. *Pentest Tools* [online]. [cit. 2023-04-04]. Dostupné z: https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap

Threatbutt Internet Hacking Attack Attribution Map, 2023. *Threatbutt* [online]. [cit. 2023-04-07]. Dostupné z: https://threatbutt.com/map/

TURING, Alan Mathison, 1936. *On Computable Numbers, with an Application to the Entscheidungsproblem* [online]. [cit. 2023-03-24]. Dostupné z: https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf

UDP Port Scan, c2013-2023. *Pentest Tools* [online]. [cit. 2023-04-04]. Dostupné z: https://pentest-tools.com/network-vulnerability-scanning/udp-port-scanner-online-nmap

What do LAN, WAN, and SD-WAN mean?, 2016. In: *Sonoran Integrations* [online]. [cit. 2023-03-24]. Dostupné z: https://www.sonoranintegrations.com/what-are-lan-wan-and-sd-wan

What is a router?, 2023. *Cloudflare* [online]. [cit. 2023-04-09]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-a-router/

What is a VPN and how can you benefit from it?, 2020. In: *Forscope* [online]. [cit. 2023-03-25]. Dostupné z: https://www.forscope.eu/blog/what-is-vpn/

What is SSL VPN?, 2023. In: *Fortinet* [online]. [cit. 2023-03-25]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/ssl-vpn

WIDUP, Suzanne et al., 2022. Data Breach Investigations Report. *ResearchGate* [online]. [cit. 2023-04-09]. Dostupné z: https://www.researchgate.net/publication/362160949_2022_Data_Breach_Investigations_Report

WILSON, Duane C., 2021. *Cybersecurity*. Cambridge, Massachusetts: The MIT Press. ISBN 9780262542548.

YWORKS, c2000-2023. YEd Graph Editor 3.23.1. *YWorks* [software]. [cit. 2023-03-03]. Dostupné z: https://www.yworks.com/products/yed/download#download. Požadavky na systém: Windows Vista, Windows 7, Windows 8, Windows 10, Windows 11, Linux, Mac OS X; velikost 116 MB.

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2023-04-08]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2023-04-08]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

TUHÝ, Radan, 2013. NAS: Jak na firewall a zabezpečení?. *Svět hardware* [online]. [cit. 2023-04-25]. Dostupné z: https://www.svethardware.cz/nas-jak-na-firewall-a-zabezpeceni/37842-4

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
AP	Antivirový program
BIOS	Basic Input-Output System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DPPC	Dohledové přijímací poplachové centrum
FTP	File Transfer Protocol
FW	Firewall
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICT	Information and Communication Technologies
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP (adresa)	Internet Protocol (adresa)
IPsec	Internet Protocol Security
ISMS	Information Security Management System
IT	Information Technologies
KI	Kritická infrastruktura
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC (adresa)	Media Access Control (adresa)
MAN	Metropolitan Area Network
MS	Microsoft

NAS	Network Attached Storage
NAT	Network Address Translation
NSA	National Security Agency
NÚKIB¨	Národní úřad pro kybernetickou a informační bezpečnost
NVR	Network Video Recorder
OS	Operační systém
P2P	Peer-to-peer
PIR	Pasivní infračervené čidlo
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PZTS	Poplachový zabezpečovací tísňový systém
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSTP	Secure Socket Tunneling Protocol
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP	Transmission Control Protocol
TSL	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UDP	User Datagram Protocol

UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU FYZICKÉ BEZPEČNOSTI CHRÁNĚNÝCH AKTIV METODOU FMEA

objekt: obchodní společnost Taurus															číslo FMEA: 1
odpovědnost za proces: Bc. Tomáš Hájek															rok výroby modelu / procesu: 2023
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	možná chyba	možné následky chyby	závažnost	možná příčina chyby	výskyt	stávající opatření	stávající řízení procesu	odhalení	rizikové číslo	doporučená opatření	odpovědnost	závažnost	výskyt	odhalení	rizikové číslo
fyzická bezpečnost chráněných aktiv	elektrický výboj	poškození prvků ICT, ztráta SW, ztráta dat	**5**	nepředvídatelný nahodilý jev	**5**	přepěťová ochrana, zálohování dat	žádné	**5**	**125**	beze změny	beze změny	**5**	**5**	**5**	**125**
	přepětí v elektrické síti		**5**		**5**			**5**	**125**			**5**	**5**	**5**	**125**
	požár		**7**		**5**	zálohování dat		**5**	**175**	instalace (přidání) kouřových detektorů ke stávajícímu PZTS	správce PZTS	**5**	**5**	**5**	**125**
	přehřátí prvků ICT		**4**		**3**	klimatizační jednotka	klimatizační jednotka	**3**	**36**	beze změny	beze změny	**4**	**3**	**3**	**36**
	neoprávněný vstup osob do serverovny	neoprávněná manipulace s prvky ICT	**6**	úmysl konkrétní osoby	**5**	serverovna je trvale uzamčena	žádné	**5**	**150**	vytvoření samostatné sekce v rámci stávajícího PZTS, jasná delegace oprávnění ke vstupu konkrétních osob	správce PZTS	**4**	**4**	**4**	**64**

objekt: obchodní společnost Taurus										číslo FMEA: 1					
odpovědnost za proces: Bc. Tomáš Hájek										rok výroby modelu / procesu: 2023					
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
	neoprávněný přístup osob k prvkům ICT		**5**		**2**	PZTS, uzamčené kanceláře	PZTS	**2**	**20**			**5**	**2**	**2**	**20**
	chybějící záložní zdroj napájení (UPS)	ztráta SW, ztráta dat, nedostupnost služeb	**4**	nedbalost odpovědné osoby	**4**	záložní zdroj napájení (UPS) v serverovně	záložní zdroj napájení (UPS) v serverovně	**2**	**32**	beze změny	beze změny	**4**	**4**	**2**	**32**
	přerušení metalického (optického) kabelu	nedostupnost služeb, možná ztráta dat	**5**	nepředvídatelný nahodilý jev	**5**	kabely vedeny v ochranných lištách	žádné	**5**	**125**			**5**	**5**	**5**	**125**
	chybějící zálohování dat	ztráta SW, ztráta dat	**5**	nedbalost odpovědné osoby	**2**	pravidelná záloha dat na NAS	OS	**2**	**20**			**5**	**2**	**2**	**20**

PŘÍLOHA P II: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU ADMINISTRACE CHRÁNĚNÝCH AKTIV METODOU FMEA

objekt: obchodní společnost Taurus															**číslo FMEA: 2**
odpovědnost za proces: Bc. Tomáš Hájek															**rok výroby modelu / procesu: 2023**
ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
administrace chráněných osob	neurčena odpověd-ná osoba	nelze reagovat na dění v LAN	**10**	chybějící IT pracovník s vhodnou odborností	**9**	žádné	žádné	**8**	**720**	určit (zaměstnat) správce IT s vhodnou odbornou kvalifikací, vypracovat náplň práce pro tuto pozici	majitel společnosti Taurus	**5**	**5**	**4**	**100**
	nepravi-delná údržba LAN a prvků ICT	přímé ohrožení kyberne-tickými útoky, ztráta dat, zašifrování dat, fyzické zničení prvků ICT	**10**		**10**			**7**	**700**			**6**	**6**	**4**	**144**
	nepravi-delný monito-ring LAN a prvků ICT	chybějící historická data, chybějící povědomí o dění v LAN	**10**		**10**			**7**	**700**			**6**	**6**	**4**	**144**
	nepravi-delné vyhodno-cování logů		**7**		**10**			**7**	**490**			**4**	**5**	**4**	**80**
	neprová-dění pravidel-ných aktuali-zací prvků ICT	přímé ohrožení kyberne-tickými útoky, ztráta dat, zašifrování dat,	**10**		**5**	automatic-ké aktualizace OS a firmware	OS/ firmware	**5**	**250**			**6**	**3**	**3**	**54**

objekt: obchodní společnost Taurus										číslo FMEA: 2					
odpovědnost za proces: Bc. Tomáš Hájek										rok výroby modelu / procesu: 2023					
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
	nedosta-tečná pravidel-ná fyzická kontrola prvků ICT	fyzické zničení prvků ICT	**8**		**5**	částečná kontrola ze strany uživatelů při každo-denní činnosti	žádné	**5**	**200**			**4**	**3**	**3**	**36**

PŘÍLOHA P III: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU VPN METODOU FMEA

objekt: obchodní společnost Taurus										**číslo FMEA: 3**					
odpovědnost za proces: Bc. Tomáš Hájek										**rok výroby modelu / procesu: 2023**					
ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
VPN	využívání slabého (zastaralého) bezpečnostního protokolu	získání přístupu do lokální sítě, přímé ohrožení kybernetickými útoky	**10**	neznalost/ nedbalost odpovědné osoby	**10**	PPTP protokol	Wi-Fi router	**7**	**700**	změna využívaného protokolu, změna routeru	autor diplomové práce	**5**	**5**	**6**	**150**
	neimplementovaný firewall		**10**		**10**	žádné	žádné	**7**	**700**	změna routeru, nebo přidání firewallu		**5**	**5**	**4**	**100**
	špatná delegace demilitarizovaných zón	vzdálený přístup k celé lokální síti	**10**		**7**			**5**	**350**	konfigurace demilitarizovaných zón, jasné stanovení přístupů přes technologii VPN		**5**	**4**	**3**	**60**

PŘÍLOHA P IV: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU LAN/WLAN METODOU FMEA

objekt: obchodní společnost Taurus									**číslo FMEA: 4**					
odpovědnost za proces: Bc. Tomáš Hájek									**rok výroby modelu / procesu: 2023**					
ANALÝZA SOUČASNÉHO STAVU									**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
LAN/ WLAN	používání zastaralého bezpečnostního protokolu Wi-Fi	využití známé slabiny k průniku do sítě ze strany crackera	**10**	chybějící IT správce s vhodnou odborností	**10**	WPA2	žádné	**8**	**800**	konfigurace protokolu WPA3, případně změna routeru podporujícího tento bezpečnostní protokol	autor diplomové práce	**6**	**6**	**5**	**180**
	neaktivní filtrování bezdrátových zařízení dle MAC adres	nekontrolované připojení bezdrátového zařízení	**8**		**8**			**5**	**320**	aktivování filtrování bezdrátových zařízení dle MAC adres		**5**	**5**	**4**	**100**
	aktivní DHCP server bez využití rezervačního listu	nedostupnost prvků ICT při změně IP adresy	**8**		**7**			**6**	**336**	aktivování rezervačního DHCP listu, vložení serveru, tiskáren, NAS a NVR		**5**	**4**	**3**	**60**
	crackerský útok	zničení, nedostupnost prvků ICT, ztráta dat, zašifrování dat, ztráta SW	**10**	úmyslný útok crackera	**8**	žádné		**9**	**720**	změna routeru (router s FW a online ochranou před kybernetickými útoky)		**6**	**5**	**5**	**150**
	infiltrace malware		**10**		**8**			**9**	**720**			**6**	**5**	**5**	**150**
	chybějící online ochrana před kybernetickými útoky		**10**	router nepodporuje tuto funkci	**8**			**8**	**640**			**6**	**5**	**4**	**120**

objekt: obchodní společnost Taurus										číslo FMEA: 4					
odpovědnost za proces: Bc. Tomáš Hájek										rok výroby modelu / procesu: 2023					
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	možná chyba	možné následky chyby	závažnost	možná příčina chyby	výskyt	stávající opatření	stávající řízení procesu	odhalení	rizikové číslo	doporučená opatření	odpovědnost	závažnost	výskyt	odhalení	rizikové číslo
	možnost konfigu-rovat router přes webové rozhraní za využití veřejné statické IP adresy	využití známé slabiny k průniku do sítě ze strany crackera	**10**	router nepodpo-ruje tuto funkci, chybějící IT správce s vhodnou odborností	**10**	žádné	žádné	**9**	**900**	změna routeru (router s FW), bezpečné nastavení vzdálených přístupu, povolení pouze potřebných portů		**5**	**5**	**4**	**100**
	otevřené nepouží-vané síťové TCP nebo UDP porty		**8**		**10**			**9**	**720**			**4**	**5**	**4**	**80**

PŘÍLOHA P V: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU PRVKŮ ICT METODOU FMEA

objekt: obchodní společnost Taurus										číslo FMEA: 5					
odpovědnost za proces: Bc. Tomáš Hájek										rok výroby modelu / procesu: 2023					
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
prvky ICT	neaktu-ální BIOS/ UEFI nebo firmware	využití známé slabiny k průniku do systému ze strany crackera	**4**	neznalost/ nedbalost odpovědné osoby, blokovaný přístup k internetu	**2**	žádné	žádné	**2**	**16**	beze změny	beze změny	**4**	**2**	**2**	**16**
	neaktuál ní operační systém		**7**		**4**	Windows Update	Windows Update	**4**	**112**			**7**	**4**	**4**	**112**
	chybějící antiviro-vý program		**6**		**4**	AP ESET	žádné	**4**	**96**			**6**	**4**	**4**	**96**
	neaktu-ální antiviro-vý program		**5**	blokovaný přístup k internetu	**3**		AP ESET	**3**	**45**			**5**	**3**	**3**	**45**
	nevhod-ná delegace přístupo-vých účtů	neoprávně-ná konfigura-ce ICT prvků	**5**	neznalost/ nedbalost odpovědné osoby, špatně nastavená bezpeč-nostní politika	**4**	přístupové účty jsou delegová-ny	žádné	**4**	**80**			**5**	**4**	**4**	**80**
	používá-ní default-ních přihlašo-vacích údajů	neoprávně-ný přístup k prvkům ICT, neoprávně-ná konfigura-ce prvků ICT	**10**		**8**	žádné		**8**	**640**	změna přihlašovacích údajů	autor diplomové práce	**5**	**5**	**5**	**125**
	používá-ní slabých hesel		**10**		**8**			**6**	**480**	změna používaných hesel v souladu s podmínkami na silné heslo		**5**	**5**	**5**	**125**

objekt: obchodní společnost Taurus											číslo FMEA: 5				
odpovědnost za proces: Bc. Tomáš Hájek											rok výroby modelu / procesu: 2023				
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	možná chyba	možné následky chyby	závažnost	možná příčina chyby	výskyt	stávající opatření	stávající řízení procesu	odhalení	rizikové číslo	doporučená opatření	odpovědnost	závažnost	výskyt	odhalení	rizikové číslo
	nevhodný přístup k osobním složkám	neoprávněný přístup k uloženým datům	**10**	špatně řešené připojování k osobním složkám	**8**			**8**	**640**	vzdálené připojování výhradně prostřednictvím technologie VPN, vytvoření okenní aplikace zajišťující připojení k osobním složkám					**128**
	BIOS/ UEFI nechráněno heslem	neoprávněný přístup ke konfiguraci prvků ICT	**10**	neznalost/ nedbalost odpovědné osoby	**9**	žádné	žádné	**7**	**630**	zaheslování BIOS/UEFI		**6**	**4**	**4**	**96**
	aktivní bootování z externích zařízení		**10**		**10**			**7**	**700**	deaktivování bootování z externích zařízení		**5**	**5**	**4**	**100**
	neaktivní služba BitLocker	neoprávněný přístup k datům	**10**		**10**			**7**	**700**	aktivování služby BitLocker		**5**	**5**	**4**	**100**

PŘÍLOHA P VI: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU KAMEROVÉHO SYSTÉMU METODOU FMEA

objekt: obchodní společnost Taurus										**číslo FMEA: 6**					
odpovědnost za proces: Bc. Tomáš Hájek										**rok výroby modelu / procesu: 2023**					
ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
kamerový systém	používání default-ních přihlašo-vacích údajů	neoprávně-ný přístup k NVR	**10**	neznalost/ nedbalost odpovědné osoby	**8**	žádné	žádné	**8**	**640**	změna přihlašovacích údajů	autor diplomové práce	**5**	**5**	**5**	**125**
	využívání aplikací třetích stran	neoprávně-ný přístup k obrazo-vým záznamům, únik obrazo-vých záznamů	**8**		**5**			**5**	**200**	přístup ke kamerovému systému výhradně prostřednictvím technologie VPN		**5**	**4**	**4**	**80**
	využívání P2P sítě		**7**		**5**			**5**	**175**			**5**	**4**	**4**	**80**

PŘÍLOHA P VII: ANALÝZA KYBERNETICKÝCH RIZIK NA ÚSEKU PROVOZU WEBOVÉ APLIKACE A SQL DATABÁZE METODOU FMEA

objekt: obchodní společnost Taurus															**číslo FMEA: 7**
odpovědnost za proces: Bc. Tomáš Hájek															**rok výroby modelu / procesu: 2023**
ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
prvek	**možná chyba**	**možné následky chyby**	**závažnost**	**možná příčina chyby**	**výskyt**	**stávající opatření**	**stávající řízení procesu**	**odhalení**	**rizikové číslo**	**doporučená opatření**	**odpovědnost**	**závažnost**	**výskyt**	**odhalení**	**rizikové číslo**
webová aplikace a SQL databáze	chybějící dvoufaktorová autentizace	neoprávněný přístup k webové aplikaci	**8**	špatný návrh aplikace	**5**	žádné	žádné	**5**	**200**	nasadit dvoufaktorovou autentizaci	vývojář webové aplikace	**5**	**5**	**5**	**125**
	chybějící šifrování databáze		**8**		**3**	databáze je zašifrována	Microsoft SQL Server	**5**	**120**	beze změny	beze změny	**8**	**3**	**5**	**120**