Kybernetická bezpečnost vybrané obce

Tomáš Hájek

Bakalářská práce
2021

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: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Hájek**
Osobní číslo:	**L18078**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost vybrané obce**

Zásady pro vypracování

1. Proveďte rešerši dostupných zdrojů týkající se problematiky kybernetické bezpečnosti ve vztahu k územním samosprávním celkům.
2. Proveďte průzkum současné situace v dané problematice u vybraného samosprávního celku.
3. Navrhněte opatření pro zlepšení současného stavu kybernetické bezpečnosti vybraného samosprávního celku a vhodně je prezentujte.

Forma zpracování bakalářské práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
2. KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. ISBN 978-80-247-5453-6.
3. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Valášek**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

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

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

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou 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 – bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 14. 5. 2021

Jméno a příjmení studenta: Tomáš Hájek

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá kybernetickou bezpečností vybrané obce a s ní související analýzou kybernetických rizik prostřednictvím vybrané metody FMEA. Teoretická část je věnována definici základních pojmů, dále pak kyberprostoru a kybernetické bezpečnosti jako takové. V praktické části je popsána vybraná obec, budova obecního úřadu a lokální síť, která je zde provozována. Následuje samotná analýza kybernetických rizik prostřednictvím vybrané metody FMEA, která je rozčleněna na tři samostatné pohledy. Závěrem je na základě provedené analýzy doporučeno několik opatření ke zlepšení současného stavu kybernetické bezpečnosti.

Klíčová slova: kybernetická bezpečnost, vybraná obec, IT infrastruktura, analýza rizik, metoda FMEA

ABSTRACT

The bachelor's thesis deals with the cyber security of a selected municipality and the related analysis of cyber risks through the FMEA method. The theoretical part is devoted to the definition of basic concepts, then cyberspace and cyber security as such. The practical part describes the selected municipality, the municipal office building and the local network, which is operated here. The analysis of cyber risks itself follows, using the selected FMEA method, which is divided into three separate views. Finally, based on the analysis, several measures are recommended to improve the current state of cyber security.

Keywords: cyber security, selected municipality, IT infrastructure, risk analysis, FMEA method

Touto cestou děkuji vedoucímu bakalářské práce Ing. Pavlu Valáškovi, jenž mi věnoval svůj čas a vstřícným přístupem poskytl cenné rady a podněty, díky kterým tato práce mohla vzniknout. Poděkování také patří starostovi vybrané obce, který mi umožnil vstup na půdu obecního úřadu i shromáždění dostatečného množství dat k realizaci analýzy kybernetické bezpečnosti vybrané obce.

V neposlední řadě děkuji své přítelkyni a členům rodiny za podporu v průběhu celého studia.

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

OBSAH

ÚVOD

Cílem autora této bakalářské práce, jejíž téma sám navrhl, je vhodně zpracovat problematiku kybernetické bezpečnosti náhodně zvoleného nižšího územního samosprávního celku, respektive obce. V samotné podstatě je pak bakalářská práce rozdělena na teoretickou a praktickou část.

Teoretická část je úvodem věnována definici základních pojmů, které se na sebe navzájem vrství, úzce spolu souvisejí a objektivně představují problematiku kybernetické bezpečnosti ve vztahu k tématu. Prvním takto definovaným pojmem je počítač, který v této práci představuje především předmět útoku. Na něj navazuje definice kyberprostoru, počítačové sítě a závěrem zvláštní případ celosvětově nejznámější sítě internet.

Následná kapitola je věnována samotné kybernetické bezpečnosti, která i přes svoji velkou publicitu nemá ustálenou definici, případně jsou tyto ze strany mnoha autorů odborných publikací protichůdné. Práce následně přechází ke kapitole, kterou představují kybernetické a bezpečnostní hrozby ve formě hackingu (crackingu), sociálního inženýrství a malwaru. Předposlední kapitola teoretické části je věnována Národnímu úřadu pro kybernetickou a informační bezpečnost, který v tomto odvětví představuje ústřední správní orgán. Poté je teoretická část uzavřena popisem vybrané metody FMEA, která je aplikována v praktické části práce. V kapitole zabývající se vybranou metodou FMEA jsou ze strany autora práce vymezeny i její mantinely v podobě stanovení intervalů rizikového čísla.

Praktická část je uvedena popisem vybrané obce, kam spadá i popis budovy obecního úřadu, včetně jejího vyhotoveného půdorysu. Dále je zde popsána lokální síť s přímým přístupem k internetu, která je v této budově provozována. Nejrozsáhlejší kapitolu bakalářské práce pak tvoří samotné hodnocení kybernetických rizik, kdy je samotná analýza pro přehlednost rozdělena do tří samostatných pohledů. Ty představují analýzu rizik ve vztahu k fyzické bezpečnosti, lokální síti a koncovým prvkům ICT. Samozřejmostí této kapitoly je i vymezení oblastí, které nejsou cílem bakalářské práce, respektive samotné analýzy. Jako příklad lze uvést ztrátu dat v důsledku neodborné manipulace ze strany uživatele nebo konec životnosti hardwaru, zpravidla pevného disku.

Poslední kapitola je věnována doporučením, která autor práce ve vztahu k provedené analýze navrhuje. Doporučení jsou následně prezentována starostovi vybrané obce, aby došlo ke zlepšení současného stavu kybernetické bezpečnosti tohoto nižšího územního samosprávního celku.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

Cílem této kapitoly je definovat hlavní pojmy, které bezprostředně souvisejí s tématem, a z praktického pohledu tvoří kybernetickou bezpečnost vybrané obce nebo jsou její součástí. Jmenovitě se pak jedná o počítač, kyberprostor, počítačovou síť a zvláštní případ počítačové sítě – internet.

1.1 Počítač

Přelomovým rokem, kdy se začíná mluvit o počítači, který ani zdaleka nebyl podobný těm dnešním, je rok 1945. Předchůdcem tohoto stroje byl programovatelný počítací stroj německé výroby označovaný jako Z3 z roku 1941, případně americký Harvard Mark I, dnes označovaný jako počítač nulté generace. Již v roce 1936 navrhl moderní počítač Alan Turing v seminární práci On Computable Numbers, with an Application to the Entscheidungsproblem. Toto zařízení Alan Turing nazval Universal Computing Machine a provedl důkaz, že je schopno vypočítat vše, co z matematického hlediska vypočítat lze. Konkrétně v seminární práci uvádí, že: *„…the computable numbers are those whose decimals are calculable by finite means.“* (Touring, © 2020).

Universial Computing Machine je dnes známý jako univerzální Turingův stroj a je předmětem studia teorie výpočtu. V již zmíněném roce 1945 počítačový odborník John von Neumann přišel s prvním elektronickým počítačem, který se následně zapsal do dějin jako EDVAC (Electronic Discrette Variable Automatic Computer), a položil tak základy von Neumannovy architektury, která je dnes v kombinaci s hardvardskou architekturou stále využívána. Dnešní moderní počítač je tedy stroj, který automaticky vykonává operace prostřednictvím počítačového programu, dnes známého jako operační systém. Počítač lze rozdělit dle několika kritérií, avšak pro účely této práce postačí jeho rozdělení na viditelnou, respektive hmatatelnou část označovanou jako hardware, a jeho programové vybavení, tj. software. Stejně tak bude pro účely této práce počítačem myšlen zpravidla předmět útoku v oblasti kybernetické bezpečnosti, bez ohledu na to, zda se jedná například o stolní počítač, server, nebo notebook. (Smejkal, 2015), (Touring, © 2020), (Computer)

1.1.1 Hardware

Každý výše definovaný počítač je tvořen fyzickými součástmi, bez kterých by nebyl jeho provoz možný. Tyto součásti zpravidla představují počítačovou skříň (case), napájecí zdroj, ventilátory, případně chladiče, základní desku (mainboard), alespoň jeden procesor a pevný

disk (HDD, dnes častěji SSD), operační paměť (RAM) a speciální karty. Ty mohou být integrované (například integrovaná grafická karta na procesoru), nebo externí. Samostatnou skupinu tvoří periferní zařízení počítače, která nejsou pro jeho provoz nutná, ale usnadňují a především zrychlují práci. Periferní zařízení lze rozdělit na vstupní, prostřednictvím kterých se zadávají do počítače data, a na výstupní, která zajišťují výstup dat. Jako příklad periferních zařízení lze tedy uvést monitor, klávesnici, myš, mikrofon, reproduktor, tiskárnu, dataprojektor a mnoho dalších. Z pohledu kybernetické bezpečnosti patří hardware počítače do prvků kybernetické bezpečnosti představujícího technologie, a je nutné ho chránit před nepříznivými vlivy, jako je vlhko, prach nebo teplo. A také před často opomíjeným neoprávněným zásahem. Této problematice je věnována kapitola Kybernetická bezpečnost. (Smejkal, 2015)

1.1.2 Software

Softwarem je označováno programové vybavení počítače, které zajišťuje správné pracování hardwaru počítače. Podmnožinou softwaru je firmware, který tvoří BIOS (Basic Input-Output Systém), jenž při startu počítače inicializuje a nakonfiguruje připojené hardwarové zařízení a následně zavede konkrétní operační systém. Zdrojový kód BIOS je implementován přímo na základní desce počítače ve stále paměti a jeho vhodné nastavení (např. funkce Secure Boot) hraje klíčovou roli v oblasti kybernetické bezpečnosti. Nejznámějším operačním systémem je Windows od firmy Microsoft, případně MacOS od společnosti Apple. Mezi ty méně známé patří Linux, nebo Raspbian používající se pro malé jednodeskové počítače.

Samostatné odvětví softwaru tvoří firewall. V případě nejpoužívanějšího operačního systému Windows je to softwarově řešená brána Windows Firewall, která je součástí tohoto operačního systému. Prostřednictvím brány Windows Firewall je možné aktivovat tři síťové profily:

a) doménový profil,

b) privátní profil a

c) veřejný profil.

Pro účely této práce postačí zmínit, že doménový profil je nejméně omezující, což je dáno samotným členstvím počítače v doméně, zatímco veřejný profil z důvodu vyšší bezpečnosti

neumožňuje širší sdílení dat v rámci sítě, zpravidla WAN. (Smejkal, 2015), (Windows Firewall)

Součástí definovaného softwaru je i celá škála antivirových programů, které v kombinaci se správně nastavenými příchozími a odchozími pravidly firewallu, ať už toho v operačním systému Windows nebo například implementovaného v routeru, zvyšují bezpečnost počítače, respektive uživatele.

Další skupinu tvoří nespočet programů, které usnadňují kancelářskou práci, umožňují práci s videem a audiem, zajišťují surfování v nejznámější celosvětové síti internet nebo svým způsobem zajišťují uživateli relax prostřednictvím počítačových her. Bohužel skrze tuto skupinu softwaru může být do počítače implementován škodlivý kód, který se souhrnně označuje jako malware. Je mu věnována samostatná kapitola Kybernetické a bezpečnostní hrozby.

1.2 Kyberprostor

Definice kyberprostoru je mnohem složitější, než jak bývá často matematicky zapsána: internet = kyberprostor. Zde je nutné si uvědomit, že existuje celá řada lokálních počítačových sítí (LAN), které nemají z povahy své činnosti a z bezpečnostních důvodů zajištěný prostup na internet, a přesto jsou součástí kyberprostoru. Jako příklad lze uvést LAN provozovanou Policií ČR, Armádou ČR, zpravodajskými službami a dalšími bezpečnostními sbory, ozbrojenými sílami, složkami Integrovaného záchranného systému apod. Tyto sítě jsou pak označovány jako intranet.

Kyberprostor jako takový vizionářsky definoval již v roce 1983 William Gibson ve svém díle Neuromancer takto:

„*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)

Takto definovaný virtuální svět je možno, na základě díla od pana Gibsona, navštívit propojením lidského mozku s počítačem. Toto spojení se uskutečňuje prostřednictvím elektrod, které spojení zajistí. Samozřejmě, že se jedná o jistou fikci. Nicméně dle autora této práce je právě kyberprostor fikcí. Fikcí, 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. Fikce sama o sobě svým způsobem pojem kyberprostoru vysvětluje, neboť jediné

prvky, které kyberprostor zhmotňují, jsou s jistou nadsázkou počítačové (případně serverové) komponenty a kabely, vše ostatní je jenom fikcí. Kyberprostor je ovládán pouze uživateli, kteří ho zároveň navštěvují, a paradoxně je sám o sobě závislý na hmotné podstatě, díky které existuje. (Kolouch, 2016), (Jirovský, 2007)

Ve vztahu k dnešní době pracuje s vlastní, stručnou, ale výstižnou definicí i stěžejní zákon v této oblasti, tedy zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Tento zákon pak tedy kyberprostor definuje následně:

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

Bohužel z této definice nevyplývá, že tento virtuální svět lze rozdělit, respektive je rozdělen na viditelnou a neviditelnou část. Většina autorů odborných publikací v oblasti kybernetické bezpečnosti přirovnává kyberprostor k pomyslnému ledovci, kde viditelnou část představují pouze 4 procenta obsahu internetu. Tato viditelná část indexovaného webu je označována jako Surface Web a běžní uživatelé internetu ji navštěvují při každodenní činnosti. Zbylých 96 procent obsahu této celosvětové sítě tvoří její neviditelné části, odborně označované jako Darknets. Tudíž zmíněný vznik, zpracování a výměna informací probíhá dle zákona č. 181/2014 Sb. ve viditelné i neviditelné části kyberprostoru. V očích mnoha uživatelů je označení pro Darknets, Dark Web a Freenet nebo Tor Browser špatné, či dokonce nelegální a jsou přesvědčeni o nezpochybnitelném faktu, že Darknets slouží jako místo pro obchod s drogami, zbraněmi a dětskou pornografií. Mezi světlé stránky Tor Browseru, prostřednictvím kterého je možno se připojit k neviditelné části kyberprostoru, patří jeho schopnost zajistit uživateli anonymitu, chránit si svoje soukromí a obejít cenzuru. V následující kapitole je dále definována počítačová síť, která s kyberprostorem velmi úzce souvisí a ve své podstatě ho mimo jiné tvoří. (Česko, 2014), (Kolouch, 2016), (Nutil, 2015), (Why we need Tor)

1.3 Počítačová síť

Počítačovou síť je možno definovat, respektive si představit jako spojení nejméně dvou zařízení, zpravidla počítačů, která spolu vzájemně komunikují. Realizace takovéhoto prvního síťového propojení mezi čtyřmi počítači, nacházejícími se na amerických univerzitách, se odehrála v roce 1968. Do dějin se pak tento významný historický moment zapsal jako Arpanet (Advanced Research Projects Agency Network). O 15 let později, tedy na začátku roku 1983, byl trvale uveden do provozu dnes neznámější a nejrozšířenější hlavní protokol TCP/IP (Transmission Control Protocol/Internet Protocol), umožňující díky souboru pravidel komunikaci a výměnu dat mezi zařízeními. Tvůrci tohoto protokolu v době

jeho implementace nekladli důraz na bezpečnost, což dnes vyústilo k páchání, mimo jiné, trestných činů, jejichž pachatelé využívají právě slabin z rodiny protokolu TCP/IP. (Jirovský, 2007)

Počítačovou síť lze rozdělit dle mnoha kritérií, jako je například dělení dle přepojování, postavení uzlů, jejich rozlehlosti nebo dle druhu přenášení signálu. V praxi se zpravidla rozlišují dva druhy počítačových sítí, a to lokální počítačová síť LAN (Local Area Network), případně WLAN (Wireless Local Area Network) a rozlehlá počítačová síť spojující několik lokálních počítačových sítí WAN (Wide Area Network). Nejznámější počítačovou sítí řady WAN je pak Internet. Počítačovou síť jako takovou tvoří celá řada síťových prvků, díky kterým se realizuje spojení a probíhá výměna dat mezi zařízeními, která jsou v této konkrétní síti připojena. Pro účely této práce budou počítačové sítě rozděleny pouze dle způsobu propojení připojených zařízení, neboť dle autora této práce je to stěžejní a často podceňovaná problematika v oblasti kybernetické bezpečnosti.

Propojení jednotlivých zařízení v síti je tedy možné uskutečnit:

a) fyzickým zapojením (LAN i WAN) nebo dnes již častěji
b) bezdrátovou technologií (WLAN) a ve specifických případech
c) virtuálně (VLAN).

1.3.1 Fyzické zapojení (LAN)

Při fyzickém propojení zařízení v počítačové síti je využíváno metalických i optických kabelů, případně jejich kombinace. Příkladem metalického kabelu je stále používaná kroucená dvoulinka osazená konektory RJ-45. Výhodou této metody jsou vysoké přenosové rychlosti a z hlediska kybernetické bezpečnosti je to i vyšší stupeň bezpečnosti, samozřejmě v kombinaci s dalšími opatřeními, jako je fyzická bezpečnost, pod ní spadající režimová opatření, bezpečnost informačních nebo komunikačních systémů a další. Tento fakt je zapříčiněn samotnou podstatou fyzického zapojení, respektive kabeláží, kterou jsou připojena v síti veškerá zařízení. V kombinaci se správným umístěním klíčových síťových prvků v zabezpečené místnosti (serverovně) je v případě útoku na takto vybudovanou podnikovou síť, bez prostupu na internet, nutné překonat uvedená opatření a fyzicky se dostat ke klíčovým síťovým prvkům, což je velmi obtížné. Za nevýhodu fyzického zapojení lze s ohledem na rozlehlost této sítě považovat vyšší finanční náklady spojené především s nákupem kabeláže. (Česko, 2005)

1.3.2 Bezdrátová technologie (WLAN)

Podnikovou i domácí počítačovou síť je možno vybudovat i bez použití metalických či optických kabelů, pak je využíváno bezdrátové technologie, označované jako Wi-Fi (méně častěji WLAN), využívající standardu IEEE 802.11. Ovšem stále se jedná o lokální počítačovou síť (LAN). Zde autor této práce považuje za nutné upozornit na skutečnost, že v praxi se často chybně za Wi-Fi označuje připojení na internet (nejčastěji prostřednictvím mobilního telefonu), ale ve skutečnosti, jak již bylo výše zmíněno, Wi-Fi označuje pouze bezdrátovou komunikaci jednotlivých zařízení v počítačové síti. Nikoli připojení k internetu, které musí být realizováno jiným způsobem. Provoz této bezdrátové technologie využívá tzv. bezlicenční frekvenční pásmo na základě všeobecných oprávnění VO-R/12/12.2019-10 a VO-R/10/12.2019-9 pro pásmo 2400 – 2483,5 MHz (známé jako 2,4 GHz) a dále VO-R/12/12.2009-10 a VO-R/10/12.2019-9 pro pásmo 5 GHz, v čemž spočívá jeho velká výhoda představující vybudování levné a zároveň poměrně výkonné počítačové sítě. Naopak nevýhodu tohoto řešení představuje z hlediska této práce bezpečnost takto realizované počítačové sítě, neboť nelze omezit šíření signálu mimo žádoucí prostory a potencionální útočník může, za využití potřebných speciálních zařízení, do této počítačové sítě získat přístup. Jsou všeobecně známé případy, kdy byla ze strany útočníka narušena integrita bezdrátové sítě využívající standard (bezpečnostní protokol) WPA3, který byl vydán v roce 2018 společností Wi-Fi Alliance jako standard nové generace neumožňující prolomení hesla. (Two security researchers find WPA3 vulnerabilities, 2014 – 2021), (Vulnerabilities in the WPA3 Wi-Fi Security Protocol)

1.3.3 Virtuální řešení (VLAN)

Virtuální lokální počítačovou síť je možno vybudovat prostřednictvím speciálních síťových prvků, zatímco ty v praxi nejpoužívanější nabízí firma Cisco. Z pohledu běžného uživatele informačních systémů není VLAN nikterak odlišná od klasické LAN, ale pro správce počítačových sítí představuje nedoceněné usnadnění správy, umožňující i simulaci před nasazením nových technologií. Podstatou je rozdělení jedné fyzické lokální počítačové sítě (LAN) na více virtuálních lokálních sítí (VLAN), v souladu se standardem IEEE 802.1Q, mezi kterými je možno libovolně trasovat síťový provoz. Klíčové jsou zde trunk linky, které představují fyzické spoje jednotlivých VLAN. Výhodou tohoto řešení je z pohledu této práce vyšší efektivita a bezpečnost takto řešených sítí a nedoceněná možnost fyzicky propojená zařízení v počítačové síti rozdělit do několika sítí, jako by propojená nebyla. Nevýhodou

jsou vyšší finanční náklady v podobě speciálních síťových prvků a potřebné znalosti správce sítě.

1.4 Internet

S mírnou nadsázkou lze uvést, že internet je zvláštním případem počítačové sítě. Jak již bylo uvedeno k pojmu počítačové sítě, kdy se jedná o spojení alespoň dvou zařízení, která spolu navzájem komunikují, v případě internetu (WAN) se jedná o síť, kterou tvoří několik desítek tisíc výše definovaných počítačových sítí, ať už LAN, WLAN nebo VLAN. Provoz těchto jednotlivých počítačových sítí zajišťují vlády, univerzity, národní a nadnárodní organizace, obchody a v krajním případě i domácnosti. Česká republika se k této celosvětové síti připojila roku 1992.

Je podstatné podotknout, že veškeré informace, případně data, která uživatel publikuje na internetu, je možno kýmkoli, kdo má k této síti přístup, uložit, zkopírovat nebo libovolně přenášet. K této skutečnosti dochází mnohdy automaticky ze strany webových vyhledávačů, které si do své mezipaměti ukládají data o webové stránce, kterou uživatel navštívil. Tato data jsou dále využívána k cílené reklamě ze strany provozovatelů webových vyhledávačů. Obdobně je v rámci celého internetu zajištěn i archiv webových stránek. V České republice je tato služba známá pod názvem Webarchiv a její provoz zajišťuje Národní knihovna České republiky. Závěrem je tedy zřejmé, že v internetové síti zůstávají veškeré informace a data, která sem kdy byla vložena, i přesto, že jsou z původního zdroje vymazána. (Barták, Bečvář a Bechyně et al., 1999), (How it Works), (Webarchiv)

2 KYBERNETICKÁ BEZPEČNOST

Po definování pojmů v předchozí kapitole je snadnější uchopit pojem bezpečnosti, respektive kybernetické bezpečnosti. I přesto, že neexistuje žádná ustálená definice, je tento pojem velmi skloňovaný napříč mnoha odvětvími. Většina odborných publikací pojem kybernetické bezpečnosti neobjasňuje, pouze se o něm zmiňuje a případné definice jsou mnohdy protichůdné. Nejlogičtější se zdá to, když budeme hledat definici tohoto pojmu v legislativě. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, definuje v čl. 1 bezpečnost takto:

„*Zajištění svrchovanosti a území celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu*.“ (Česko, 1998)

Bohužel v případě definice již zmíněného pojmu kybernetické bezpečnosti je to složitější. Důvodem je mimo jiné i fakt, že většina lidí nevěnuje této oblasti patřičný důraz a je toho názoru, že se touto oblastí zabývají pouze zainteresovaná oddělení státní správy. Opak předchozí věty je však pravdou. Je důležité si uvědomit, že každý uživatel informačních a komunikačních technologií je stěžejním prvkem v oblasti kybernetické bezpečnosti.

Další důležitou judikaturou v této oblasti je bezesporu zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, jeho prováděcí vyhlášky a dále pak zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů. Bohužel ani tyto právní předpisy nepracují s vlastním pojmem kybernetické bezpečnosti. Pouze se zmiňují o stavu kybernetického nebezpečí, kdy je ohrožena bezpečnost informací v informačních a komunikačních systémech, případně bezpečnost celistvosti sítí elektronických komunikací. (Kolouch, 2016), (Kolouch, Bašta et al., 2019), (Česko, 2014), (Česko, 2005)

Poměrně výstižná definice kybernetické bezpečnosti je uvedena v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020:

„*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)

Takto definovaný pojem kybernetické bezpečnosti není dle autora této práce vhodný, protože se omezuje jen na území České republiky a opomíjí lokální informační a komunikační technologie, které nemusí být součástí v definici uvedeného kyberprostoru. Zajímává definice kybernetické bezpečnosti je pak uvedena ve Výkladovém slovníku kybernetické bezpečnosti:

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

K takto definované Jiráskově kybernetické bezpečnosti ve Výkladovém slovníku kybernetické bezpečnosti Kolouch a kol. v publikaci CyberSecurity uvádí:

„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)

Po důkladném rozboru Jiráskovy definice v kombinaci s argumentem z publikace CyberSecurity nezbývá než dát Kolouchovi a kol. za pravdu. Naštěstí tito autoři přicházejí v tomto díle s vlastní definicí kybernetické bezpečnosti:

„*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)

Autor této práce považuje tuto definici kybernetické bezpečnosti za komplexní, neboť naprosto vystihuje současné chápání tohoto pojmu a nesklouzává, jako jiné definice, do uvádění dalších nedefinovaných pojmů. Dále se tato definice jako ta v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 neomezuje pouze na území konkrétního státu, případně jeho součásti, pamatuje i na nutnost reagovat na kybernetické útoky a předpokládá obnovu funkčnosti napadených počítačových systémů

a služeb. Závěrem tato definice pamatuje i na lokální informační a komunikační technologie, které nejsou součástí kyberprostoru.

Alfou a omegou kybernetické bezpečnosti jsou bezesporu její triády, prostřednictvím kterých se kybernetická bezpečnost aplikuje v praxi. Pro účely této práce budou v následujících kapitolách vymezeny neznámější triády.

2.1 Triáda CIA

Podstata této triády vychází z ustanovení §5 písm. e) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, kdy se pravděpodobně jedná o nejznámější triádu kybernetické bezpečnosti tvořenou dle výše uvedeného ustanovení důvěrností, integritou (celistvostí) a dostupností dat či informací. Zkratka CIA pak vychází z počátečních písmen anglického Confidentiality, Integrity a Availability:

a) Důvěrnost v tomto kontextu představuje zpřístupnění informací pouze autorizovaným osobám, tedy osobám, které jsou oprávněny se s nimi seznamovat. Jako příklad lze uvést rozdělení informací dle citlivosti jejich obsahu na Vyhrazené, Důvěrné, Tajné a Přísně tajné v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,

b) integrita, případně celistvost, znamená nutnost ochránit systém nebo službu tak, aby nedocházelo k jejich neoprávněné úpravě, případně k jejich úpravě neoprávněnou osobou,

c) závěrem se rozumí dostupností zajištění vlastního běhu systému vždy, kdy to uživatel vyžaduje. Stupnice pro hodnocení důvěrnosti, integrity a dostupnosti je pak uvedena v příloze č. 1 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti. (Česko, 2005), (Kolouch, Bašta et al., 2019)

Parkerian Hexad

Dle některých autorů odborných publikací je však výše uvedený model nedostačující a v praxi je mnohdy rozšiřován. Nejznámější rozšíření provedl Donn B. Parker, který triádu CIA rozšířil o držení či kontrolu, pravost a užitečnost.

Odborně se pak tento model nazývá Parkerian Hexad:

a) držení či kontrolu představuje v tomto modelu stav, kdy dojde ze strany neoprávněné osoby k získání kontroly nad systémem nebo službou, kterou nevlastní, a zároveň nedojde k zneužití získaných dat, případně informací,

b) k narušení pravosti dojde v případě, že výměna dat nebo informací probíhá mezi zdroji (zdrojem), které se za pravé pouze vydávají (například zrcadlení webových stránek),

c) užitečností dat či informací je zamýšlen často opomíjený fakt, zda jsou neoprávněně získaná data či informace v užitečném stavu, tedy zda jsou nebo nejsou zašifrována. Pokud data zašifrována jsou a neoprávněná osoba nemá dešifrovací klíč, nejsou získaná data v užitečné podobě, a nedošlo tak k narušení kybernetické bezpečnosti. (Pender-Bey)

Obrázek 1: Parkerian Hexad (Pender-Bey)

2.2 Prvky kybernetické bezpečnosti

Mezi prvky kybernetické bezpečnosti, které ji určitou mírou tvoří, případně zajišťují, patří lidé, technologie a procesy:

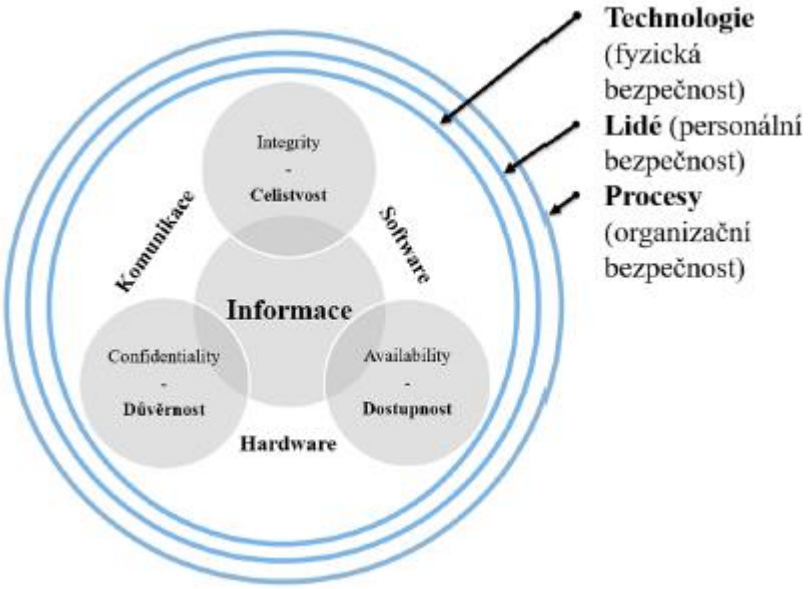
a) Lidé jsou velmi často stěžejním prvkem v oblasti kybernetické bezpečnosti a bohužel mnohdy představují nejslabší článek.

„Only amateurs attack machines; professionals target people“ (Schneier, 2000)

Této skutečnosti si je vědoma i drtivá část útočníků, kteří následně v kyberprostoru cíleně útočí na lidi. Podstatným krokem k eliminaci rizika spočívajícího právě v uživatelích je oblast sebevzdělávání. Je nutné, aby uživatelé pochopili alespoň základní principy kybernetické bezpečnosti, a předcházeli tak kybernetickým útokům.

b) Technologie čítají poměrnou část vložených finančních prostředků do zabezpečení, představují celou řadu technologických zařízení, počínaje zařízením nainstalovaným na vstupní bráně (firewallem) přes antivirovou ochranu až po kancelářské balíčky pro tvorbu a úpravu dokumentů. Naprostou samozřejmostí je, aby veškeré technologie byly provozovány a udržovány aktuální, jak po stránce hardwarové, tak po stránce softwarové.

c) Závěrem je tu činnost označovaná jako procesy. Tu je nutné vynaložit, aby lidé mohli využívat výše uvedené technologie a s nimi spojené poskytované služby. Tato činnost je bezesporu nejnáročnější pro administrátory, kteří nastavováním a údržbou procesů kybernetickou bezpečnost vytvářejí a udržují. (Kolouch, Bašta et al., 2019)



Obrázek 2: Triáda CIA doplněná o technologie, lidi a procesy (Kolouch, Bašta et al., 2019)

2.3 Životní cyklus kybernetické bezpečnosti

Při samotném aplikování kybernetické bezpečnosti je nutné, mimo triádu CIA a prvky kybernetické bezpečnosti, brát ohled také na prevenci, detekci a reakci na potencionální útok. Samotný životní cyklus kybernetické bezpečnosti je zpravidla prezentován prostřednictvím různých diagramů.

Dle jedné z odborných definic je možno popisovaný životní cyklus přirovnat k analýze rizik, u které bude v průběhu času donekonečna přibývat výčet možných chyb ve vztahu ke kybernetické bezpečnosti zájmového objektu. (Kolouch, Bašta et al., 2019)

Obrázek 3 Znázornění životního cyklu kybernetické bezpečnosti (Kolouch, Bašta et al., 2019)

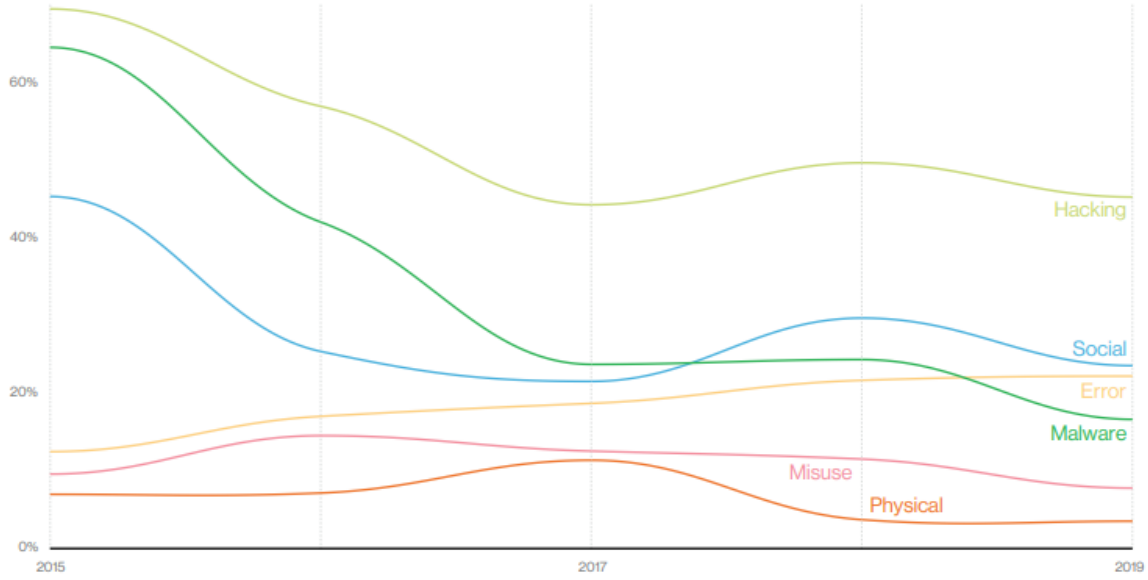
Ve své podstatě je tedy životní cyklus kybernetické bezpečnosti neustále se opakující smyčka, kdy na jedné straně jsou nové kybernetické hrozby a na straně druhé odpovídající opatření. Ve vztahu k této smyčce je potencionální útočník vždy o krok napřed.

Tento fakt je zřejmý i z následujícího obrázku, který prezentuje životní cyklus exploitu, tedy programu, který využívá slabin zájmového objektu. (Jirovský, 2007)

Obrázek 4 Životní cyklus exploitu (Jirovský, 2007)

3 KYBERNETICKÉ A BEZPEČNOSTNÍ HROZBY

Pro mnoho uživatelů informačních a komunikačních technologií představuje pojem kybernetické, případně bezpečností hrozby ve vztahu k této oblasti pouze škodlivý kód, označovaný jako malware, který se bez jejich vědomí dostal do počítače a obecně má za cíl škodit. Bohužel je faktem, že v posledních třech letech je škodlivá činnost malwaru z celosvětového hlediska na ústupu a v popředí se dle dat (pro rok 2020) z Data Breach Investigations Report stále drží hacking a sociální inženýrství.



Obrázek 5: Nežádoucí aktivity v průběhu času ve světě (Data Breach Investigations Report, 2020)

Na tento fakt má dle autora této práce zásadní vliv vědomí útočníků, že jsou v kyberprostoru na rozdíl od skutečného světa jen těžko polapitelní. Kyberprostor, jak již bylo v jeho definici zmíněno, je virtuální svět bez hranic. Útočníci velice často svými aktivitami přesahují v kyberprostoru skutečné hranice států a v kombinaci s poměrně nízkými tresty, které se za prokázanou protiprávní činnost v této oblasti udělují, pro ně není potencionální postih odstrašující. Nejen z tohoto důvodu byla v roce 2001 sjednána Úmluva Rady Evropy o počítačové kriminalitě a Česká republika ji v roce 2013 ratifikovala. Předmětem této úmluvy je sjednocení skutkových podstat trestných činů v oblasti kybernetické kriminality a možnost jednoduššího stíhání pachatelů. (Donát a Tomíšek, 2016)

Předmětná Úmluva o počítačové kriminalitě v čl. 2 až čl. 10 jmenovitě definuje tyto trestné činy:

a) nezákonný přístup,

b) nezákonný odposlech,

c) zasahování do dat,

d) zasahování do systému,

e) zneužívání zařízení,

f) počítačové padělání,

g) počítačový podvod,

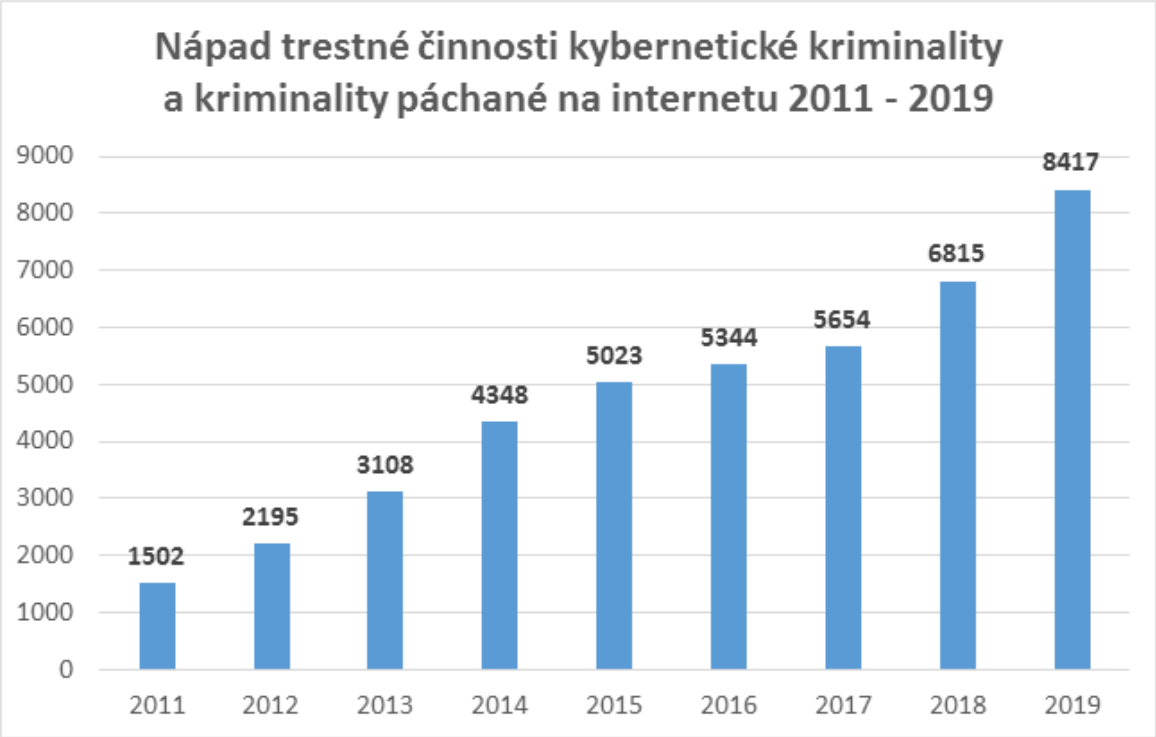
h) trestné činy související s dětskou pornografií,

i) trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským. (Česko, 2013)

Při zohlednění známé triády CIA, která byla popsána v kapitole Kybernetická bezpečnost, je zřejmé, že trestné činy definované úmluvou, výše uvedené v bodě a) až e), jsou v rozporu s touto triádou, neboť bezprostředně narušují důvěrnost, integritu a dostupnost dat prvků ICT.

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019 jasně vyplývá, že kybernetická kriminalita v posledních letech rapidně stoupá a bohužel je ve většině případů mířena proti státní správě a územní samosprávě. Ze zprávy dále vyplývá, že státní správa a samospráva se v drtivé většině setkává se spamem (52 %) a podvodnými e-maily (23 %). (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020, online)

Dle statistiky nápadu trestné činnosti kybernetické kriminality je zřejmé, že za rok 2011 byl nápad trestné činnosti v této oblasti 1502 případů, po dvou letech, tedy v roce 2013, se počet případů zdvojnásobil, zatímco rok 2019 zaznamenal rapidní nárůst nápadu trestné činnosti kybernetické kriminality, v České republice je evidováno 8417 případů. (Kyberkriminalita, © 2020)



Obrázek 6: Nápad trestné činnosti kybernetické kriminality (Kyberkriminalita, © 2020)

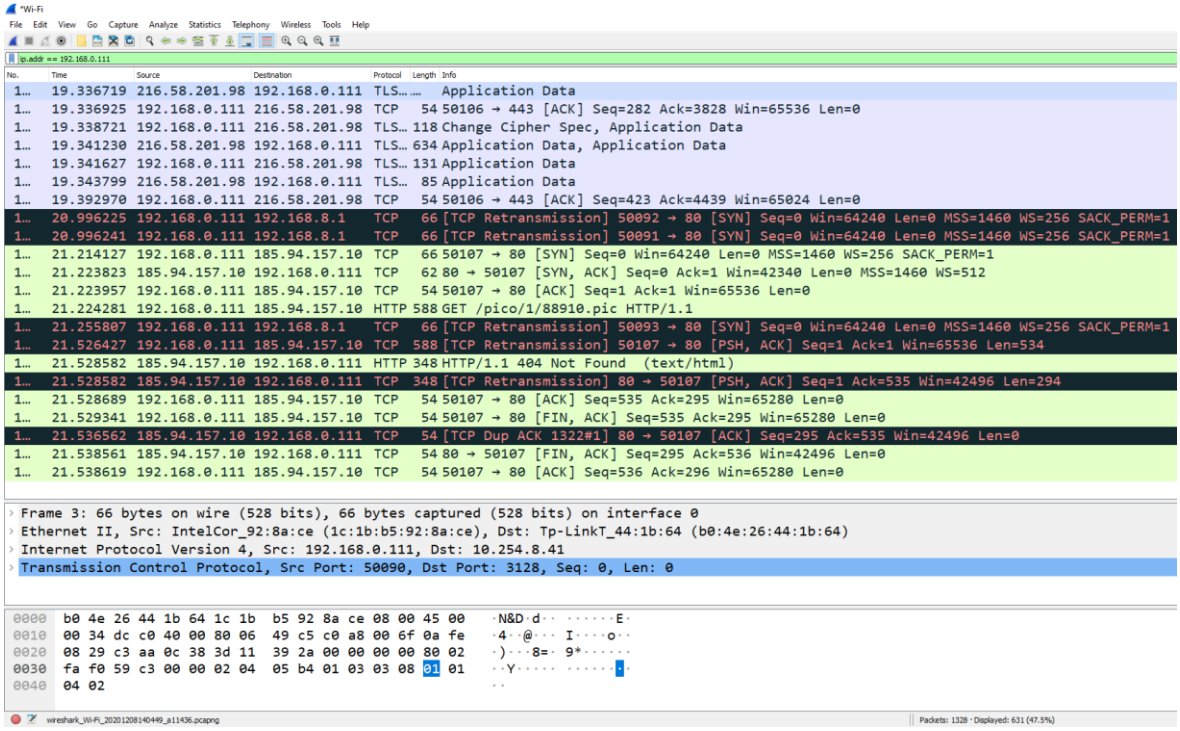
Z výše uvedených dat je již známo, že kybernetických a bezpečnostních hrozeb je celá řada. Prostřednictvím těchto hrozeb jsou naplňovány skutkové podstaty výše vyjmenovaných trestných činů. Velice často je však autory odborných publikací opomíjena zhrzenost zaměstnanců, neodbornost administrátorů, špatné řešení fyzické bezpečnosti, ale i třeba drobnosti v podobě neprováděných záloh dat nebo neumístění důležitých prvků ICT do klimatizované a bezprašné místnosti. Pro účely této práce budou definovány pouze základní kybernetické a bezpečnostní hrozby, které jsou často zmiňované v médiích.

3.1 Hacking, cracking

Jako hacker byl v padesátých letech minulého století označován technicky zdatný jedinec. S příchodem počítačů se začal slovem hack označovat způsob vyřešení určitého problému. Vůbec za prvního hackera je pak považován John Draper, který využil nedokonalého zabezpečení telefonní sítě a pomocí pravděpodobně prvního hackerského nástroje blue-box uskutečňoval telefonní hovory zdarma. Téměř o třicet let později, kdy byl zaveden pojem hacker, nastal rozmach této činnosti. Začaly vznikat první hackerské skupiny, které sdílely informace o zjištěných heslech prvních počítačů, případně se je snažily prolomit. (Jirovský, 2007)

Po nástupu prvních webových technologií vznikají speciální hackerské nástroje, které jsou označovány různými názvy a jsou sdíleny na prvních hackerských webových stránkách. Tyto nástroje i dnes využívají tzv. zadních vrátek, respektive bezpečnostních děr v systémech. Tato činnost vyvrcholila na přelomu tisíciletí, kdy byly mimo jiné ukradeny zdrojové kódy operačního systému Windows. Microsoft na to zareagoval tak, že přerušil vývoj operačního systému a asi osm tisíc programátorů vyškolil v oblasti bezpečnosti. Od té doby používají hackeři diagnostické nástroje na analýzu síťového provozu a zautomatizování útoků. (Jirovský, 2007)

Příkladem výše zmíněného nástroje pro analýzu síťového provozu může být Wireshark, který je volně dostupný na internetu. Pro názornou ukázku autor práce vybudoval testovací WLAN, ke které připojil počítač, tento nástroj na něm spustil a přes webový prohlížeč provedl připojení na server seznam.cz, viz obrázek č. 7.



Obrázek 7: Analýza síťového provozu prostřednictvím nástroje Wireshark

S nástupem celosvětové sítě internet si mnoho firem začalo chránit svoje soukromí a data, což změnilo pohled na hackery. Hackeři jsou stále považováni za osoby s nadprůměrnými znalostmi v oblasti výpočetní techniky, ale veřejně jsou chápáni v negativním slova smyslu. Pozitivem na činnosti hackerů je jejich tlak na zvyšování bezpečnosti informačních a komunikačních technologií. (Jirovský, 2007)

V poslední době však došlo k vymezení dalšího pojmu, a to cracker. Crackerem je ve své podstatě myšlen hacker, tedy člověk, který má velmi vysoké znalosti, zpravidla v oblasti programování, avšak tyto znalosti využívá k páchání trestné činnosti proti informačním a komunikačním technologiím. Zatímco hacker je v dnešní době ceněn, neboť zpravidla upozorňuje na bezpečnostní díry a nezabývá se, na rozdíl od crackera, nelegální činností. Bohužel média tyto dva pojmy často zaměňují, státní správa a jí vydávané dokumenty, například Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, mluví o hackerech jakožto o útočnících zaměřujících se na lukrativní cíle, které pro ně mohou znamenat vyšší zisk. Případně se zavádí obecný pojem hacktivisté, ale pojem crackera se nezmiňuje. (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020)

Pro účely této práce tedy nezbývá než pojem hackingu i crackingu sjednotit a obecně ho chápat jako nelegální či trestnou činnost útočníků (hacktivistů) namířenou proti informačním a komunikačním technologiím, zpravidla za účelem zisku.

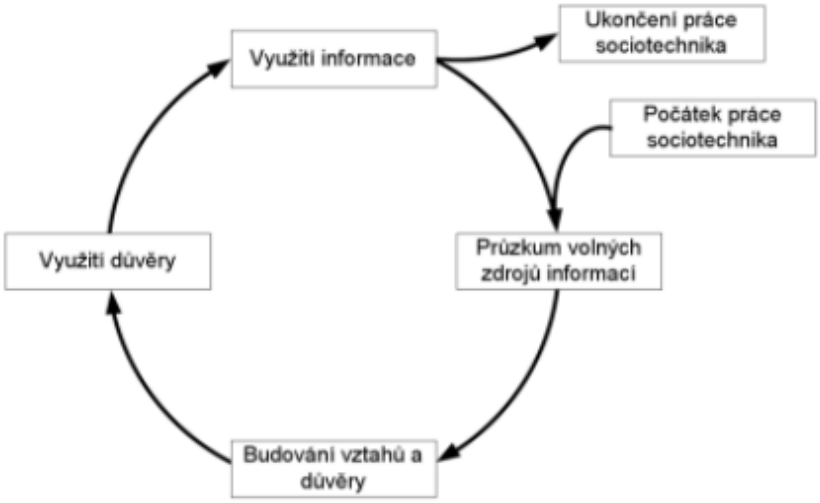
3.2 Sociální inženýrství

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

Takto úvodem před třinácti lety definoval Jirovský v publikaci Kybernetická kriminalita dějiny sociálního inženýrství, potažmo sociální inženýrství jako takové. Bohužel i dnes jsou jeho slova více než aktuální. Útočník praktikující sociální inženýrství není hacker (cracker) a mnohdy nemá ani potřebné znalosti v oblasti počítačů. V odborné literatuře je nazýván sociotechnikem, tedy člověkem, který vzbuzuje důvěru a následně manipuluje nejslabší článek kybernetické bezpečnosti – člověka. Tuto činnost zpravidla provádí za účelem získání citlivých informací z různých institucí. Nejznámějším případem sociálního inženýrství je tzv. Mitnickova aféra. (Jirovský, 2007)

Kevin Mitnick byl odsouzen za nelegální počítačovou činnost, prostřednictvím které se mimo jiné naboural do počítačových sítí známých firem, jako je Nokia, Motorola nebo IBM. I přesto, že měl vysokoškolské vzdělání v oblasti informatiky, výše uvedené nelegální činnosti vykonal prostřednictvím sociálního inženýrství, kdy pod různými záminkami manipuloval se zaměstnanci těchto firem, kteří ho pak lidově řečeno pustili do systému. Kevin Mitnick si za tuto činnost vysloužil trest odnětí svobody v délce trvání pěti let a zákaz používání jakýchkoliv informačních a komunikačních technologií, včetně zákazu přístupu na internet. V roce 2002 vydal svoji knihu s názvem The Art of Deception: Controlling the

Human Element of Security a dnes je vyhledávaným bezpečnostním konzultantem. (Kevin Mitnick, 2020)



Obrázek 8: Sociotechnický cyklus (Jirovský, 2007)

Metod sociálního inženýrství je celá řada, všechny ale mají společný cíl, který spočívá ve vzbuzení důvěry zpravidla významného zaměstnance, prostřednictvím kterého pak sociotechnik získá přístup do systému. Nejznámější a bohužel i nejčastější případy sociálního inženýrství, respektive útoku, jsou praktikovány prostřednictvím podvodných e-mailů nebo v kombinaci s nimi, jejichž cílem může být například získání hesla uživatele. Dle dat Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019 je zřejmé, že jsou tyto techniky praktikovány stále častěji, především pak cílí na státní správu, samosprávu a zdravotnictví. (Jirovský, 2007), (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020)

3.3 Malware

Tento pojem je spojením dvou anglických slov, tedy malicious (zákeřný, zlomyslný, škodlivý) a software. Malware, jak již v této práci bylo zmíněno, je jakýkoli škodlivý program, který se bez vědomí uživatele dostal do jeho, v práci definovaného, počítače a obecně má za cíl škodit. Paylodem se pak nazývají instrukce v konkrétním škodlivém kódu, tedy příkazy, které tento zlomyslný software provádí. I s ohledem na fakt, že malware se může šířit mnoha způsoby, nejohroženější jsou počítače připojené k celosvětové síti internet. Malware lze rozdělit mnoha způsoby. Bohužel s ohledem na rostoucí množství, kvalitu a kombinaci různých druhů malwaru není možné toto rozdělení provést aktuálně. S ohledem na zaměření této práce a s přihlédnutím ke Zprávě o stavu kybernetické

bezpečnosti České republiky za rok 2019, kdy byly podlé této nejčastějšími typy útoků především spam, phishing a podvodné e-maily, kdy:

„Největší výskyt byl zaznamenán u územních samosprávných celků…“ (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019),

budou následně vymezeny pouze základní druhy malwaru. (Donát a Tomíšek, 2015), (Král, 2015), (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020), (2015 Internet Security Threat Report: Attackers are bigger, bolder, and faster, 2015)

3.3.1 Základní dělení malwaru

Adware

Adware představuje jakoukoliv reklamu, která je nevyžádaná, ať už ve formě automatického vyskakování oken při otevření internetového odkazu nebo jako nenápadná součást zpravidla bezplatného softwaru. Nejznámější celosvětová síť je adwarem přímo zahlcena. (Král, 2015)

Backdoor

Backdoor, čili zadní vrátka, je druh malwaru, který zpravidla sám o sobě žádnou činnost nevykonává, ale umožňuje útočníkům nepozorovaně vstoupit do počítače (i jiných zařízení) a jeho data nebo výkon využívat ke svému dalšímu prospěchu. (Král, 2015)

Dialer

Původní předmět činnosti tohoto škodlivého kódu již téměř vymizel. Dnes lze dialerem označit napadení mobilního telefonu, kdy takto infikované zařízení následně nepozorovaně odesílá prémiové textové zprávy (SMS). (Král, 2015)

Spyware

Spyware je označení pro „šmíráky“, potažmo špinonážní programy shromažďující údaje o uživateli napadeného zařízení. Mezi tyto údaje pak mohou patřit zvyklosti uživatele, osobní údaje, přístupové údaje a další. Speciálním typem tohoto malwaru je pak keylogger. (Král, 2015)

Keylogger

Jedná se o druh škodlivého softwaru zaznamenávajícího stisky kláves, které následně útočníci zpravidla dále využijí. (Král, 2015)

Ransomware

Prostřednictvím tohoto škodlivého programu útočníci, konkrétně tedy crackeři, požadují zaplacení smyšlené pokuty, často pod zástěrkou státní instituce. Horším případem je zašifrování dat na disku počítače, na základě čehož cracker požaduje peníze výměnou za dešifrování dat. (Král, 2015)

Scareware

Scareware je nabízen jako anti-malware, tedy antivirový nebo jiný bezpečnostní program, kdy jeho tvůrce tvrdí, že odstraní veškerý malware ze zařízení. Po instalaci a prvotní kontrole operačního systému detekuje několik infikovaných souborů, k jejichž odstranění požaduje provedení platby. Uživatel tak často zaplatí za bezcenný a fiktivní program, neboť neexistuje jediný program, který by byl schopen odstranit veškerý škodlivý obsah ze zařízení. (Král, 2015), (Bazzell, © 2014)

3.3.2 Způsob infiltrace malwaru

Trojský kůň

Trojský kůň je program tvářící se užitečně, někdy i potřebně. Může se jednat o hru, již zmíněný anti-malware, zaručující odstranění veškerého nežádoucího obsahu ze zařízení, i přehrávač médií, plnící svou zdánlivou funkci, avšak na pozadí vykonává další, často nežádoucí činnost k prospěchu crackera. V praxi se může například jednat o shromažďování dat za účelem cílené reklamy apod. (Král, 2015), (Doseděl, 2004), (Bazzell, © 2014)

Virus

Pojem viru je díky hrozbě, kterou představuje, velmi známý. Každoročně je na problematiku konkrétního viru upozorňováno sdělovacími prostředky. Obdobně jako biologický virus potřebuje i ten počítačový hostile, prostřednictvím kterého se nepozorovaně šíří, přičemž nejoblíbenějším hostitelem jsou flash disky. Pro samotné šíření a spuštění počítačového viru je využíváno spustitelných souborů (exe, bin apod.), které po spuštění aktivují samotný virus. Cílem samotného viru je pak získání kontroly nad infikovaným zařízením, ideálně celou počítačovou sítí. Počítačové viry lze dále rozdělit na jednotlivé typy:

a) boot viry,

b) viry programové,

c) makroviry,

d) groupwarové viry,

e) škodlivé Java a Active-x Aplety a

f) speciální viry.

V praxi však není toto dělení jednoduché, neboť většina virů je na základě typu a principu vykonávané činnosti kombinací výše uvedených. (Král, 2015), (Doseděl, 2004), (Kuchař, 1999)

Worm (červ)

Červ je škodlivý program, který ke svému šíření používá počítačovou síť, zpravidla tu největší internetovou. Nepotřebuje tedy hostitele jako virus. Jeho nejoblíbenější forma šíření je prostřednictvím elektronické pošty s lákavým názvem přílohy. Následné spuštění přílohy (červa) je obdobné jako spuštění počítačového viru. (Král, 2015), (Doseděl, 2004)

Bot a botnet

Bot a botnet je souhrnné označení pro další typ škodlivého programu infikujícího napadené zařízení a následně plnícího vzdálené příkazy útočníka. Takto infikovaná zařízení se označují jako „bot“ (od slova robot) a jsou shlukována do sítě „botnet“. V době, kdy crackerova síť čítá stovky takovýchto zařízení, je začne využívat ve svůj prospěch, který se navenek projevuje a dále dělí následovně:

a) DoS nebo DDoS útoky,

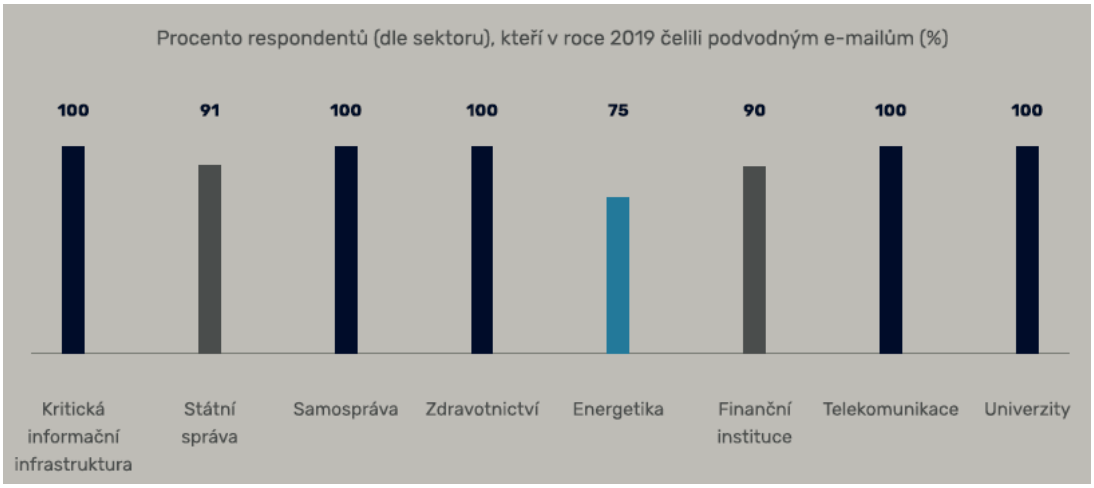
b) poplašné zprávy (hoax),

c) phishing a pharming,

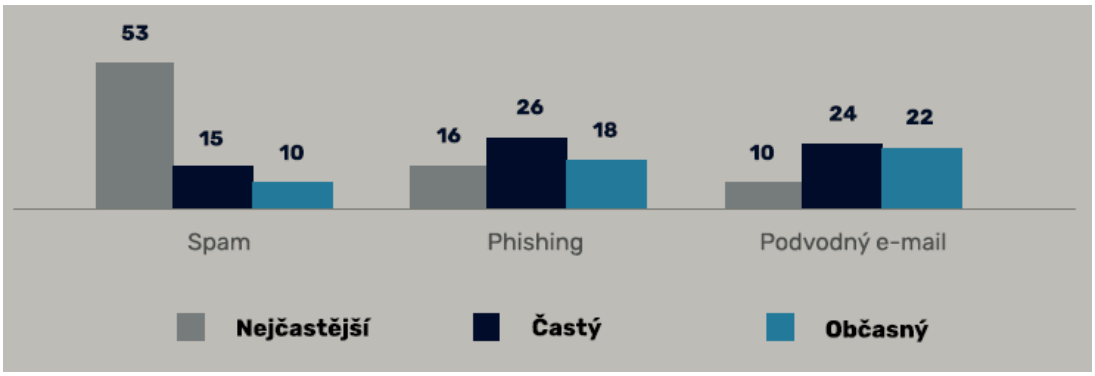
d) nigerejské podvodné e-maily,

e) falešné loterie,

f) spam a další. (Král, 2015)



Obrázek 9 Procento respondentů, kteří čelili podvodným e-mailům (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020)



Obrázek 10 Nejčastější typy útoků za rok 2019 (%) (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020)

4 NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) a po zdárném legislativním procesu i Vojenské zpravodajství ČR plní (bude plnit) významnou roli v oblasti kybernetické bezpečnosti (obrany), nejenom na úseku územních samosprávních celků. Ředitelé obou jmenovaných institucí se pak pravidelně účastní jednání Bezpečnostní rady státu a jsou členy Výboru pro kybernetickou bezpečnost. (Česko, 2017), (Vojenské zpravodajství zajišťuje kybernetickou obranu České republiky, 2021)

NÚKIB byl zřízen k 1. srpnu roku 2017 na základě zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), čímž získal roli hlavního orgánu pro kybernetickou bezpečnost v České republice. NÚKIB na úseku kybernetické bezpečnosti dále plní funkci správního orgánu a zajišťuje ochranu utajovaných informací v oblasti ICT a kryptografické ochrany. Součástí NÚKIB je i jeho výkonná sekce Národní centrum kybernetické bezpečnosti (dále jen „NCKB“) a organizačně pod něj spadající tzv. Vládní CERT. Jedná se o vládní bezpečnostní tým, který plní významnou roli v oblasti ochrany kritické informační infrastruktury i významných informačních systémů a provozovatele základní služby.

Kritéria, která určují, zda se jedná o jeden z výše jmenovaných, a tím pádem spadajících pod přímou působnost NÚKIB, potažmo NCKB, určují nařízení vlády č. 432/2010 Sb., nařízení vlády o kritériích pro určení prvku kritické infrastruktury, vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb., a konečně vyhláška č. 437/2017 Sb., vyhláška o kritériích pro určení provozovatele základní služby (NÚKIB, 2021), (NCKB, 2021), (Govcert.cz, 2021)

Ve vztahu k územním samosprávním celkům je pak, na základě uvedených vyhlášek, rozhodující například fakt, jaký má konkrétní obec počet obyvatel, respektive kolik osob je vedeno v její databázi, kdy pomyslná hranice je stanovena nad 12 500 osob (obyvatel). Pokud obec nesplní tuto a další podmínky vyplývající z uvedených právních předpisů, je vyňata z působnosti NÚKIB a správa její IT infrastruktury je zpravidla zajišťována za úplatu externí firmou z tohoto oboru. Následně se může jednat o kompletní správu v podobě dedikovaného serveru nebo údržbu prvků ICT, které jsou ve vlastnictví obce. Vybraná obec nesplňuje výše uvedená kritéria, a nespadá tak pod působnost NÚKIB. (Česko, 2010)

5 POPIS VYBRANÉ METODY FMEA

K provedení samotné analýzy rizik ve smyslu kybernetické bezpečnosti obce zvolil autor bakalářské práce metodu FMEA (Failure Mode and Effect Analysis). Tuto metodu mimo jiné upravuje norma ČSN EN 60812, a co se týče oblasti použití, nemá FMEA stanoveny žádné limity, proto se s nadsázkou hodí k analýze většiny procesů, systémů apod. Jejím cílem je nalézt potencionální chyby (selhání), jejichž závažnost vyjadřuje mírou rizika, označovanou jako RPN, či rizikové číslo. To je dáno výpočtem, který tvoří součin bodového hodnocení závažnosti, výskytu a odhalení potencionální chyby, přičemž interval bodových hodnocení výše uvedených tvoří celá čísla od 1 do 10 bodů ve vzestupné míře (dopadu). (Kocourek, 2012)

Prvním krokem při aplikování této metody je stanovení cíle analýzy a následné svolání týmu odborníků, kteří (například formou brainstormingu) provedou výčet možných problémů a z nich plynoucích následků. Následně se za využití stanoveného formuláře FMEA do tohoto vepíší výše uvedené potencionální problémy a následky a poté se těmto přiřazují bodová hodnocení ve smyslu jejich závažnosti, výskytu a odhalení, díky čemuž je na základě výpočtu stanoveno pro každý možný problém rizikové číslo. Závěrem se naleznou a vyhodnotí všechna riziková čísla, která přitahují naši pozornost, a k těmto možným chybám doplníme vhodná opatření. (Kocourek, 2012)

Tabulka 1 Kritérium závažnosti potencionální chyby

Slovní hodnocení závažnosti	Závažnost
Zanedbatelná závažnost možné chyby pro kybernetickou bezpečnost	**1**
Nezásadní závažnost možné chyby, bez většího ohrožení kybernetické bezpečnost	**2÷3**
Zvýšená závažnost možné chyby pro kybernetickou bezpečnost	**4÷6**
Vysoká závažnost možné chyby, kybernetická bezpečnost je ohrožena	**7÷8**

Slovní hodnocení závažnosti	Závažnost
Velmi vysoká závažnost možné chyby, hrozí bezprostřední ohrožení kybernetické bezpečnosti	**9÷10**

(Čech, 2001)

Tabulka 2 Kritérium (pravděpodobnosti) výskytu potencionální chyby

Slovní hodnocení (pravděpodobnosti) výskytu	Výskyt
Zanedbatelná pravděpodobnost výskytu možné chyby	**1**
Nízká (malá) pravděpodobnost výskytu možné chyby	**2÷3**
Zvýšená pravděpodobnost výskytu možné chyby	**4÷6**
Vysoká pravděpodobnost výskytu možné chyby	**7÷8**
Velmi vysoká pravděpodobnost výskytu možné chyby	**9÷10**

(Čech, 2001)

Tabulka 3 Kritérium (pravděpodobnosti) odhalení potencionální chyby

Slovní hodnocení (pravděpodobnosti) odhalení	Odhalení
Zanedbatelná pravděpodobnost neodhalení možné chyby	**1**
Nízká (malá) pravděpodobnost, že možná chyba nebude odhalena, současné zabezpečení je schopno odhalit možnou chybu	**2÷3**
Zvýšená pravděpodobnost, že možná chyba nebude odhalena, současné zabezpečení je schopno jen stěží odhalit možnou chybu	**4÷6**
Vysoká pravděpodobnost, že možná chyba nebude odhalena, současné zabezpečení není schopno možnou chybu odhalit	**7÷8**

Slovní hodnocení (pravděpodobnosti) odhalení	Odhalení
Velmi vysoká pravděpodobnost, že možná chyba nebude odhalena, současné zabezpečení není schopno možnou chybu odhalit	**9÷10**

(Čech, 2001)

Rizikové číslo je, jak již bylo zmíněno, vypočteno jako součin závažnosti, výskytu a odhalení potencionální chyby. Pro účely této bakalářské práce její autor stanovil tři rozsahy (intervaly) tohoto čísla následovně:

Tabulka 4 Intervaly rizikového čísla

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

Pomyslné hranice 125 a 614 bodů byly dány výpočtem, který autor práce stanovil pro:

a) zanedbatelné riziko jako součin 50% závažnosti, výskytu a odhalení (rizikové číslo $= 0{,}50^3 x\ 1000 = 125$),

b) závažné riziko jako součin 85% závažnosti, výskytu a odhalení (rizikové číslo $= 0{,}85^3 x\ 1000\ \doteq 614$).

Následná doporučení plynoucí z provedené analýzy budou stanovena pouze pro oblast významného a závažného rizika, tedy na intervalu rizikového čísla od 126 do 1000 bodů.

Brainstorming

Brainstorming označuje techniku prováděnou ve skupině, jejímž cílem je sestavit pro danou oblast či téma seznam možných idejí. Tak jako u metody FMEA je oblast použití brainstormingu velice široká a zpravidla se používá před samotnou metodou FMEA, kdy takto získáme výčet možných chyb, na jejichž základě postavíme analýzu metodou FMEA. (Brainstorming, © 2011-2016)

Pro účely bakalářské práce byla metoda brainstormingu omezena na konzultaci autora práce s kolegou ze zaměstnání, kdy takto byl stanoven výčet možných chyb.

II. PRAKTICKÁ ČÁST

6 POPIS VYBRANÉ OBCE

Vybraná obec se nachází v Jihomoravském kraji, přibližně 50 km jihozápadně od Brna. Rozloha této obce činí necelých 10 km^2 a trvale zde žije zhruba 1100 obyvatel. Z pohledu dopravní sítě prochází obcí jediná pozemní komunikace, silnice II. třídy. Tvar zastavěné části obce představuje pomyslný ležatý ovál, přičemž výše zmíněná silnice tvoří vodorovnou osu tohoto oválu. Jednotlivé stavby se pak nacházejí na obou polovinách pomyslného oválu a v obci jich je evidováno okolo čtyř set. Uprostřed horní poloviny pomyslného oválu leží náměstí, které obklopuje obecní úřad, základní škola a velmi lákavá kulturní památka, která je především v letních měsících velmi žádaná. Díky této turistické atrakci je poblíž, ze strany obce, zřízeno placené parkoviště, kdy takto získané příjmy tvoří nemalý příjem obce. Samotná platba za parkování se pohybuje v řádech desítek korun za den a je realizována prostřednictvím parkovacího automatu, který je obsluhován serverem umístěným na obecním úřadě. Obec je také vybavena kamerovým systémem, který tvoří 4 kamery, umístěné v okolí náměstí a již zmíněné kulturní památky, dále bezdrátovým místním rozhlasem, schopným plnit i funkci bezprostředního varování a vyrozumění obyvatelstva, a dále kvalitně zpracovaným a provozovaným webem i mobilní aplikací, informující především o dění v obci a poskytující bližší informace o již zmíněné kulturní památce.

Vybraná obec je také místem kontaktu veřejné správy (služba Czech POINT), zajišťující občanům výpisy z různých rejstříků. Důležité je o obci zmínit, že se nejedná o prvek kritické infrastruktury ve smyslu nařízení vlády č. 432/2010 Sb., nařízení vlády o kritériích pro určení prvku kritické infrastruktury, ani o provozovatele základní služby ve smyslu vyhlášky č. 437/2017 Sb., vyhláška o kritériích pro určení provozovatele základní služby, z čehož vyplývá, že obec je vymaněna z působnosti Národního úřadu pro kybernetickou a informační bezpečnost, což bylo zmíněno i v teoretické části. V praxi je pak veškerá správa informačních technologií obce zajišťována za úplatu externí firmou.

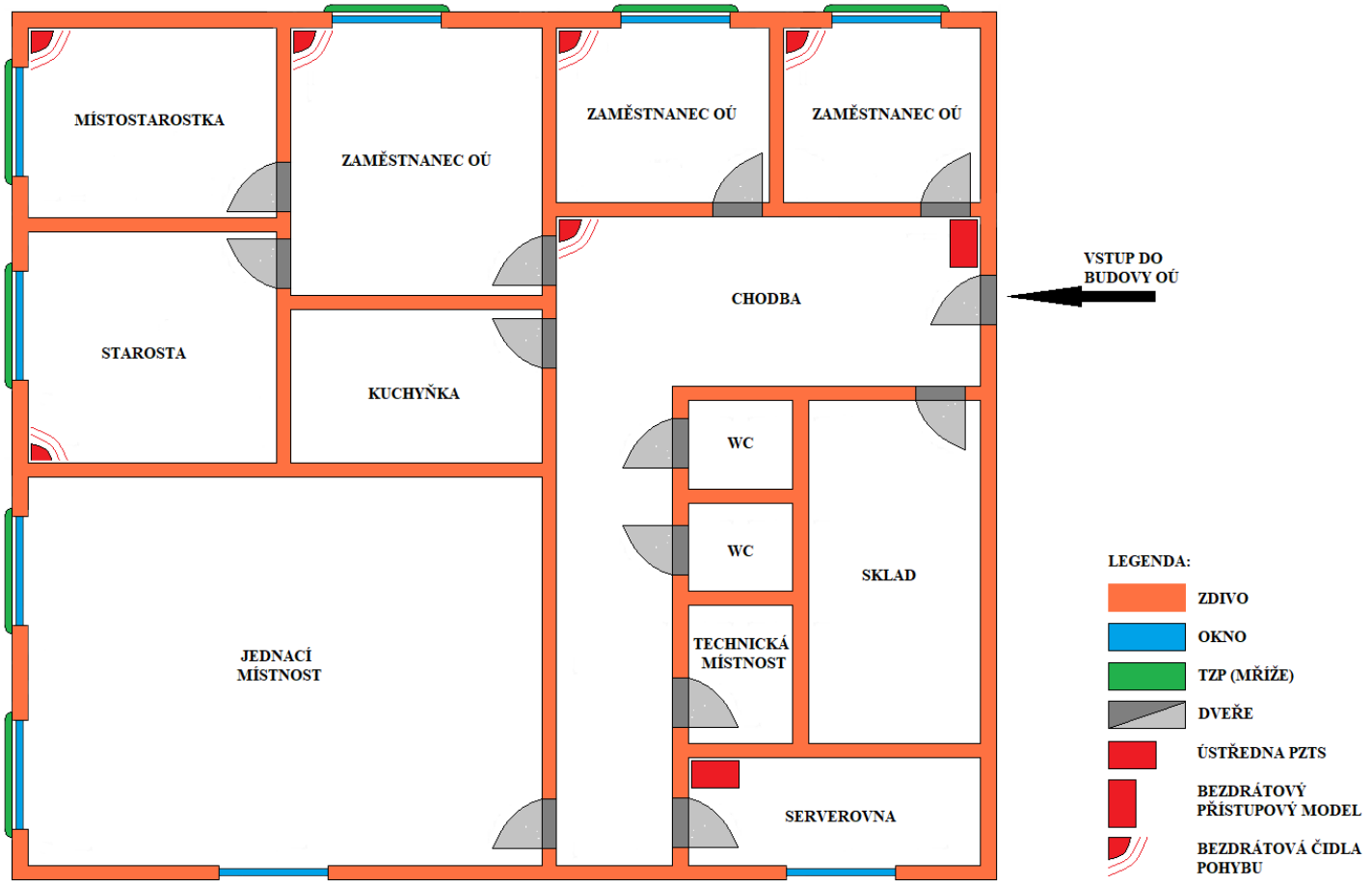
Výše zmíněný kamerový systém obce a bezdrátový místní rozhlas představují uzavřené systémy, bez přístupu k internetu. Z hlediska zaměření této práce bude kamerový systém i bezdrátový místní rozhlas obce opomenut.

Důležité je závěrem k této kapitole zmínit, že se nejedná o model obce, respektive obecního úřadu i lokální sítě. Vybraná obec i data prezentovaná v bakalářské práci jsou zcela reálná. Pouze na přání pana starosty diskutované obce zůstává tato anonymní.

6.1 Popis budovy obecního úřadu

Jak již bylo částečně zmíněno výše, obecní úřad vybrané obce společně se základní školou a kulturní památkou obklopuje náměstí této obce. Jedná se o jednu z nejstarších staveb, která se v obci nachází. Tento objekt má téměř čtvercový půdorys a tvoří jej jediné nepodsklepené podlaží se sedlovou střechou. Do budovy má trvale přístup pět osob: starosta, místostarostka, a další tři zaměstnanci, přičemž úklid budovy je zajištěn externí uklízečkou za dozoru některého ze zaměstnanců. Budova obecního úřadu je částečně zabezpečena PZTS od Jablotronu. Vstup do budovy je realizován jedinými dveřmi, které nejsou chráněny mřížemi. Při vstupu do objektu je vpravo za dveřmi umístěn bezdrátový přístupový modul s klávesnicí ovládající PZTS, přičemž celá budova obecního úřadu představuje ve smyslu PZTS jedinou sekci. Všech pět osob má tedy do budovy totožná přístupová práva. Samotná budova obecního úřadu pak disponuje pěti kancelářemi, kde jsou umístěny bezdrátové detektory pohybu a okna jsou z venku chráněna mřížemi, dále kuchyňkou, jednací místností, která je vybavena třemi okny, z nichž jsou pouze dvě zabezpečena mřížemi, serverovnou, taktéž vybavenou jedním oknem, které není chráněno mřížemi, skladem, technickou místností a pánskými i dámskými toaletami.

Nejzajímavější místností z pohledu zaměření této bakalářské práce je serverovna. Vstup do serverovny je realizován z chodby prostřednictvím dřevěných dveří, které se neuzamykají, tudíž do ní má přístup všech pět osob. Zde se nacházejí veškeré klíčové prvky zajišťující provoz lokální sítě vybrané obce: server, switch, Wi-FI router, záložní zdroj napájení, dále ústředna PZTS, síťový videorekordér zajišťující provoz a nahrávání videozáznamu z obecních kamer a ústředna místního rozhlasu včetně mikrofonu. Kabely spojující jednotlivé prvky sítě jsou vedeny po zdech v kabelové liště. Serverovna není vybavena klimatizací ani zabezpečena PZTS. Okno není z venku chráněno mřížemi, což již bylo výše zmíněno.

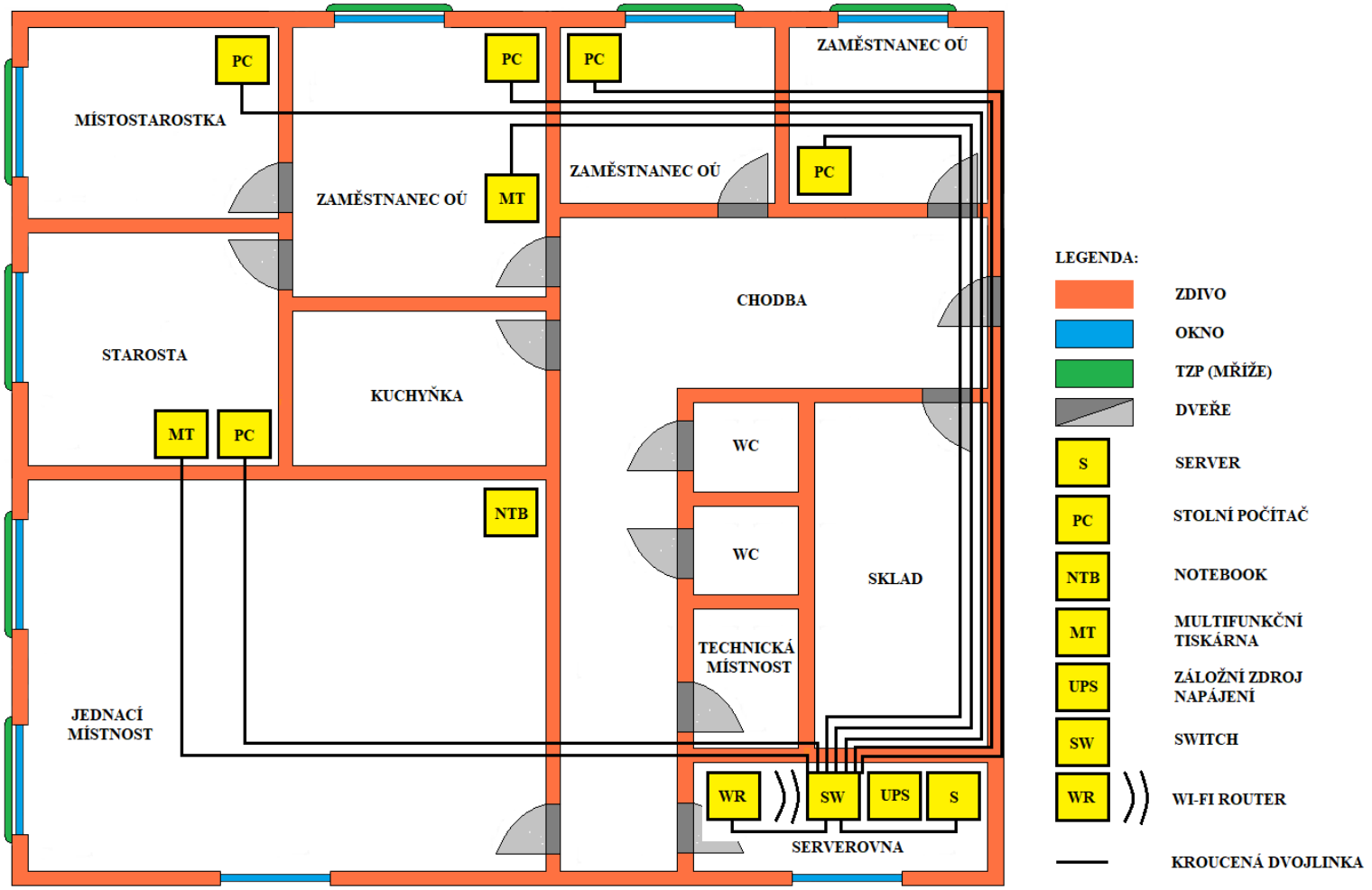


Obrázek 11 Půdorys budovy obecního úřadu

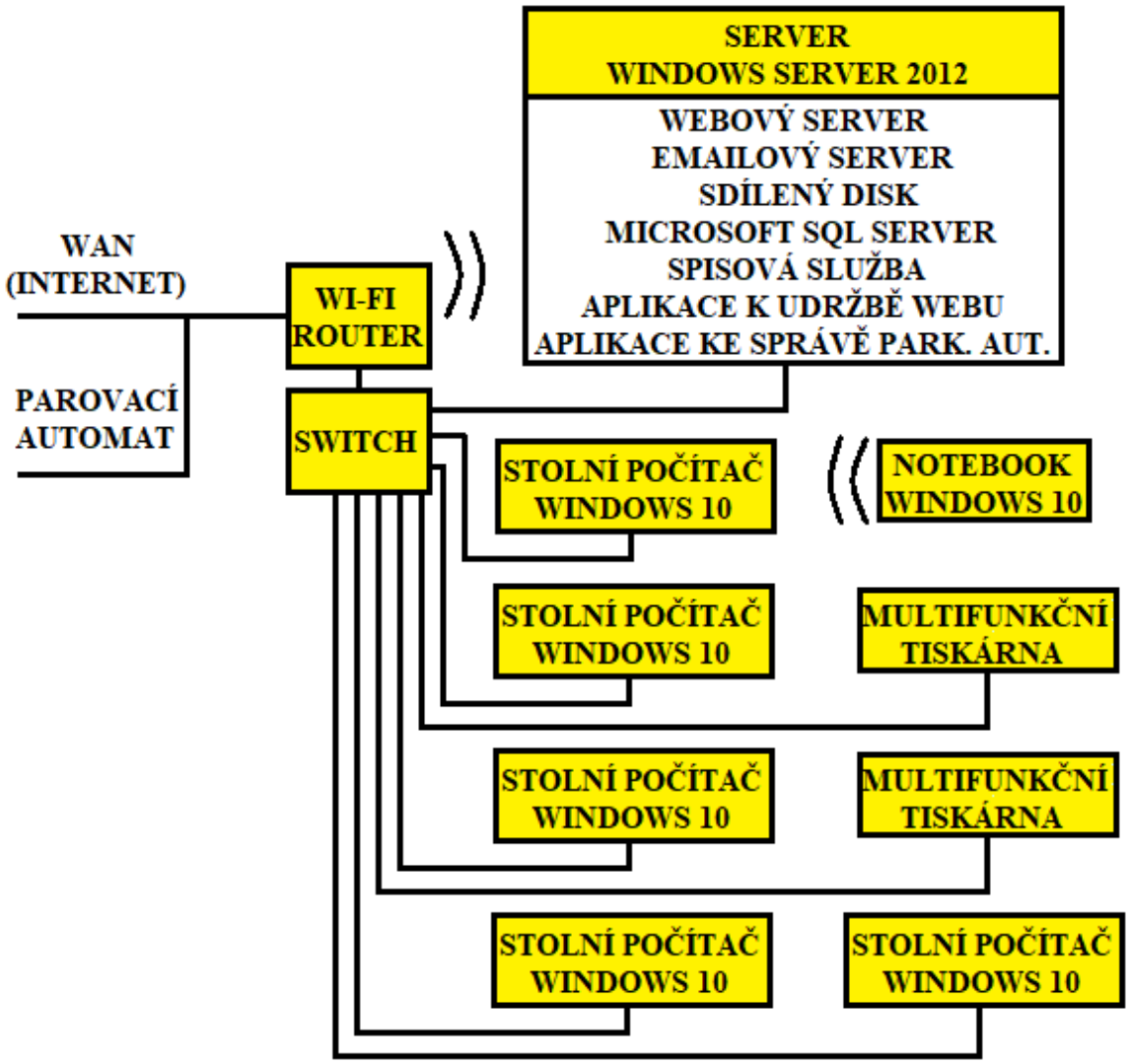
6.2 Popis LAN obecního úřadu

Samotná LAN vybrané obce, respektive obecního úřadu, představuje již zmíněný server, záložní zdroj napájení, switch, Wi-Fi router, dále pak pět stolních počítačů umístěných po jednom v popsaných kancelářích, notebook umístěný v jednací místnosti a dvě multifunkční tiskárny. Tato lokální síť má zajištěný přímý přístup na internet prostřednictvím optického kabelu, připojení tedy není realizováno prostřednictvím proxy serveru. Na vstupní bráně není nainstalovaný firewall. Vstupní optický kabel je přivedený přímo do Wi-Fi routeru. Spojení jednotlivých síťových prvků je realizováno částečně fyzickým spojením za využití metalických kabelů, tak pomocí bezdrátové technologie Wi-Fi (připojení notebooku v jednací místnosti). Na všech počítačích, včetně notebooku, běží operační systém Windows 10 s nainstalovaným antivirovým programem. Výměna dat mezi těmito zařízeními probíhá prostřednictvím sdíleného disku na serveru, kde nejsou data nikterak zálohována.

Na serveru je nainstalován operační systém Windows Server 2012 včetně antivirového programu a běží na něm několik služeb. Pro případný výpadek proudu je server připojený k záložnímu zdroji napájení. Mezi služby, které tento běžný komerční server obsluhuje, patří: webový server zajišťující provoz webových stránek obce (i mobilní aplikace), komerční aplikace, prostřednictvím které zaměstnanci úřadu provádějí aktualizaci informací na webových stránkách (i mobilní aplikaci), e-mailový server, Microsoft SQL server a s ním spojená komerční aplikace zajišťující spisovou službu. Závěrem se jedná o komerční aplikaci umožňující veškerou správu, včetně evidence dat, z parkovacího automatu na parkovišti.



Obrázek 12 Umístění jednotlivých síťových prvků na obecním úřadě



Obrázek 13 Grafické znázornění LAN

7 HODNOCENÍ KYBERNETICKÝCH RIZIK VYBRANÉ OBCE

V této kapitole jsou analyzována rizika ve smyslu kybernetické bezpečnosti vybrané obce. Pro větší přehlednost a srozumitelnost prováděné analýzy je tato vhodně rozdělena do tří pohledů, které spolu dohromady tvoří kybernetickou bezpečnost.

Zaprvé se bude jednat o analýzu fyzické bezpečnosti objektu obecního úřadu, potažmo serverovny. Důležité je však zmínit, že se nejedná o posouzení fyzické bezpečnosti ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, nýbrž čistě z pohledu kybernetické bezpečnosti a s ní souvisejícího možného přístupu neoprávněné osoby k prvkům lokální sítě vybrané obce apod.

Druhý pohled bude věnován analýze rizik z pohledu bezpečnosti lokální sítě obce jako takové a s ní souvisejícího třetího pohledu, tedy bezpečnosti jednotlivých počítačů, serveru i ostatních prvků ICT, které tuto lokální síť tvoří.

Cílem následné analýzy není analyzovat hrozby zapříčiněné v přímé souvislosti uživatelem nebo administrátorem (úmyslné smazání nebo zneužití dat apod) a hrozby, které jsou podmíněny životností hardwaru jednotlivých prvků ICT.

Po provedení samotné analýzy budou všechny tři pohledy vyhodnoceny a i přes fakt, že jedině neoddělitelně spolu tvoří kybernetickou bezpečnost, budou pro přehlednost případné návrhy na zlepšení současného stavu opět rozděleny do tří skupin.

7.1 Analýza rizik z pohledu fyzické bezpečnosti

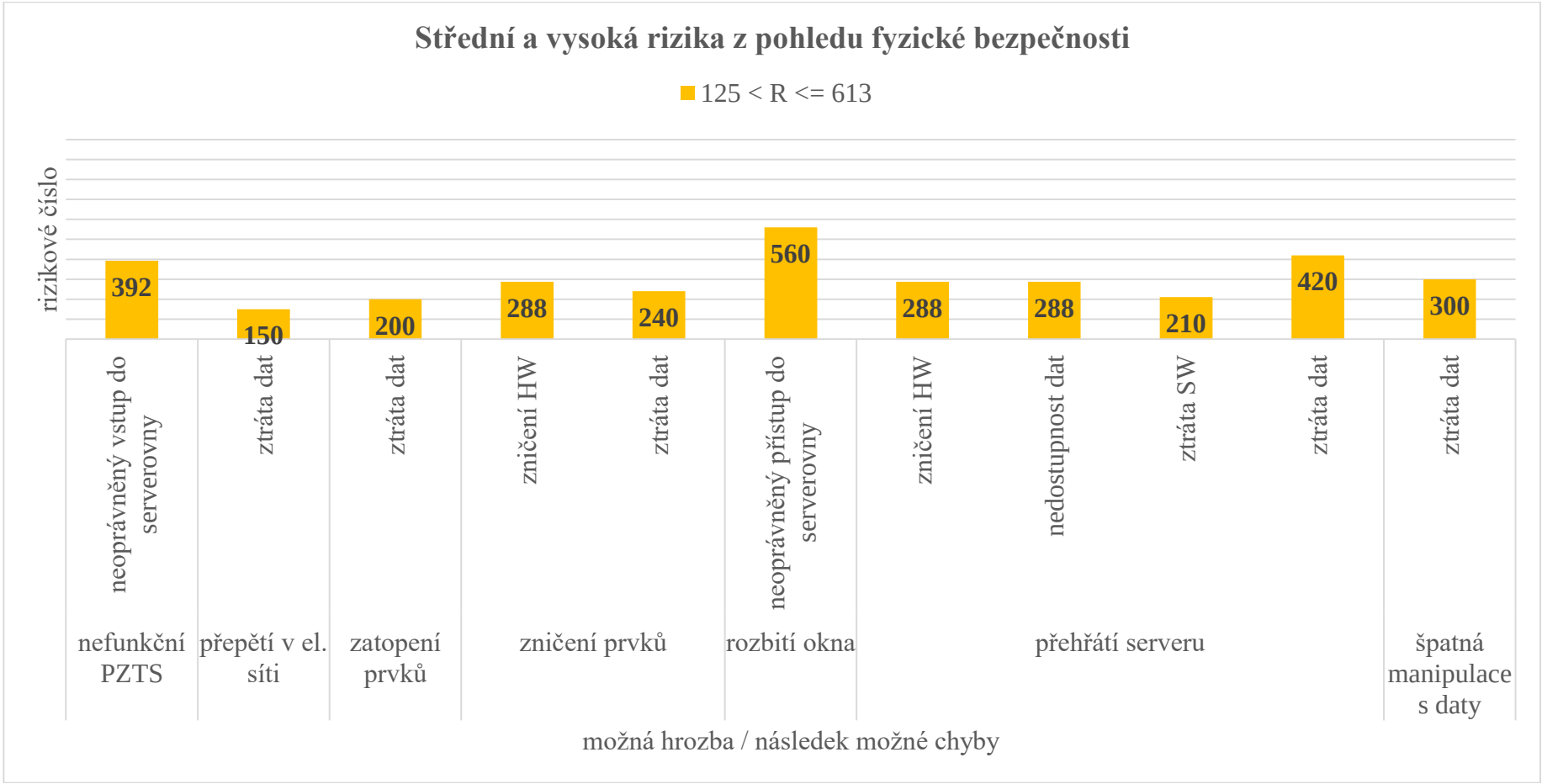
Tabulka 5 Analýza rizik z pohledu fyzické bezpečnosti

objekt: obecní úřad vybrané obce									**číslo FMEA: 1**					
odpovědnost za proces: Tomáš Hájek									**rok výroby modelu / procesu: 2021**					
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**
ICT	nefunkční PZTS	neoprávněný vstup do serverovny	**8**	výpadek elektřiny	**7**	záložní baterie v ústředně PZTS, mříže ve vybraných oknech	žádné	**7**	**392**	zamřížování zbývajících oken a dveří obecního úřadu	obec	**8**	**4**	**4**	**128**

objekt: obecní úřad vybrané obce										číslo FMEA: 1					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
	přepětí v el. síti	zničení HW	8	technická závada, klimatické podmínky	5	přepěťová ochrana	žádné	3	120	beze změny		8	5	3	120
		ztráta SW	5			žádné			75	záloha dat na NAS (RAID 1)	obec	5			75
		ztráta dat	10						150			10	3		90
	zatopení prvků	zničení HW	8	povodeň	3	žádné	žádné	4	96	beze změny		8		4	96
		ztráta SW	5		4				80	záloha dat na NAS (RAID 1)	obec	5	4		80
		ztráta dat	10		5				200			10	3		120

objekt: obecní úřad vybrané obce										číslo FMEA: 1					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
	zničení prvků	zničení HW	8	požár	6	2x hasící přístroj	žádné	4	288	instalace detektorů kouře	obec	8	5	3	120
		ztráta SW	5						120	záloha dat na NAS (RAID 1)		5			75
		ztráta dat	10						240			7			105
	rozbití okna	neoprávněný přístup do serverovny	10	vichřice	7	aktivní PZTS, mříže ve vybraných oknech	žádné	8	560	zamřížování zbývajících oken a dveří, instalace čidel pohybu	obec, správce PZTS	8	4	4	96
				úmysl osoby											

objekt: obecní úřad vybrané obce										číslo FMEA: 1					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
	přehřátí serveru	zničení HW	8	vysoká teplota v serverovně	6	žádné	žádné	6	288	instalace klimatizace nebo pronájem dedikovaného serveru	obec	8	3	3	72
		nedostup-nost dat													
		ztráta SW	5		7				210	záloha dat na NAS (RAID 1)		5	3		45
		ztráta dat	10						420			7			63
	špatná manipula ce s daty	ztráta dat	10	neodbor-nost uživatele	6	obnova dat z koše	Windows 10 Pro	5	300						63



Obrázek 14 Střední a vysoká rizika z pohledu fyzické bezpečnosti

7.2 Analýza rizik z pohledu LAN

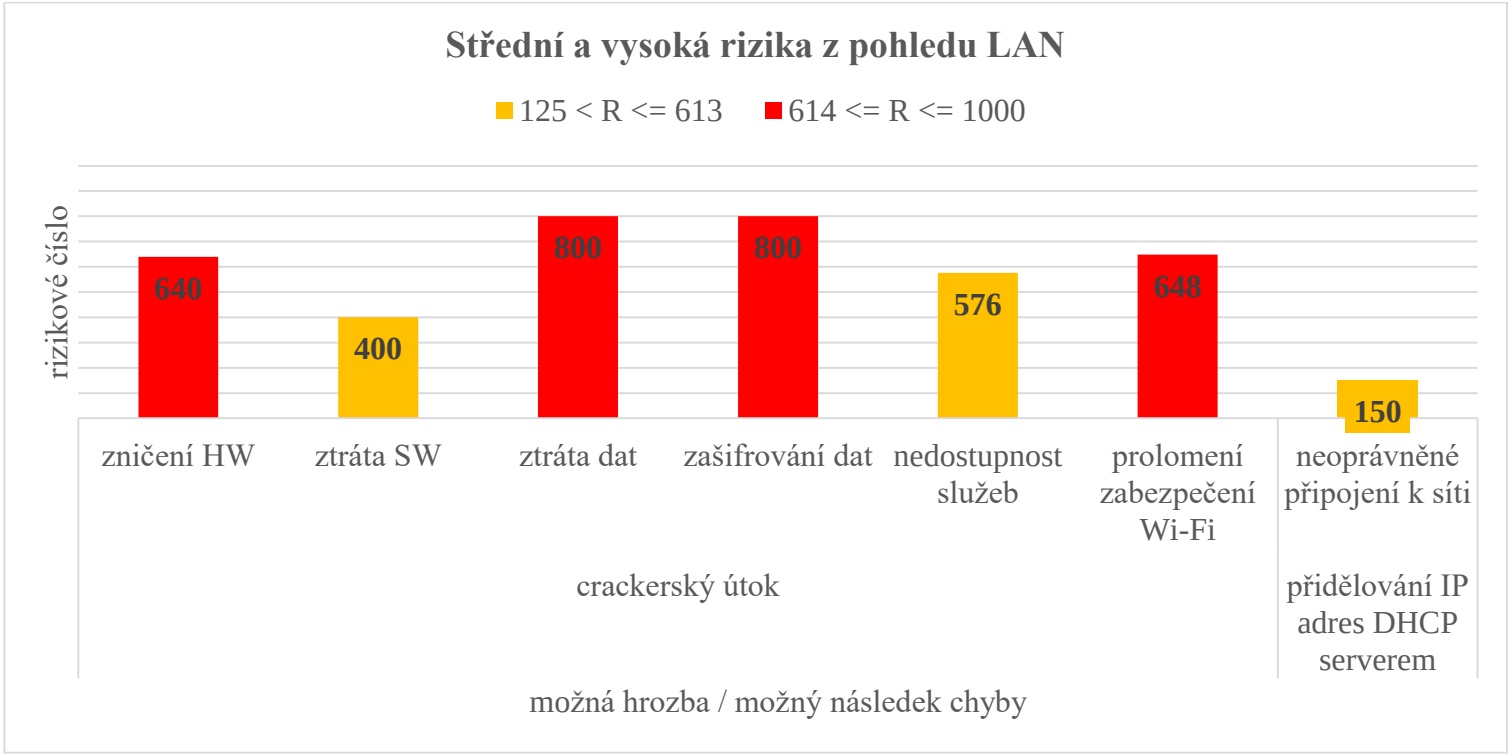
Tabulka 6 Analýza rizik z pohledu LAN

objekt: obecní úřad vybrané obce										číslo FMEA: 2					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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	cracker-ský útok	zničení HW	8	přímý přístup LAN na internet	10	žádné	žádné	8	640	instalace FW a záloha dat na NAS (RAID 1)	IT technik, obec	8	7	6	336
		ztráta SW	5						400			5			210
		ztráta dat	10						800			7			294
		zašifrování dat													

objekt: obecní úřad vybrané obce										číslo FMEA: 2					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
	cracker-ský útok	nedostup-nost služeb	**9**	umístění webového serveru v LAN	**8**	žádné	žádné	**8**	**576**	instalace FW, umístění webového serveru za FW nebo pronájem dedikovaného serveru	IT technik, obec	**7**	**6**	**4**	**168**
		prolomení zabezpe-čení Wi-Fi	**8**	nedosta-tečné	**9**	standard WPA	žádné	**9**	**648**	změna standardu WPA na WPA3	IT technik	**8**	**7**	**5**	**280**

objekt: obecní úřad vybrané obce										číslo FMEA: 2					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
				zabezpečení Wi-Fi routeru						zrušení Wi-Fi připojení (použití metalického kabelu)		6	5	3	90
	přidělování IP adres DHCP serverem	neoprávněné připojení k síti	6	nevhodné nastavení Wi-Fi routeru	5	žádné	žádné	5	150	přidělování statických IP adres	externí IT firma	4	4	4	80

objekt: obecní úřad vybrané obce									číslo FMEA: 2					
odpovědnost za proces: Tomáš Hájek									rok výroby modelu / procesu: 2021					
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
	neaktivní filtrování dle MAC adres		5		5			5	125	aktivace filtrace připojených zařízení dle MAC adres	externí IT firma	3	4	4	48
	přerušení metalic-kého kabelu	ztráta připojení k síti	4	neopatr-nost zaměstnan-ců	3	kabelová lišta	žádné	2	24	beze změny		4	3	2	24



Obrázek 15 Střední a vysoká rizika z pohledu LAN

7.3 Analýza rizik z pohledu prvků ICT

Tabulka 7 Analýza rizik z pohledu prvků ICT

objekt: obecní úřad vybrané obce										**číslo FMEA: 3**					
odpovědnost za proces: Tomáš Hájek										**rok výroby modelu / procesu: 2021**					
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**
Wi-Fi router	cracker-ský útok, infiltrace malwaru	zničení HW	**8**	neaktuální firmware	**10**	žádné	žádné	**8**	**640**	aktualizace firmwaru	IT technik	**8**	**6**	**5**	**240**
		napadení LAN	**10**	defaultní přístupové údaje		žádné	žádné		**800**	změna defaultních přístupových údajů	IT technik	**10**			**300**

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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**
			9	chybějící FW ve firmwaru		žádné	žádné		720	nákup FW nebo změna Wi-Fi routeru (s FW)	IT technik, obec	9	5	6	270
multifunkční tiskárny	cracker-ský útok, infiltrace malwaru	zničení HW	8	neaktuální firmware	10	žádné	žádné	8	640	aktualizace firmwaru	IT technik	8	6	4	192
		napadení LAN	10						800			10			240
	přístup k nastavení			defaultní přístupové údaje	4				320	změna defaultních přístupových údajů			1		40

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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**
server	cracker-ský útok, infiltrace malwaru	napadení webového serveru	**9**	neaktuální OS	**10**	Windows Server 2012	AP ESET	**9**	**810**	Instalace Windows Server 2019 nebo pronájem dedikovaného serveru	IT technik, obec	**6**	**6**	**4**	**144**
		napadení emailové-ho serveru							**810**						**144**
		nedostup-nost služeb							**810**						**144**
		zničení HW	**8**						**720**			**5**			**120**
		ztráta SW	**5**						**450**	záloha dat na					**120**

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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**
		ztráta dat	**10**						**900**	NAS (RAID 1)		**7**			**168**
		zašifrování dat							**900**						**168**
	cracker-ský útok, infiltrace malwaru	napadení webového serveru	**5**	chybějící AP, neaktuální virová databáze	**5**	AP ESET s online přístupem k aktuální virové databázi	AP ESET	**5**	**125**	beze změny		**5**	**5**	**5**	**125**
		napadení e-mailové-ho serveru							**125**						**125**
		nedostup-nost služeb							**125**						**125**

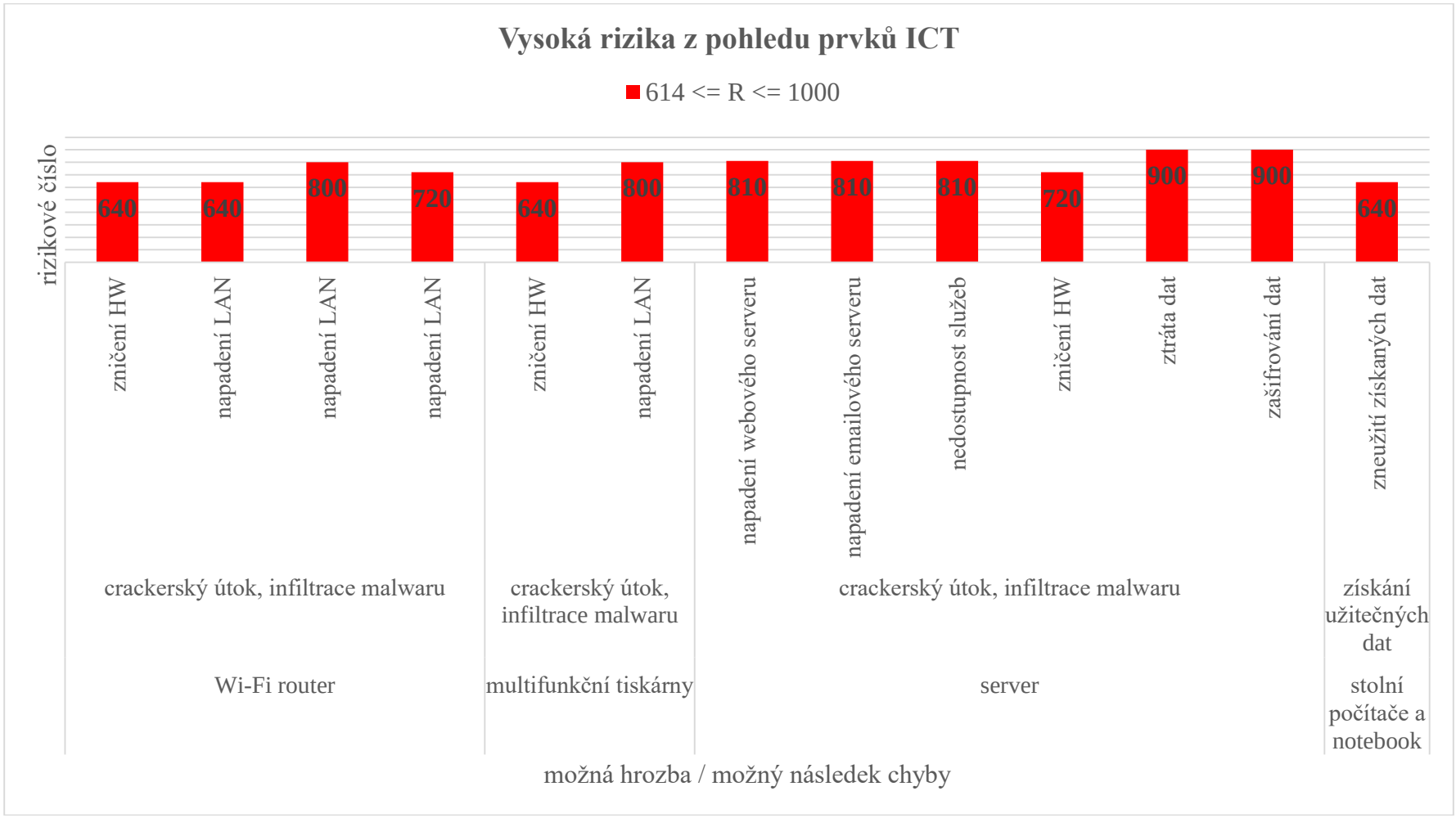
objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
prvek	možná chyba	možné následky chyby	závažnost	možná příčina chyby	výskyt	stávající opatření	stávající řízení procesu	odhalení	rizikové číslo	doporučená opatření	odpovědnost	závažnost	výskyt	odhalení	rizikové číslo
		zničení HW	4						100			4			100
		ztráta SW	5						125	záloha dat na NAS (RAID 1)		5			125
		ztráta dat	10						250			7	4	4	112
		zašifrování dat							250						112
	přístup do BIOS	neoprávněná manipulace s OS		BIOS nechráněn heslem	3	BIOS chráněný heslem	žádné	4	120	beze změny		10	3		120

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
	booto-vání z VM		10	aktivní bootování z VM	5	žádné		3	150	deaktivace bootování z VM	IT technik	10	3	3	90
	přístup do OS			účet administrá-tora nechráněn heslem	4	účet administrá-tora chráněný heslem		3	120	beze změny			4		120

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
stolní počítače a notebook	cracker-ský útok, infiltrace malwaru	zničení HW	8	neaktuální OS	4	Windows 10 Pro, verze 2004	AP ESET	3	96			8	4	3	96
		ztráta SW	5						60	záloha dat na NAS (RAID 1)	IT technik	5			60
		ztráta dat	10						120			7			84
		zašifrování dat							120						84
		zničení HW	8	chybějící AP, neaktuální		AP ESET s online přístupem k	AP ESET		96	beze změny		8			96
		ztráta SW	5						60	záloha dat na NAS (RAID 1)	IT technik	5			60
		ztráta dat	10						120			7			84

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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
		zašifrování dat		virová databáze		aktuální virové databázi			120						84
	přístup do BIOS	neoprávněná manipulace s OS	10	BIOS nechráněn heslem	8	žádné	žádné	4	320	aktivace vyžádání hesla při vstupu do BIOSu	IT technik	10	3	4	120
	bootování z VM			aktivní bootování z VM					320	deaktivace bootování z VM					120

objekt: obecní úřad vybrané obce										číslo FMEA: 3					
odpovědnost za proces: Tomáš Hájek										rok výroby modelu / procesu: 2021					
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**
	získání užitečných dat	zneužití získaných dat		deaktivace šifrování HDD/SSD		žádné	žádné	**8**	**640**	aktivace nástroje BitLocker	IT technik	**5**	**5**	**5**	**125**
	přístup do OS	získání dat		nechráněné přístupové účty heslem	**6**	přístupové účty chráněny heslem	žádné	**1**	**60**	beze změny		**10**	**6**	**1**	**60**



Obrázek 16 Střední a vysoká rizika z pohledu prvků ICT

8 DOPORUČENÍ NA ZÁKLADĚ PROVEDENÉ ANALÝZY

Společným jmenovatelem většiny zjištěných nedostatků ve smyslu možné chyby je crackerský útok (nebo infiltrace malwaru), který má za následek zpravidla nedostupnost služeb na serveru, zničení hardwaru, ztrátu nebo zašifrování dat apod. V praxi se pak zpravidla jedná o kombinaci obou uvedených možných chyb. Jeden z důvodů, proč je riziko crackerského útoku či infiltrace malwaru na IT infrastrukturu vybrané obce zvýšeno, je absence firewallu na vstupní bráně LAN v kombinaci s umístěním webového serveru (služby) v LAN. Naopak společným jmenovatelem většiny doporučených opatření je nákup a následná záloha dat na NAS tak, aby v případě ztráty nebo zašifrování dat mohlo dojít k jejich obnově.

Jednotlivá doporučení autora této bakalářské práce budou následně rozčleněna do tří kapitol tak, jak byla rozdělena a provedena samotná analýza možných rizik (v předchozí kapitole), která mají zpravidla bezprostřední vliv na kybernetickou bezpečnost vybrané obce.

8.1 Doporučení ve vztahu k fyzické bezpečnosti

Pomyslné prvenství patří zjištěné možné chybě, která představuje rozbití nezamřížovaného okna (rizikové číslo = 560) v důsledku vichřice nebo úmyslu osoby apod. Současná opatření představují mříže v některých oknech budovy a aktivní PZTS. V případě výpadku elektřiny může dojít k možné chybě ve formě nefunkční PZTS, kdy současné opatření opět tvoří mříže v některých oknech a baterie v ústředně PZTS, jakožto zdroj náhradního napájení. Společným jmenovatelem možného následku těchto chyb je neoprávněný přístup do serverovny, v důsledku čehož doporučuje autor práce **zamřížování zbývajících oken, vstupních dveří a instalaci dvou dalších čidel pohybu** (serverovna a jednací místnost).

Jakožto druhé doporučení ve vztahu k fyzické bezpečnosti míní autor práce **nákup a instalaci NAS (RAID 1)**, které bude sloužit k záloze dat a SW, jakožto opatření proti možným chybám v podobě přepětí v elektrické sítí, zničení či zaplavení prvků ICT, špatné manipulace s daty ze strany uživatele i přehřátí serveru, které bude dále eliminováno doporučeným **nákupem a instalací klimatizace** do prostor serverovny. Druhou variantou, jak předejít nejen přehřátí serveru, je **pronájem dedikovaného serveru** u příslušné instituce, která zajistí jeho správu, a obci tak odpadne veškerá agenda.

Závěrem k fyzické bezpečnosti doporučuje autor práce **nákup a instalaci detektorů kouře** jakožto součást již provozovaného PZTS, které budou předcházet zničení prvků ICT v důsledku začínajícího požáru.

8.2 Doporučení ve vztahu k LAN

Nejzávažnější možnou chybu z pohledu LAN představuje crackerský útok (nebo infiltrace malwaru) v důsledku přímého přístupu LAN na internet a také nevhodného umístění webového serveru v LAN. Na základě této možné chyby pak hrozí celá řada možných příčin, od zničení HW přes ztrátu či zašifrování dat až po nedostupnost služeb, které poskytuje server jako takový. V této souvislosti autor práce, tak jako z pohledu fyzické bezpečnosti, **doporučuje nákup a instalaci NAS (RAID 1)**, které bude sloužit k záloze dat a SW, a dále **nákup a instalaci firewallu** na vstupní bránu, kdy tento oddělí LAN od internetu, čímž dojde k eliminaci rizika ve výše uvedené podobě. Nutností je také **přesunutí webového serveru za firewall** (z pohledu vnitřní sítě), aby uživatelé internetu neměli zprostředkovaný přístup do vnitřní sítě.

Provedenou analýzou byl dále zjištěn možný následek crackerského útoku (či infiltrace malwaru) – prolomení zabezpečení Wi-Fi, kdy stávající opatření představuje standard zabezpečení WPA. Autor práce doporučuje urychlenou **změnu standardu zabezpečení na WPA3** nebo úplné **zrušení bezdrátového řešení a použití metalického kabelu**, neboť se jedná o jediné zařízení využívající této technologie (notebook v jednací místnosti). Při zachování bezdrátové technologie doporučuje autor práce **deaktivovat přidělování IP adres DHCP serverem a zároveň aktivovat přidělování statických IP adres**, čímž dojde k eliminaci pomyslně posledního zjištěného rizika ve formě neoprávněného připojení k síti z pohledu LAN.

8.3 Doporučení ve vztahu k prvkům ICT

Crackerský útok nebo infiltrace malwaru jsou alfou a omegou této práce a zároveň se jedná o možnou chybu, která může nejčastěji způsobit většinu zjištěných možných následků, nejinak je tomu i u jednotlivých prvků ICT.

Wi-Fi router

Ve vztahu k tomuto zařízení byly odhaleny dvě, respektive tři možné následky chyby, kterou opět může zapříčinit crackerský útok nebo infiltrace malwaru. Jako příčiny byly definovány: neaktuální firmware, defaultní přístupové údaje a chybějící firewall, tentokrát jako součást

firmwaru. Na základě těchto zjištění autor práce **doporučuje aktualizaci firmwaru a změnu defaultních přístupových údajů**. K absenci firewallu již byla doporučení zmíněna ve formě jeho nákupu a instalace jakožto samostatného zařízení.

Multifunkční tiskárny

Multifunkční tiskárny představují výstupní periferní zařízení a bohužel jsou mnohdy opomíjenými prvky v oblasti kybernetické bezpečnosti. Na základě provedené analýzy doporučuje autor práce, shodně jako u Wi-Fi routeru, **aktualizaci firmwaru a změnu defaultních přístupových údajů**.

Server

Ve vztahu k serveru je nutné na základě provedené analýzy **doporučit přeinstalovaní zastaralého operačního systému Windows Server 2012 nejlépe na nejnovější Windows Server 2019** a dále několikrát zmíněný **nákup a instalaci NAS** sloužící k záloze dat, která nyní není na serveru prováděna. Na základě analýzou zjištěného **aktivního bootování z vyměnitelného média autor práce doporučuje deaktivaci této funkce**.

Stolní počítače a notebook

U těchto prvků byly zjištěny pouze nedostatky ve formě přístupu do BIOS, bez vyžádání hesla, aktivního bootování z vyměnitelného média a deaktivovaného šifrování HDD/SSD. Autor práce tedy doporučuje aktivaci vyžádání hesla při vstupu do BIOS, deaktivaci bootování z vyměnitelného média a aktivaci nástroje BitLocker.

8.4 Dílčí závěr

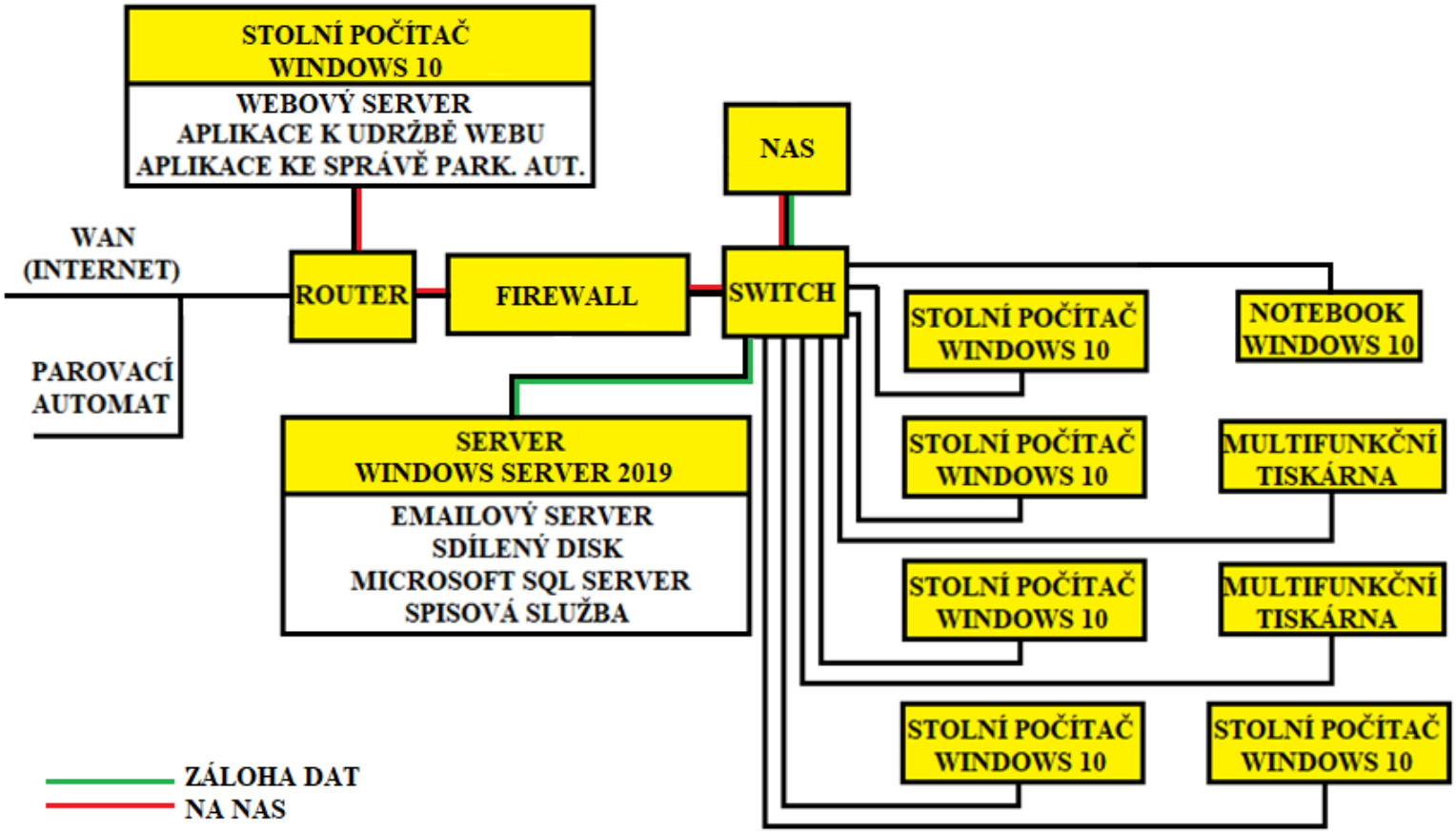
I přes fakt, že autor práce z důvodu větší přehlednosti rozdělil analýzu rizik kybernetické bezpečnosti vybrané obce na tři samostatné pohledy, lze závěrem konstatovat, že všechny tyto pohledy jedině spolu tvoří kybernetickou bezpečnost. Tento fakt potvrzuje i shodnost většiny doporučených opatření, která byla napříč zmíněnými pohledy totožná. Především se jedná o nákup a instalaci NAS sloužícího k zálohování dat a dále o nákup a instalaci firewallu, jakožto samostatného prvku ICT, který oddělí LAN od internetu, a bude tak chránit uživatele i jejich data, samozřejmostí je pak přesunutí webového serveru (služby) za firewall (z pohledu vnitřní sítě). Vhledem k vytíženosti webových stránek obce postačí přesunutí webového serveru (služby) na běžný komerční počítač s nainstalovaným potřebným SW (například Apache HTTP Server). Samozřejmostí je záloha dat z webového serveru na již doporučené NAS, které bude umístěno ve vnitřní síti. Na firewallu pak bude

aktivní příchozí pravidlo ve formě povoleného portu 445, které umožní prostup zálohovaných dat přes firewall, přičemž toto pravidlo bude aktivní jen pro nezbytně nutnou dobu. Nevýhodou tohoto řešení by byla nízká odolnost takto řešeného webového serveru proti DoS a DDoS útokům. Návrh tohoto řešení je však zpracován na následující straně.

V případě, že se obec nejenom s ohledem na vyšší pořizovací cenu nutných komponent rozhodne upustit od vlastního serveru, je možné přejít na zmíněnou alternativu v podobě pronájmu dedikovaného serveru u příslušné instituce.

Průzkumem trhu bylo zjištěno, že pronájem dedikovaného serveru včetně SW, který obec potřebuje ke svému chodu, nabízí mnoho institucí. Jedná se například o IS Munis nebo Kompletní evidenci obce, přičemž oba tyto informační systémy nabízejí přívětivé uživatelské rozhraní a jsou schopny plnohodnotně zastávat službu webového i e-mailového serveru a veškerou spisovou službu, která je v obci potřeba. Odhadovaná cena za pronájem dedikovaného serveru, včetně jednoho z výše uvedených informačních systémů se vzhledem k velikosti obce pohybuje okolo 3 000 Kč za měsíc. Obci při tomto řešení odpadnou mimo jiné i náklady v podobě platby za veřejnou IP adresu, která je při stávajícím řešení nezbytná.

S přihlédnutím k použité metodě FMEA (respektive tří samotných pohledů), jejíž součástí je i vyhodnocení rizik po aplikaci nápravných opatření, autor bakalářské práce upouští od další kapitoly ve smyslu výše uvedeného, neboť by došlo k duplikaci těchto informací.



Obrázek 17 Návrh jednoho z opatření kybernetické bezpečnosti – LAN

ZÁVĚR

Cílem autora bakalářské práce bylo zpracovat téma kybernetické bezpečnosti vybrané obce. V této souvislosti byla první kapitola bakalářské práce věnována definici podstatných klíčových pojmů. Sem byl zařazen počítač, kyberprostor, počítačová síť a internet, neboť tyto pojmy spolu úzce souvisejí a s nadsázkou lze říci, že od počítače k internetu představují podmnožinu předchozího.

Následně práce přešla k samotné definici kybernetické bezpečnosti, která, jak se ukázalo, byla poměrně obtížně uchopitelná, neboť nemá oporu v české legislativě ani ustálenou definici. Třetí kapitola popsala nejvýznamnější kybernetické a bezpečností hrozby, přičemž v oblasti malwaru stručně popsala i jeho dělení a způsob infiltrace.

Kapitola Národní úřad pro kybernetickou a informační bezpečnost popsala tento ústřední správní orgán, vymezila jeho působnost a především představila kritéria, která musí splňovat konkrétní obec, aby spadala pod jeho působnost. Autorem práce vybraná obec však tato kritéria nesplňuje, proto je z působnosti NÚKIB vyňata a kybernetickou bezpečnost má na svých bedrech.

Poslední kapitola teoretické části představila vybranou metodu FMEA, včetně autorem práce zvolených kritérií, která byla následně použita v praktické části.

Samotná podstata bakalářské práce je pak zakotvena v praktické části, kde je úvodem popsána náhodně vybraná obec, budova obecního úřadu, místnost serverovny a lokální síť. Tento obsah je také doplněn odpovídajícími nákresy. Následná analýza kybernetické bezpečnosti je pro přehlednost rozdělena na tři samostatné části, které však jedině neoddělitelně spolu tvoří kybernetickou bezpečnost.

Nejvýznamnější zjištěné riziko představuje samotný provoz lokální sítě s přímým přístupem k internetu, kdy toto zajišťuje Wi-Fi router s defaultními přístupovými údaji a zastaralým zabezpečením WPA. Za zmínku také stojí server se zastaralým operačním systémem nebo ohrožení samotných dat z důvodu neexistence jejich zálohy.

Poslední kapitola je věnována doporučením ke zlepšení i nápravě zjištěných nedostatků. V této souvislosti autor práce mimo jiné doporučuje pronájem dedikovaného serveru u příslušné organizace, čímž odpadne obci veškerá agenda. Jako alternativa je nabídnuto rozšíření lokální sítě o firewall nainstalovaný na vstupní bráně a s tím související oddělení lokální sítě od internetu. Vhodný je také nákup síťového uložiště nabízející RAID 1 a vyšší.

Nakonec byly veškeré zjištěné nedostatky a následná doporučení předneseny starostovi vybrané obce. Ze strany autora práce mu také byla nabídnuta odborná pomoc ve smyslu implementace doporučení ke zlepšení současného stavu kybernetické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

[1] 2015 Internet Security Threat Report: Attackers are bigger, bolder, and faster, 2015. In: *Broadcom Inc.* [online]. [cit. 2020-12-29]. Dostupné z: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=451ff1ff-4dc9-46fa-9590-d102309e7abd&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[2] BARTÁK, Jan, Jinřich BEČVÁŘ a Miroslav BECHYNĚ et al., 1999. *Malá ilustrovaná encyklopedie: A-Ž*. Praha: Encyklopedický dům. ISBN 80-860-4412-2.

[3] BAZZELL, Michael, 2014. *Hiding From the Internet: Eliminating Personal Online Information*. Německo: CCI. ISBN 978-1500397814.

[4] Brainstorming, © 2011-2016. *Management Mania* [online]. [cit. 2021-04-29]. Dostupné z: https://managementmania.com/cs/brainstorming

[5] Computer. *Wikipedia, the free encyclopedia* [online]. [cit. 2020-11-23]. Dostupné z: https://en.wikipedia.org/wiki/Computer#First_computing_device

[6] ČECH, Karel, 2001. ÚLOHA A APLIKAČNÍ MOŽNOSTI METODY FMEA PŘI ZABEZPEČOVÁNÍ SPOLEHLIVOSTI: PROVEDENÍ FMECA PRO ZAŘÍZENÍ PROVOZOVANÉ NA CVIČNÉM LETADLE L159. *Česká společnost pro jakost* [online]. [cit. 2021-04-29]. Dostupné z: https://www.csq.cz/fileadmin/user_upload/Spolkova_cinnost/Odborne_skupiny/Spolehlivost/Sborniky/05_FMEA.pdf

[7] ČESKO, 1998. Ústavní zákon č. 110/1998 Sb. Ústavní zákon o bezpečnosti České republiky. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-110

[8] ČESKO, 2005. Zákon č. 127/2005 Sb. Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

[9] 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

[10] ČESKO, 2010. Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.takonyprolidi.cz/cs/2010-432

[11] ČESKO, 2013. Sdělení č. 104/2013 Sb. m. s. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě. In: *Sbírka mezinárodních smluv*. Dostupné také z: https://www.zakonyprolidi.cz/ms/2013-104

[12] 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

[13] ČESKO, 2017. *Příloha k usnesení vlády ze dne 10. května 2017 č. 360 ve znění usnesení vlády ze dne 18. dubna 2018 č. 247 a usnesení vlády ze dne 25. ledna 2021 č. 65: Statut Výboru pro kybernetickou bezpečnost*. In: . Dostupné také z: https://www.vlada.cz/assets/ppov/brs/pracovni-vybory/Kyberneticka_bezpecnost/statut-2021.pdf

[14] Data Breach Investigations Report, 2020. In: *ResearchGate* [online]. [cit. 2021-01-28]. Dostupné z: https://www.researchgate.net/profile/Suzanne_Widup/publication/343239809_2020_Verizon_Data_Breach_Investigations_Report/links/5f1f2b5292851cd5fa4e0c22/2020-Verizon-Data-Breach-Investigations-Report.pdf

[15] DONÁT, Josef a Jan TOMÍŠEK, 2016. *Právo v síti: průvodce právem na internetu*. Praha: C.H. Beck. ISBN 978-80-7400-610-4.

[16] DOSEDĚL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press. ISBN 80-251-0106-1.

[17] GIBSON, William, 2003. *Neuromancer*. Ace Books. ISBN 978-0-441-56959-5.

[18] Govcert.cz, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-04-06]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[19] How it Works. *Internet Society* [online]. [cit. 2020-11-20]. Dostupné z: https://www.internetsociety.org/internet/how-it-works/Webarchiv

[20] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník kybernetické bezpečnosti* [online]. In: . Praha: Policejní akademie ČR

[cit. 2020-12-21]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

[21] JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada. ISBN 9788024715612.

[22] Kevin Mitnick, 2020. In: *Wikipedia, the free encyclopedia* [online]. [cit. 2020-12-29]. Dostupné z: https://en.wikipedia.org/wiki/Kevin_Mitnick

[23] KOCOUREK, Jaromír, 2012. Kvalita/Procesní řízení. *Vlastní cesta* [online]. [cit. 2021-04-29]. Dostupné z: https://www.vlastnicesta.cz/metody/fmea/

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

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

[26] KRÁL, Mojmír, 2015. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing. ISBN ISBN978-80-247-5453-6.

[27] KUCHAŘ, Miloš, 1999. *Bezpečná síť: jak zajistíte bezpečnost vaší sítě*. Praha: Grada. ISBN 80-716-9886-5.

[28] Kyberkriminalita, © 2020. In: *Policie České republiky* [online]. [cit. 2020-12-29]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[29] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, 2015. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-12-28]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf

[30] NCKB, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-04-06]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/

[31] NÚKIB, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-04-06]. Dostupné z: https://nukib.cz/cs/o-nukib/

[32] NUTIL, Petr, 2015. Darknet, aneb cesta do hlubin internetu. *KurzyCZ* [online]. [cit. 2020-11-20]. Dostupné z: https://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu/Tor project, 2020 online

[33] PENDER-BEY, Georgie. *The Parkerian Hexad: The CIA Expanded* [online]. In: . [cit. 2020-11-30]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[34] SCHNEIER, Bruce, 2000. Semantic Attacks: The Third Wave of Network Attacks. In: *Schneier on Security* [online]. [cit. 2020-11-30]. Dostupné z: https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

[35] SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-501-2.

[36] TURING, A. M., © 2020. On Computable Numbers, with an Application to the Entscheidungsproblem. In: *Journals | Oxford Academic* [online]. Oxford University Press [cit. 2020-11-23]. Dostupné z: https://academic.oup.com/plms/article-pdf/s2-42/1/230/4317544/s2-42-1-230.pdf

[37] Two security researchers find WPA3 vulnerabilities, 2014 - 2021. *Tech Xplore - Technology and Engineering news* [online]. Science X Network [cit. 2021-01-5]. Dostupné z: https://techxplore.com/news/2019-04-wpa3-vulnerabilities.html

[38] Vojenské zpravodajství zajišťuje kybernetickou obranu České republiky, 2021. *Vojenské zpravodajství* [online]. [cit. 2021-04-06]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46

[39] Vulnerabilities in the WPA3 Wi-Fi Security Protocol. *Schneier on Security* [online]. [cit. 2020-11-15]. Dostupné z: https://www.schneier.com/blog/archives/2019/04/vulnerabilities_7.html

[40] Webarchiv. *Webarchiv* [online]. [cit. 2020-11-20]. Dostupné z: https://www.webarchiv.cz/cs/

[41] Why we need Tor. *Tor* [online]. [cit. 2020-11-20]. Dostupné z: https://2019.www.torproject.org/about/overview.html.en#whyweneedtor

[42] Windows Firewall. *Wikipedia, the free encyclopedia* [online]. [cit. 2020-12-25]. Dostupné z: https://en.wikipedia.org/wiki/Windows_Firewall

[43] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019, 2020. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-12-29]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Antivirový program
BIOS	Firmware pro osobní počítače (Basic Input-Output System)
DHCP	Protokol z rodiny TCP/IP, používá se k automatické konfiguraci počítače připojeného k síti (Dynamic Host Configuration Protocol)
FMEA	Analýza možných vad a jejich následků (Failure Mode and Effect Analysis)
FW	Firewall
HDD	Pevný disk (Hard Disk Drive)
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IP adresa	Číslo, které jednoznačně identifikuje zařízení v počítačové síti (IP address)
LAN	Lokální síť (Local Area Network)
MAC adresa	Jedinečný identifikátor, který výrobce přiřazuje konkrétnímu zařízení (Media Access Control)
NAS	Datové (síťové) uložiště (Network Attached Storage)
NCKB	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
PZTS	Poplachový zabezpečovací a tísňový systém
RAM	Elektronická polovodičová paměť (Random Access Memory)
SSD	Pevný (polovodičový) disk (Solid-State Drive)
SW	Software
VLAN	Virtuální lokální síť (Virtual Local Area Network)
VM	Virtuální stroj (Virtual Machine)
WAN	Rozsáhlá síť (Wide Area Network)

Wi-Fi	Bezdrátová komunikace v počítačových sítích (Wireless Ethernet Compatibility Aliance)
WLAN	Bezdrátová lokální síť (Wireless Local Area Network)
WPA	Bezpečnostní protokol používaný k šifrování a ochraně bezdrátových sítí (Wi-Fi Protected Access)
WPA3	Bezpečnostní protokol používaný k šifrování a ochraně bezdrátových sítí (Wi-Fi Protected Access). Poskytuje vyšší zabezpečení než WPA

SEZNAM OBRÁZKŮ

SEZNAM TABULEK