Identifikace a posouzení rizik informačního systému vybrané organizace

Šimon Kovalčík

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Šimon Kovalčík**
Osobní číslo:	**L21602**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Identifikace a posouzení rizik informačního systému vybrané organizace**

Zásady pro vypracování

1. Proveďte rešerši dané problematiky.
2. Charakterizujte vybranou organizaci a analyzujte její aktuální stav v oblasti kybernetické bezpečnosti.
3. Na základě výsledků provedené analýzy navrhněte opatření pro informační systém.

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

Seznam doporučené literatury:

1. BOURGEOIS, David T. et al., *Information Systems for Business and Beyond* [online]. In: Saylor Academy, 2019. [cit. 2023--10-31]. Dostupné z: https://digitalcommons.biola.edu/open-textbooks/1/ ISBN 9781533064165
2. KOLOUCH, Jan, *CyberCrime* [online]. Praha: CZ.NIC. z.s.p.o., 2016. [cit. 2023-10-31]. ISBN 978-80-88168-18-8.
3. NONNEMANN, František, Vlastimil ČERVENÝ a Dominik VÍTEK, *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* Praha: Wolters Kluwer, 2022. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7676-515-3.

Další doporučená literatura dle vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Lukáš Pavlík, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

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: 3.5.2024

Jméno a příjmení studenta: Šimon Kovalčík

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá identifikací a posouzením rizik informačního systému v organizaci na úrovni územní samosprávy. V teoretické části jsou vymezeny základní pojmy jako informační systém, jeho typy a jednotlivé moduly. Dále se práce zabývá kybernetickou bezpečností v České republice a přehledem kybernetických útoků a jak se proti nim bránit. Praktická část začíná představením obecního úřadu v Bílovicích, jakožto zkoumané organizace. Stav organizace z pohledu kybernetické bezpečnosti je zjištěn za pomocí rozhovoru se správcem sítě. Výsledná zjištění jsou promítnuta do What-if analýzy a SWOT analýzy. Na identifikovaná rizika vycházející z obou analýz jsou v závěru navržena opatření.

Klíčová slova: informační systémy, kybernetická bezpečnost, riziko, rozhovor, SWOT analýza, what-if analýza

ABSTRACT

This bachelor thesis deals with the identification and assessment of information system risks in an organization at the local government level. In the theoretical part, basic concepts such as information system, its types and individual modules are defined. Furthermore, the thesis deals with cyber security in the Czech Republic and an overview of cyber attacks and how to defend against them. The practical part begins with an introduction of the municipal authority in Bílovice, as the organization under study. The status of the organization from the perspective of cyber security is determined by interviewing the network administrator. The resulting findings are reflected in a What-if analysis and a SWOT analysis. Finally, measures are proposed to address the identified risks based on both analyses.

Keywords: information systems, cyber security, risk, interview, SWOT analysis, what-if analysis

Děkuji vedoucímu bakalářské práce panu Ing. Lukáši Pavlíkovi, Ph.D. za ochotu a odborné vedení při zpracovávání práce. Dále bych chtěl poděkovat panu Ing. Adamu Skovajsovi za spolupráci a zprostředkování informací. V neposlední řadě bych pak chtěl poděkovat panu Ing. Liboru Bartasovi za poskytnutí rozhovoru jako podklad pro praktickou část práce.

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

OBSAH

ÚVOD

Informační systémy jsou zaryty hluboko do novodobé problematiky ochrany obyvatelstva. Je možné je spatřit v rámci integrovaného záchranného systému, u orgánů krizového řízení a samozřejmě taky v soukromých institucích. Když se použije pojem informační systém, většina lidí si představí pouze software, který plní funkci tohoto informačního systému. Pod tento pojem však spadá celý soubor komponent do sebe zapadajících jako je hardware, software a také lidi, kteří to všechno obsluhují.

Z pohledu bezpečnosti je tedy na místě zajistit, aby všechny tři pomyslné pilíře fungovaly správně a především, aby rizika, která s nimi souvisí byla snížena na co nejnižší hodnotu čili na hodnotu, která je z hlediska bezpečnosti přijatelná. Každý z těchto prvků informačního systému má svá specifická úskalí. Co se týče lidí, je to selhání lidského faktoru, u hardwaru porucha zařízení, avšak u samotného softwaru, kterému je věnována větší část této práce, je těchto rizik nespočet a řada z nich se vztahuje k lidskému pochybení, nebo mají co dočinění s hardwarem. Z toho vyplývá, že všechny tři pilíře jsou vzájemně propojeny.

Kybernetická bezpečnost za poslední léta nabrala na důležitosti hlavně díky četným útokům tzv. hackerů po celém světě i v České republice. Takový útok dokáže podnik, nebo dokonce i prvek kritické infrastruktury vyřadit na dlouhou dobu a způsobit tak majetkové škody, v těch nejhorších případech i ztráty na životech. Není tedy divu, že se na kybernetickou bezpečnost zaměřují organizace všech velikostí a dosahů jako třeba i obecní úřady.

Bakalářská práce si dává za cíl posoudit obecní úřad v Bílovicích z pohledu kybernetické bezpečnosti, identifikovat možná rizika, která zde mohou nastat, a nakonec navrhnout opatření proti těmto rizikům. Metody použité v práci jsou literární rešerše, rozhovor, What-if analýza, SWOT analýza a metody indukce a dedukce.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ SYSTÉM

Informační systém, používající zkratku IS je možné technicky definovat, jako soubor vzájemně propojených komponent, které spolu spolupracují a doplňují se ve věcech jako je zpracování, uchovávání, či distribuce dat a informací, které dále slouží na podporu rozhodování a řízení v rámci organizace.

Dále lze informační systém (IS), také chápat jako kombinaci hardwaru a softwaru spolu s telekomunikační sítí, které jsou tvořeny a obsluhovány lidmi k vytváření a distribuci užitečných dat, obvykle právě v prostředí nějaké organizace, ať už se jedná o firmu, nemocnici, nebo školu (Bourgeois et al., 2019).

Podle další definice je možné informační systém jednoduše definovat podobně jako v té předchozí, a to jako softwarové vybavení firmy, které pracuje na základě přijatých informací, pomáhá řídit jednotlivé interní procesy a dál ve spolupráci s lidskými zdroji, kterým předává informace pro efektivnější kontrolu a veškerou pracovní činnost (Aira GROUP, s.r.o., © 2022).

1.1 Typy informačních systémů

Typů informačních systémů existuje celá řada. Nejdůležitějším kritériem při výběru informačního systému pro svou organizaci je určit, na co všechno bude váš informační systém využíván. Důležitou rolí bude tedy především velikost a specializace dané organizace, informační systémy navržené pro školy a univerzity se budou lišit od těch, které využívají například nemocnice, nebo velké, či malé podniky. Možností je opravdu hodně, a navíc je možné daný informační systém ušít na míru dle požadavků organizace (Koďousková, 2021).

Obecně jsou informační systémy členěny do dvou základních kategorií, na základě specializace:

a) Podnikové informační systémy – informační systém vztahující se ke konkrétnímu podniku, který pracuje s daty a informacemi uvnitř podniku. Většinou k němu mají přístup pouze zaměstnanci, nebo povolané osoby. Může mít celou řadu funkcí od vedení docházky, objednávání obědů až po procesy ve výrobě, v případě, že se jedná o nějakou firmu (Koďousková, 2021).

b) Veřejné informační systémy – Tento typ informačních systémů se liší od těch podnikových v tom smyslu, že je většinou přístupný široké veřejnosti např. přes online

webové stránky. Služby těchto informačních systémů využívají třeba veřejné knihovny, či muzea.

Podnikové informační systémy se dále rozdělují na 3 typy podle druhu jejich využití:

- Univerzální systémy – Jak už z názvu vypovídá, univerzální systémy mají největší škálu využití a díky velké nabídce funkcí se dají dále přizpůsobit dle daného podniku a jeho specializaci.
- Informační systémy pro specifické účely – Určeno pro podniky se specifickými požadavky, které by rozšířené funkce univerzálního systému plně nevyužily a investice jak finanční, tak implementační by se zde nevyplatila.
- Informační systémy navržené na míru – Zákazník přijde za poskytovatelem informačního systému s konkrétními požadavky na to, jak by měl tento systém vypadat jak už z hlediska funkcionality, zabezpečení, nebo třeba designu. Vytvoření a implementace takového IS je však nákladnější a časově náročnější (Koďousková, 2021).

1.2 Moduly informačních systémů

Jak veřejné, tak podnikové informační systémy v sobě mají zabudovány další informační systémy v podobě modulů, které se zaměřují na konkrétní oblast použití. Nejčastěji ve formě desktopové, či webové aplikace. Patří mezi ně následující moduly:

ERP

Enterprise Resource Planning – řadí se mezi nejčastěji používané informační systémy, slouží k plánování podnikových zdrojů, standardizaci procesů, hledá místa možné automatizace a celkově přispívá k větší efektivitě práce. ERP informační systémy jsou často vytvářeny na míru dle požadavků jednotlivých firem. Mají v sobě zabudovány také další moduly jako třeba CRM, SCM, nebo MIS (Koďousková, 2021).

CRM

Customer Relationship Management – jak už název z angličtiny napovídá, tento modul informačního systému se zabývá především na zdokonalení vztahů, mezi firmou a zákazníky a jsou vhodné pro podniky, které komunikují s větším množstvím zákazníků. Tento IS v sobě uchovává veškeré informace o svých zákaznících a klientech, co nejčastěji nakupují,

jaké jsou jejich preference a díky tomu může forma pružně reagovat a upravovat svoji nabídku služeb, či produktů (Koďousková, 2021).

- SCM – Supply Chain Management – modul starající se o dodavatelský řetězec.
- APS – Advanced Planning and Scheduling – zajišťuje plánování, dodavatelský řetězec (může být součástí ERP).
- HRM – Human Resource Management – řízení lidských zdrojů, ve firmě v gesci HR oddělení, obsahuje záznamy o zaměstnancích, školení, nábory, či další věci týkající se lidského kapitálu uvnitř organizace.
- MIS – Management Information Systém – slouží na úrovní operativního a taktického rozhodování, pomáhá řídit procesy v oblasti nákupu a prodeje.
- EAM – Enterprise Asset Management – správa podnikových zdrojů, pomocný nástroj který je schopen snižovat náklady na údržbu a obnovu strojů.
- DMS – Document Management System – má na starost elektronické dokumenty a veškerou práci s nimi a jejich obsahem.
- BPM – Business Process Management – pomáhá ke zvýšení konkurenceschopnosti podniku, znázorňuje a realizuje určité procesy v podniku a efektivní rozvržení času.
- BI – Business Intelligence – statistické a analytické práce ve smyslu big data.
- CMS – Content Management Systém – správa a tvorba obsahu (WordPress, Joomla…). (Koďousková, 2021).

2 KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE

Kapitola pojednává o nástrojích starajících se o kybernetickou bezpečnost v České republice, jako je zákon č. 181/2014 Sb. o Kybernetické bezpečnosti, nebo vládní a národní CERT tým.

2.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. o Kybernetické bezpečnosti je základním právním rámcem, sloužícím pro zajištění ochrany kyberprostoru v České republice. Mezi hlavní cíle patří především bezpečnost a ochrana informačních systémů a služeb, které jsou nezbytné pro chod státu, stejně tak jako ochrana klíčových odvětví, jakými jsou např. zdravotnictví, energetika, finančnictví, či doprava (Zákon č. 181/2014 Sb.).

Hlava I.

Zákon vymezuje práva a povinnosti jak osob, tak orgánů veřejné moci působící v oblasti kybernetické bezpečnosti. Stejně tak ukládá práva a povinnosti poskytovatelům elektronických komunikací, správcům a provozovatelům kritické informační infrastruktury a významných informačních systémů. Dále zpracovává a navazuje na předpisy EU (Zákon č. 181/2014 Sb.).

Zákon vymezuje také pojmy, které jsou nezbytné pro oblast kybernetické bezpečnosti:

Bezpečnost informací – podle triády zajištění důvěrnosti, integrity a dostupnosti informací a dat.

Kritická informační infrastruktura – prvek, či soubor prvků kritické infrastruktury v oblasti informačních systémů, komunikací a kybernetické bezpečnosti, které jsou nezbytné pro chod státu.

Kybernetický prostor – jedná se o digitální prostor, ve kterém dochází ke vzniku, zpracování a výměně informací na síti, je tvořen informačními systémy, službami a sítěmi elektronických komunikací.

Provozovatel systémů – opět se jedná o orgán, nebo osobu, která zajišťuje chod těchto systémů (informačních i komunikačních) a to po technické a programové stránce.

Správce systémů – jak informačního, tak komunikačního systému je osoba, nebo orgán, který určuje účel zpracování informací/komunikačního systému a také podmínky, které jsou spojen s jejich provozem (Zákon č. 181/2014 Sb.).

Významné informační systémy – je to takový informační systém, který spadá pod správu orgánu veřejné moci, který se neřadí mezi kritickou infrastrukturu, nebo informační systém základní služby a při jeho narušení by mohlo dojít k ohrožení výkonnosti orgánu veřejné moci.

Významné sítě – síť elektronických komunikací, je síť, která propojuje Českou republiku do veřejných komunikačních sítí v zahraničí, nebo poskytuje přímé připojení ke kritické informační infrastruktuře.

Základní služby – poskytování této služby závisí na sítích elektronických komunikací, nebo informačních systémech a jejich narušení by mohlo vést k mnoha problémům při zabezpečení společenských, nebo ekonomických činností v některé z následujících oblastí:

Energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura, chemický průmysl (Zákon č. 181/2014 Sb.).

2.2 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

Kybernetická bezpečnostní událost se definuje jako potenciální hrozba, která má schopnost narušit bezpečnost informací v informačních systémech, narušení bezpečnostních služeb, nebo narušení bezpečnosti a integrity elektronických komunikačních sítí. Spadá zde velké množství událostí, které mohou ohrozit kybernetickou bezpečnost a za bezpečnostní událost se považují ještě předtím, než dojde k jakémukoliv opravdovému narušení systému (Zákon č. 181/2014 Sb.).

Kybernetický bezpečnostní incident je na rozdíl od kybernetické bezpečnostní události již specifičtější a je tím myšleno opravdové narušení právě bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb, nebo narušení bezpečnosti a integrity v elektronických komunikačních sítích. Jedná se o následek kybernetické bezpečnostní události a představuje konkrétní narušení systému a ohrožení bezpečnosti (Zákon č. 181/2014 Sb.).

Vládní CERT tým

Vládní CERT tým, v ČR známý jako GovCERT.CZ z anglického Computer Emergency Response Team a týmy CSIRT (Computer Security Incident Response Team), jsou hlavními subjekty pro ochranu kritické informační infrastruktury a významných informačních systémů v souladu se zákonem č. 181/2014 o kybernetické bezpečnosti. Tyto týmy tvoří účinnou složku pro efektivní zvládání a předcházení kybernetických hrozeb a bezpečnostních incidentů v kyberprostoru. Mimo to mají tyto týmy za úkol poskytování bezpečnostních informací a pomoc jak státním orgánům, tak i veřejným organizacím a v neposlední řadě také občanům České republiky, kde přispívají k větší vzdělanosti a rozšiřují povědomí o kybernetické bezpečnosti (NÚKIB).

Národní CERT tým

Národní CERT tým České republiky (CSIRT.CZ) pod záštitou organizace CZ.NIC, která je provozovatelem české národní domény .cz je důležitým prvkem v oblasti národní kybernetické bezpečnosti. V rámci českého kyberprostoru se stará především o reakci na kybernetické bezpečnostní incidenty, kdy monitoruje a analyzuje hlášení a poskytuje technickou podporu postiženým osobám a organizacím. Dále šíří osvětu a stará se o prevenci kybernetických bezpečnostních incidentů, pořádá školení a v rámci spolupráce s mezinárodními CERT/CSIRT týmy, vládními organizacemi, soukromým sektorem i akademickou sférou si vyměňují informace a poznatky, čímž zdokonalují kolektivní obranu v kyberprostoru (CZ.NIC).

3 KYBERNETICKÝ ÚTOK

Kybernetický útok je možné definovat jako anonymní, nezákonný a neoprávněný přístup k počítačovým systémům, zařízením, či počítačovým sítím, s cílem poškodit tyto systémy, zařízení, nebo sítě v podobě deaktivace služeb, krádeže dat a informací, nebo zmocnění se systému pro spuštění dalších útoků a nezákonných praktik. Za kybernetickými útoky často stojí jednotlivci, tzv. „hackeři“, „hacktivisté“, či „crackeři“, nebo dokonce i celé organizované skupiny. Hlavní motivací za těmito útoky jsou především peníze, které se snaží pomocí svých útoků a podvodů získat od svých obětí, nebo v případě kyberterorismu může jít o snahu oslabit svého protivníka. Kybernetické útoky se s rozvojem nových technologií stávají stále sofistikovanější a propracovanější a pro bezpečnostní experty, kteří se zabývají právě problematikou kyberbezpečnosti je to jedna velká výzva jak zabezpečit sebe, své organizace nebo celý stát (Legislativa s.r.o, 2022).

Podle Jana Koloucha pak jde definovat kybernetický útok jako „jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby“. Nemusí se vždy jednat o trestný čin a za kybernetické útoky jsou považovány i pouhé pokusy, či přípravy na takovou akci (Kolouch, 2016).

Podle expertů se uvádí tři hlavní a taky základní stavební kameny, které tvoří kybernetickou bezpečnost. Jsou jimi lidé, procesy a technologie. Kybernetický útok a pravděpodobnost, že útok uspěje tak záleží na každém jednotlivém článku a na tom, jak dobře je zabezpečený. Míra zabezpečení jednotlivých prvků by měla být na stejně vysoké úrovni, aby bylo zamezeno výskytu tzv. „zranitelností“. Zabezpečení lidského kapitálu, procesů a technologií je úzce spojena s respektováním a dodržováním tzv. „triády“ „C“ „I“ „A“ (Kolouch, 2016). Je to zkratka vycházející z anglických slovíček, které mají vztah k zabezpečení dat a informací v kyberprostoru a jsou to:

Confidentiality (důvěrnost) – k informacím mohou přistupovat pouze osoby s oprávněním a je vyloučeno zneužití informací. Při narušení důvěrnosti mohou být data zkompromitována a v držení nesprávné osoby (APTIEN.COM, 2023).

Integrity (Neporušenost, integrita) – znamená to, že informace např. v komunikaci mezi dvěma zařízeními nebyla pozměněna a informace jsou správné a úplné. Při narušené integritě lze hovořit o útočníkovi, který se dostal k informacím, které následně poškodil, nebo upravil (APTIEN.COM, 2023).

Availability (dostupnost) – uživatel má svá data dostupná a může k nim přistupovat kdy se mu zachce. Narušení dostupnosti značí nedostupnost, nebo ztrátu dat (např. zašifrování pomocí ransomware útoku) (APTIEN.COM, 2023).

3.1 Typy kybernetických útoků

Malware

Malware je běžně využívaný nástroj používaný útočníky k tomu, aby pronikli do zařízení, či systémů ať už se jedná o osobní počítače, nebo zařízení používána v práci. Malware – z anglického malicious software (škodlivý software), na sebe může vzít celou řadu podob jako jsou spyware (software určený pro sledování), adware (reklamní software), nebo často používaný a známý ransomware a další. Díky malwaru je útočník schopen získat přístup do míst, kde by se jinak nedostal (osobní účty, citlivá data), v jiných případech lze hovořit o kompletním převzetí kontroly nad cíleným zařízením. Způsobů, jak se malware může dostat do uživatelova počítače je hned několik. Často však bývá spojen s lidskou neopatrností, která zahrnuje klikání na podezřelé odkazy, návštěva nezabezpečených internetových stránek, nebo stahování neznámých souborů, které mohou být nakaženy škodlivým softwarem (Kresa, 2018).

Adware

Adware pochází z anglického advertising supported software (software podporující reklamu) a jedná se o nejméně nebezpečného zástupce z řad malwarů. Projevuje se nejčastěji „vyskakovacími okny“ buďto na ploše počítače, nebo na internetových stránkách. Používán je s vidinou zisku na zobrazených reklamách. Na první pohled se může zdát, že tento typ malwaru je pouze otravný a nemůže způsobit větší škody, avšak je zde možné riziko, které spočívá ve spojení se spywarem, což je sledovací software, který je schopný odcizit uživatelská data (Kolouch, 2016).

Spyware

Pojem spyware je složen ze dvou anglických slov spy (špion) a software a jedná se tedy o sledovací software, který je schopný bez vědomí uživatele získávat statistická data o provozu počítače a tyto data následně odesílá do úložiště útočníka, který se jimi probere a zjistí, jestli nenarazil na něco užitečného. Mohou to být informace o spuštěných aplikacích/procesech, navštívených internetových stránkách, nebo informace osobnějšího charakteru (Kolouch, 2016).

Viry

Virus je typ malwaru, který je připojován ke spustitelným souborům, či dokumentům a je aktivován v momentě, kdy dojde ke spuštění, nebo otevření takového souboru. Ke množení těchto virů dochází již bez zásahu a vědomí uživatele a dál se šíří pomocí sdílení a posílání infikovaných souborů napříč různými systémy. Viry byly používány spíše v minulosti a dnešní trendy kybernetických útoků s nimi již moc nepočítají (Kolouch, 2016).

Červi

Počítačoví červi (anglicky „worms“), se od virů liší tím, že ke své reprodukci nepotřebují hostitelský soubor. Napadnou systém a dokáží se rychle šířit samostatným rozesíláním vlastních kopií do dalších zařízení, či systémů. Počítačoví červi se také využívají pro svoji schopnost vyhledávat bezpečnostní slabiny například v napadených informačních systémech (Kolouch, 2016).

Trojský kůň

Trojské koně jsou typy počítačových programů, které v sobě skrývají další potenciálně nebezpečné programy, o kterých uživatel nemá ponětí. Tyto programy mohou být maskovány jako legitimní software nebo přidány do bezpečně vypadajících aplikací. Trojské koně však na rozdíl od virů postrádají funkci se sami množit bez přičinění uživatele. Pokud se stane, že se trojský kůň aktivuje uvnitř systému, může dojít k mazání souborů, blokování, či úprava dat a narušení celého provozu počítačového systému nebo sítě (Kolouch, 2016).

Ransomware

Ransomware, pravděpodobně nejznámější zástupce ze skupiny Malware, také známý pod spojením „vyděračský malware“, je druh škodlivého softwaru, který je specifický v tom, že uživatelům zabrání přístup k počítačovým souborům, nebo celému systému, dokud oběť nezaplatí výkupné. Existují dva hlavní typy ransomware. První typ z pravidla blokuje úplný přístup k operačnímu systému a zamezuje uživateli jakékoliv využívání svého zřízení. Druhý typ ransomware, který se objevuje častěji, též nazývaný crypto-ransomware se zaměřuje na konkrétní cíle a jsou při něm zašifrována uživatelská data, jako soubory, složky, nebo dokonce celý pevný disk. Pokud se uživatel chce proklikat ke svým zašifrovaným souborům, vyskočí na něj zpráva s žádostí o výkupné k tomu, aby mohla být data dešifrována a navrácena zpět. Šíření je opět nejčastější prostřednictvím infikovaných webových stránek, e-mailových příloh, nebo v podobě trojského koně. Výkupné je nejčastěji

požadováno ve virtuálních měnách jako je třeba Bitcoin a je stanovena časová lhůta pro zaplacení (Kolouch, 2016).

Phishing

Phishing je jednou z nejznámější a nejvíce užívanou podvodnou taktikou kyber-útočníků, který má za cíl vylákat z obětí citlivé informace jako jsou uživatelská jména, hesla, čísla kreditních karet apod. Nejčastěji je útok spojován s na první pohled legitimně vypadajícími webovými stránkami, například web internetového bankovnictví, který je však falešný a po přihlášení jsou vámi zadané údaje odeslány útočníkovi. Odkazy na podobné stránky, které mají za cíl obalamutit uživatele jsou distribuovány především pomocí e-mailů, či zpráv na sociálních sítí od lidí, kteří se vydávají za někoho, kým nejsou (příbuzní, někdo z banky atd.). Důležité je si pečlivě prohlédnout URL adresu webové stránky, ve které bývají často chyby, nebo se neshoduje s adresou opravdového webu za který se útočník vydává. Existují i různé stránky na internetu, které jsou schopny zjistit, zda je adresa stránky v pořádku a zda je bezpečná (Kolouch, 2016).

Pharming

Pharming je propracovanější a také nebezpečnější metoda phishingu, která zahrnuje útok prostřednictvím DNS serveru (Domain Name Systém), který slouží k překladu doménového jména webové stránky na ip adresu a obráceně. V praxi to vypadá tak, že uživatel se chce dostat na webové stránky například internetového bankovnictví, avšak v okamžiku, kdy zadá adresu do vyhledávače, dojde k přepojení na falešnou stránku útočníka, která je téměř k nerozeznání od originálu. Poté všechny údaje zadané na této falešné stránce jsou přeposlány útočníkovi jako v případě Phishingu (Kolouch, 2016).

Spear phishing

Další metodou phishingu, která se podobně jako je tomu u pharmingu od klasického phishingu liší svou komplexností, a navíc ještě konkrétním zaměřením na cíl. U klasického phishingu dochází spíše k nahodilým útokům, kdy útočník pomyslně rozhazuje sítě a čeká kdo se chytí. Spear phishing je oproti tomu důslednější a cílí na konkrétní organizaci, skupinu, nebo jednotlivce s cílem vylákat z nich finanční údaje, obchodní strategie, nebo citlivé, či utajované informace. V počáteční fázi útoku jsou shromažďovány veškerá data a informace o cílené organizaci ze zdrojů, které jsou veřejně dostupné. Poté útočník vytvoří na míru ušitou např. e-mailovou komunikaci se zaměstnancem uvnitř organizace a začne se vydávat za kolegu z práce. Získá si důvěru oběti a tohoto pracovníka následně využije jako

prostředníka pro šíření dalších zpráv, nebo škodlivého softwaru s cílem dostat se hlouběji do organizace. Jelikož se útočník vydává za „známou“ osobu, není důkladněji prověřován (Kolouch, 2016).

Man in the Middle útok

Man in the middle útok znamená, že se útočník dostane do komunikace mezi dvě zařízeními. Tuto komunikaci může poté následně odposlouchávat a získávat tak citlivé informace, nebo je schopný komunikaci pozměnit. Kyber útočníci tento typ útoku využívají většinou pro získání informací, které mohou využít k dalším zločineckým praktikám.

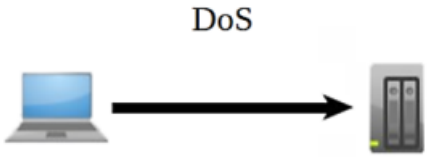
Jedním ze způsobů jak je tento útok prováděn útočníky je ten, že vytvoří veřejnou wifi síť, kterou monitorují a v případě, že se na ni někdo připojí a přihlásí se prostřednictvím této sítě například do internetového bankovnictví, tak útočník je schopen získat přihlašovací údaje oběti a provést krádež peněz. Dalším problémem mohou být nezabezpečené webové stránky, které fungují podobným způsobem jako pasti v podobě veřejných wifi sítí. Proto se na veřejných wifi nedoporučuje se kamkoliv přihlašovat, nebo zadávat citlivé údaje (Digitální pevnost, 2018).

DoS, DDoS, DRDoS útoky

Termín DoS z anglického „denial of service“, což v překladu do českého jazyka znamená odepření služby, druh útoku, který cílí na dostupnost internetových služeb, buď se snahou omezit jejich chod, nebo úplně přerušit. Útok probíhá tak, že se cílový počítačový systém, nebo síťový prvek zaplaví nadměrným množstvím požadavků, které se systém snaží zpracovat. Důsledkem velkého množství požadavků cílící na jeden počítač může být výrazné zpomalení poskytované služby, nebo její dočasný výpadek, například v případě webových stránek (Kolouch, 2016).

DoS

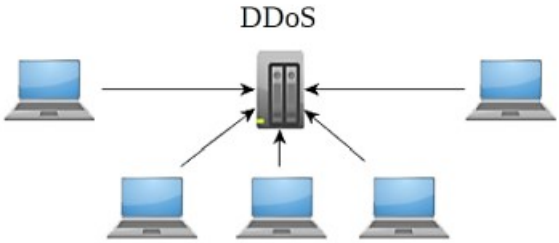
U DoS dochází k útoku pouze z jednoho zdroje (počítače), tudíž cílový systém nedostane takové množství požadavků najednou a lze mu snadněji zabránit zablokováním útočníkova zařízení (Kolouch, 2016).



Obrázek 1 – Denial of Service (Kolouch, 2016)

DDoS

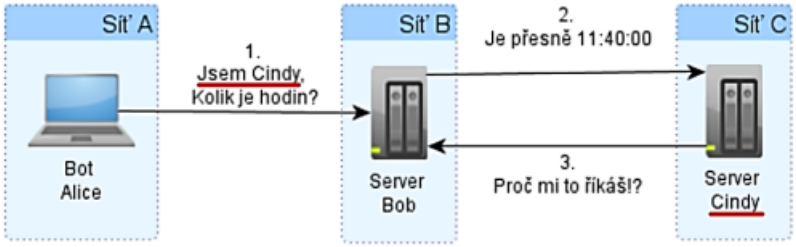
Distributed Denial of Service, což je distribuované odepření služby spočívá v zaplavení cílového systému požadavky z více počítačů, které se navíc mohou nacházet na různých místech což přispívá k obtížnější identifikaci a obraně proti útočníkovi. Takový typ je nejčastěji provozován nějakou větší skupinou tzv. „hackerů“, nebo pomocí botnetů – síť softwarově propojených botů (počítačů), kdy je jejich výkon využit na nějakou konkrétní aktivitu dle příkazu správce této sítě (například pro odeslání požadavků v rámci DDoS útoku) (Kolouch, 2016).



Obrázek 2 – Distributed Denial of Service (Kolouch, 2016)

DRDoS

Distributed Reflected Denial of Service znamená distribuované odražené odepření služby. Tento typ útoku využívá tzv. odražení, kdy útočník odesílá mnoha počítačům a serverům falešné žádosti na komunikaci a použije při tom zdrojovou adresu oběti. Ostatní systémy a počítače, které byly požádány o komunikaci tak správně odpoví, avšak ne na adresu útočníka, který všechno inicioval, ale na adresu oběti a cílový systém se tak stane přehlcený odpověďmi od ostatních systémů, což může opět vést ke zpomalení, či výpadku služby. Počítače a servery, které správě odpovídají na falešný požadavek se tak stanou nedobrovolnými účastníky DRDoS útoku (Kolouch, 2016).



Obrázek 3 – Distributed Reflected Denial of Service (Kolouch, 2016)

Kybernetických útoků je celá řada, avšak pro potřeby této bakalářské práce je tento výběr možných hrozeb dostačující.

3.2 Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022

Oproti roku 2021 se počet incidentů, které NÚKIB – Národní úřad pro kybernetickou bezpečnost, vyhodnotil jako hrozbu pro kybernetickou bezpečnost České republiky snížil ze 157 na 146.

Byly to převážně nejrůznější druhy phishingu, spear-phishingu, scanningu, DDoS útoky na dostupnost a velká spousta podvodných e-mailů, které patřily k těm nejčetnějším útokům za uplynulý rok. Naopak zaznamenali menší výskyt ransomwarových útoků a zneužívání zranitelností, či škodlivého kódu. Avšak i tyto metody stále představují relevantní hrozbu.

Data byla čerpána ze zprávy o kybernetické bezpečnosti ČR za rok 2022, ve které byl subjektům rozeslán dotazník se 77 otázkami týkající se kybernetické bezpečnosti. Šlo o subjekty regulované zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů, tak i organizacím a institucím, které tímto zákonem regulovány nejsou. Dotazník byl vyplněn dohromady 317 subjekty, z toho bylo 236 regulovaných a 81 neregulovaných (NÚKIB, 2023).

V roce 2023 bylo evidováno 262 kybernetických incidentů, podle zpráv z letošního ledna. Avšak zpráva o stavu kybernetické bezpečnosti ČR za rok 2023 ještě nebyla zpracována. Velký podíl na zvýšeném počtu kybernetických incidentů mají DDoS útoky směřující především ze stran proruských hacktivistů (NÚKIB, 2024).

4 ZABEZPEČENÍ

Poslední kapitola teoretické části bude věnována zabezpečení informačních systémů a možnosti, jak předcházet kybernetickým útokům.

4.1 Ověřování

Při snaze zabezpečit informační systém je nutné docílit toho, aby do systému, nebo k informacím měla přístup pouze pověřená osoba. K tomu jsou použity nástroje pro ověřování, které nám pomůžou zjistit, zda je daná osoba skutečně ta, za kterou se vydává. Autentizace, jak je tento proces nazýván je možné dosáhnout podle tří „vlastností“ osoby, která do systému přistupuje. Ověřuje se zda:

1. Osoba něco zná.
2. Osoba něco má.
3. Nebo osoba něco, nebo někým je.

Nejběžnější metodou první formy, kdy osoba něco zná je uživatelské jméno a heslo, které se nyní používá takřka všude, avšak může být snadněji kompromitovaná. Další metodou, kdy osoba něco má, je myšleno například fyzický předmět, jako je čip, nebo přístupová karta. Avšak i zde může dojít ke ztrátě předmětu a potencionální útočník tuto např. přístupovou kartu je schopen využít. Polední metodou využívanou v posledních letech je faktor toho, že osoba někdo je. Tím se má na mysli fyzická charakteristika člověka, jako je otisk prstu, sken sítnice v oku, či face id (systém pro rozpoznávání tváře). Identifikace osoby na základě jeho fyzických vlastností se nazývá biometrika (Bourgeois et al., 2019).

Vícefaktorové ověřování

Vícefaktorové ověřování kombinuje více metod ověřování a násobí tak bezpečnost prováděné autentizace. Typickým příkladem může být třeba, že zaměstnanec před vstupem do budovy, nebo do systému přiloží svou id kartu a poté je vyzván z zadání hesla, či pinu. Jde tedy o způsob snižování rizika, kdy pravděpodobnost, že útočník odcizí přístupovou kartu a zároveň bude znát i přístupové heslo je znatelně nižší (Bourgeois et al., 2019).

4.2 Zálohování

Jedním z nejdůležitějších nástrojů pro ochranu a zabezpečení dat a informací uvnitř organizace je správné zálohování. Zálohována by měla být, pokud možno všechna data jak

už na serverech, tak i na jednotlivých počítačích, které jsou využívány zaměstnanci. Zálohování obsahuje několik důležitých částí:

Znalost informačních zdrojů organizace

To znamená především jaké informace organizace doopravdy má, kde jsou uloženy a také zda jsou uloženy všechny na jednom místě, nebo jsou různě rozmístěny. Uloženy mohou být na serverech organizace, na pevných discích, nebo využitím cloudové služby. V takovémto případě je dobré si vypsat všechny informace a data, jejich umístění a zvolit nejvhodnější způsob zálohy (Bourgeois et al., 2019).

Pravidelné zálohování

To, jak často se organizace rozhode data zálohovat záleží na tom, jak moc si tato data cenní a zda je dokáží v případě ztráty nahradit. Data, která jsou nezbytná pro chod firmy by bylo vhodné zálohovat denně a u dat méně důležitých by se mohlo jednat o zálohu každý týden (Bourgeois et al., 2019).

Úložiště mimo místo organizace

V ideálním scénáři jsou data zálohována i na jiném místě, než pouze v budově organizace. Tak lze předejít, že při nějaké mimořádné události organizace přijde jak o veškerá svá data, tak i o své zálohy. K tomu lze využít například cloudových služeb (Bourgeois et al., 2019).s

4.3 Provozní bezpečnosti

Provozní bezpečnosti zahrnují celou řadu procesů a opatření, kterými lze zabezpečit informační systém v organizaci na více úrovních. Patří mezi ně například oddělení vývoje, testování a provozu. Nové věci zaváděné do systému mají větší riziko zranitelnosti a vzniku chyb, a proto pro vývoj nových technologií a jejich následné testování je dobré mít oddělené prostředí, které nezasahuje do provozu organizace.

Další důležité opatření je nějaká forma ochrany proti malware. Prevence a včasná detekce škodlivého softwaru je nezbytná pro bezproblémový chod organizace. Nejčastěji je toto opatření zajišťováno pomocí antivirových programů, nebo bezpečnostních služeb jako jsou webové proxy servery. Proxy servery zamezují šíření škodlivého softwaru pomocí internetu a blokují stránky, které mohou malware obsahovat. Populární technologií v ochraně proti škodlivému obsahu je systém EDR (Endpoint Detection and Response), v češtině znamená systém detekce a zabezpečení koncových zdrojů. Obsahuje v sobě ochranu proti malware, hledání zranitelností nebo monitorování podezřelých aktivit (Nonnemann et al., 2022).

Firewall

Další metodou, jak zvýšit úroveň bezpečnosti ve své síti, jak už v rámci organizace, tak u osobních počítačů je Firewall. Firewall existuje jak ve formě hardwaru, tak i softwaru. V případě hardwaru se jedná o zařízení, které je připojené do sítě a filtruje jak komunikaci z internetu do místní sítě, tak naopak. Takovou funkci může vykonávat např. klasický router. Softwarová brána firewall je spuštěna v operačním systému a zachycuje pakety (bloky dat) při jejich vstupu do počítače. Jedná se tak o jakýsi filtr, který do místí sítě nevpustí nevyžádanou komunikaci, nebo případné pokusy o útok. Firewall funguje na základě pravidel, která povolují, nebo zakazují určité pakety. Pravidla mohou být nastavena jak pro vstup paketů do počítače, tak pro odchozí komunikaci do sítě (Bourgeois et al., 2019).

II. PRAKTICKÁ ČÁST

5 OBECNÍ ÚŘAD BÍLOVICE

Obec Bílovice se nachází ve Zlínském kraji, 8 km od Uherského Hradiště, které je okresním městem a zároveň obcí s rozšířenou působností, pod kterou Bílovice spadají. Obec je rozdělena na dvě části – Bílovice a Včelary.

- Celková rozloha obce je 6,56 km^2.
- Počet obyvatel v obci je 1922 (URBITECH, 2024).

Obrázek 4 – Obec Bílovice (Bílovice, 2024)

Obrázek 5 – Obecní úřad Bílovice (Bílovice – obecní úřad, 2024)

Organizační struktura obce

- Obec Bílovice má jednoho starostu a dva místostarosty, rovněž má obec v zastupitelstvu 15 členů.
    - Starosta: Petr Fusek
    - Místostarosta: Eliška Kozelková
    - Místostarosta: Ing. Adam Skovajsa
- Oddělení administrativy a účetní má dvě pracovnice
    - Administrativní pracovnice: Marcela Dostálková
    - Účetní: Jana Gajarská
- Technická správa obce TSO
    - Vedoucí: Boleslav Stašek
- Místní knihovna Bílovice
    - Knihovnice: Hana Krystýnová
- Stavební úřad
- Matrika (URBITECH, 2024)

6 ROZHOVOR

Rozhovor je jednou z metod sběru dat, kdy tazatel pokládá otázky dotazovanému a ten na ně odpovídá. Podle míry připravenosti otázek a volnosti, kterou tazatel dá dotazovanému lze rozhovory dělit na strukturované, polostrukturované, nebo nestrukturované. Rozhovor lze provádět osobně, pomocí hovoru, či videohovoru, nebo pomocí elektronické pošty. V této práci byl zvolen strukturovaný rozhovor, kdy byly otázky předem dány a rozhovor proběhl pomocí e-mailové komunikace (Recmanová, 2022).

6.1 E-mailová korespondence

E-mailová korespondence s panem Ing. Liborem Bartasem, správcem sítě obecního úřadu Bílovice.

„Vážený pane inženýre,

Jsem studentem 3. ročníku UTB na Fakultě logistiky a krizového řízení v oboru Ochrana obyvatelstva. Téma mé bakalářské práce je Identifikace a posouzení rizik informačního systému vybrané organizace. Obracím se na Vás s prosbou o poskytnutí rozhovoru jako podklad pro mou praktickou část.

Po domluvě s panem Ing. Skovajsou bych Vás touto cestou chtěl poprosit o zodpovězení 12 otázek týkajících se informačního systému na obecním úřadu v Bílovicích. Otázky jsou přiloženy v příloze.

Jsem si vědom citlivosti některých informací a proto, kdyby byl problém v zodpovězení některých otázek, je možnost se domluvit a v práci některé informace anonymizovat. Děkuji.

Hezký zbytek večera,

Šimon Kovalčík“

6.2 Otázky rozhovoru

1. **Jaké informační systémy používáte?**
   - *Windows Server 2016 Standard*
   - *Windows 10 / 11 PRO*
   - *Gordic GINIS*
   - *VITA Stavební úřad* (Bartas, 2024)

2. **Popište mi prosím tok dat ve Vašem informačním systému.**
   - *Síťové aplikace instalovány na serveru – sdílené databáze, na lokálních PC pouze klientské aplikace, připojují se na společná data na serveru….*
3. **Jaká máte aktiva na obecním úřadě?**
   - *data z evidence obyvatel a matriky (RČ, trvalý pobyt…)*
   - *účetnictví, opět aplikace Gordic*
   - *síťová pokladna – přístup účetní a pokladní*
   - *ostatní účetní agendy lokálně na PC účetní, přístup pouze ona*

     (v současnosti přecházíme na novou verzi, která poběží na SQL)
   - *VITA Stavební úřad, nutná ochrana a záloha databáze*
   - *zde je veškerá agenda SÚ pro Bílovice a okolní vesnice*
   - *Dokumenty jednotlivých uživatelů, síťová záloha na NAS, individuální zálohy uživatelů*
   - *Outlook – maily zálohovány na serveru provozovatele, nemáme vlastní mailový server*
   - *webovky – opět na serveru provozovatele*
4. **Setkali jste se zde s nějakým kybernetickým útokem, nebo zranitelností v rámci IS?**
   - *Zatím ne …*
5. **Jaké aktivum je pro Vás nejcennější?**
   - *tak nejnutnější je ochrana dat z evidence obyvatel a matriky (RČ, trvalý pobyt…)*

     data se nachází v aplikaci Gordic v jedné databázi
     přístup má pouze matrikářka, nic se nesdílí
6. **Jak byste zhodnotil obecní úřad z pohledu kybernetické bezpečnosti?**
   - *Server, router, switch, PC zabezpečeny dle našich možností a požadavků ISZR, určitě by se dalo pracovat na zlepšení. E-mailová korespondence zabezpečena dle požadavků NÚKIB.*

     Do budoucna uvidíme, co přinese nová směrnice NIS2. (Bartas, 2024)

Nic není neprolomitelné, pokud se na vás někdo zaměří, tak už je to jenom o tom, jaké máte zálohy na externím HDD, všechno, co je na síti se dá napadnout…

Nejbezpečnější je PC bez internetu … :-)

7. **Jsou zaměstnanci seznámeni s problematikou Kybernetické bezpečnosti?**
   - *Ano, průběžně je informuji o možných rizicích a podvodných e-mailech…*
8. **Pořádali jste / pořádáte nějaké školení zaměstnanců v oblasti Kybernetické bezpečnosti?**
   - *Zaměstnanci absolvují školení pořádané Zlínským krajem, myslím, že nějaké proběhli….*
9. **Vidíte nějaké mezery v zabezpečení Vašeho Informačního systému?**
   - *VPN tunel pro přístup na vzdálenou plochu (zatím se na tom pracuje).*
10. **Mohl byste vyjmenovat možná rizika, které by se mohl objevit v rámci Vašeho IS?**
    - *nedokončená VPN*
    - *lidský faktor*
    - *DDoS - zřejmě by to znamenalo dlouhé načítání a případnou nedostupnost aplikací umístěných na serveru, ale v našich podmínkách to nevidím jako největší zlo, jak jsem psal většina jede lokálně..*
    - *Ramsomware – zašifrovaná data, problém na celé síti, výkupné, …. Byl jsem svědkem u několika firem a nebylo to nic příjemného, v podstatě neřešitelná situace…*
11. **Jaké nástroje používáte pro zabezpečení Vašeho IS?**

    Dle požadavků GDPR musí být všechny PC zabezpečeny heslem, včetně spořiče obrazovky. Server a jednotlivá PC chráněny systémem ESET PROTECT (monitoring sítě, vzdálená správa, antivirová ochrana)

    V informačním systému Gordic GINIS nastaveny přístupy dle jednotlivých uživatelů a funkcí (jméno / heslo).

    Czech POINT – certifikáty QCA a VCA uloženy na tokenu, chráněno PINem
12. **Jak řešíte zálohování dat na obecním úřadu v rámci IS?**
    - *Zálohy probíhají na síťové úložiště NAS Synology v rámci lokální sítě*
    - *na konci měsíce záloha na externí USB disk (šuplíková záloha) ….* (Bartas, 2024)

7 INFORMAČNÍ SYSTÉMY

V této kapitole se nachází výčet informačních systému, které jsou používány na obecním úřadu v Bílovicích. Na konci je graficky znázorněn tok dat v informačním systému obce.

7.1 Typy informačních systémů na obecním úřadu

Windows server 2016

Windows server je operační systém od společnosti Microsoft navržený pro ulehčení správy serveru. Zaměřuje se na podniky a organizace, kterým se snaží ulehčit práci řadou funkcí, mezi které patří například správa uživatelských účtů, možnost udělovat uživatelská práva, nebo poskytování internetových služeb. Nejnovější verze Windows Serveru je z roku 2022.

Další funkcí, kterou disponuje Windows Server je služba Active Directory, která organizaci umožní spravovat strukturu celé sítě od uživatelských účtů až po všechna zařízení v síti, což znamená třeba možnost instalovat a aktualizovat programy na koncových zařízeních.

Za zmínku stojí také vyzdvihnout síťovou službu v podobě DHCP serveru, který automaticky přiřazuje IP adresu a masku sítě pro každé zařízení a DNS server překládající IP adresy na doménová jména (Alza, 2024).

Windows 10 / 11 PRO

V roce 2015 vydala společnost Microsoft novou verzi operačního systému Windows, a to konkrétně verzi Windows 10, který tak nahradil své předchůdce Windows 7 a Windows 8. Tento operační systém je vhodný jak pro klasické uživatele i pro organizace či větší podniky. Oproti minulým verzím přichází s vylepšeným designem a řadou nových funkcí. Společnost Microsoft slíbila podporu verze Windows 10 až do října roku 2025.

Microsoft Windows 10 existuje ve třech verzích – Windows 10 Home/Pro/Enterprise. Home je určena pro běžné uživatele za nejdostupnější cenu. Verze Pro je směřována na podniky, které využijí funkce jako připojení k firemní doméně, šifrování dat, virtualizaci nebo funkci vzdálené plochy. Poslední Enterprise je určena pro ještě větší firmy a nabízí ještě o něco větší paletu služeb.

Windows 11 byl uveden na trh v roce 2021 a je tak nejnovější verzí operačního systému z dílny Microsoftu. Od své předchozí verze se liší opět novějším designem, je zde vylepšené uživatelské prostředí a je zde i podpora aplikací pro Android. Uživatelé si mohou aktualizaci z předchozí verze udělat kdykoliv a zcela zdarma (Alza, 2024).

Gordic GINIS

Gordic GINIS je jednou z nejvíce rozšířených platforem pro veřejnou správu využívaných v České republice. Své uplatnění si tento informační systém našel na všech úrovních veřejné správy od ministerstev, přes krajské a městské úřady až po menší obecní úřady. Láká především svou přívětivostí vůči uživatelům, provázanosti jednotlivých funkcí a také klade velký důraz na bezpečnost.

Digitalizace veškerých činností na úřadech ulehčuje spoustu času a úsilí jak pracovníkům ve státním sektoru, tak obyčejným lidem. Informační systém GINIS k tomu přispívá celou řadou nástrojů pro práci v sekci řízení lidských zdrojů, ekonomické části a účetnictví, správních agend a další. GINIS je také možno propojit s jinými aplikacemi pro práci v podobném sektoru, a tak ulehčuje spousty práce. Systém je neustále vyvíjen a následuje bezpečnostní požadavky dnešní doby, potřeby uživatelů i změny v právním rámci.

Zmíněný informační systém od společnosti GORDIC je nabízen ve třech verzích a to Standrad (spíše větší organizace), iFIS (veřejné instituce a vysoké školy) a Express vhodný spíše pro menší organizace jako právě obecní úřady. Nabízí jednoduché a vzájemně propojené moduly, které pokryjí veškerou práci v rámci obecního úřadu (Gordic).

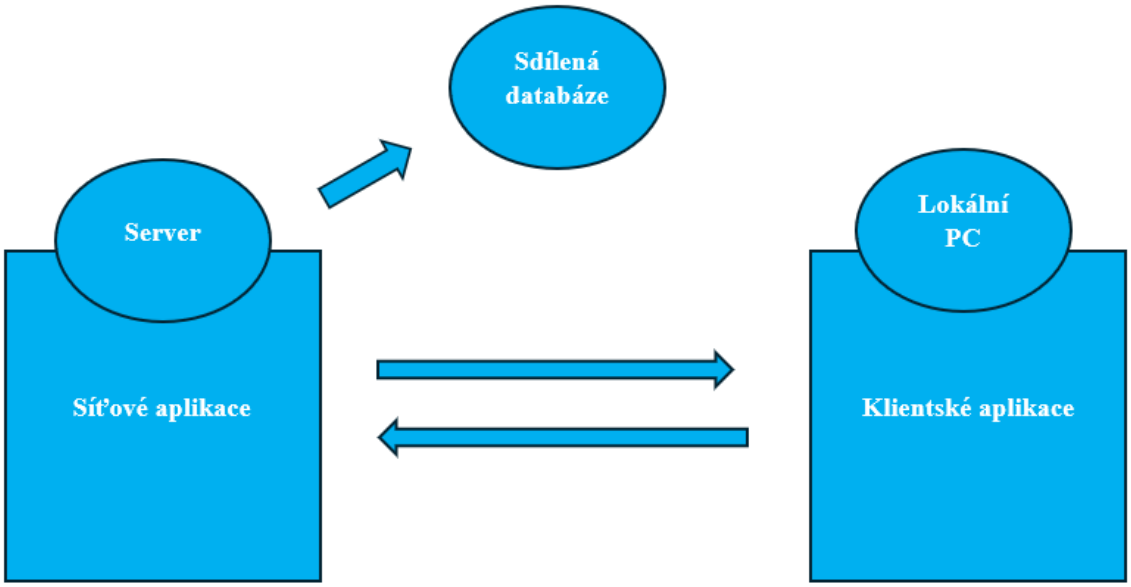
VITA stavební úřad

Agendové informační systémy (AIS) slouží pro usnadnění práce na stavebních úřadech, spadající pod stavební zákon. AIS je používán na více než 500 stavebních úřadech v České republice.

Mezi základní vlastnosti, kterými tento software disponuje je uvedena například evidence spisů v elektronické podobě, uvádí aktuální informace o účastnících a dotčených orgánech, odvolávací a přezkumné řízení, elektronická komunikace mezi jednotlivými orgány, tisk složenek a mnohé další (VITA Software).

7.2 Tok dat v informačním systému

Tok dat v informačním systému je neviditelný proces, který může být poněkud matoucí. Proto je dobré si ho graficky znázornit na zjednodušeném obrázku níže.



Obrázek 6 – Tok dat v informačním systému (vlastní)

Na PC zařízeních zaměstnanců se nachází pouze jejich klientské aplikace. K síťovým aplikacím a společným datům přistupují pomocí serveru, kde jsou tyto aplikace nainstalovány. Server zároveň komunikuje se sdílenou databází pomocí dotazů.

8 OBECNÍ ÚŘAD Z POHLEDU KYBERNETICKÉ BEZPEČNOSTI

V této kapitole je přehled zabezpečení jednotlivých zařízení nacházejících se na obecním úřadu společně s nástroji sloužící na zabezpečení informačního systému.

8.1 Zabezpečení jednotlivých zařízení

PC

Klientské počítače zaměstnanců jsou zabezpečeny firewallem v kombinaci s platformou ESET PROTECT.

Server

Obecní úřad používá Windows Server 2016, který v sobě má zabudován řadu funkcí, podporující bezpečnost. Zde je výčet některých z nich:

- Secure Boot – zabraňuje převzetí kontroly nad počítačem, v případě napadení se server nespustí.
- Shielded Virtual Machines – virtuální stroje jsou a zašifrovány pomocí nástroje BitLocker, který útočníkovi neumožní přistupovat k obsahu virtuálního stroje bez patřičného klíče.
- Insights & Analytics – nástroj, který sleduje aktivitu na serveru a monitoruje případné podezřelé chování uživatelů na serveru. S tím souvisí i snadné nastavování práv uživatelům dle obsahu jejich práce.
- Windows Defender – je součástí všech operačních systémů Windows a není tomu výjimkou ani zde. Jedná se o spolehlivý antivirový a antimalwerový program (ROOT.cz, 2016).

Switch

Switch neboli přepínač je přístroj, který propojuje zařízení v rámci organizace, respektive v její síti. Umožní tak různým zařízením jako jsou počítače, či tiskárny komunikovat mezi sebou a serverem nehledě na to, kde v podniku se nacházejí. Díky této schopnosti se Switch stává nezbytným komponentem v sítích menších organizací (Cisco, 2024).

Některé switche v sobě mají následující bezpečnostní prvky:

- Vlastní VPN – virtuální privátní síť.
- Firewall.
- Filtrování IP/MAC adres.

- Šifrování WPA 2/3 (Alza, 2024).

Router

Router, česky směrovač funguje podobně jako Switch, ale ve větším měřítku. To znamená, že na rozdíl od propojování zařízení, router propojuje přepínače (celé sítě) a přispívá tak k vytvoření ještě větší sítě. Dále také funguje jako jakási pomyslná brána do internetu pro všechna zařízení v dané síti. Díky směrovači je tak možné navázat kontakt s libovolnou webovou stránkou, nebo odesílání e-mailů po síti do cílového zařízení. Stejně tak, jak se stará o pohyb informací z vašeho zařízení dál do sítě, se stará i o to, aby všechna data směřující z internetu byla bezpečná a nezávadná (Cisco, 2024).

Zabezpečení routeru:

- Šifrování WPA2-AES a novější.
- Firewall.
- Rozdílné heslo routeru a WIFI sítě.
- Aktuální firmware (Asus, 2024).

ESET PROTECT

Společnost ESET nabízí na trh svoji platformu ESET PROTECT, která se snaží propojit všechny části kybernetické bezpečnosti jako je předcházení bezpečnostním incidentům, odhalení, že se něco děje a včasná reakce a odstranění problému. Platforma je nabízena ve verzích ENTRY, ADVANCED, COMPLETE, ELITE, MDR je neustále aktualizována a podle verze, kterou si zvolí zákazník nabízí širokou škálu všemožných služeb:

- Moderní ochrana koncových bodů.
- Zabezpečení serveru.
- Šifrování.
- Vícefázové ověřování.
- Pokročilá ochrana proti hrozbám.
- Zabezpečení e-mailu.
- Ochrana cloudových aplikací (Microsoft 365).
- Správa zranitelností a záplat a další.

Platforma je jednoduchá na používání a je vybudována tak, aby byla kompatibilní se všemi operačními systémy. Lze ji používat jako cloudovou službu, což organizaci umožní přístup do platformy kdykoliv a odkudkoliv, nebo je možné lokální řešení. Na obecním úřadu v Bílovicích se platforma ESET PROTECT stará o bezpečnost jak PC, tak serveru, která zde řeší monitoring sítě, antivirovou ochranu a vzdálený přístup (Eset, 2024).

8.2 Zabezpečení informačního systému

Informační systém základních registrů

Informační systém základních registrů se zkratkou ISZR vznikl se snahou zjednodušit a urychlit poskytování služeb státní sféry pro občany České republiky. Dříve zmíněné agendové informační systémy ověřují správnost dat základních registrů. Informační systém základních registrů se stará o to, aby byla data nedotčená, zajišťuje jejich aktuálnost a bezpečné sdílení mezi zúčastněnými úřady. Nabízí také možnost výměny dat s ostatními členskými zeměmi v Evropské unii. Důraz je také kladen na zabezpečení přenášených dat a informací. Všem zúčastněným orgánům veřejné moci ISZR posílá aktuální novinky a aktualizace potřebné pro správné fungování agend veřejné správy (Digitální a informační agentura, 2024).

E-mailová korespondence zabezpečena dle požadavků NÚKIB

E-mail patří mezi nejrozšířenější typy komunikačních kanálů, především ve státní sféře. Není však žádným tajemstvím, že nepatří mezi ty nejbezpečnější, protože se poměrně často stává také prostředkem pro šíření virů, či pokusů o phishing. Národní úřad pro kybernetickou bezpečnost proto dospěl k závěru, že tuto oblast posílí a vydal tak povinná plošná opatření pro všechny subjekty spadající pod zákon o kybernetické bezpečnosti. Pro ostatní subjekty jsou tato opatření doporučena také.

Opatření se vztahuje na celou řadu institucí působící ve státní sféře, konkrétně ministerstva, důležité úřady a krajské úřady a také organizace působící na nižších úrovních řízení. Nevynechává však ani soukromé organizace, které vzhledem ke svému podnikání často využívají e-mailové pošty.

Cílem těchto opatření bylo především posilnit bezpečnost komunikace mezi orgány státní veřejné moci. To by však nebylo možné, pokud by tato opatření byla zavedena pouze u některých orgánů, nebo subjektů, protože kdyby zavedené zabezpečení bylo jenom na jedné straně, celá komunikace by se tím pádem mohla stát zranitelnou. To by mohlo lákat

útočníky k provedení tzv. Man in the middle útok (MITM), kdy je nešifrovaná komunikace odposlouchávána, nebo pozměněna. Z toho důvodu se NÚKIB rozhodl zavést tato opatření pro všechny orgány, kterým tímto uložil povinnost. Opatření byla vydána v říjnu roku 2021. Jednalo se zejména o zavedení nejnovějších protokolů a standardů v oblasti elektronické pošty a zákazu používání těch zastaralých (NÚKIB, 2021).

NIS2

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Tak zní název první směrnice NIS, která byla přijata Evropskou unií v roce 2016. Česká republika výrazně přispěla k obsahu této první směrnice zejména díky znalostem z oblasti bezpečnosti sítí a informačních systémů ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti. V prosinci 2022, tedy po 8 letech byla publikována nová verze této směrnice NIS2, která vstoupila v platnosti již 16. ledna 2023, avšak členským státům byla udělena časová lhůta 21 měsíců na to, aby tuto směrnici zakomponovali do svého právního rámce. Pro Českou republiku to připadá na říjen 2024, kdy dojde k novelizaci stávajícího zákona o kybernetické bezpečnosti.

Změny se budou týkat nejenom organizací na nejvyšší úrovni – NÚKIB a Evropská agentura pro bezpečnost sítí a informací (ENISA), ale zasáhnou i do práv a povinností subjektů a společností působících v České republice.

Mezi nejvýznamnější změny, které tato nová směrnice NIS2 přinese je především povinné přijetí národní strategie kybernetické bezpečnosti a kybernetických bezpečnostních politik pro určité oblasti např. koordinované zveřejňování informací o zranitelnostech.

Tato národní strategie kybernetické bezpečnosti přijatá jednotlivými členskými státy, bude mít jasně vytyčené strategické cíle a zdroje, které budou potřeba k dosažení požadovaných cílů.

Další povinností bude v pověření některého ze svých CERT týmů, který se stane koordinátorem v oblasti zveřejňování zranitelností. Koordinátor se tak stane prostředníkem ve snaze zjednodušit komunikaci mezi subjektem oznamujícím zranitelnost a firmou, nebo poskytovatelem zranitelné služby, či produktu. Správcem nově vzniklé Evropské databáze zranitelností se stane Evropská organizace pro bezpečnost sítí a informací (NÚKIB, 2024).

GDPR

GDPR z anglického General Data Protection Regulation, neboli obecné nařízení o ochraně osobních údajů z rozhodnutí rady z roku 2016, které má za úkol chránit fyzické osoby v souvislosti se zpracováním osobních údajů. GDPR se stalo platným 25. května 2018.

V praxi musí tak správce a zpracovatel dat evidovat souhlas se zpracováním údajů subjektů, záznamy o zpracování, hlášení incidentů atd. Dále GDPR ukládá povinnost použití silných hesel dle pokynů administrátora sítě (Chytrá organizace).

CZECH POINT

CZECH POINT neboli Český Podací Ověřovací Informační Národní Terminál byl navržen s cílem zjednodušit komunikaci mezi občanem a veřejnou správou. Myšlenkou CZECH POINTU je změnit to, kdy občan musel obíhat několik úřadů k vyřešení nějakého problému a vytvořit takové místo, kde to všechno půjde vyřešit najednou. Na tomto místě je tedy možné získávat informace, ověřit si data, která jsou veřejná, ale i data z neveřejných informačních systémů a mnohé další (Czech Point).

Od roku 2009 byla zavedena povinnost zřídit si tzv. token, což je nosič dat, na který se ukládají certifikáty QCA (kvalifikovaný) a VCA (komerční), prostřednictvím kterých se přistupuje do systému CZECH POINT. Opatření bylo zavedeno z důvodu zvýšení bezpečnosti celého systému, tento token je chráněn pinem (Czech Point, 2009).

Zálohování

Zálohy probíhají na síťové úložiště NAS od společnosti Synology v rámci celé lokální sítě. Na konci každého měsíce navíc probíhá celková záloha systému na externí USB disk.

NAS Synology

Společnost Synology vyvinula zařízení NAS (Network Attached Storage), což lze volně přeložit jako úložiště na síti. Slouží tak pro bezpečné ukládání dat v rámci celé sítě vaší organizace a umožňuje tvorbu vlastního soukromého cloudu pro ukládání dat, sdílení souborů, nebo tvorbu záloh. NAS Synology je velmi dobrým nástrojem pro zálohování dat v rámci organizace. Je vybaven technologií pro pořizování snímků, které jsou schopny obnovit předchozí verzi souborů při náhlé ztrátě dat například v případě ransomware útoku.

Díky technologii deduplikace dat je možné na toto zařízení zálohovat soubory a data ze všech PC, serverů a dalších zařízení nacházejících se v organizaci, ukládají se však pouze unikátní

bloky dat a dochází tak k optimalizaci úložiště. Nabízí také flexibilní obnovení záloh, kdy je možné si zvolit obnovu celého systému, nebo pouze některých souborů (Synology, 2024).

9 ANALÝZA RIZIK

Kapitola obsahuje dvě metody pro analýzu rizik, a to konkrétně metodu What-if a SWOT analýzu.

9.1 Metoda What-if

What-if analýza (co se stane když…) je kvalitativní metoda analýzy rizik, která se používá při rozhodování v souvislosti řízení rizik. Je oblíbená především pro svoji časovou nenáročnost a jednoduché a přehledné zpracování. Metoda je většinou prováděná ve skupině lidí, kteří jsou seznámeni s danou problematikou, která je řešena prostřednictvím What-if analýzy. V následující části se kladou otázky „Co se stane když…" v souvislosti se vznikem nějakého rizika. Každému riziku se přiřadí následek, které by mělo na zkoumaný subjekt a následně je navrženo opatření, které by toto riziko zmírnilo, nebo úplně zklikvidovalo (Managment Mania, 2015).

Tabulka 1 – What-if analýza (vlastní)

Co se stane když …	Následek	Opatření
Phishing	Šíření virů v systému, převzetí kontroly nad PC	Školení zaměstnanců; antivirová ochrana
Ransomware útok	Zašifrování dat	NAS, obnova dat ze záloh
DDoS útok (pro obecní úřad z důvodu povahy organizace není vážná hrozba)	Zpomalení systému, nedostupnost aplikací na serveru	Blokování ip adres; technologie pro distribuci síťového provozu;
Man In the Middle útok	Odposlech/kompromitace dat	Zabezpečení e-mailové komunikace podle NÚKIB
Neoprávněný fyzický přístup k PC v organizaci	Přístup do informačního systému organizace	Zamykání PC; silné heslo; nepouštět cizí osoby na obecní úřad
VPN zranitelnosti	Odposlech citlivých informací, přístup do interní sítě	Správně nastavená VPN; Silné šifrování

Prolomení/Získání hesla některého ze zaměstnanců	Neoprávněný přístup do některého z informačních systémů	Silné heslo; Vícefaktorové ověření
Únik dat	Zneužití dat, porušení GDPR	Opatrná manipulace s daty; Zabezpečení dat vícefaktorovým ověřením

- Phishing – Nejčastěji pomocí e-mailů, může se stát, že některý ze zaměstnanců nebude na síti opatrný a klikne na nezabezpečený soubor.
- Ransomware útok – Často spojeno s phishingem, opět je zde scénář s e-mailovou přílohou, nebo nezabezpečenou stránkou.
- DDoS útok – Scénář, kdy by někdo chtěl uskutrčnit DDoS útok na informační systém obecního úřadu je méně pravděpodobný, neběží zde žádné služby, které by v případě výpadku mohli způsobit např. finanční škody.
- Man In the Middle útok – odposlech konverzace mezi zaměstnanci obecního úřadu a případně jinými subjekty je možný k získání citlivých informací.
- Neoprávněný fyzický přístup k PC v organizaci – vzhledem k tomu, že se jedná o malou organizaci, kde se všichni znají, je nepravděpodobné, že by se na obecní úřad dostal někdo cizí bez povšimnutí. Jakékoliv podezřelé chování by tak bylo včas zatrhnuto.
- VPN zranitelnosti – Útočníci mohou cílit na zastaralé/neaktualizované VPN softwary obsahující skulinky pomocí, kterých by se mohly dostat do pomyslného VPN tunelu a páchat škody uvnitř informačního systému organizace.
- Prolomení/Získání hesla některého ze zaměstnanců – Opět může souviset s phishingem, nebo pharmingem, kdy zaměstnanec „dobrovolně“ odevzdá přihlašovací údaje útočníkovi.
- Únik dat – Únik dat může být buďto nechtěný, nebo záměrný ze strany zaměstnance. V jiných případech, když už se útočník pomocí některého z výše zmíněných způsobů dostane do systému tyto data je schopen zveřejnit sám.

9.2 SWOT analýza

SWOT (Strenghts, Weaknesses, Opportunities, Threats) analýza je jedním z nejzákladnějších a nejčastěji používaných nástrojů pro tvorbu analýzy organizace, nebo budoucího projektu. Oblíbená je především díky své přehlednosti a časové nenáročnosti. SWOT analýza zkoumá interní část organizace (Silné a slabé stránky) a externí část (Příležitosti a hrozby). Výsledkem analýzy je graf, který určí, jakou strategií by se měla např. daná organizace ubírat:

- Ofenzivní strategie (SO) – převažují zde silné stránky a příležitosti nad slabými stránkami a hrozbami.
- Defenzivní strategie (ST) – zde převažují silné stránky nad slabými, avšak hrozby jsou větší než příležitosti.
- Strategie spojenectví (WO) – Slabé stránky převažují nad silnými, ale příležitosti jsou větší než hrozby.
- Strategie úniku/likvidace (WT) – Převaha slabých stránek nad silnými a hrozeb nad příležitostmi (EUROEKONÓM.SK, 2024).

Silné stránky

- Malá organizace – snadnější monitorování sítě a zjišťování případných zranitelností, zaměstnanci se mezi sebou znají, nejsou kladeny tak velké nároky na bezpečnost.
- Správce sítě přímo v obci – správce sítě sídlí přímo v obci, takže kdyby se cokoliv stalo měl by být připraven zasáhnout, je odborníkem z praxe.
- Kladen důraz na zálohování – data v celém systému jsou pravidelně zálohována na síťové úložiště NAS synology a každý měsíc je prováděna navíc záloha na externí disk.
- Solidní ochrana zařízení a systému v rámci KB – každý hardware a software v informačním systému má patřičnou ochranu proti napadení zvenčí.

Slabé stránky

- Jednofaktorové zabezpečení na zařízeních – Zabezpečení na zařízeních pouze stylem jméno + heslo, ale na úrovni obecního úřadu by to mělo být dostačující.

- Nedokončený VPN tunel – v procesu zavádění VPN (Virtual Private Network), mohou vzniknout zranitelnosti při nedostatečném zabezpečení privátní sítě (Digitální pevnost, 2018).
- Chybí školení zaměstnanců v rámci organizace – z rozhovoru nebylo zřejmé kdy a jak často školení probíhají v rámci Zlínského kraje, vhodnější by bylo školení přímo v rámci obecního úřadu
- Pouze jeden USB disk se zálohami – v případě ztráty USB disku, nebo kdyby došlo ke zničení dat příčinou mimořádné události, organizace by přišla o značnou část svých záloh.

Příležitosti

- NIS2 – v rámci zavedení nové směrnice NIS2 se očekává celkové zvýšení kybernetické bezpečnosti v České republice.
- Vzdělávací kurzy pro zaměstnance – školení zaměstnanců v oblasti kybernetické bezpečnosti interaktivní formou.
- Dokončení VPN tunelu – zesílení bezpečnosti komunikace v rámci sítě, zvýšená ochrana např. proti Man in the Middle útokům (Digitální pevnost, 2018).
- Zvyšující se důraz na kybernetickou bezpečnost – Po celém světě, ale i v České republice je poslední roky kladen velký důraz na kybernetickou bezpečnost, a proto je očekávané, že se v této oblasti bude stále inovovat.

Hrozby

- Narůstající počet kybernetických útoků – Podle výročních zpráv o stavu kybernetické bezpečnosti v České republice je možné sledovat narůstající trend kybernetických zločinů každým rokem a v budoucnu tomu nebude jinak.
- Umělá inteligence – Za minulý rok umělá inteligence zažila velký pokrok a projevilo se to i v oblasti kybernetických zločinů, kdy umělá inteligence je schopna generovat např. škodlivé kódy (NÚKIB, 2024).
- Zdokonalování hackerů – Stejně jak jde dopředu inovace v oblasti zabezpečení proti kybernetickým útokům, je dobré počítat i s tím, že zlo nikdy nespí a pokrok je i na straně hackerů ať už v jejich kreativitě, nebo s příchodem nových nástrojů jako třeba AI.

- Potíže na straně poskytovatele služeb – Je třeba také počítat s možnými výpadky na straně poskytovatele ať už informačních systémů, nebo bezpečnostních řešení, avšak společnosti jako třeba GORDIC nebo ESET jsou velice spolehlivé a pravděpodobnost takového výpadku, který by zaznamenali koncoví uživatelé je velmi malá.

Tabulka SWOT analýzy

Bodování bylo zvoleno od 1 do 5 podle důležitosti, stejně tak byla ukládána i váha, která v součtu musí dávat 1. Pro dosažení výsledku např. Silných stránek nejprve vynásobíme jednotlivé body s váhami a poté výsledky sečteme pod sebou.

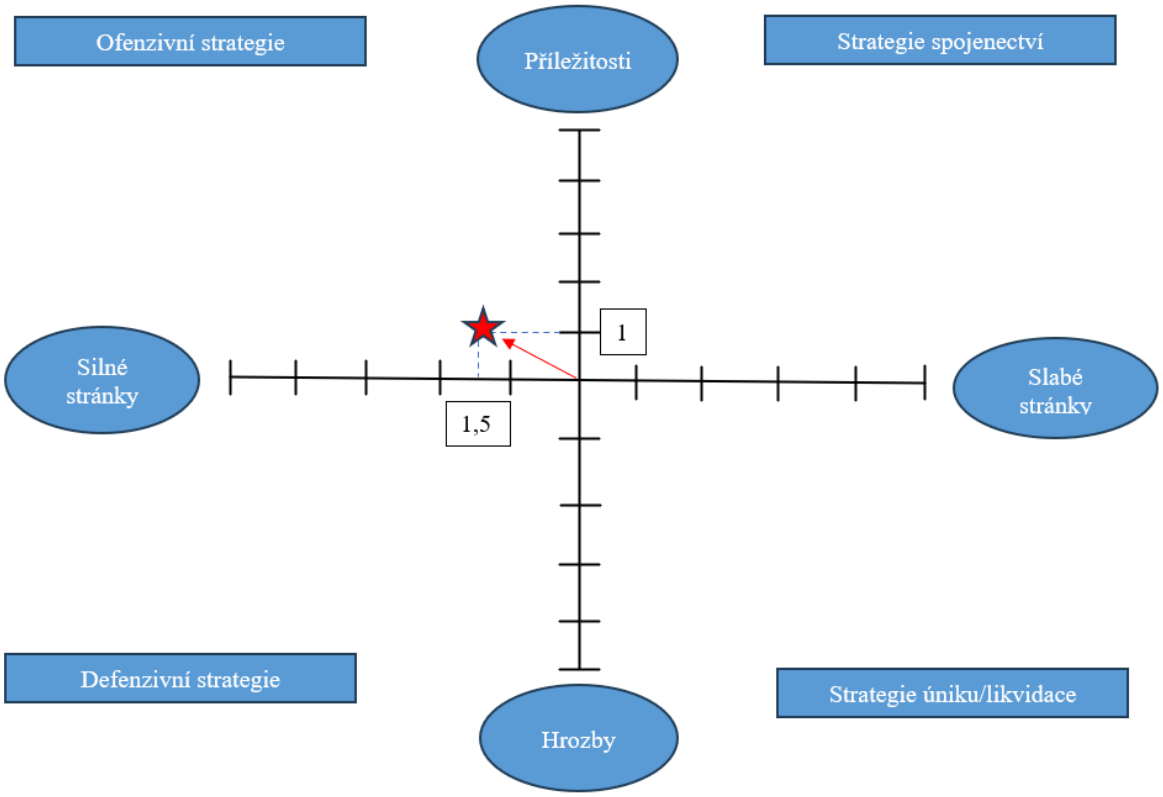
Tabulka 2 – SWOT analýza (vlastní)

Silné stránky	**Body**	**Váha**	**Celkem**
Malá organizace	3	0,2	0,6
Správce sítě přímo v obci	4	0,25	1
Kladen důraz na zálohování	4	0,25	1
Solidní ochrana zařízení a systému v rámci KB	5	0,3	1,5
	<1;5>	Σ 1	Σ 4,1
Slabé stránky	**Body**	**Váha**	**Celkem**
Jednofaktorové zabezpečení na zařízeních	-2	0,2	-0,4
Nedokončený VPN tunel	-3	0,3	-0,9
Chybí školení zaměstnanců v rámci organizace	-2	0,2	-0,4
Pouze jeden USB disk se zálohami	-3	0,3	-0,9
	<-1;-5>	Σ 1	Σ -2,6
Příležitosti	**Body**	**Váha**	**Celkem**
NIS2	3	0,15	0,45
Vzdělávací kurzy pro zaměstnance	4	0,3	1,2
Dokončení VPN tunelu	3	0,25	0,75
Zvyšující se důraz na kybernetickou bezpečnost	4	0,3	1,2
	<1;5>	Σ 1	Σ 3,6
Hrozby	**Body**	**Váha**	**Celkem**
Narůstající počet kybernetických útoků	-3	0,3	-0,9
Umělá inteligence	-3	0,25	-0,75
Zdokonalování hackerů	-3	0,25	-0,75
Potíže na straně poskytovatele služeb	-1	0,2	-0,2
	<-1;-5>	Σ 1	Σ -2,6

Výstupem SWOT analýzy je graf určující strategii, kterou by se organizace měla ubírat. K tomu, abychom zjistili hodnoty, které následně naneseme do grafu je třeba vypočítat výsledek interní a externí části organizace.

Interní část: 4,1 – (- 2,6) = 1,5

Externí část: 3,6 – (-2,6) = 1



Obrázek 7 – Výsledný graf SWOT analýzy (vlastní)

Na obrázku je možné vidět výsledný graf SWOT analýzy, kdy bylo na vertikální osu Příležitostí a Hrozeb nanesena hodnota **1**, čili hodnota externí části organizace a na vodorovnou osu Silných stránek a Slabých stránek byla nanesena hodnota **1,5** která značí hodnotu interní části organizace. Průsečík značený hvězdičkou a šipka ukazují do levého horního kvadrantu, který náleží Ofenzivní strategii.

Ofenzivní strategie = je nejlepší možná strategie, kdy v organizaci převažují silné stránky nad slabými a zároveň je organizace schopna využívat příležitosti pro další rozvoj a odolávat hrozbám (EUROEKONÓM.SK, 2024).

10 NÁVRH OPATŘENÍ

Na základě výsledků obou analýz, kdy ve What-if analýze byla zjištěna možná rizika, která mohou působit na informační systém obecního úřadu a pomocí SWOT analýzy byly identifikovány slabé stránky v interním prostředí organizace a hrozby působící zvenčí, je nutné navrhnout vhodná opatření.

Školení zaměstnanců

V oblasti kybernetické bezpečnosti je nesmírně důležitá prevence. Je dobré vnímat antivirové programy, pravidelné zálohování a další nástroje k zajištění bezpečnosti v kyberprostoru jako takovou záchranou brzdu, kdyby se náhodou něco stalo. Je jasné, že pohybovat se na internetu bez výše zmíněných nástrojů je značně riskantní, ještě k tomu, pokud jste veřejná instituce, nebo soukromý podnik. Ale je nutné zmínit, že pomocí prevence lze riziko napadení kyberzločinci značně snížit. Člověk, který je obeznámen s problematikou phishingu ví, že nemá otevírat ani stahovat neznámé soubory, které mu přistály v e-mailové poště, je si vědom toho, že by neměl pobývat na nezabezpečených stránkách a že veřejné wifi sítě nejsou vhodné ke kontrolování internetového bankovnictví, značně přispívá ke snížení riziku svého napadení. Cílem není udělat ze všech lidí experty na kybernetickou bezpečnost, ale pouze šířit základy bezpečného chování na internetu, především pak v prostorách organizace. Proto by bylo dobré se ještě více zaměřit na vzdělávání a osvětu zaměstnanců v rámci obecního úřadu. Vhodné proto mohou být třeba online kurzy, které jsou zdarma dostupné na vzdělávacím portálu Národního úřadu pro kybernetickou a informační bezpečnost.

- Snižuje riziko: Především phishingu díky znalostem, jak se chovat na nezabezpečených stránkách a v přítomnosti neznámých souborů. S tím souvisí také snížení rizika ransomware útoků, který se často šíří právě v přílohách neznámých souborů. A díky znalostem o veřejných wifi sítích, které mohou sloužit jako pasti se snižuje i riziko MITM útoku (NÚKIB, 2024).

Vícefaktorové ověření

Na první pohled se může zdát, že by to bylo na obecní úřad už trochu moc a že investice do podobných systémů by se nevyplatila. Ale i na obecním úřadu jsou uchovávána data, kterých se bude třeba někdy v budoucnu někdo chtít zmocnit a zneužít je. Pro zaměstnance, kteří nepracují s citlivými údaji by takové řešení bylo zbytečné, ale pokud je řeč třeba o oddělení účetnictví, nebo matriky, zde by se nad tím do budoucna dalo uvažovat. Při přihlašování na

některé stránky je možné využít mobilní aplikaci jako je například Microsoft Authenticator. Ten nám v případě prvního přihlášení do webové stránky přidá onen druhý faktor pomocí unikátního číselného kódu, který uživatel obdrží na svůj mobilní telefon. Při dalších přihlášeních již bude stačit pouze jméno a heslo. Kdyby se ale chtěl někdo cizí přihlásit na uživatelův účet a dělal by tak z jiného zařízení, tak i kdyby se mu podařilo nějak prolomit heslo, kód by přišel na telefon majiteli účtu a k tomu by se útočník nedostal.

- Snižuje riziko: Úniku dat, ke kterým mají přístup pouze pověřené osoby; prolomení hesla zaměstnance a teoreticky i fyzický přístup k PC v organizaci, kdyby byly zavedeny například přístupové karty (Microsoft, 2024).

Metoda zálohování 3-2-1 a cloudové řešení

I přes to, že je informační systém organizace na tom se zálohami velice dobře, dalo by se to ještě trochu vyšperkovat. Metoda 3-2-1 pojednává o vytvoření 3 kopií dat, které se rozdělí na 2 externí disky a z toho 1 se bude nacházet vždy na jiném místě než ten druhý. Je to forma jakéhosi rozložení rizika na více nosičů. K tomu by se ještě mohlo přidat externí cloudové úložiště, které není součástí interní sítě organizace. Na českém trhu je spousta společností nabízející takovéto řešení, například váš hosting, společnost CRA, nebo Algotech. Avšak je nutné zmínit, že nynější zálohovací politika obecního úřadu v Bílovicích je na organizaci takového typu dostačující.

- Snižuje riziko: Dopad ransomware útoku by při takovém množství záloh neměl organizaci nijak zvlášť poškodit (Algotech, 2024).

Dokončit VPN

Dokončením Virtuální privátní sítě obecní úřad zesílí svoji bezpečnost a zjednoduší vzdálený přístup do interní sítě organizace. Na tomto opatření se již pracuje.

- Snižuje riziko: Hlavně se bude jednat o znemožnění odposlechu a kompromitace dat v podobě Man in the middle útoku.

ZÁVĚR

Bakalářská práce byla zaměřena na téma Identifikace a posouzení rizik informačního systému vybrané organizace, konkrétně obecního úřadu, který spadá v rámci krizového řízení do oblasti územní samosprávy. Práce byla rozdělena na dvě hlavní části. V teoretické části byly vymezeny základní pojmy jako informační systém a jeho jednotlivé typy a moduly. Dále zde byl představen související zákon č. 181/2014 Sb. o kybernetické bezpečnosti, zejména jeho I. Hlava, popisující základní pojmy jako bezpečnost informací a kybernetický prostor a dále rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickou bezpečnostní událostí. Čtenáři se také mohli dozvědět o různých typech kybernetických útoků a jak jim předcházet.

Praktická část byla věnována obecnímu úřadu v Bílovicích, který byl krátce představen spolu s jeho organizační strukturou. První metodou, která se objevila v praktické části byl rozhovor se správcem sítě zkoumané organizace. Na základě odpovědí, byla později zpracována charakteristika organizace z pohledu kybernetické bezpečnosti, jakožto i výčet informačních systémů, které jsou zde využívány a tok dat v nich. Posouzení organizace z pohledu kybernetické bezpečnosti zahrnovalo výčet jednotlivých zařízení důležitých pro chod informačního systému společně s jejich zabezpečeními jako je například platforma ESET PROTECT. Následovala kapitola o zabezpečení informačního systému jako celku, ke kterému přispívá například i nařízení o zabezpečení e-mailové komunikace od Národního úřadu pro kybernetickou a informační bezpečnost, nebo zálohování do technologie NAS Synology. Pomocí dříve zjištěných informací byly vypracovány dvě analýzy rizik. První metoda What-if pracovala se scénáři osmi rizik, u kterých byly uvedeny následky a možná opatření, jak jim předcházet. V další analýze, kterou byla SWOT analýza bylo zjištěno, že v organizaci převažují silné stránky nad slabými a příležitosti nad hrozbami a patří tak do ofenzivní strategie. Bylo zjištěno, že informační systém organizace je poměrně slušně zajištěn proti hrozbám z kyberprostoru, avšak jeden z cílů bylo mimo posouzení organizace z pohledu KB a identifikací rizik také navržení vhodných opatřeních pro tato rizika. Navržená opatření se soustředila na rizika a slabé stránky z obou analýz a byla následující: Školení zaměstnanců, vícefaktorové ověřování, Metoda 3-2-1 + cloudové řešení záloh a dokončení VPN sítě. Tímto byly cíle stanoveny v úvodu práce splněny.

SEZNAM POUŽITÉ LITERATURY

AIRA GROUP, S.R.O., © 2022. *Co je informační systém*. Online. Www.sprava-site.eu. Dostupné z: https://www.sprava-site.eu/informacni-system/. [cit. 2024-03-16].

ALGOTECH, 2024. *Pravidlo 3-2-1 překonáno, aneb jak zálohovat data v roce 2023*. Online. Algotech.cz. Dostupné z: https://www.algotech.cz/novinky/pravidlo-3-2-1-prekonano-aneb-jak-zalohovat-data-v-roce-2023. [cit. 2024-04-30].

ALZA, 2024. *Jak vybrat switch domů nebo do firmy?* Online. Alza.cz. Dostupné z: https://www.alza.cz/jak-vybrat-switch. [cit. 2024-04-30].

ALZA, 2024. *Microsoft Windows 10*. Online. Alza.cz. Dostupné z: https://www.alza.cz/windows-10/18860426.htm?evt=re&exps=windows+10. [cit. 2024-04-30].

ALZA, 2024. *Microsoft Windows Server*. Online. Alza.cz. Dostupné z: https://www.alza.cz/windows-server/18860429.htm. [cit. 2024-04-30].

APTIEN.COM, 2023. *Co je CIA triáda informační bezpečnosti*. Online. Aptien. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad. [cit. 2024-03-17].

ASUS, 2024. *Jak zabezpečit router?* Online. Asus. Dostupné z: https://www.asus.com/cz/support/faq/1039292/. [cit. 2024-04-30].

BARTAS, Libor. 2024-04-24. *Rozhovor otázky*. E-mailová komunikace.

Bílovice, 2024. Online. In: Mapy.cz. Dostupné z: https://mapy.cz/zakladni?x=17.5465634&source=muni&id=3277&y=49.0961160&z=13. [cit. 2024-05-02].

Bílovice – obecní úřad, 2024. Online. In: Firmy.cz. Dostupné z: https://www.firmy.cz/detail/349990-bilovice-obecni-urad-bilovice.html. [cit. 2024-05-02].

BOURGEOIS, David T.; SMITH, James L.; WANG, Shouhong a , Joseph Mortati, 2019. *Information Systems for Business and Beyond*. Online. In: . Saylor Academy. ISBN 9781533064165. Dostupné z: https://digitalcommons.biola.edu/open-textbooks/1/. [cit. 2023-10-31].

CISCO, 2024. *What is a Switch vs a Router?* Online. Cisco.com. Dostupné z: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html. [cit. 2024-04-30].

CZ.NIC. *O týmu CSIRT.CZ.* Online. CSIRT.CZ. Dostupné z: https://www.csirt.cz/cs/o-nas/. [cit. 2024-05-01].

CZECH POINT. *Co je Czech POINT? Online.* Czech Point. Dostupné z: https://www.czechpoint.cz/public/statistiky-a-informace/co-je-czech-point/. [cit. 2024-04-30].

CZECH POINT, 2009. *Od 1. března autentizace pracovníků kontaktních míst Czech POINT možná jen s pomocí certifikátů.* Online. Czech Point. Dostupné z: https://www.czechpoint.cz/public/od-1-brezna-autentizace-pracovniku-kontaktnich-mist-czech-point-mozna-jen-s-pomoci-certifikatu/. [cit. 2024-04-30].

DIGITÁLNÍ A INFORMAČNÍ AGENTURA, 2024. *INFORMAČNÍ SYSTÉM ZÁKLADNÍCH REGISTRŮ*. Online. DIA_. Dostupné z: https://www.szrcr.cz/cs/informacni-system-zakladnich-registru. [cit. 2024-04-30].

DIGITÁLNÍ PEVNOST, 2018. *MITM (Man in the middle).* Online. Digitální pevnost. Dostupné z: https://www.digitalnipevnost.cz/viki/mitm-man-middle. [cit. 2024-04-30].

DIGITÁLNÍ PEVNOST, 2018. *VPN*. Online. Digitální pevnost. Dostupné z: https://www.digitalnipevnost.cz/viki/vpn. [cit. 2024-04-30].

EUROEKONÓM.SK, 2024. *SWOT analýza*. Online. EuroEkonóm.sk. Dostupné z: https://www.euroekonom.sk/manazment/strategicka-diagnostika/swot-analyza/. [cit. 2024-04-30].

ESET, 2024. *ESET PROTECT PLATFORM*. Online. Eset. Dostupné z: https://www.eset.com/cz/firmy/platforma-protect/. [cit. 2024-04-30].

GORDIC. *GINIS.* Online. Gordic. Dostupné z: https://www.gordic.cz/ginis. [cit. 2024-04-30].

KOLOUCH, Jan, 2016. *CyberCrime.* Online. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-18-8. [cit. 2023-10-31].

KRESA, Dan, 2018. *Jaké jsou nejčastější typy kybernetických útoků?* Online. KYBEZ. Dostupné z: https://kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/. [cit. 2024-03-17].

LEGISLATIVA S.R.O, 2022. *Kybernetický útok (kyberútok). Definice, typy, následky a prevence*. Online. Legislativa. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok. [cit. 2024-03-17].

MANAGMENT MANIA, 2015. *Čo - keď analýza (What-if Analysis).* Online. ManagementMania. Dostupné z: https://managementmania.com/sk/co-ked-analyza-what-if-analysis. [cit. 2024-04-30].

MICROSOFT, 2024. *Co je: Vícefaktorové ověřování*. Online. Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-v%C3%ADcefaktorov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-e5e39437-121c-be60-d123-eda06bddf661. [cit. 2024-04-30].

NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik, 2022. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* Právní monografie (Wolters Kluwer ČR). Praha: Wolters Kluwer. ISBN 978-80-7676-515-3.

NÚKIB. Vládní CERT. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/. [cit. 2024-05-01].

NÚKIB, 2021. *Správci klíčových systémů musí zabezpečit své e-mailové schránky*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1758-spravci-klicovych-systemu-musi-zabezpecit-sve-e-mailove-schranky/. [cit. 2024-04-30].

NÚKIB, 2023. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/. [cit. 2024-04-30].

NÚKIB, 2024. *Vítejte na vzdělávacím portálu NÚKIB.* Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://osveta.nukib.gov.cz/local/dashboard/. [cit. 2024-04-30].

NÚKIB, 2024. *NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů*. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/. [cit. 2024-04-30].

NÚKIB, 2024. *Nová směrnice EU o kybernetické bezpečnosti „NIS2“.* Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=145. [cit. 2024-04-30].

RECMANOVÁ, Ivana, 2022. *Rozhovor jako průzkum trhu nebo zákaznické zkušenosti.* Online. BlueGhost. Dostupné z: https://www.blueghost.cz/clanek/rozhovor-jako-pruzkum-trhu-nebo-zakaznicke-zkusenosti/. [cit. 2024-04-30].

ROOT.CZ, 2016. *Bezpečnost má Windows Server 2016 přímo ve své DNA*. Online. ROOT.cz. Dostupné z: https://www.root.cz/pr-clanky/bezpecnost-ma-windows-server-2016-primo-ve-sve-dna/. [cit. 2024-04-30].

SYNOLOGY, 2024. *Co je to NAS?* Online. Synology. Dostupné z: https://www.synology.com/cs-cz/dsm/solution/what-is-nas/for-business. [cit. 2024-04-30].

URBITECH, 2024. *Obec Bílovice.* Online. Obec Bílovice. Dostupné z: https://bilovice.cz/. [cit. 2024-04-30].

VITA SOFTWARE. *Správní agendy*. Online. VITA Software. Dostupné z: https://vitasw.cz/?pg=/www_sto/idx/index_sx.html. [cit. 2024-04-30].

Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: © AION CS, S.R.O. 2010–2024. Zákony pro lidi. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181. [cit. 2024-03-16].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI Artificial intelligence

ČR Česká republika

KB Kybernetická bezpečnost

NAS Network Attached Storage

PC Personal Computer

VPN Virtual Private Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁZEV PŘÍLOHY