ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

KYBERNETICKÁ BEZPEČNOST Z POHLEDU PODNIKOVÉ INFRASTRUKTURY

CYBER SECURITY FROM THE PERSPECTIVE OF CORPORATE INFRASTRUCTURE

Bakalářská práce

Studijní program:	Plánování a řízení krizových situací
Studijní obor:	Plánování a řízení krizových situací
Autor bakalářské práce:	Petr Miženko
Vedoucí bakalářské práce:	Ing. Václav Navrátil

Kladno 2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Miženko**	Jméno:	**Petr**	Osobní číslo:	**491717**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Plánování a řízení krizových situací**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kybernetická bezpečnost z pohledu podnikové infrastruktury

Název bakalářské práce anglicky:

Cyber Security from the Perspective of Corporate Infrastructure

Pokyny pro vypracování:

Bakalářská práce se bude zabývat problematikou kybernetické bezpečnosti ve společnosti se statutem bankovní instituce. V teoretické části nejprve autor identifikuje aktuální kybernetické hrozby, podložené případy skutečných incidentů, objasní jejich příčiny a uvede je do kontextu světového dění v oblasti kybernetické bezpečnosti. V praktické části se pak bude autor věnovat přípravě organizačních, procesních a technologických doporučení, vytvořených na základě klasifikační analýzy aktuálních hrozeb, předešlých bezpečnostních incidentů a SWOT analýzy zkoumané společnosti. Výstupem práce bude soubor organizačních, procesních a technologických doporučení pro české instituce mající za cíl zvýšení úrovně jejich kybernetické bezpečnosti.

Seznam doporučené literatury:

[1] KOLOUCH, Jan a Pavel BAŠTA, CyberSecurity, Praha: CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7
[2] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019, ISBN 978-80-7380-765-8
[3] ŠULC, Vladimír, Kybernetická bezpečnost, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, ISBN 978-80-7380-737-5
[4] Rising, P. , Microsoft 365 Security Administration: MS-500 Exam Guide: Plan and implement security and compliance strategies for Microsoft 365 and hybrid environments, Packt Publishing, 2020, ISBN 978-1838983123

Jméno a příjmení vedoucí(ho) bakalářské práce:

Ing. Václav Navrátil

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2022**
Platnost zadání bakalářské práce: **22.09.2023**

doc. Mgr. Zdeněk Hon, Ph.D. vedoucí katedry	prof. MUDr. Jozef Rosina, Ph.D., MBA děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Kybernetická bezpečnost z pohledu podnikové infrastruktury vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Mělníku dne 04.03.2022

Petr Miženko

PODĚKOVÁNÍ

V první řadě bych především rád poděkoval mé sestře Tereze Miženkové DiS. Za trpělivost, cenné rady a dohled nad tvorbou mé práce. Děkuji také za strávený čas nad mou prací a konstruktivní kritiku napomáhající k úspěšnému dokončení práce.

Dále bych rád poděkoval PhDr. Monice Donevové Ph. D. z katedry zdravotnických oborů a ochrany obyvatelstva za cenné rady stěžejní pro mou práci.

ABSTRAKT

Kybernetická bezpečnost je přehlíženou nicméně velice důležitou součástí každé společnosti. Kybernetičtí zločinci neustále hledají cesty, jak se do síťové infrastruktury společnosti dostat a odcizit tajná a hodnotná data za účelem prodeje nebo poškození jména společnosti. Tato práce shrnuje aktuální bezpečnostní rizika a typy útoků. Výsledkem práce jsou organizační, procesní a technologická doporučení vycházející z dostupných technologií a metod již využívaných po celém světě. Bakalářská práce se zaměřuje na identifikaci jednotlivých kybernetických hrozeb v dnešním světě, kategorizaci podnikatelských subjektů v společnosti a navázaní hrozeb na dané kategorie. Dále popisuje zákonné povinnosti pro společnosti dle učených kategorií a popisu případy kybernetických událostí v roce 2021. V praktické části se bakalářská práce věnuje úpravě a doporučení pro spolupracující společnost v oblasti kybernetické bezpečnosti pomocí SWOT analýzy a dotazníku určeném pro standardní zaměstnance společnosti a IT oddělení starající se o kybernetickou bezpečnost. V závěru jsou vydána a implementována doporučení na základě výsledku dotazníku ve spolupráci se zkoumanou společností.

Klíčová slova

IT bezpečnost, kybernetika, phishing, ransomware, útok, virus, ISO2700, business, heslo, kyberbezpečnost

ABSTRACT

Cyber security is a neglected but very important part of every society. Cybercriminals are constantly looking for ways to get into a company's network infrastructure and steal secret and valuable data to sell or damage the company's name. This work summarizes the current security risks and types of attacks. The result of the work is organizational, process, and technological recommendations based on available technologies and methods already used worldwide. This work summarizes the current security risks and types of attacks. The result of the work is organizational, process and technological recommendations based on available technologies and methods already used worldwide. The bachelor thesis focuses on the identification of individual cyber threats in today's world, the categorization of business entities in society and the linking of threats to the given categories. It also describes the legal obligations for companies according to learned categories and a description of cases of cyber events in 2021. In the practical part of the bachelor thesis deals with adjustments and recommendations for cooperating companies in cyber security using SWOT analysis and questionnaire on cyber security. In the end, recommendations are issued and implemented based on the results of the questionnaire in cooperation with the surveyed company.

Keywords

IT Security, Phishing, Cyberspace, Attack, Ransomware, Virus, ISO2700, Business, password, cybersecurity

Obsah

1 ÚVOD

Notebooky, mobilní telefony, tablety, chytré hodinky a další zařízení, které nám nabízí dnešní doba a bez kterých si nedovedeme představit každodenní život. Veškerá z těchto zařízení jsou 24 hodin, 7 dní v týdnu připojeny k veřejnému internetu, kde na uživatele číhá nespočet nebezpečí. Tím se vlastník těchto zařízení stává potencionálním rizikem jak pro sebe, tak i pro své okolí včetně místa výkonu zaměstnání. Ve valné většině případů se právě zaměstnanec stává zdrojem nevítaných bezpečnostních incidentů ve společnostech po celém světě.

Tato práce se zabývá soupisem návrhů a doporučení s cílem zvýšit úroveň kybernetické bezpečnosti v českým podnikatelských subjektech. Téma jsem si vybral z důvodu tristního přístupu ke kybernetické bezpečnosti v mnoha českých společnostech. Společnosti se buď příliš zaměřují na obchodní stránku věci nebo se obávají výdajů, které se zdokonalováním úrovně kybernetické bezpečnosti přímo souvisí. Nicméně myšlenka ztráty důvěry ze strany široké veřejnosti nebo ztráta dosavadních dat či finančních prostředků je už příliš netíží.

Ve své práci poukážu na kategorie společností, ke kterým se vztahuje právní úprava a subjekty jsou povinni je dodržovat. Zároveň popíšu metody, které jsou svým charakterem natolik levné, že je může nasadit jakákoli společnost bez nutnosti velkých výdajů.

Cílem práce je ukázat českým podnikatelským subjektům, že kybernetická bezpečnost není problémem. Pomocí jednoduchých mechanismů nasazení politik, pravidel nebo výběru správného řešení se dá docílit silnému automatizovanému štítu, který společnost ochrání proti nevítaným návštěvníkům z internetu.

2 CÍLE PRÁCE

Cílem bakalářské práce je analýza jednotlivých bezpečnostních hrozeb a popis jejich funkce s následnou kategorizací podniků. Bakalářská práce také popíše aktuální metody pro zabezpečení podnikové infrastruktury. Výsledkem bude vytvoření souboru organizačních, procesních a technologických doporučení na základě SWOT analýzy a strukturovaného dotazníku mající za cíl zvýšení úrovně kybernetické bezpečnosti u českých podnikatelských subjektů.

3 PŘEHLED SOUČASNÉHO STAVU

21. století z pohledu technologie je ve znamení internetu. Už od předškolního věku se děti setkávají s nástrahami, které internet skrývá. To se s nimi vleče až do produkčního věku, kde tyto hrozby mají dopad na víc než jen na danou osobu. V této kapitole shrnu nejčastější hrozby skryté v aplikacích používaných každý den snad ve všech odvětvích profesního i soukromého života.

3.1 Přehled aktuálních hrozeb

3.1.1 Phishing

Slovo phishing vychází z anglického slova pro lov ryb neboli fishing. Útočník (lovec) nahodí háček s návnadou například v podobě neodolatelné nabídky a čeká na oběť. Záměna písmena f za ph má původu ze slova „phreaks“, což byla hackerská skupina v USA, která ilegálně experimentovala s telekomunikačními systémy v devadesátých letech [1].

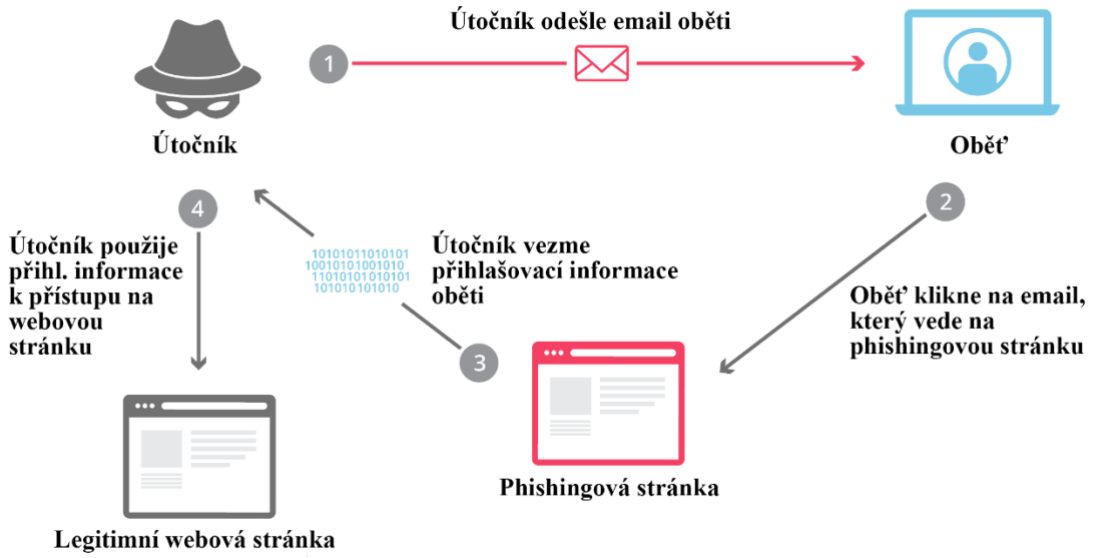
Phishingový útok se vyznačuje tím, že útočník vyhledá a převezme identitu (zpravidla e-mailovou adresu) známého a důvěryhodného člověka (zpravidla vysoce postaveného v hierarchii firmy nebo člena rodiny). Útoky mohou usnadnit přístup k online účtům a osobním údajům, získat oprávnění k úpravám a kompromitaci připojených systémů – jako jsou terminály v místě prodeje a systémy na zpracování objednávek – a v některých případech napadnout celé počítačové sítě.

Někdy se hackeři spokojí se získáním osobních údajů či údajů o zákaznicích za účelem finančního zisku. V jiných případech se zasílají phishingové e-maily, aby shromáždily přihlašovací údaje zaměstnanců nebo jiné informace pro použití při zákeřnějších útocích proti několika jednotlivcům nebo konkrétní společnosti [1].

Dnes rozeznáváme několik druhů phishingových útoků:

- **„Spear“ phishing** je nejčastějším typem phishingu. Zaměřuje se na jednotlivce. Útočníci si mohou přizpůsobit komunikaci, tak aby byla co nejdůvěryhodněji. „Spear“ phishing je často prvním krokem k proniknutí do obrany společnosti a provedení cíleného útoku.

- **Microsoft 365 phishing** je cílenější metodou. Zaměřuje se na e-mailové schránky uživatelů cloudového řešení od společnosti Microsoft. Mají obvykle podobu falešného e-mailu od podpory společnosti Microsoft. E-mail obsahuje žádost o přihlášení, v ní se uvádí, že uživatel potřebuje obnovit heslo, v poslední době se nepřihlásil nebo že je problém s účtem, který vyžaduje jeho pozornost. Je zahrnuta URL adresa, která uživatele láka ke kliknutí, aby problém napravil.
- **BEC (Business Email Compromise)** je metoda podobná Microsoft 365 phishingu. Útok je pečlivě připraven na základě dlouhodobějšího zkoumání cílové společnosti – hierarchie, zaměstnanci, týmy, dodavatelé apod. s cílem nalézt co nejlepší možnou identitu pro útok.
- **Whaling** neboli „útok na velkou rybu“ cílí na nejvyšší představitele cílové společnosti jako je generální ředitel. Tito útočníci často tráví značný čas profilováním cíle, aby našli vhodnou chvíli a prostředky ke krádeži přihlašovacích údajů. Tento útok je svým charakterem velice nebezpečný, jelikož lidé na vysokých pozicích mají často přístup k mnoha citlivým firemním informacím a prostředkům.
- **Social Media Phish** je díky dostupnosti sociálních sítí poměrně jednoduchý a velice častý. Tento typ necílí na specifického uživatele – jeho úkolem je rozšířit se mezi co možná nejvíce uživatelů a odcizit jakékoli osobní údaje. Balíky těchto informací jsou pak prodávány.
- **Voice phishing** neboli vishing je formou sociálního inženýrství. Jde o podvodný telefonát určený k získání citlivých informací, jako jsou přihlašovací údaje. Útočník může volat a vydávat se za pracovníka podpory nebo zástupce společnosti [1].

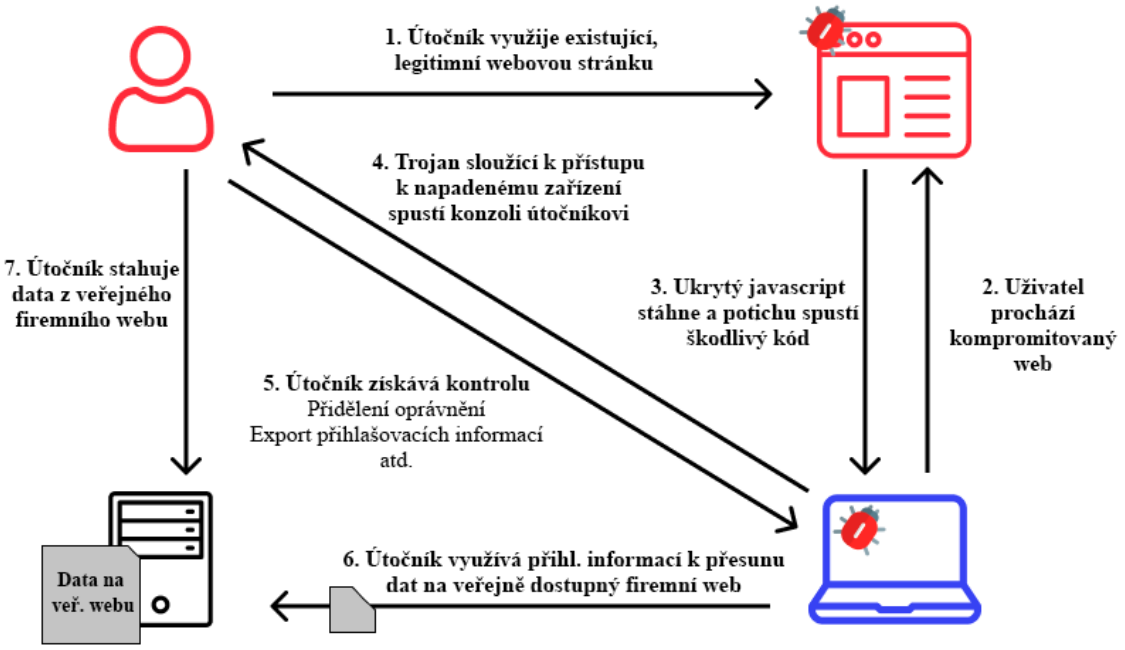


Obrázek 1 - Průběh phishingového útoku (https://www.wallarm.com/what/types-of-phishing-attacks-and-business-impact)

3.1.2 Drive-by útoky

Drive-by útok je zjednodušeně nedobrovolné stažení škodlivého kódu při procházení webovými stránkami. Kyberzločinci následně mohou napadené zařízení číst – tedy stahovat osobní údaje, sledovat práci oběti na daném zařízení nebo dokonce infikovat celou síť.

K drive-by útokům může dojít několika způsoby. Pouhá návštěva upraveného webu může stačit ke stažení části HTML nebo JavaScript kódu ukrytého na stránce. Uživatel často nemusí vyvolat žádnou přímou akci, aby vyvolal jeho stažení. V jiných scénářích může být kliknutí na reklamu umístěnou na zdánlivě bezpečném webu nebo stažení si nějaké přílohy. Po kliknutí na tento odkaz se vám sice podaří stáhnout chtěnou aplikaci nebo se dostat na stánku recenzenta, nicméně se do zařízení dostane i tento nechtěný kód [2].



Obrázek 2 - Popis drive-by útoku (https://www.wallarm.com/what/drive-by-attack)

3.1.3 Ransomware

Ransomware je neustále se vyvíjecí forma malwaru navržená k šifrování souborů v zařízení, čímž se jakékoli soubory a systémy, které na ně spoléhají, stávají nepoužitelnými. Útočníci následně vyzvou oběť k zaplacení nemalé částky výměnou za dešifrování. V případě nesplnění požadavku hrozí prodejem nebo únikem zašifrovaných informací. V posledních letech jsou incidenty ransomwaru stále více rozšířené mezi soukromými a vládními subjekty a organizacemi kritické infrastruktury.

Existuje celá řada způsobů, jak dostat ransomware do zařízení. Nejčastější metoda je bezesporu phishingový útok. Často se ukrývají v e-mailových přílohách a jsou navrhnuty tak, aby se tvářili co nejdůvěryhodněji. Jednodušší aplikaci obsahující ransomware vyzvou uživatele k zadání administrátorských údajů. Ty agresivnější využívají bezpečnostních děr v systému nebo přidružených aplikacích a mohou běžet bez vědomí uživatele. Vzhledem k charakteru útoku se oběť může rozloučit se svými zašifrovanými soubory, protože k dešifrování je zapotřebí znát matematický klíč, který je velice složité rozluštit a zná je pouze vývojář – tedy útočník daného ransomwaru [3].

3.1.4 Malware

Zkratka pro „škodlivý software“, označuje jakýkoli rušivý software vyvinutý kyberzločinci za účelem krádeže dat, poškození nebo zničení počítačových systémů. Příklady běžného malwaru zahrnují viry, červy, trojské koně, spyware, adware a ransomware [4].

3.1.5 Trojský kůň

Trojský kůň je z historie známý jako dřevěná socha, kterou dal Odysseus trojskému králi Priamovi jako znamení ukončení 10leté války o turecké město Troja. Tento nevinný dar v sobě však ukrýval řecké vojáky, kterým se díky soše podařilo dostat za hradby a Troju dobýt. Stejně tak z pohledu IT bezpečnosti je tento program určený k zmatení uživatele. Aplikace tvářící se jako chtěná však ukrývá škodlivý kód s cílem poškodit nebo dokonce zničit cílové zařízení nebo celou počítačovou síť [5].

Někdy je trojský kůň nesprávně nazýván jako trojský virus. Na rozdíl od klasických virů se trojský kůň nemůže replikovat přes další soubory či aplikace v počítači.

Rozlišujeme několik typů trojských koní:

- **Backdoor Trojan** není nějak nebezpečný po jeho prvním spuštění. Dnešní antimalware a antivirové programy dokážou zpozorovat jeho přítomnost a překazit spuštění kódu. Nicméně pokud je systém, na kterém běží zranitelný, vytvoří pro útočníka „zadní vrátka“ přes které je útočník schopen se kdykoli připojit a spouštět další škodlivé programy, popř. mít přístup k datům.
- **Trojan ukrývající DDoS útok** je především typem, který útočníci používají pro zakrytí své vlastní identity či lokality. Na cílový počítač se schová program – nejčastěji do jednoho ze systémových procesů – a díky přístupu k internetu posílá dotazy na jiné zařízení s cílem přetížit jej. V podstatě se jedná o posílení jiného útoku s úplně jiným cílem.
- **Trojan tvářící se jako AntiVirus** je velice známou a dnes už méně používanou metodou. Ve valné většině případů se tento Trojan tváří, že nalezl na zařízení škodlivý software, který je třeba zneškodnit. Nicméně uživatel je vyzván, aby zaplatil za tuto nápravu. Samozřejmě je vše připravené tak,

že hlášku o nalezeném škodlivém softwaru dostane i naprosto zabezpečené zařízení. V poslední době jej můžeme zpozorovat hlavně v mobilních prohlížečích ve formě adwaru.

- **Trojan – zloděj her** je metodou cílící na nesportovní smýšlení hráčů online her. Ve chvíli, kdy hráče přestane nějaká hra bavit nebo v ní není příliš dobrý, hledá, jak by se hře nebo hráčům mohl pomstít. Většina takto smýšlejících uživatelů zvolí stažení softwaru, který jim umožní být zvýhodněn v dané hře nad svými protivníky. Nicméně software toho typu v sobě obsahuje kód, který vykrade uživateli přihlašovací údaje k dané platformě a útočník si pak tento účet přivlastní [5].

3.1.6 Man-in-the-middle

Tento útok využívá komunikace mezi dvěma subjekty – obětí a nic netuším prostředníkem. Útok vyžaduje po útočníkovi znalost prostředí, oběti a způsob komunikace s prostředníkem. Jedná se o velice propracovaný typ útoku, kde si útočník zvolí oběť, o které ví například v jaké bance má tato osoba svůj účet. Útočník si připraví phishingový e-mail, který se tváří velice podobně jako oznámení z dané banky. Vytvoří si jednoduchou webovou stránku a zkopíruje podobu pravého webu. Ve chvíli, kdy uživatel klikne na odkaz ve phishingovém e-mailu se dostane na webovou stránku vzhledově stejnou jako banka u které má založený svůj účet. Následně zadá přístupové údaje a problém je na světě. Uživatel právě předal své údaje útočníkovi.

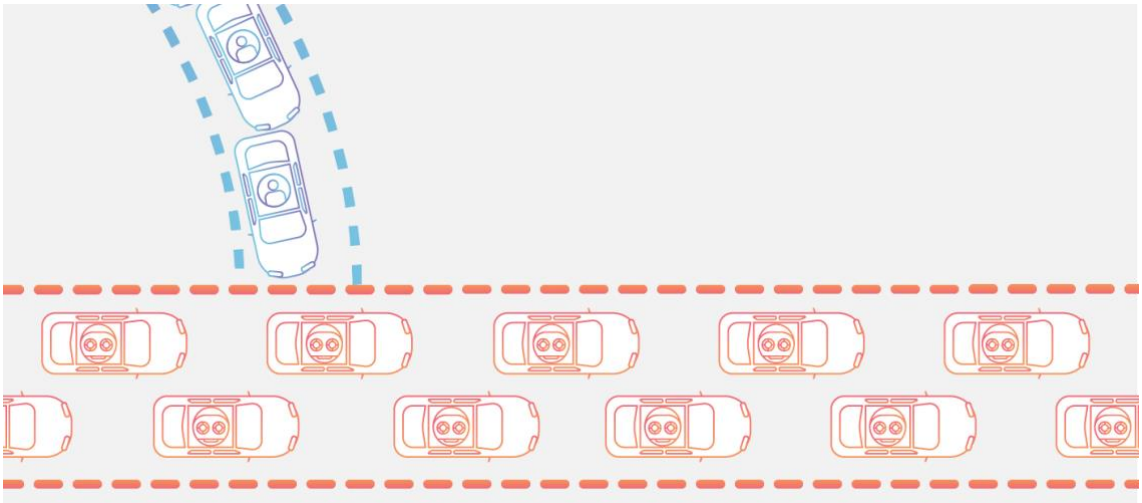
V současnosti je tento typ útoku velice ztížen existencí dvou-faktorových ověření u masivní většiny oficiálních webových stránek. Díky tomuto mechanismu jsou útočníkovi obyčejné přihlašovací informace k ničemu [6].

3.1.7 DDoS

Distribuovaný útok typu denial-of-service (DDoS) je zákeřný pokus narušit normální provoz cíleného serveru, služby nebo sítě zahlcením cíle nebo jeho okolní infrastruktury záplavou internetového provozu.

Útoky DDoS dosahují účinnosti tím, že jako zdroje útočného provozu využívají více kompromitovaných počítačových systémů. Využívané stroje mohou zahrnovat počítače a další síťové zdroje, jako jsou zařízení IoT (Internet Věcí) [7].

Pro zjednodušení můžeme útok DDoS vysvětlit pomocí metafory jako neočekávanou dopravní zácpu ucpávající dálnici, která brání pravidelné dopravě dorazit do cíle.



Obrázek 3 - DDoS Metafora (https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/)

DDoS útoky se provádějí pomocí sítí počítačů připojených k internetu. Tyto sítě se skládají z počítačů a dalších zařízení (jako jsou zařízení IoT), které byli infikovány malwarem, což umožňuje jejich vzdálené ovládání útočníkem. Tato jednotlivá zařízení se označují jako „boti“ (nebo zombie) a skupina botů se nazývá botnet.

Po vytvoření botnetu je útočník schopen řídit útok zasláním vzdálených pokynů každému botovi. Když se botnet zaměří na server nebo síť oběti, každý bot odešle požadavky na IP adresu cíle, což může způsobit zahlcení serveru nebo sítě, což má za následek odmítnutí služby běžnému provozu.

Vzhledem k tomu, že každý robot je legitimním internetovým zařízením, může být obtížné oddělit útočný provoz od běžného provozu [7].

3.1.8 DNS Tunneling

Jednoduše řečeno, DNS je telefonní seznam internetu. Při procházení internetu většina uživatelů dává přednost zadání domény nebo adresy URL webové stránky, kterou chtějí navštívit (např. https://www.checkpoint.com). Internetové servery a infrastruktura však používají IP adresy k identifikaci cíle provozu a směrování tam [17].

DNS poskytuje převody mezi názvy domén a IP adresami. Je organizován jako hierarchický systém se servery pro různé subdomény. Návštěvník webu checkpoint.com

by požádal server DNS .com o IP adresu serveru DNS checkpoint.com. Druhý požadavek na tento DNS server by pak poskytl IP adresu serveru hostujícího požadovanou webovou stránku. Uživatel nyní může navštívit požadovanou stránku [17].

DNS je jedním ze základních protokolů internetu. Bez vyhledávacích služeb, které poskytuje, by bylo téměř nemožné na internetu cokoliv najít. Pokud bychom chtěli navštívit webovou stránku, museli bychom znát přesnou IP adresu serveru, který ji hostí, což je nemožné. V důsledku toho je provoz DNS jedním z nejdůvěryhodnějších provozů na internetu. Organizace umožňují průchod přes jejich firewall (příchozí i odchozí), protože je nutné, aby jejich interní zaměstnanci navštěvovali externí stránky a externí uživatelé našli jejich webové stránky [8].

Tunelování DNS využívá této skutečnosti pomocí požadavků DNS k implementaci příkazového a řídicího kanálu pro malware. Příchozí DNS provoz může přenášet příkazy do malwaru, zatímco odchozí provoz může odesílat citlivá data nebo poskytovat odpovědi na požadavky provozovatele malwaru. Funguje to proto, že DNS je velmi flexibilní protokol. Existuje velmi málo omezení na data, která požadavek DNS obsahuje, protože je navržen tak, aby vyhledával názvy domén webových stránek. Vzhledem k tomu, že názvem domény může být téměř cokoliv, lze tato pole použít k přenosu citlivých informací. Tyto požadavky jsou navrženy tak, aby směřovaly na servery DNS ovládané útočníky, čímž je zajištěno, že mohou přijímat požadavky a odpovídat v odpovídajících odpovědích DNS [8].

Útoky tunelování DNS se snadno provádějí a existují četné sady nástrojů pro tunelování DNS. To umožňuje i nenáročným útočníkům použít tuto techniku k propašování dat přes řešení zabezpečení sítě organizace.

3.1.9 Brute Force

Útok Brute Force, také známý jako vyčerpávající vyhledávání, je kryptografický hack, který spoléhá na hádání možných kombinací cíleného hesla, dokud není nalezeno správné heslo. Čím delší heslo, tím více kombinací bude potřeba otestovat. Útok Brute Force může být časově náročný, obtížně proveditelný a někdy dokonce nemožný. Pokud je však heslo slabé, může to trvat jen několik sekund bez vynaložení velkého úsilí. Slabá hesla jsou pro útočníky jako střílení ryb v sudu, a proto by všechny organizace měly prosazovat politiku silných hesel napříč všemi uživateli a systémy [9].

Útoky Brute Force se obvykle používají k získání osobních informací, jako jsou hesla, přístupové fráze, uživatelská jména a osobní identifikační čísla (PIN), a používají skript, hackerskou aplikaci nebo podobný proces k provádění řady nepřetržitých pokusů získat požadované informace [9].

Mezi cíle útoku Brute Force patří:

- Krádež osobních údajů, jako jsou hesla, přístupové fráze a další informace používané pro přístup k online účtům a síťovým zdrojům.
- Sběr přihlašovacích údajů k prodeji třetím stranám.
- Vystupování jako uživatelé za účelem odesílání phishingových odkazů nebo šíření falešného obsahu.
- Znehodnocování webových stránek a dalších informací ve veřejné doméně, které by mohly poškodit pověst organizace.
- Přesměrování domén na stránky obsahující škodlivý obsah.
- Mohou být také použity pro pozitivní zisky. Mnoho IT specialistů používá tuto metodu útoku k testování zabezpečení sítě a konkrétněji síly šifrování používaného v síti [9].

3.1.10 SQL Injection

Structured Query Language (SQL) Injection je technika vkládání kódu používaná k úpravě nebo načítání dat z databází SQL. Vložením specializovaných SQL příkazů do příkazového řádku je útočník schopen provádět příkazy, které umožňují získání dat z databáze, zničení citlivých dat nebo jiné manipulativní chování.

Při správném provedení příkazu SQL je neoprávněný uživatel schopen podvrhnout identitu privilegovanějšího uživatele, učinit ze sebe nebo z jiných správce databáze, manipulovat se stávajícími daty, upravovat transakce a zůstatky a získávat anebo zničit všechna data serveru. V moderní výpočetní technice k SQL Injection obvykle dochází přes internet odesláním škodlivých SQL dotazů do koncového bodu API poskytovaného webem nebo službou. Ve své nejzávažnější formě může SQL Injection umožnit útočníkovi získat administrátorský přístup k počítači a poskytnout mu úplnou kontrolu [10].

3.2 Kategorizace podnikatelských subjektů

Donedávna byly hlavním cílem kybernetických útoků hlavně finanční firmy a vlády. Nicméně potřeba využití IT technologií roste, tak i ostatní společnosti se přidávají do světa internetu a stávají se potencionálním cílem útoku. Jen 16 % vedoucích pracovníků tvrdí, že jejich společnosti jsou dobře připraveny se vypořádat s kybernetickým útokem. Ve většině průmyslových odvětví se přechází na nové technologie, jako například umělá inteligence, pokročilá analytika, internet věcí (IoT), které přinesou několik výhod, ale také vystaví společnost a její zákazníky novým druhům kybernetického rizika.

V nynější době můžeme rozdělit podnikatelské subjekty do několika kategorií z hlediska použití IT technologií – tedy i odhadnout potencionální riziko.

Tabulka 1 - Kategorie podnikatelských subjektů [18]

	Název kategorie	Zkrácené označení
Kategorie I	Subjekty používající IT pro práci s dokumenty, účetnictví a archivování	Běžné užití IT
Kategorie II	Subjekty uchovávající informace o zákaznicích	Údaje o zákaznících
Kategorie III	Subjekty používající průmyslové řídicí systémy	ICS / SCADA
Kategorie IV	Poskytovatelé online obsahu a služeb	Online portály
Kategorie V	Subjekty chránící si know-how	Chráněné know-how

3.2.1 Subjekty používající IT pro práci s dokumenty, účetnictví, archivování

Do této kategorie spadá většina podnikatelských subjektů využívající IT technologii pro usnadnění podnikání nebo potřeby plnit povinné evidence. Potřeba využití IT vyplívá ze zákona o uchovávání dokumentů, potřeba využívat komunikační služby, plánování služeb, archivace dat a faktur, správa jednoduchého účetnictví apod. Počítáme zde například s manufakturami, řemeslníky, maloobchodníky, subjekty poskytující služby.

Tyto subjekty nejsou hlavním zájmovým cílem pro útočníky. Nicméně v důsledku nesprávného a neopatrného používání internetu se cílem stát mohou. A to nechtěným stažením škodlivého softwaru a následnému automatickému odeslání dat z koncového zařízení útočníkovi.

Největším rizikem pro tyto subjekty jsou sami kmenový zaměstnanci. Z pohledu aktuálních hrozeb to jsou Adware, Phishing, Malware a Ransomware [18].

3.2.2 Uchovávající údaje o zákaznících

Do druhé kategorie spadají subjekty užívající IT pro zpracovávající osobních údajů ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů:

„a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu"(https://www.zakonyprolidi.cz/cs/2000-101).

Podnikatelský subjekt uchovávající osobní údaje o zákaznících, případně o vlastních zaměstnancích, je ohrožen už o něco více než malé subjekty. Když pomineme riziko vycházející z pochybení zaměstnance, zůstane tu útok typu SQL Injection, Brute Force a Man-in-the-middle. Samozřejmě společnosti této kategorie jsou náchylnější na propracovanější útoky typu Phishing nebo ostatními útoky využívající e-mailovou komunikaci [18].

3.2.3 Subjekty používající průmyslové řídicí systémy (typu ICS/SCADA)

ICS (Industrial Control System) je zkratka obecně pro všechny průmyslové řídicí systémy. Pod tuto obecnou kategorii můžeme zařadit prvky „SCADA" (viz dále), distribuované kontrolní systémy, programované logické obvody a jiné prvky používané převážně ve výrobě a infrastruktuře.

Při hledání příkladů kybernetických útoků z praxe se ukázalo, že často používaným pojmem zejména v zahraničních zdrojích je právě „SCADA". Je to zkratka pro „Supervisory Control And Data Acquisition", což může být volně přeloženo jako „dozorčí řízení a sběr dat". Prakticky se jedná o to, že například průmyslová výroba nebo distribuce je řízena jednotlivými technickými prvky a člověk provádí jenom dohled (často vzdálený) nebo případnou změnu nastavení [18].

Využití tyto řídící prvky naleznou zejména v následujících oblastech:

- procesy ve strojní výrobě, procesní výrobě
- procesy v energetice nebo distribuci plynu, tepla, ropy, elektřiny
- vodní hospodářství (čističky, zásobárny, distribuce vody)
- procesy v dopravě (řízení semaforů a jiné dopravní signalizace, větrání v tunelech)

Využití řídících prvků tohoto typu ve velkém a čím dál větší automatizace je spojována s pojmem „Průmysl 4.0“ nebo čtvrtou průmyslovou revolucí. Průmysl 4.0 je označení pro nadcházející inovace a proměny výrobních procesů. Internet a digitalizace umožňují kompletní propojení a automatizaci veškerých výrobních procesů a také služeb s nimi spojených [18].

Speciálně subjekty spadající do kategorie kritické infrastruktury jsou dostatečně velkým cílem pro velice sofistikované útoky, které hraničí s kybernetickou sabotáží.

3.2.4 Poskytovatelé online obsahu nebo služeb

Každým rokem přibývají služby, které lidem poskytují zábavu, ale také jsou nedílnou součástí pracovní náplně. Podstatou pro zařazení do této kategorie je, že nedostupnost jimi provozovaného internetového portálu způsobí zásadní finanční ztráty, jelikož na poskytování online obsahu nebo služeb jsou závislí [18].

Příkladem mohou být:

- e-mailové a cloudové služby (Google, Microsoft, Seznam apod.)
- poskytovatelé streamované hudby (Spotify, Apple Music apod.)
- poskytovatelé pracovních nástrojů (Adobe, SAP apod.)
- zpravodajské portály (Novinky.cz, Aktualne.cz, idnes.cz apod.)
- elektronické obchody (Alza.cz, eBay.com, Amazon.com apod.)
- zprostředkovatelé služeb (taxi, ubytování, úklid atd.)

Ve většině případů jsou útoky na tyto weby objednávány konkurencí těchto subjektů. Jedná se především o útok s cílem způsobit nedostupnost služeb nebo obsahu.

3.2.5 Subjekty chránící si know-how

Kategorie určená pro podnikatelské subjekty užívající IT pro uchovávání neveřejného duševního vlastnictví (know-how), zejména v oblastech:

- výzkumný nebo akademický sektor
- energetický, petrochemický nebo plynový průmysl
- telekomunikace
- zbrojní a obranný průmysl

Tyto subjekty jsou cílem moderních špionážních kampaní, vedených zpravidla ze zahraničí za účelem ekonomické špionáže [18].

3.2.6 Příklady zařazení typových podnikatelských subjektů

Tato kapitola má uvést vybrané příklady zařazení typových subjektů:

1. **Poskytovatelé streamované hudby:**

- KI – Běžné užití IT
- KII – Údaje o zákaznících
- KIV – Online portály

2. **Truhlářská společnost o deseti zaměstnancích:**

- KI – Běžné užití IT

3. **Výrobce jedinečné technologie**

- KI – Běžné užití IT
- KII – Údaje o zákaznicích
- KV – Know-how

4. **Poskytovatel služeb s věrnostními kartami**

- KI – Běžné užití IT
- KII – Údaje o zákaznících
- KIV – Online portály

5. **Bankovní instituce**

- KI – Běžné užití IT
- KII – Údaje o zákaznících
- KIV – Online portály
- KV – Know-how

3.3 Zákonné povinnosti a doporučená opatření

Účelem této kapitoly je popsat jednotlivé zákonné povinnosti ke specifikovaným kategoriím a následně popsat základní doporučení na základě charakteru užití IT v daném průmyslu. Doporučení budou vyplívat z obecných pravidel kybernetické bezpečnosti a mých vlastních zkušeností a jsou navrženy tak, aby každý uživatel mohl snížit pravděpodobnost útoku na minimum [18].

3.3.1 KI – Běžné užití IT

Z pohledu kybernetické bezpečnosti nevyplívá pro tuto kategorii žádná zákonná povinnost. V přeneseném významu však má subjekt povinnost chránit svá data proti zpronevěření či znehodnocení. V českém právním řádu je hned několik povinností ohledně archivace některých typů dokumentů a vedení účetnictví.

Aktuálně se svět nachází v mezidobý, kdy elektronické dokumenty podepsané elektronickým podpisem mají stejnou váhu jako dokumenty fyzické s manuálním a ověřeným podpisem. Příkladem je česká datová schránka a fyzická přítomnost na úřadě. Tato technologie umožňuje šetřit čas jak právním subjektům, tak i osobám, nicméně vzniká větší potřeba využívat právě IT z pohledu elektronických kartoték, databází, podpory elektronických podpisů apod.

Zároveň máme dnes mnoho účetních aplikací, které usnadňují práci v této nedílné součásti podnikání. Málokdy můžeme být svědky toho, jak účetní bere do ruky tužku a papír s cílem vyřešit účetnictví [18].

Podle § 7b zákona č. 586/1992 Sb., o daních z příjmů mají i menší podnikatelské objekty, neplátci DPH, povinnost archivovat daňovou evidenci vč. souvisejících dokladů tři roky po uplynutí roku, v němž podávali daňové přiznání k dani z příjmů [23].

Vzhledem k tomu, že zákon nezná termín „zničená evidence“ (ať už ztrátou fyzických dokumentů, tak i ztrátu virtuálních dat z důvodu selhání hardwaru nebo kybernetického útoku), tak ochrana před ztrátou těchto důležitých dat je jedním z důležitých témat při řešení podnikání.

Plátci DPH, mají povinnost podle § 35 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty ve znění:

(2) Daňové doklady se uchovávají po dobu 10 let od konce zdaňovacího období, ve kterém se plnění uskutečnilo (https://www.zakonyprolidi.cz/cs/2004-235#p35-2).

Podnikatelské subjekty vedoucí účetnictví mají i tyto povinnosti, vyplývající z § 31 zákona č. 563/1991 Sb., o účetnictví:

(2) Účetní záznamy se uschovávají

a) účetní závěrka a výroční zpráva po dobu 10 let počínajících koncem účetního období, kterého se týkají,

b) účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh, přehledy po dobu 5 let počínajících koncem účetního období, kterého se týkají,

c) účetní záznamy, kterými účetní jednotky dokládají vedení účetnictví (§ 33), po dobu 5 let počínajících koncem účetního období, kterého se týkají (https://www.zakonyprolidi.cz/cs/1991-563#p31-2).

S ohledem na aktuální kybernetické hrozby a jejich četnost na veřejném internetu bych doporučil nedávat kybernetickou bezpečnost i v malé společnosti na vedlejší kolej. Pro řešení kybernetické bezpečnosti není jenom povinnost stanovená zákonem archivovat data, ale i proto, že hrozba může zcela zničit výsledky práce a způsobit tím ztráty jak hmotného, tak i finančního charakteru [18].

Zákonem dané povinnosti:

- Podnikatelské subjekty mají povinnost uchovávat účetní dokumenty po dobu několika let. Zároveň je umožněno je uchovávat pouze v elektronické podobě, což usnadňuje logistiku. Povinnost dodržet určitou úroveň kybernetické bezpečnosti není zákonem upravena.

Mezi doporučená opatření je vhodné zařadit i obezřetnost v chování a způsobu používání IT vybavení. Uživatele je vhodné pravidelně školit, aby byli sami schopni odhalit nebo alespoň odhadnout podezřelý e-mail nebo podezřelou webovou stránku.

Doporučená opatření:

- Obezřetnost při otevírání e-mailů – speciálně od neznámých odesílatelů.
- Obezřetnost při stahování různých souborů z internetu.
- Zálohování dat na více než jednom médiu.
- Zálohování práce s využitím dostupných cloudových služeb.
- Záložní nosič by měl být připojen v počítači jen po dobu potřebnou pro zálohu nebo obnovu dat.
- Pravidelně aktualizovat aplikace a operační systém z důvodu přijetí nových bezpečnostních aplikací.
- Spravovat zařízení zaměstnanců centrálně a poskytovat jim užívání jen s omezenými oprávněními, např. s omezením instalací aplikací a spouštění jen předem schválených aplikací.

3.3.2 KII – Údaje o zákaznicích

Podnikatelské subjekty zpracovávající osobní údaje mají podle § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů tyto povinnosti:

> *„jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům (https://www.zakonyprolidi.cz/cs/2000-101).“*

V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření (podle odstavce výše) povinen také:

- *zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,*
- *zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,*
- *zabránit neoprávněnému přístupu k datovým nosičům (https://www.zakonyprolidi.cz/cs/2000-101).*

Zjednodušeně zákon vyžaduje, aby k citlivým datům tohoto charakteru měla přístup pouze osoba, která je k tomu oprávněná. To ovšem neznamená jen fyzický přístup, ale také přístup z pozice kybernetické bezpečnosti. O údaje o zákaznících je velice velký

zájem, zejména u konkurence s cílem tyto zákazníky přesvědčit pro změnu poskytovatele služby. Ukradená data se následně prodávají na „dark webu“ za různé částky. Hackeři získávají denně velké množství osobních dat, a dokonce i velmi citlivá data například ze zdravotních pojišťoven. Zákon bohužel neudává, jak mají být opatření zavedena. Nicméně v případě úniku dat nastane otázka, zda byla určitá kybernetická opatření provedena [18] [19].

Zákonem dané povinnosti:

Obecně:

- Povinnost chránit data před neoprávněným nebo nahodilým přístupům s cílem stáhnout osobní data, změnit je, zničit je, popř. šířit.

Automatizované zpracování:

- Zajištění přístupu k automatizačním systémům zpracování osobních údajů pouze oprávněným osobám.
- Zajištění osobám oprávněným k přístupu k automatizačním systémům zpracování osobních údajů v minimální míře pro zabezpečení jejich pracovní náplně.

Doporučená opatření:

- Omezit nebo úplně zamezit přístupu k databázím obsahující osobní údaje z internetu. V případě potřeby vzdálenému přístupu využít technologií VPN (Virtual Private Network) nebo IA (Identity Awerness) v rámci Firewallu.
- Využít velmi složitá hesla pro správu těchto databází.
- Pravidelná aktualizace softwaru, zejména instalovat bezpečnostní aktualizace.
- Provádět bezpečnostní a penetrační testování webů napojených na tyto databáze, zejména proti SQL Injection.

3.3.3 KIII – ICS / SCADA

Pokud subjekt provozuje průmyslové řídicí systémy (typu ICS/SCADA), je možné, že bude součástí kritické infrastruktury.

Kritickou informační infrastrukturou (dále KII) se rozumí prvek nebo systém prvků kritické infrastruktury (podle § 2, písm. g) a písm. i) zákona č. 240/2000 Sb.) v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti

(§ 2 písm. b) zákona č. 181/2014 Sb.). V praxi se jedná o takové informační nebo komunikační systémy, příp. ICS/SCADA systémy, které naplní kritéria pro určení prvků KII (GovCERT, 2014) [22] [24].

Některými z kritérií je, jestli narušením funkce budou překročeny mezní hodnoty (tzv. průřezová kritéria dle § 2 písm. l) zákona č. 240/2000 Sb., krizový zákon), které zahrnují rozsah ztrát na životech, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života. GovCERT (2014) na svých stránkách zveřejnil i pomocné schéma.

Určení daného prvku nebo systému prvků za KII nastává až po vzájemném projednání se zástupci Národního bezpečnostního úřadu (dále NBÚ), respektive jemu podřízeného Národního centra kybernetické bezpečnosti (dále NCKB). V takovém případě, že dojde k zařazení mezi prvky KII, podnikatelskému subjektu přibývá podle § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti několik povinností:

> *(2) … jsou povinny v rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření … a vést o nich bezpečnostní dokumentaci.*
>
> *(3) … povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro informační systém (https://www.zakonyprolidi.cz/cs/2014-181#cast1).*

A podle § 8 téhož zákona:

> *(1) … jsou povinny hlásit kybernetické bezpečnostní incidenty … a to bezodkladně po jejich detekci (https://www.zakonyprolidi.cz/cs/2014-181#cast1) …*

Bezpečností opatření, která musí být zavedena nebo prováděna v nezbytném rozsahu jsou organizační a technická, což dále upřesňuje § 5 tamtéž:

Organizačními opatřeními jsou:

- systém řízení bezpečnosti informací
- řízení rizik
- bezpečnostní politika
- organizační bezpečnost

- stanovení bezpečnostních požadavků pro dodavatele
- řízení aktiv
- bezpečnost lidských zdrojů
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému
- akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- řízení kontinuity činností a kontrola a audit kritické informační infrastruktury a významných informačních systémů.

Technickými opatřeními jsou:

- fyzická bezpečnost
- nástroj pro ochranu integrity komunikačních sítí
- nástroj pro ověřování identity uživatelů
- nástroj pro řízení přístupových oprávnění
- nástroj pro ochranu před škodlivým kódem
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- nástroj pro detekci kybernetických bezpečnostních událostí
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- aplikační bezpečnost
- kryptografické prostředky
- nástroj pro zajišťování úrovně dostupnosti informací
- bezpečnost průmyslových a řídicích systémů [18].

„Významné informační systémy“ veřejné správy jsou definovány také tímto zákonem.

Pokud tedy bude subjekt zahrnut do KII, legislativa mu přikazuje zavést a provádět bezpečnostní opatření organizačního tak technického charakteru, a navíc také hlásit NCKB kybernetické incidenty, které u subjektu nastanou.

Pokud subjekt v této kategorii není zahrnut mezi prvky KII, žádné povinnosti v kontextu kybernetické bezpečnosti se mi nepodařilo dohledat.

Zákonem dané povinnosti:

Pouze pro subjekty zařazené do kritické infrastruktury:

- V rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření a vést o nich bezpečnostní dokumentaci.

Doporučená opatření:

- Znepřístupnit vzdálenou správu ICS/SCADA prvků z internetu
- Pro správu ICS/SCADA prvků nastavit silná přístupová hesla
- Pravidelně aktualizovat veškerý SW, zejména instalovat bezpečnostní aktualizace [18]

3.3.4 KIV – Online portály

Poskytovatelé online služeb nebo obsahu nemají žádné zákonné povinnosti z pohledu minimální úrovně kybernetické bezpečnosti. Nicméně hrozba v podobě DDoS útoků nutí tyto subjekty kybernetickou bezpečnost řešit.

Ve specifickém případě lze uplatnit přenesená povinnost např. listovního tajemství nebo ochrany soukromí u poskytovatelů e-mailových služeb. U těchto online poskytovatelů nastává povinnost zabezpečit uživatelské účty a jejich e-mailové schránky tak, aby k nim měli přístup jen a pouze jejich vlastníci.

Obecně by měli být poskytovatelé online služeb natolik znalí, že kybernetická bezpečnost bude pro ně samozřejmostí. Pokud by to tak nebylo – na trhu by měli velký problém prorazit, popřípadě se udržet.

Infrastruktura poskytovatelů online služeb musí být dost silná, aby udržela denní návaly uživatelů. Velikáni, jakými jsou například Spotify, Youtube, Apple Music, Netflix apod. mají svá data centra zabezpečená několika různými mechanismy z pohledu bezpečnosti. Poměr mezi útoky a aktivními uživateli je přímá úměrnost. Tedy jmenované společnosti jsou každou vteřinou zkoušeny z pohledu kybernetických útoků. Pro menší

společnosti nebo start-upy je doporučeno využívat veřejných cloudových služeb – Microsoft Azure, Google Cloud nebo Amazon Web Services (AWS). Pokud si subjekt nemůže dovolit z finančních důvodů provoz ve veřejném cloudu – existují outsourcované bezpečnostní řešení. Společnost Cloudflare, zabývající se online bezpečnostními mechanismy, nabízí svou cloudovou DDoS ochranu. Jednoduše postaví DDoS zeď před „domácím“ rozhraním [18].

Doporučená opatření:

- Servery by měli být umístěné v datacentrech s více internetovými konektivitami.
- V případě vlastní infrastruktury zahrnout síťové prvky schopné reagovat na případné DDoS útoky
- Zvážit použití dostupných cloudových bezpečnostních služeb

3.3.5 KV – Chráněné know-how

Obecně know-how není chráněno ani českým zákonem, tak ani evropským. Nicméně know-how je možnost chránit jako obchodní tajemství podle zákona § 504 zákona č. 89/2012 Sb., občanský zákoník:

> *„Obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení (https://www.zakonyprolidi.cz/cs/2012-89#p504).“*

Druhou možností je zaregistrovat know-how jako patent u Úřadu průmyslového vlastnictví. V obou případech však nevyplívají žádné povinnosti pro zajištění kybernetické bezpečnosti [18].

Doporučená opatření:

- Šifrovat dokumenty, které mají kategorii know-how
- Uchovávat takové dokumenty na izolovaných zařízeních jak od běžné uživatelské sítě, tak i od internetu
- Pokud se objeví citlivá forma know-how v e-mailové komunikaci – vytvořit šifrovací mechanismus pro tyto e-maily.

- V dlouhodobém horizontu zavést ve společnosti kategorizaci dat ISMS podle normy ISO/IEC řady 2700

3.4 Případy skutečných incidentů

Tato kapitola se věnuje popisu a krátké analýze bezpečnostních incidentů, které se stali v roce 2021 poměrně velkým společnostem.

3.4.1 Spotify – útok na databázi uživatelů

V únoru roku 2021 se světový gigant ve streamování hudby potýkal s útokem s cílem získat informace o uživatelích a jejich přístupové údaje, pouze tři měsíce po posledním incidentu. Dle veřejně dostupných informací útok způsobil odcizení více než 100 000 uživatelských údajů a účtů – mezi nimi i spoustu českých účtů. Společnost Spotify byla donucena všem obětem, které přišli o své účty, obnovit heslo, což znehodnotilo odcizená data. Nicméně se ukázalo, že útok nenapadl přímo společnost Spotify, ale přístupové údaje byli získány z mnoha jiných zdrojů. Byla nalezena podvodná databáze, která obsahovala několik stovek tisíc různých účtů. Automatický script pak následně z této databáze zkouší přístupové údaje na jiných platformách než na té, ze které je získal [26].

Příkladem, pokud došlo k úspěšnému napadení účtu u portálu Alza.cz – tedy se skript nebo útočník úspěšně dostal přes autentizační část, je tento údaj uložen do databáze. V následujících dnech, týdnech či měsících se tyto přihlašovací údaje zkusí oproti jinému portálu – v tomto případě Spotify. Jelikož se tato aktivita většinou děje v jednu chvíli s mnoha účty – může to působit tak, že cílový subjekt nemá dostatečné zabezpečení a může to zákazníky donutit tuto platformu opustit [26].

V případě Spotify byla použita databáze, která obsahovala více než 300 milionů záznamů přihlašovacích informací. Ty následně byli v jednu chvíli použity proti Spotify.

Doporučení prevence této situace:

- Využít bezpečný způsob uchovávaní hesel, kde je potřeba si pamatovat jen hlavní heslo a následně si pro každý účet generovat heslo
- Nesdílet online účet s dalšími lidmi.

3.4.2 Microsoft Exchange Server – zero-day útok

2.3.2021 došlo k odhalení bezpečnostních děr u Microsoft Exchange serveru (nástroj pro stavbu e-mailového řešení v soukromých datacentrech společností). Útočník využil těchto děr k úplnému odcizení všech uživatelských e-mailových schránek na serveru bez potřeby ověření, bez přístupu k danému prostředí a zároveň bez speciálních znalostí [27].

Je odhadováno, že více než 250 000 serverů bylo napadeno touto mechanikou, včetně serverů patřícím více než 30 000 organizacím ve Spojených státech a 7 000 organizacím ve Velké Británii. Mezi obětmi jsou také například Evropská Bankovní Autorita, Norský parlament nebo Čilská komise pro finanční trh [27] [28].

3.4.3 Colonial Pipeline – Ransomware

V květnu roku 2021 ransomwarový útok zastavil rutinní provoz společnosti Colonial Pipeline, který přepravuje 45% paliva spotřebovaném na východní pobřeží USA, včetně nafty, benzínu a leteckého paliva. Za útokem údajně stála ruská ransomwarová zločinecká skupina DarkSide. Společnost Colonial Pipeline je největší plynovod pro rafinované produkty v USA (8 851 km), systém zapojený do přepravy více než 100 milionů galonů z texaského města Houston do přístavu New York Harbor [29] [30].

Darkside využívá model Ransomware-as-a-service (RaaS), kde se při provádění svých kybernetických útoků spoléhá na přidružený program. Colonial Pipeline zaplatil výkupné ve výši téměř 5 milionů amerických dolarů výměnou za dešifrovací klíč. Později FBI oznámila, že získala soukromý klíč účtu výkupného a získala zpět 63,7 zaplacených Bitcoinů [29] [30].

3.4.4 COVID-19 očkovací certifikát

V září roku 2021, začátek další vlny epidemie onemocnění COVID-19 a následné zavedení tzv. Covid Passu nabídla kybernetickým zločincům další možnost výdělku. Společnost Check Point monitorující dění na černých trzích rozšířených po Dark webu uvádí, že se začali prodávat falešné Covid Passy právě na těchto internetových tržnicích. Aktuálně jsou na trhu pravděpodobně všechny formy Covid Passu, které světové obyvatelstvo legálně získá po naočkování vakcínou [31].

Zpráva ze dne 23. září 2021 tvrdí, že na černém trhu jsou k sehnání Covid passy pro 29 zemí – mezi nimi i Česká republika a Polsko. 10. srpna 2021 CPR (Check Point Research) uvádí, že na aplikaci Telegram prodává tyto falešné certifikáty okolo 1000 kontaktů. O 14 dní později už bylo kontaktů dvakrát tolik. Poslední informace tvrdí, že v daných skupinách bylo více než 300 000 zájemců o falešný certifikát [31].

Certifikát se prodává v rozmezí 80–200 amerických dolarů na základě obtížnosti zadání do oficiálních systémů. Ty dražší využívali mechaniky, která umožňovala přidání daného zákazníka do systému. Mohla proběhnout díky tomu, že zločinci měli přístup do evropské databáze očkovaných lidí, resp. Evropského centra pro prevenci a kontrolu nemocí.

Levnější certifikáty obsahovali QR kód, který vedl na podobnou webovou stránku jako u originálního [31].

3.5 Aktuální metody pro zabezpečení podnikové infrastruktury

3.5.1 IAM – Identity Access Management

Správa identit a přístupu (IAM) je rámec obchodních procesů, politik a technologií, který usnadňuje správu elektronických nebo digitálních identit. Se zavedeným rámcem IAM mohou manažeři informačních technologií (IT) řídit přístup uživatelů ke kritickým informacím v rámci svých organizací. Mezi systémy používané pro IAM patří systémy jednotného přihlašování, dvoufaktorové ověřování, vícefaktorové ověřování a správa privilegovaného přístupu. Tyto technologie také poskytují schopnost bezpečně ukládat údaje o identitě a profilu a také funkce správy dat, aby bylo zajištěno, že budou sdílena pouze data, která jsou nezbytná a relevantní.

Systémy IAM lze nasadit v místní síti, poskytovat je dodavatel třetí strany prostřednictvím cloudového modelu nebo nasadit v hybridním modelu.

Na základní úrovni IAM zahrnuje následující komponenty:

- jak jsou jednotlivci v systému identifikováni (rozumějme rozdíl mezi správou identity a autentizací)
- jak jsou role v systému identifikovány a jak jsou přidělovány jednotlivcům
- přidávání, odebírání a aktualizace jednotlivců a jejich rolí v systému
- přidělování úrovní přístupu jednotlivcům nebo skupinám jednotlivců

Vedoucí představitelé podniků a IT oddělení jsou pod zvýšeným regulačním a organizačním tlakem, aby chránili přístup k podnikovým zdrojům. V důsledku toho se již nemohou při přidělování a sledování uživatelských oprávnění spoléhat na manuální procesy a procesy náchylné k chybám. IAM automatizuje tyto úkoly a umožňuje granulární řízení přístupu a auditování všech podnikových aktiv v prostorách a v cloudu.

IAM, který má stále se rozšiřující seznam funkcí – včetně biometrie, analýzy chování a umělé inteligence – se dobře hodí pro náročné podmínky nového bezpečnostního prostředí. Například přísná kontrola přístupu IAM ke zdrojům ve vysoce distribuovaných a dynamických prostředích je v souladu s přechodem odvětví od firewallů k modelům s nulovou důvěrou a s bezpečnostními požadavky IoT.

I když si IT profesionálové mohou myslet, že IAM je pro větší organizace s většími rozpočty, ve skutečnosti je tato technologie dostupná pro společnosti všech velikostí.

Nejdůležitějším principem při přípravě IAM je princip minimálního oprávnění. Princip minimálního oprávnění (POLP) je konceptem počítačové bezpečnosti, který omezuje přístupová práva uživatelů pouze na to, co je nezbytně nutné k výkonu jejich práce. Uživatelům je uděleno oprávnění číst, zapisovat nebo spouštět pouze soubory nebo prostředky nezbytné k provádění jejich úloh.

POLP může také omezit přístupová práva k aplikacím, systémům a procesům pouze na ty, kteří jsou oprávněni.

V závislosti na systému mohou být některá oprávnění založena na atributech závislých na roli uživatele v rámci organizace. Některé podnikové přístupové systémy například udělují odpovídající úroveň přístupu na základě faktorů, jako je umístění, seniorita nebo denní doba. Organizace může určit, kteří uživatelé mají k čemu v systému přístup, a systém lze nakonfigurovat tak, aby řízení přístupu rozpoznávalo pouze roli a parametry administrátorů.

Veškeré mechanismy vytváření oprávnění na základě rolí a principu POLP má za cíl vyvarovat se vytvoření tzv. „Super uživatele“. V případě velké kombinace oprávnění v jednom systému (např. vytvoření oprávnění role z několika různých již vytvořených rolí) může vzniknout role s oprávněním velice se přibližující účtu administrátora. Účet administrátora poskytuje zaměstnancům informačních technologií neomezená oprávnění, takže mají plné oprávnění ke čtení, zápisu a spouštění a mohou provádět změny v síti. To zahrnuje instalaci softwaru, úpravu nastavení a souborů a mazání dat a uživatelů. Účty

superuživatelů jsou přiděleny pouze nejdůvěryhodnějším jednotlivcům, obvykle správcům systému nebo podobným osobám. Účet administrátora je také známý jako účet správce a často se mu přiřazuje název root.

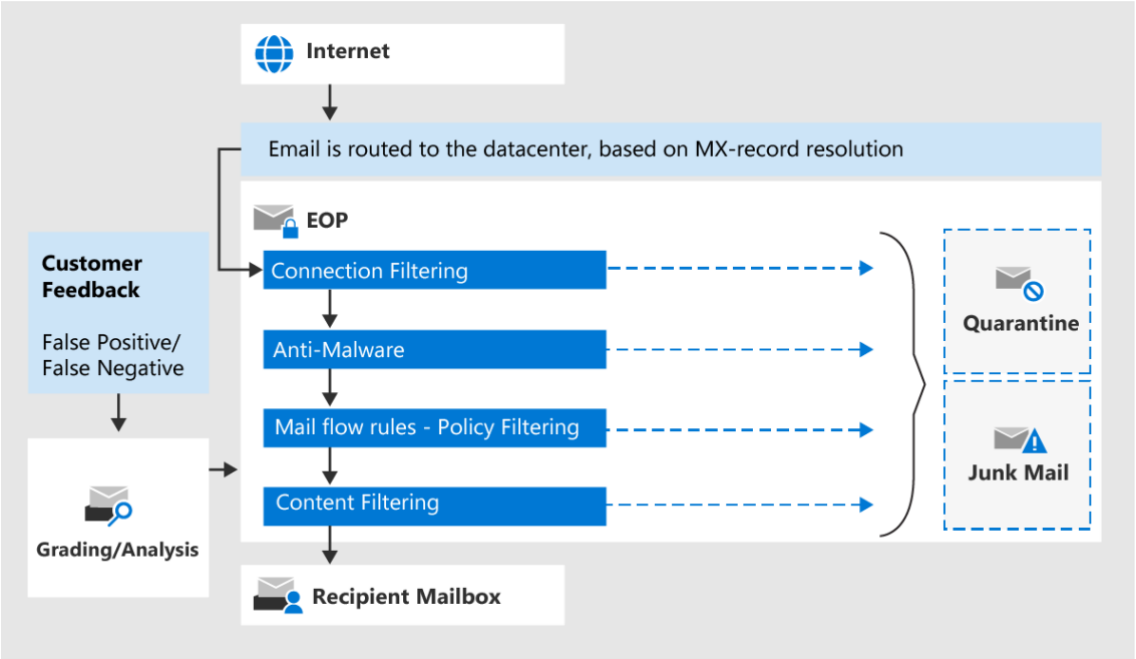
3.5.2 Mail-flow

Emailová komunikace je jedna z nejčastějších příčin napadení společnosti škodlivým softwarem. Stupeň nebezpečí se odvíjí od velikosti a důležitosti subjektu, což samozřejmě neznamená, že malá společnost nemůže být v nebezpečí. Dnešní poskytovatelé emailových řešení nabízejí mnoho systémů včetně bezpečnostních mechanismů (např. AntiSpam, Zero-Trust CDR, Vzdálená izolace, Spuštění v sandboxu apod.) pod různými formami poplatků – předplatných). Obecně se doporučuje postavit si tzv. Mail-flow co možná nejvíce automatizovaně a přísně, nicméně se společnosti dostávají do stavu, kdy vyžádaná pošta je vyhodnocena jako nebezpečná či nedůvěryhodná.

Návrh pro středně velkou společnost je postaven na jednoduchých mechanismech, které odfiltrují co nejvíce nevyžádané pošty, ale zachovají prostor pro přijímání bezpečných, ale nedůvěryhodných zdrojů, jakými jsou například osobní emailové schránky s doménami Google, Microsoft, Yahoo, iCloud, Seznam apod.

Prvním důležitým rozhodnutím je, zda vytvářet fyzické emailové řešení na síťové infrastruktuře společnosti (On-Premises) nebo přenechat a koupit hotové řešení v cloudu (SaaS – Software as a Service). Nicméně vzhledem k jednoduchosti používání a částečné odpovědnosti z pohledu bezpečnosti na straně dodavatele řešení je oblíbenou metodou právě cloudový SaaS – ve valné většině případů Exchange Online od společnosti Microsoft. Řešení už od své nejnižší formy předplatného nabízí poměrně slušnou ochranu, která by stála mnoho prostředků při vytvoření ve vlastním datacentru.

Exchange Online Protection pracuje s několika prvky ochrany pošty:



Obrázek 4 - Exchange Online Protection (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview)

Prvním krokem je kontrola důvěryhodnosti odesílatele porovnáním se známými podvodnými doménami a předchozími incidenty registrované v prostředí Microsoft. Ve chvíli, kdy se doména odesílatele nachází v těchto knihovnách – je na email hleděno jako podvodný a je zahozen. Následně pošta prochází skenovacím systémem na přítomnost škodlivého kódu přímo v těle emailu nebo v jeho přílohách. V případě nalezení neznámého kódu putuje zpráva do karantény, kde se správce rozhoduje, jak s tímto emailem naložit. Třetí mechanikou kontroly jsou pravidla vytvořená správci prostředí. Můžou mít charakter odmítnutí zprávy, přesměrování, popřípadě metoda doručení. Před samotným doručením zpráva prochází posledním mechanismem kontroly. Skenování obsahu zajistí zadržení zpráv označených jako spam, phishing, spoofing apod. Pokud zpráva vyjde jako negativní ve všech čtyřech krocích – je email doručen příjemci.

Tyto mechanismy mohou být nahrazeny nebo podpořeny řešeními třetích stran jako například Forcepoint. Je samozřejmé, že toto rozhodnutí přímo závisí na zkušenosti společnosti s IT bezpečností nebo její velikostí.

3.5.3 Kategorizace dat

Klasifikace dat v kontextu informační bezpečnosti je klasifikace dat na základě jejich úrovně citlivosti a dopadu na společnost, pokud by byla data zveřejněna, pozměněna nebo zničena neoprávněně. Klasifikace dat pomáhá určit, jaké základní bezpečnostní kontroly jsou vhodné pro ochranu těchto dat. Všechny institucionální údaje by měly být klasifikovány do jedné ze tří úrovní citlivosti nebo klasifikací:

- Vyhrazená data by měla být klasifikována jako Vyhrazená, pokud by neoprávněné zveřejnění, změna nebo zničení těchto dat mohlo způsobit značnou míru rizika pro společnost nebo její přidružené dceřiné společnosti. Příklady omezených dat zahrnují data chráněná státními nebo federálními předpisy na ochranu soukromí a data chráněná dohodami o důvěrnosti. Na omezená data by měla být aplikována nejvyšší úroveň bezpečnostních kontrol.
- Soukromá data by měla být klasifikována jako soukromá, pokud by neoprávněné zveřejnění, změna nebo zničení těchto dat mohlo vést k mírnému riziku pro společnost nebo její dceřiné společnosti. Ve výchozím nastavení by měla být všechna institucionální data, která nejsou výslovně klasifikována jako vyhrazená nebo veřejná data, považována za soukromá data. Na soukromá data by měla být uplatňována přiměřená úroveň bezpečnostních kontrol.
- Veřejná data by měla být klasifikována jako veřejná, pokud by neoprávněné zveřejnění, změna nebo zničení těchto dat mělo za následek malé nebo žádné riziko pro společnost a její dceřiné společnosti. Příklady veřejných dat zahrnují tiskové zprávy, informace o kurzech a výzkumné publikace. Zatímco k ochraně důvěrnosti veřejných údajů jsou vyžadovány malé nebo žádné kontroly, je vyžadována určitá úroveň kontroly, aby se zabránilo neoprávněné úpravě nebo zničení veřejných údajů.

Klasifikace dat by měla být provedena příslušným správcem dat. Správci dat jsou zaměstnanci společnosti na vyšších úrovních managementu, kteří dohlížejí na životní cyklus jedné nebo více sad institucionálních dat.

Bohužel neexistuje dokonalý kvantitativní systém pro výpočet klasifikace určitého datového prvku. V některých situacích může být příslušná klasifikace zjevnější,

například když zákony vyžadují, aby společnost chránila určité typy dat (např. osobní informace o zaměstnancích či zákaznících). Pokud příslušná klasifikace není ze své podstaty zřejmá, je třeba zvážit každý bezpečnostní cíl pomocí následující tabulky jako vodítka. Jde o výňatek z publikace Federal Information Processing Standards (FIPS) 199 vydané Národním institutem pro standardy a technologie, která pojednává o kategorizaci informací a informačních systémů.

	Potencionální dopad		
Bezpečnostní cíl	Nízký	Střední	Vysoký
Důvěrnost Zachování autorizovaných omezení přístupu k informacím a jejich zveřejňování, včetně prostředků na ochranu soukromí a chráněných informací.	Lze očekávat, že neoprávněné zveřejnění informací bude mít omezený nepříznivý dopad na organizační operace, organizační aktiva nebo jednotlivce.	Lze očekávat, že neoprávněné zveřejnění informací bude mít vážný dopad na organizační operace, majetek organizace nebo jednotlivce.	Lze očekávat, že neoprávněné zveřejnění informací bude mít vážný nebo katastrofální dopad na organizační operace, organizační aktiva nebo jednotlivce.
Integrita Ochrana před nevhodnou úpravou nebo zničením informací a zahrnuje zajištění nepopiratelnosti a pravosti informací.	Lze očekávat, že neoprávněná úprava nebo zničení informací bude mít omezený nepříznivý dopad na organizační operace, organizační aktiva nebo jednotlivce.	Dalo by se očekávat, že neoprávněná úprava nebo zničení informací bude mít vážný nepříznivý dopad na operace organizace, majetek organizace nebo jednotlivce.	Lze očekávat, že neoprávněná úprava nebo zničení informací bude mít vážný nebo katastrofální nepříznivý dopad na organizační operace, organizační aktiva nebo jednotlivce.
Dostupnost Zajištění včasného a spolehlivého přístupu k informacím a jejich použití.	Lze očekávat, že narušení přístupu k informacím nebo informačnímu systému nebo jejich používání bude mít omezený nepříznivý dopad na organizační operace, organizační	Lze očekávat, že narušení přístupu k informacím nebo informačnímu systému nebo jejich používání bude mít vážný nepříznivý dopad na operace organizace, majetek	Lze očekávat, že narušení přístupu k informacím nebo informačnímu systému nebo jejich používání bude mít vážný nebo katastrofální nepříznivý dopad na organizační operace, organizační

	majetek nebo jednotlivce.	organizace nebo jednotlivce.	majetek nebo jednotlivce.

Tabulka 2 - Bezpečnostní cíle a dopady

3.5.4 Vícefaktorové ověření

Vícefaktorová autentizace je metoda elektronické autentizace, při které je uživateli udělen přístup k webové stránce nebo aplikaci pouze po úspěšném předložení dvou nebo více částí faktorů autentizačnímu mechanismu: znalost (něco, co zná pouze uživatel), vlastnictví (něco pouze uživatel má) a inherence (něco, čím je pouze uživatel). vícefaktorová autentizace chrání uživatelská data – která mohou zahrnovat osobní identifikaci nebo finanční aktiva – před přístupem neoprávněné třetí strany, která mohla odhalit například jediné heslo.

Autentizační aplikace třetí strany umožňuje dvoufaktorové ověřování, obvykle zobrazením náhodně generovaného a často se měnícího kódu, který se má použít k ověření.

Ověřování probíhá, když se někdo pokusí přihlásit k počítačovému prostředku (jako je síť, zařízení nebo aplikace). Zdroj vyžaduje, aby uživatel dodal identitu, pomocí které je uživatel zdroji znám, spolu s důkazem o pravosti nároku uživatele na tuto identitu. Jednoduchá autentizace vyžaduje pouze jeden takový faktor, obvykle heslo. Pro další zabezpečení může zdroj vyžadovat více než jeden faktor – vícefaktorovou autentizaci nebo dvoufaktorovou autentizaci v případech, kdy mají být dodány právě dva faktory.

Použití více autentizačních faktorů k prokázání identity je založeno na předpokladu, že neoprávněný subjekt pravděpodobně nebude schopen poskytnout faktory potřebné pro přístup. Pokud při pokusu o autentizaci alespoň jedna z komponent chybí nebo je dodána nesprávně, identita uživatele není stanovena s dostatečnou jistotou a přístup k aktivu (např. aplikaci nebo datům) chráněnému vícefaktorovou autentizací, pak zůstává zablokován. Autentizační faktory vícefaktorového autentizačního schématu mohou zahrnovat:

- Něco, co má uživatel: Jakýkoli fyzický předmět v držení uživatele, jako je bezpečnostní token (USB klíčenka), bankovní karta, klíč atd.

- Něco, co uživatel zná: Určité znalosti, které zná pouze uživatel, jako je heslo, PIN atd.
- Něco, čím je uživatel: Některé fyzické vlastnosti uživatele (biometrie), jako je otisk prstu, oční duhovka, hlas, rychlost psaní, vzor v intervalech stisknutí kláves atd.
- Někde se uživatel nachází: Nějaké připojení ke konkrétní počítačové síti nebo pomocí signálu GPS k identifikaci polohy.

Dobrým příkladem dvoufaktorové autentizace je výběr peněz z bankomatu; pouze správná kombinace bankovní karty (něco, co uživatel vlastní) a PINu (něco, co uživatel zná), umožňuje provedení transakce. Dva další příklady jsou doplnění uživatelem řízeného hesla jednorázovým heslem (OTP) nebo kódem vygenerovaným nebo přijatým ověřovatelem (např. bezpečnostním tokenem nebo chytrým telefonem), které vlastní pouze uživatel.

Autentizační aplikace třetí strany umožňuje dvoufaktorovou autentizaci jiným způsobem, obvykle zobrazením náhodně generovaného a neustále se obnovujícího kódu, který může uživatel použít, místo aby posílal SMS nebo použil jinou metodu. Velkou výhodou těchto aplikací je, že obvykle nadále fungují i bez připojení k internetu. Příklady ověřovacích aplikací třetích stran zahrnují Google Authenticator, Authy a Microsoft Authenticator; někteří správci hesel, jako je LastPass, nabízejí tuto službu také.

3.5.5 Podmíněný přístup

Podmíněný přístup nebo systém podmíněného přístupu je ochrana obsahu vyžadováním splnění určitých kritérií před udělením přístupu k obsahu. Termín se běžně používá ve vztahu ke loudovým systémům a softwaru.

Podmíněný přístup je funkce, která vám umožňuje spravovat přístup lidí k příslušnému softwaru, jako je e-mail, aplikace, dokumenty a informace. Obvykle se nabízí jako SaaS (Software-as-a-Service) a nasazuje se v organizacích, aby byla firemní data v bezpečí. Nastavením podmínek pro přístup k těmto datům má organizace větší kontrolu nad tím, kdo a kde a jakým způsobem k informacím přistupuje.

Možné podmínky mohou být:

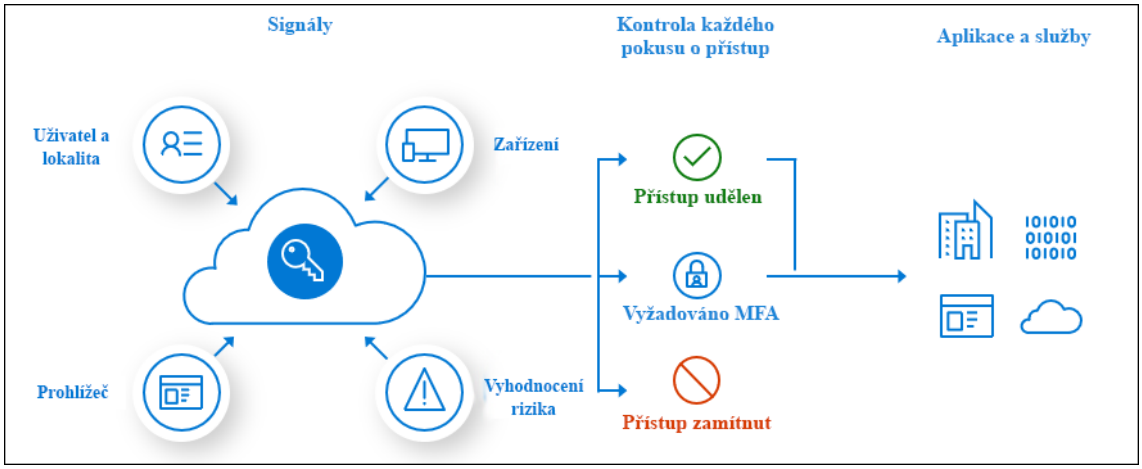
- Geografická poloha.

- IP adresa a síť.
- Použité zařízení.
- Prohlížeč.
- Operační systém (OS).

Při nastavování podmíněného přístupu lze omezit nebo zakázat přístup na zvolené podmínky. Tímto způsobem lze určit, že například přístup je možný pouze z určitých sítí nebo je z určitých prohlížečů zakázán.

Mezi současné poskytovatele podmíněného přístupu patří:

- Microsoft (včetně Office 365).
- Azure Active Directory.
- Workspace 365.



Obrázek 5 - Podmíněný přístup (https://docs.microsoft.com/cs-cz/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started)

4 METODIKA

4.1 SWOT analýza

SWOT analýza je technika strategického plánování a strategického řízení, která pomáhá osobě nebo organizaci identifikovat silné a slabé stránky, příležitosti a hrozby související s obchodní konkurencí nebo plánováním projektu. Někdy se tomu říká situační hodnocení nebo situační analýza.

Tato technika je určena pro použití v přípravných fázích rozhodovacích procesů a lze ji využít jako nástroj pro hodnocení strategické pozice organizací mnoha druhů (ziskové podniky, místní a národní vlády, nevládní organizace atd.). Je určen k identifikaci vnitřních a vnějších faktorů, které jsou příznivé a nepříznivé pro dosažení cílů podniku nebo projektu. Uživatelé SWOT analýzy často kladou otázky a odpovídají na ně, aby vytvořili smysluplné informace pro každou kategorii, aby byl nástroj užitečný a identifikovali svou konkurenční výhodu. SWOT byla popsána jako osvědčený nástroj strategické analýzy, ale byla také kritizována pro svá omezení a byly vyvinuty alternativy [33].

Název je zkratkou pro čtyři komponenty, které technika zkoumá:

- Silné stránky (Strengths): vlastnosti podniku nebo projektu, které mu dávají výhodu nad ostatními
- Slabé stránky (Weaknesses): vlastnosti, které znevýhodňují podnik nebo projekt ve srovnání s ostatními
- Příležitosti (Opportunities): prvky v prostředí, které by podnik nebo projekt mohl využít ve svůj prospěch
- Hrozby (Threats): prvky v prostředí, které by mohly způsobit potíže podniku nebo projektu [33]

Výsledky hodnocení jsou často prezentovány ve formě matice nebo jednoduše jako odstavce.

Silné a slabé stránky jsou obvykle považovány za interní, zatímco příležitosti a hrozby jsou obvykle považovány za externí. Míra, do jaké se vnitřní silné stránky firmy shodují s vnějšími příležitostmi, je vyjádřena konceptem strategické shody.

Interní faktory jsou považovány za silné nebo slabé stránky v závislosti na jejich vlivu na cíle organizace. To, co může představovat silné stránky s ohledem na jeden cíl, mohou být slabé stránky (rozptylování, konkurence) pro jiný cíl. Mezi faktory mohou patřit personál, finance, výrobní kapacity a všechna 4P marketingového mixu [33].

Mezi vnější faktory patří makroekonomie, technologické změny, legislativa a sociokulturní změny, stejně jako změny na trhu.

4.2 Dotazníkové šetření

4.2.1 Charakteristika výzkumného vzorku a způsob výběru

Realizované šetření výzkumu bakalářské práce probíhalo u dvou skupin respondentů na výzkumném vzorku 60 dotazovaných jedinců. Dotazníkové řešení probíhalo od 7. března 2022 do 18. března 2022. Celkově bylo odesláno 300 dotazníků standardním zaměstnancům společnosti s očekávanou návratností alespoň 30 %. Reálná návratnost v mém případě byla 17 %. U respondentů z IT oddělení byla zapotřebí 100% návratnost z 10 odeslaných dotazníků. První skupinu tvořilo 50 respondentů zaměstnanců zkoumané společnosti bez IT zaměření. Druhou skupinou bylo 10 respondentů, kteří jsou součástí IT týmu ve společnosti.

Vzhledem k charakteru respondentů se očekávala nižší návratnost dotazníků online formou u druhé skupiny respondentů. Dotazník byl v prvním sledu distribuován online prostřednictvím sociálních sítí a e-mailu.

Pro potřeby bakalářské práce je počet (60) šedesáti respondentů dostačující.

4.2.2 Popis dotazníku

Jako výzkumný nástroj jsem zvolil dotazník, který je součástí přílohy této práce. Před samotným sdílením formuláře bylo vedení zkoumané společnosti seznámeno s cílem mého výzkumu včetně dohodnutého dohledu nad distribucí, formou a obsahem dotazníku. Před samotným šetřením byli všichni respondenti poučeni o své dobrovolnosti a seznámeni s dotazníkem.

Z hlediska struktury dotazníku byl na začátek umístěn motivační text, pokyny pro vyplnění a informace o anonymitě a dobrovolnosti vyplnění. Vyplnění dotazníku bylo zcela anonymní a charakter odpovědí zcela subjektivní. Základem dotazníku je 17 otázek předložených respondentům v on-line formě. U několika otázek byli respondenti

požádáni o subjektivní hodnocení na bodové stupnici 1-5. V dalších otázkách odpovídali pomocí jednoduchých odpovědí „ano“ nebo „ne“.

Dotazník byl členěn do tří kategorií. První část se zaměřovala na obecný názor na IT bezpečnost ve společnosti. Druhá část tematického celku se zaměřila na zabezpečení identity a autentizaci. V poslední části respondenti odpovídali na otázky související s firemním školením o kybernetické bezpečnosti. Cílem dotazníku bylo získání potřebných informací k sestavení organizačních, procesních a technologických doporučení pro zkoumanou společnost.

5 VÝSLEDKY

5.1 Analýza zkoumané společnosti

V této kapitole popíšu zkoumanou společnost, aktuální situaci a procesy z pohledu kybernetické bezpečnosti. Pomocí SWOT analýzy rozeberu rizika a nebezpečí hrozící dané společnosti na základě dříve uvedených kategorií a aktuálních hrozeb. Provedu analýzu jednotlivých důležitých aspektů aktuální obrany proti kybernetickým útokům z pohledu technologických, organizačních a procesních mechanismů.

5.1.1 Popis a kategorizace společnosti

V první řadě je potřeba podotknout, že informace o společnosti byli na základě dohody s vedením společnosti anonymizované s cílem udržet integritu společnosti a zachování mlčenlivosti.

Česká společnost vznikla v roce 1995 s cílem poskytovat svým zákazníkům finanční, platební a další služby logistickým společnostem. Vzhledem k velkému množství společností, které využívají služby této entity – jedná se o velkého hráče v oboru finančních služeb na trhu. Od roku 2018 má tato společnost mimo jiné také licenci bankovní instituce regulovanou Českou národní bankou, čímž se stala mnohem zajímavějším cílem na poli kybernetického zločinu. Dnes společnost čítá přes 1000 kmenových zaměstnanců a 500 externích spolupracovníků.

Společnost spadá do následujících kategorií:

- KI – Běžné užití IT
- KII – Údaje o zákaznicích
- KIV – Online portály
- KV – Chránicí know-how

Podobně jako jiné společnosti stejného zaměření, využívá zkoumaná společnost IT pro každodenní práci – například zpracování objednávek, nastavení limitů zákazníků, zpracování faktur, refundace DPH, telemarketing apod. Vzhledem k potřebě dodržet vyšší úroveň zaměstnanecké spokojenosti je omezení pro využívání firemního IT vybavení minimální. Což znamená, že se zaměstnanci bez omezení dostanou například na sociální sítě, streamovací služby, soukromé emailové schránky apod. Čímž se zvyšuje

riziko necíleného kybernetického útoku z důvodu nepozornosti uživatele při procházení internetem.

Ve finanční oblasti jsou největší hrozbou kybernetické útoky mající za cíl získání údaje o zákaznících a jejich finančních úroveň za účelem prodeje konkurenčním společnostem, popřípadě dostupnost nabízených služeb a technologií pro zákazníky. Tyto útoky bývají velice dlouho připravovány a cíleny na tzv. „díry“ v bezpečnostním perimetru infrastruktury – povětšinou na samotné zaměstnance mající za cíl získání přístupových údajů do systémů.

	Pomocné dosažení cíle	Škodlivé dosažení cíle
Vnitřní původ (atributy organizace)	**Silné stránky** Technická vybavenost Partnerství s bezpečnostními experty Skenování sítě Kontrola pošty Pravidelná kontrola oprávnění MFA Podmíněný přístup	**Slabé stránky** Volný pohyb zaměstnanců po internetu Vzdálený přístup z neověřených zařízení Volné připojování zařízení k firem. zař. Využívání starých operačních systémů Nedokonalé školení zaměstnanců
Vnější původ (atributy prostředí)	**Příležitosti** Zvýšení úrovně kybernetické bezpečnosti Nové technologie a procesy Cloudová řešení Školení cílenějšími metodami	**Hrozby** Tvorba nových a sofistikovanějších hrozeb Velká fluktuace zaměstnanců Posílení pozice na úkor konkurence Únik dat Nedostatečný kapitál na školení

Obrázek 6 - SWOT analýza společnosti

S (Strengths) – Silné stránky:

Zkoumaná společnost je vlastníkem výborné technické vybavenosti z pohledu infrastruktury sítě. Značkové produkty od společností Cisco a Dell zajišťuje komptabilitu s aktuálními kybernetickými ochrannými metodami. Společnost také za dobu své existence uzavřela velmi silná partnerství s bezpečnostními experty z různých

společností a díky tomu mají přístup k expertům z nadnárodních technologických společností. Organizace zaměstnává jen prověřené školené experty v oblasti kybernetické bezpečnosti. Pravidelně kontrolují prostředí včetně instalace bezpečnostních aktualizací operačních systémů a firmwarů serverových farem. Mají proaktivní přístup ke skenování sítě a samotných firemních zařízení. Díky svému partnerství mají mnoho bezpečnostních technologických procesů jako třeba kontrolu pošty pří procházení jednotlivými, různými technologiemi v prostředí společnosti, přísnou kontrolu oprávnění skrze jednotlivé kritické aplikace a technologie společnosti. Vzhledem k využívání cloudových služeb mají vynucené zabezpečení firemního uživatelského účtu za pomocí více faktorové autentizace a podmíněného způsobu na základě několika prvků kontrol.

W (Weaknesses) – Slabé stránky:

Zaměstnanci ve společnosti mají příliš volný pohyb po veřejném internetu při využívání firemních zařízení typu laptop, mobilní telefon, tablet apod. Přístup do společnosti a sdílení dat mezi soukromým zařízením a firemním zabezpečeným prostředím není pod hlubší kontrolou. Zaměstnanci mají možnost připojovat jakékoli zařízení do firemních koncových zařízení. Vzhledem k stáří společnosti stálé využívá starších operačních systémů, které již nedostávají bezpečnostní aktualizace. A společnost má nedokonale řízené školení uživatelů.

O (Opportunities) – Příležitosti:

Vzhledem k faktu získání licence bankovní instituce regulovanou Českou národní bankou je zapotřebí zvýšit pozornost ke kybernetické bezpečnosti a její vylepšení. To by mohlo donutit vedení společnosti na uvolnění prostředků k nákupu nových technologií a vytvoření procesů ke zlepšení kybernetické bezpečnosti. Společnost má možnost využit cloudových řešení v rámci partnerství se společností Microsoft. Organizace školení zaměstnanců by mělo zahrnovat cílenější metody – například „falešný útok“.

T (Threats) – Hrozby:

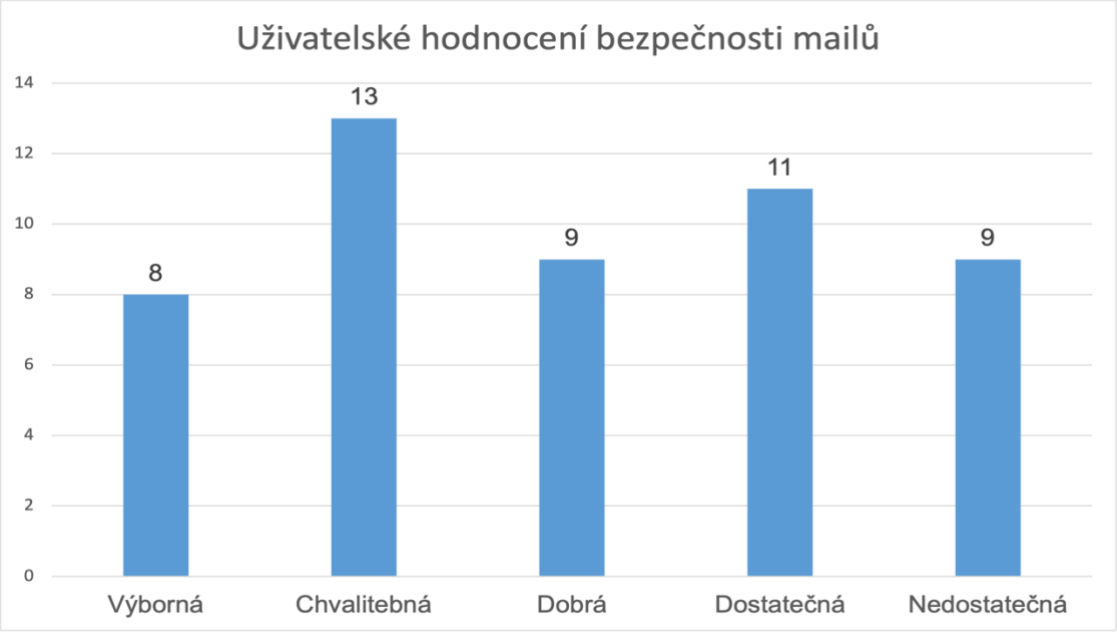
Velká rychlost vytváření nových a cílených kybernetických hrozeb a útoků. Velká fluktuace zaměstnanců je velkým problémem z pohledu expertízy a znalosti prostředí. Bankovních institucí rychle přibývá a mnohdy mají větší kapitál pro zajištění pozice společnosti na úkor konkurence. S tím souvisí i únik dat – chtěný a plánovaný, ale i nechtěný. Samozřejmě nedostatečný kapitál pro školení zaměstnanců.

5.2 Výsledky dotazníku

Otázky v první třetině dotazníku byly věnovány obecným názorům o IT bezpečnosti ve zkoumané společnosti. Jedná se především o první kontakt s respondentem. Možnost subjektivně ohodnotit procesy ve společnosti, ve které zaměstnanec pracuje, je vítaným otevřením dotazníku. Druhá část dotazníku se zaměřuje na bezpečnost uživatelských účtů a jejich oprávnění. Zjišťuje existenci bezpečnostních best-practice na poli bezpečnosti identit používaných ve světě. Poslední část dotazníků má za úkol zjistit názory a stav bezpečnostních školení pro zaměstnance zkoumané společnosti a jejich vědomosti základních rizik.

5.2.1 Otázka 1 Jakým způsobem byste ohodnotili zabezpečení emailů ve Vaší společnosti?

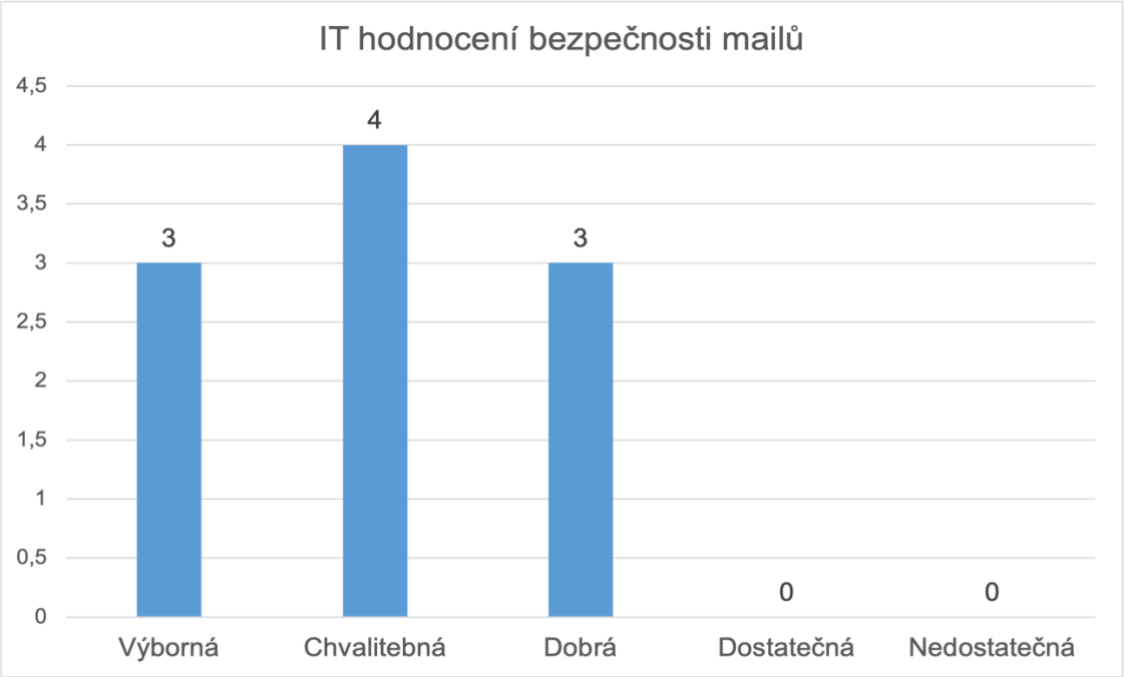
Tato otázka neměla hlubší význam. Jednalo se o typ otázky, který má donutit respondenta se zamyslet a připravit na co možná nejpravdivější odpověď (viz obr. 6).



Obrázek 7 - Uživatelské hodnocení bezpečnosti mailů

Na základě výsledku se domnívám, že uživatelé berou v potaz především proniklé reklamní kampaně, které jsou svým charakterem bezpečné, popřípadě nasazené emailové phishingové kampaně vytvořené IT bezpečnostním oddělením.

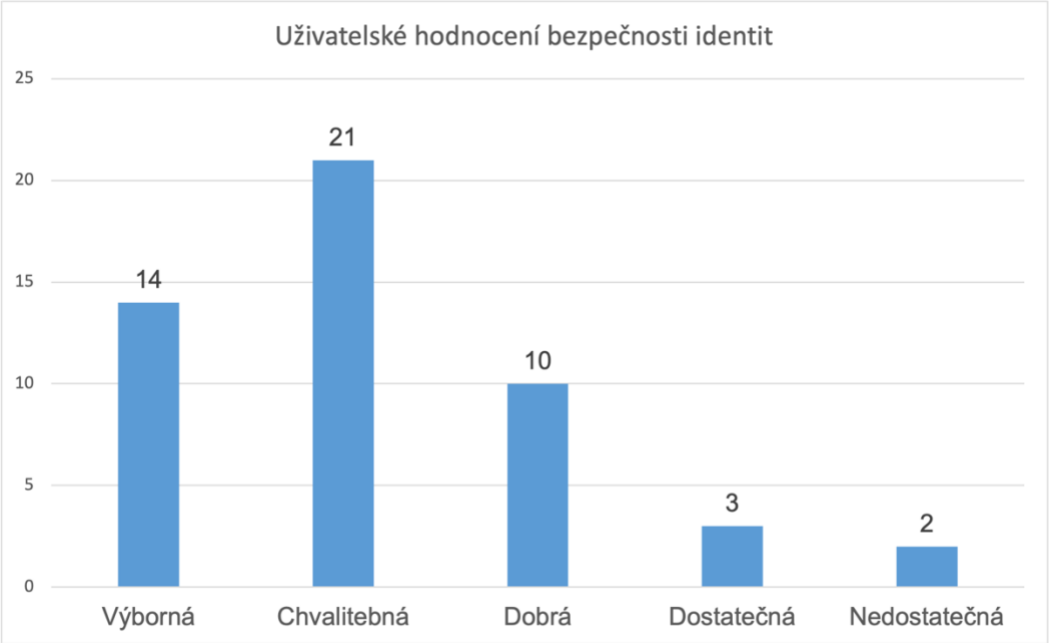
V porovnání s výsledky IT oddělení předpokládáme, že ve společnosti je nasazené nějaké řešení pro zabezpečení emailové komunikace (viz obr. 7). Nicméně nastavení tohoto řešení nebude ideální dle Mail-flow.



Obrázek 8 - IT hodnocení bezpečnosti mailů

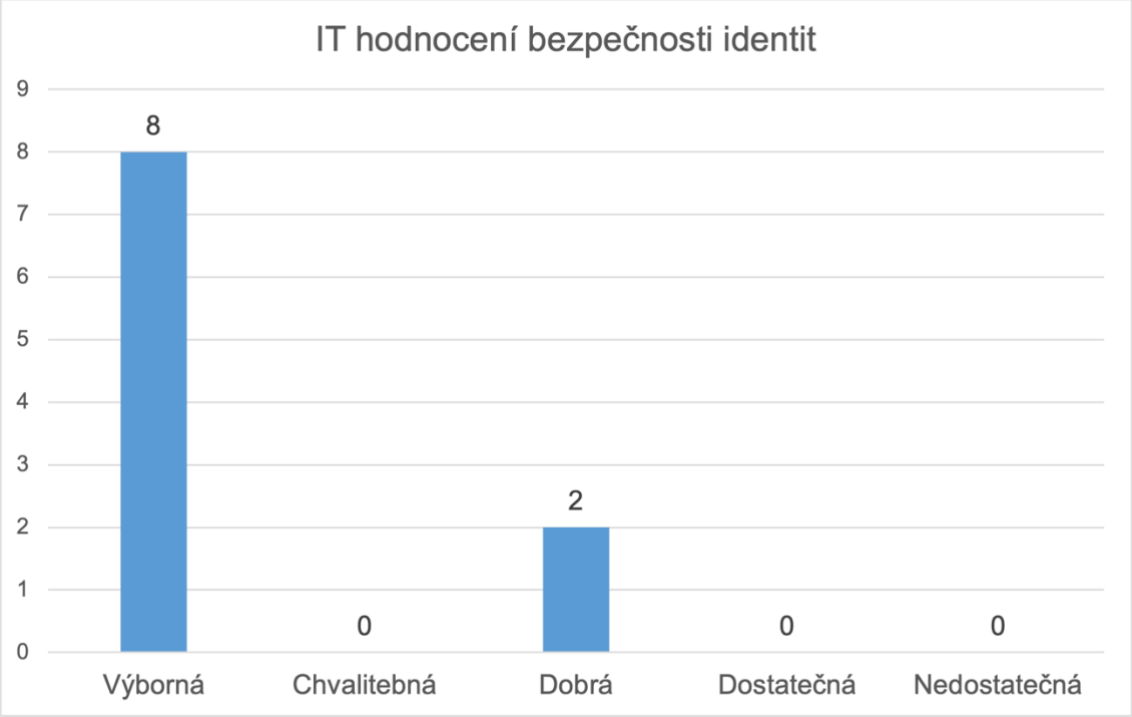
5.2.2 Otázka 2 Jakým způsobem byste ohodnotili zabezpečení identit ve Vaší společnosti?

Stejně jako u předchozí otázky je tato zaměřená na subjektivní pocit nebo názor. Na rozdíl od emailů se zde dostáváme na průměr 2,16 (viz obr. 8).



Obrázek 9 - Uživatelské hodnocení bezpečnosti identit

Uživatelé si opravdu chválí správu a bezpečnost identit. Dle informací získaných během studie společnosti využívá veškeré aktuální mechaniky v rámci identit – RBAC, POLP, MFA a pokročilé metody Single Sign On. Dle nezávislých pohovorů během šetřící praxe uživatelé nečekají na oprávnění v den nástupu do zaměstnání ani během praxe. Podobný výsledek vyšel z pohledu IT pracovníků s průměrem hodnocení 1,4 (viz obr. 9).

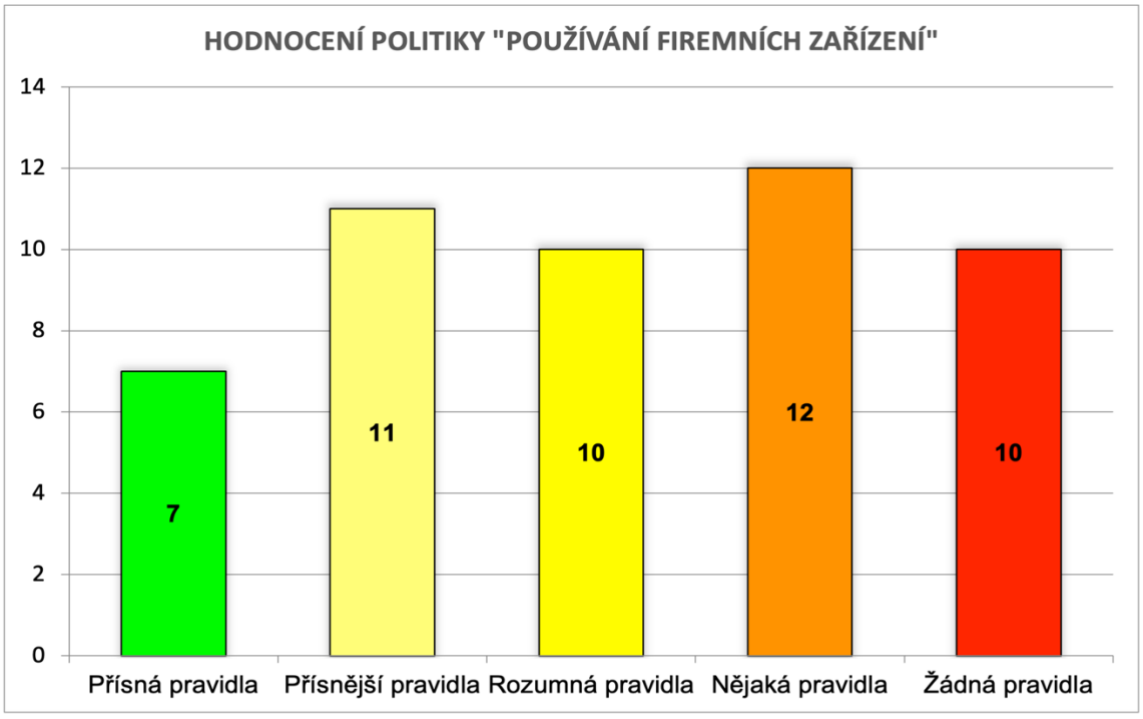


Obrázek 10 - IT hodnocení bezpečnosti identit

5.2.3 Otázka 3 Jakým způsobem byste ohodnotili firemní pravidla z pohledu kybernetické bezpečnosti?

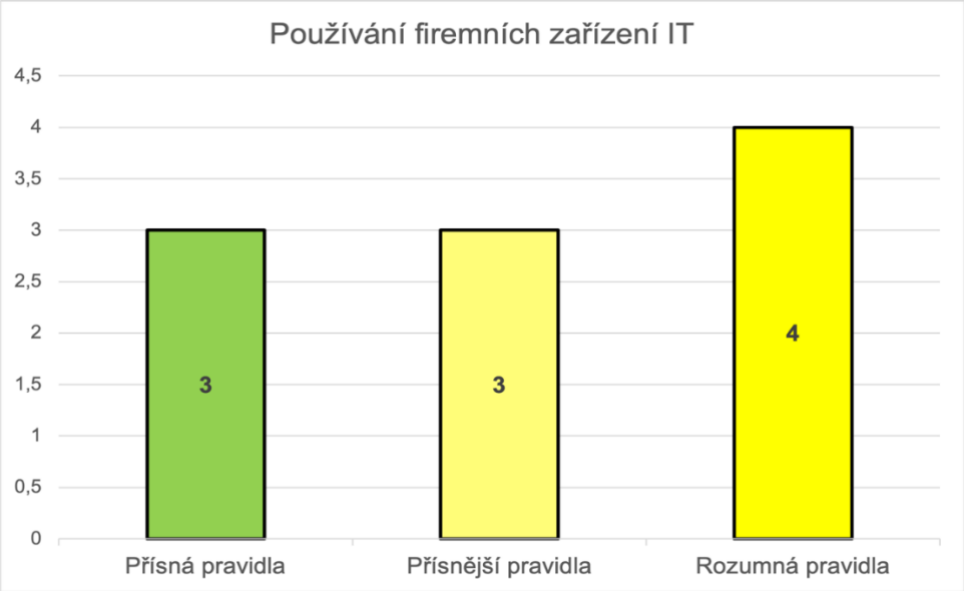
Následující otázka byla navržena tak, aby zjistila dostatečnost a sílu firemních pravidel z pohledu IT bezpečnosti. Hodnocení probíhalo na škále od „Přísných pravidel“ přes „Přísnější pravidla“, „Rozumná pravidla“, „Nějaká pravidla“ až po „Žádná pravidla“. Vybral jsem šest politik, které dle mého názoru jsou potřebné v každé společnosti bez ohledu na velikost či zaměření.

První zásadou ve společnosti by měla mít souvislost se zařízeními, které jsou uživatelům svěřovány na začátku pracovně-právního vztahu. Jedná se o všeobecně známá pravidla nařizující dohled nad svým zařízením, nepůjčovat zařízení jiným osobám, vyvarovat se provozování protiprávních aktiv na zařízení apod. Vzhledem k velké fluktuaci zaměstnanců ve zkoumané společnosti jsou výsledky průměrné. Na základě rozhovorů během vzorkování bylo zjištěno, že uživatelé pocházejí z různých společností, s různým zaměřením a různou úrovní IT bezpečnosti. Z toho důvodu se může uživatelům zdát, že jsou některá pravidla nedostatečná či naopak příliš přísná (viz obr. 10).



Obrázek 11 - Uživatelské hodnocení politiky "Používání firemních zařízení"

Z pohledu IT oddělení jsou pravidla pro zabezpečení užívání firemních zařízení dostatečná (viz obr. 11).



Obrázek 12 - IT hodnocení politiky '"Používání firemních zařízení"

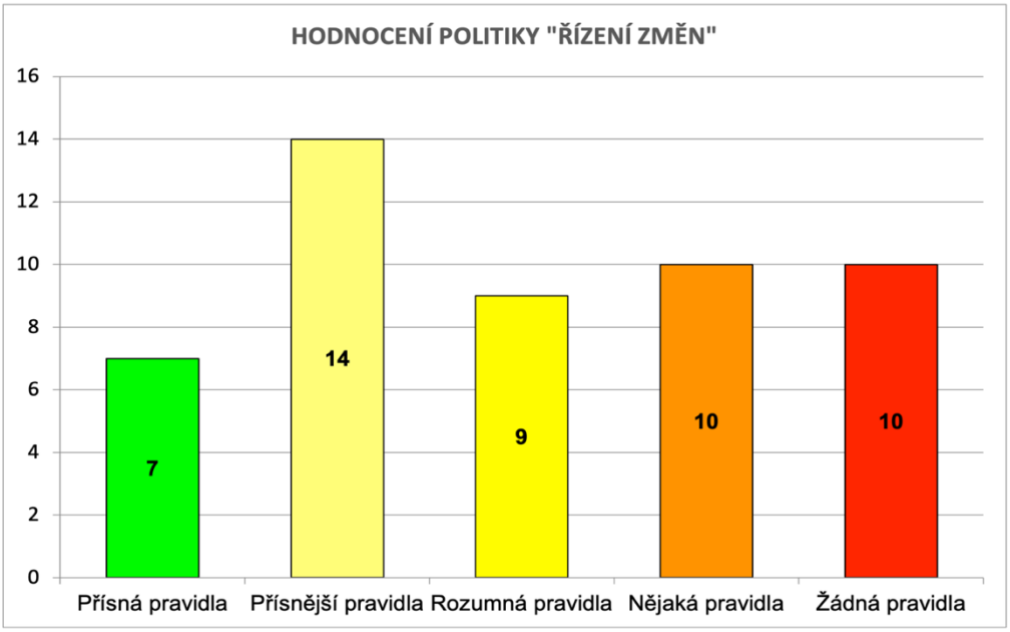
Zavedení tzn. Acceptable Use Policy (APT) nastiňuje přijatelné použití počítačového vybavení. Tato politika definuje nevhodné používání informačních systémů a rizika, která může toto jednání způsobit. Nesprávné chování může ohrozit síť společnosti a mít následně právní důsledky. Definice dovolených aktivit částečně napomůže k rozhodnutí uživatele, zda smí využít např. webové stránky nesouvisející s pracovní náplní.

V mém doporučení má APT politika znění:

- Narušení přístupu k síti pro ostatní, ať už úmyslně nebo neúmyslně. Příklady: infikované počítače zaplavující síť spamem nebo viry, aplikace pro sdílení souborů P2P, které spotřebovávají více než spravedlivý podíl síťových zdrojů, nesprávně nakonfigurovaná síťová zařízení.
- Používání technologických zdrojů k porušení jakéhokoli státního nebo federálního zákona, včetně autorských a licenčních smluv. Příklady: nelegální stahování, ukládání a/nebo sdílení materiálů chráněných autorským právem, sledování dětské pornografie, krádež důvěrných informací.
- Přenos urážlivých, výhružných nebo obtěžujících zpráv, řetězových dopisů, spamu nebo jiné komunikace, která je zakázána zákonem nebo zásadami společnosti.

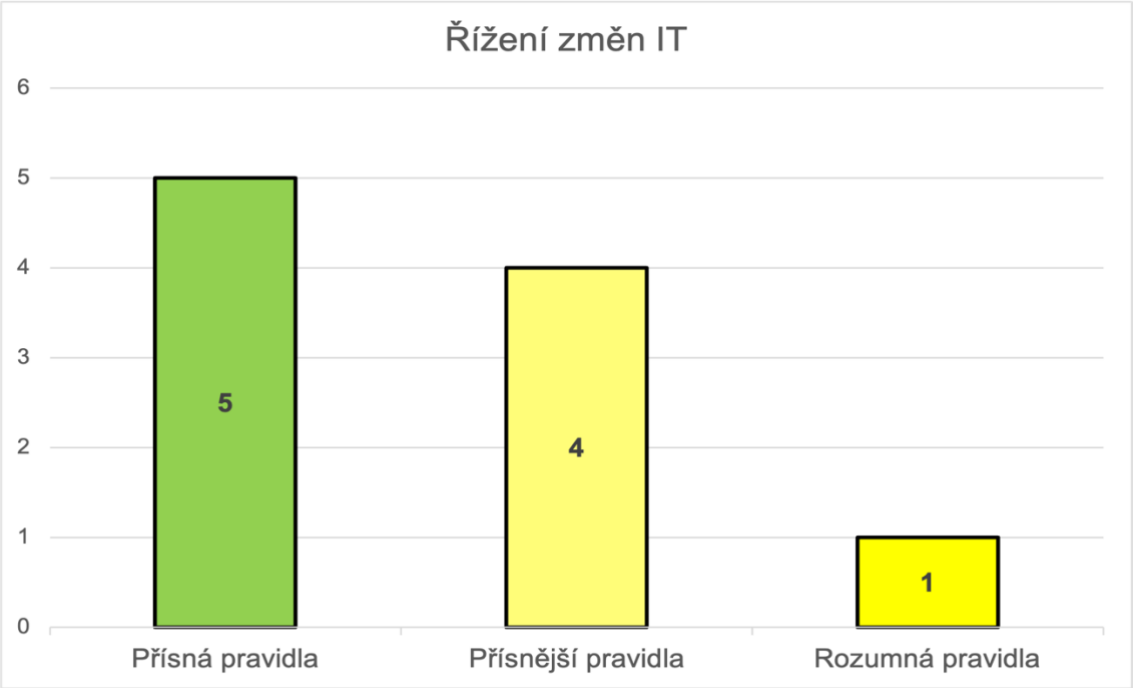
- Neoprávněné pokusy o skenování nebo získání přístupu k systémům, účtům, síťovému provozu nebo informacím, které nejsou určeny danému uživateli.

Politika řízení změn musí popisovat přesné postupy při nasazování změn do produkčního prostředí, hierarchii schvalovacího procesu a krizový plán obnovy. Vzhledem k výsledkům není zpětná vazba ze strany zaměstnanců nějak závažná. 21 respondentů připisuje nadprůměrné hodnocení, naopak jiných 20 respondentů tvrdí opak (viz obr. 12).



Obrázek 13 - Uživatelské hodnocení politiky "Řízení změn"

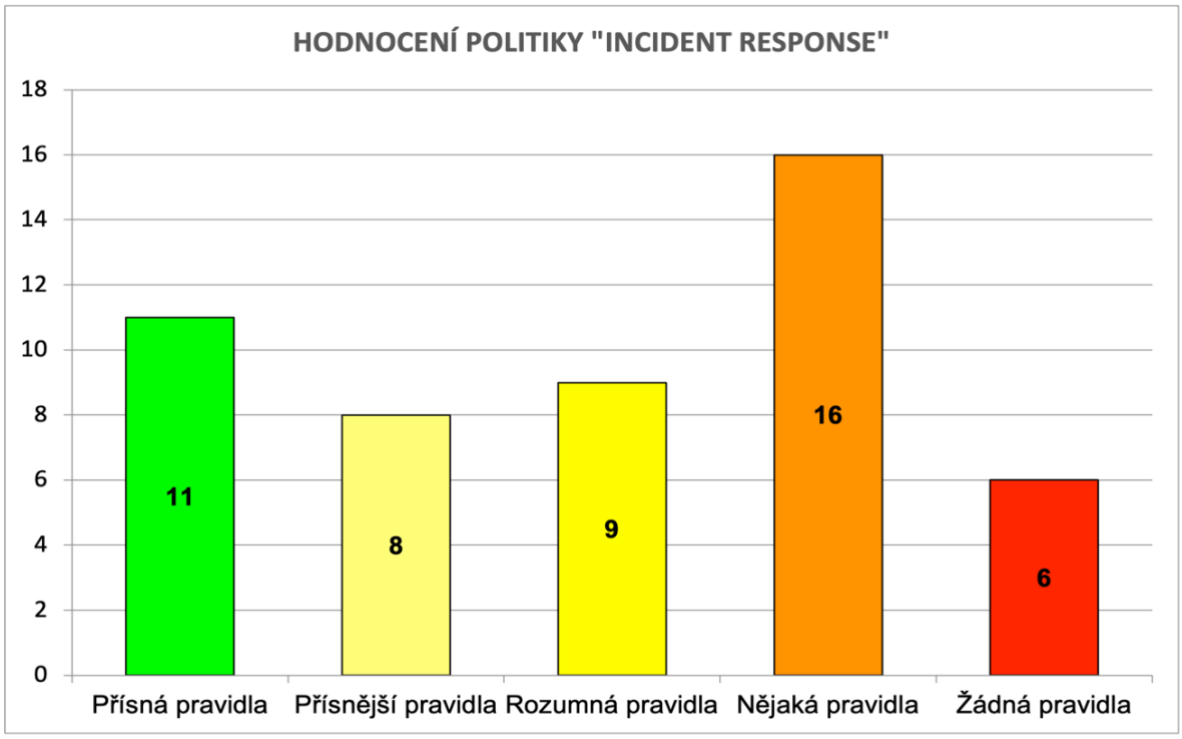
Nicméně na základě hodnocení ze strany IT se zdá, že uživatelé pouze nerozumí problematice řízení změn (viz obr. 13).



Obrázek 14 - IT hodnocení politiky "Řízení změn"

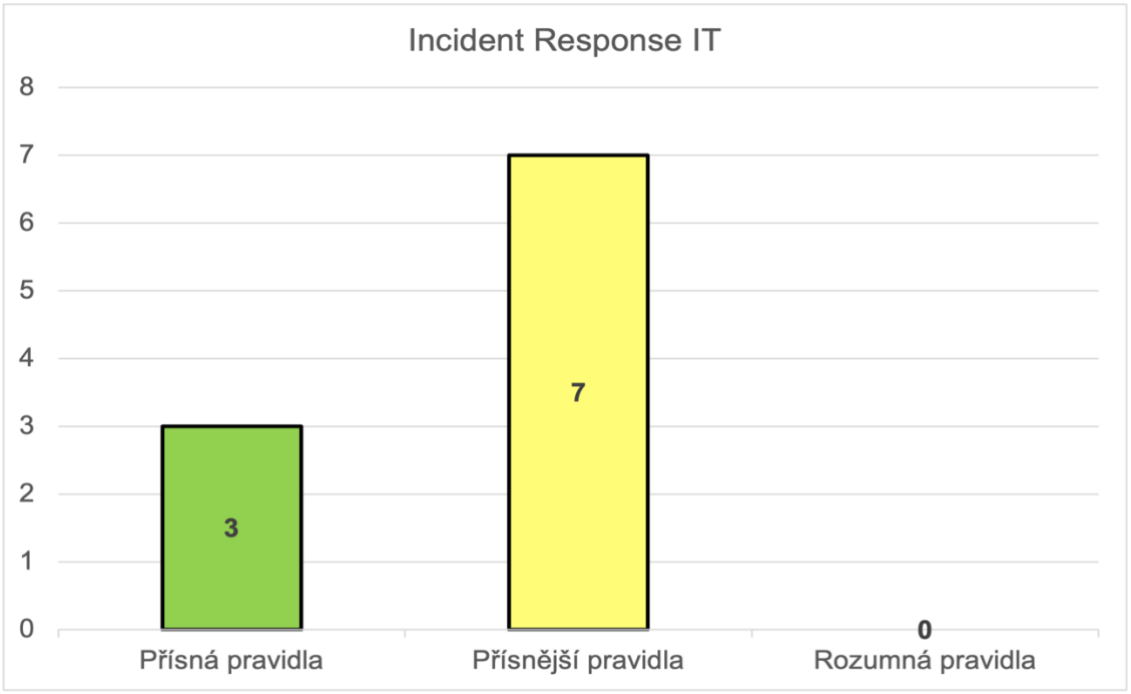
Pokusím se tedy přiblížit problematiku mým doporučením, které vyplývá z mé dlouhodobé spolupráce s DevOps týmy napříč společnostmi. Politika řízení změn organizace zajišťuje, že změny v informačním systému jsou spravovány, schvalovány a sledovány. Organizace se musí ujistit, že všechny změny jsou prováděny promyšleným způsobem, který minimalizuje negativní dopad na služby a zákazníky. Politika řízení změn zahrnuje metody plánování, hodnocení, kontroly, schvalování, komunikace, implementace, dokumentace a kontroly po změně. Řízení změn spoléhá na přesnou a včasnou dokumentaci, nepřetržitý dohled a formální a definovaný schvalovací proces. Zásady správy změn pokrývají změny Systems Development Life Cycle, hardwaru, softwaru, databáze a aplikací v konfiguraci systému včetně přesunů, přidávání a odstraňování.

Incident Response svým způsobem souvisí s předchozí politikou, nicméně ve společnostech se vytváří hlavně kvůli „Disaster Recovery“. Dle výsledků získaných od zaměstnanců je stav těchto pravidel spíše slabší (viz obr. 14).



Obrázek 15 - Uživatelské hodnocení politiky "Incident Response"

Pohled na Incident Response pravidla z IT perspektivy jsou na tom o něco lépe než veřejné části (viz obr. 15). V tomto případě je zcela pochopitelné nerovnost výsledků. Většina těchto procesů jsou důvěrná až tajná.



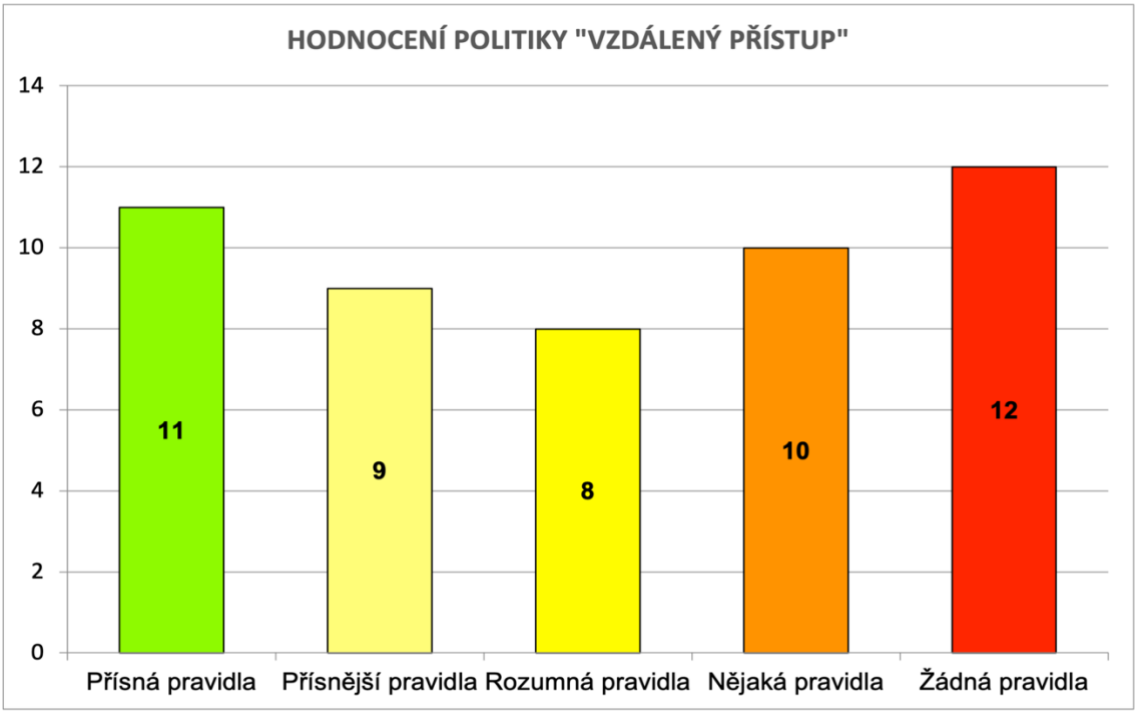
Obrázek 16 - IT hodnocení politiky "Incident Response"

Incident Response politika zahrnuje několik bodů, které jsou na sobě závislé a není možné je přeskakovat, popř. úplně odmítat:

- Příprava.
- Identifikace.
- Izolace.
- Eliminace zdroje.
- Obnova poškozených částí systémů nebo dat.
- Revize a hodnocení incidentu.

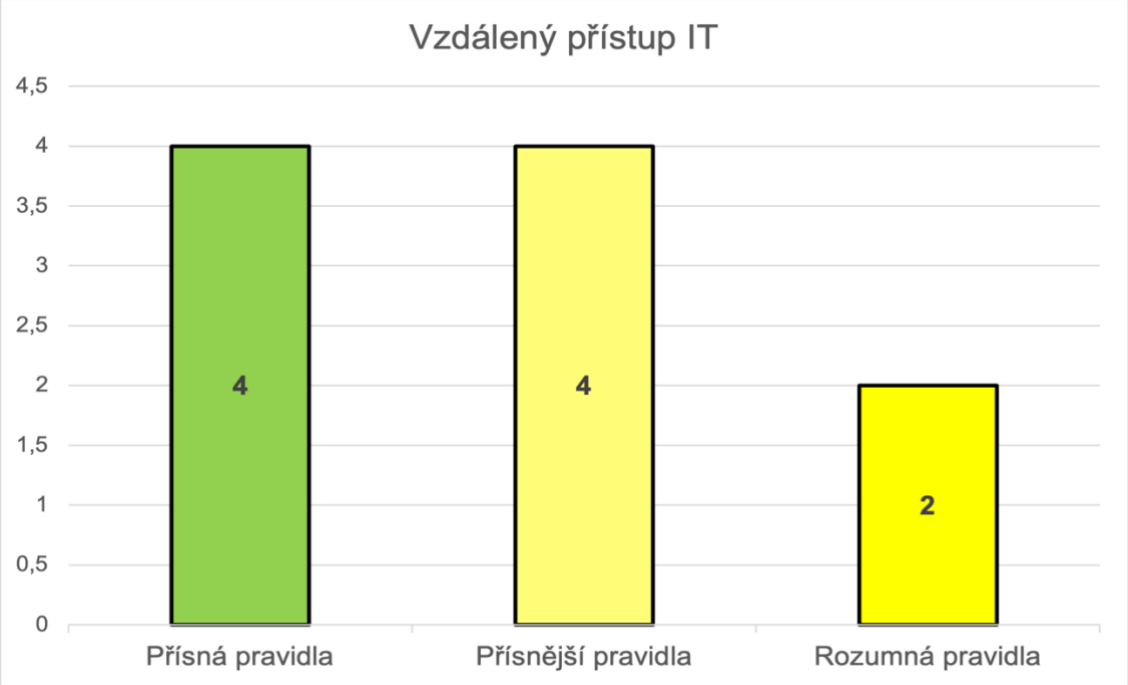
Pro Incident Response zásady je potřeba identifikovat Incident Response tým a informace o systému, jako jsou diagramy sítě a datových toků, inventář hardwaru a protokolovaná data. Postupy pro řešení incidentů by měly být podrobně popsány v politikách. Jedním z nejdůležitějších aspektů těchto zásad je poučení uživatelů o tom, komu je třeba hlásit narušení dat nebo jiný bezpečnostní incident. Vedení by mělo vždy hodnotit a monitorovat výkon, zajistit spolupráci mezi zaměstnanci a pravidelně testovat plán Incident Response.

Dalším navazujícím dotazem jsme narazili na velmi aktuální téma a tím je vzdálený přístup. Bohužel v tomto případě jsou výsledky různé. Je to z důvodu, že společnost momentálně prochází různými změnami technologií zajišťující vzdálený přístup. Ať už to je řešení od společnosti Citrix a jejich Virtual Apps & Desktops nebo řešení v podobě VPN od společnosti Checkpoint. Uživatelé se tedy vyjádřili následovně: 20 lidí hodnotí politiku nadprůměrně a 22 lidí spíše podprůměrně (viz obr. 16).



Obrázek 17 - Uživatelské hodnocení politiky "Vzdálený přístup"

V porovnání s IT oddělením, které si prošlo změnami již před nějakým časem je hodnocení na lepší úrovni (viz obr. 17).



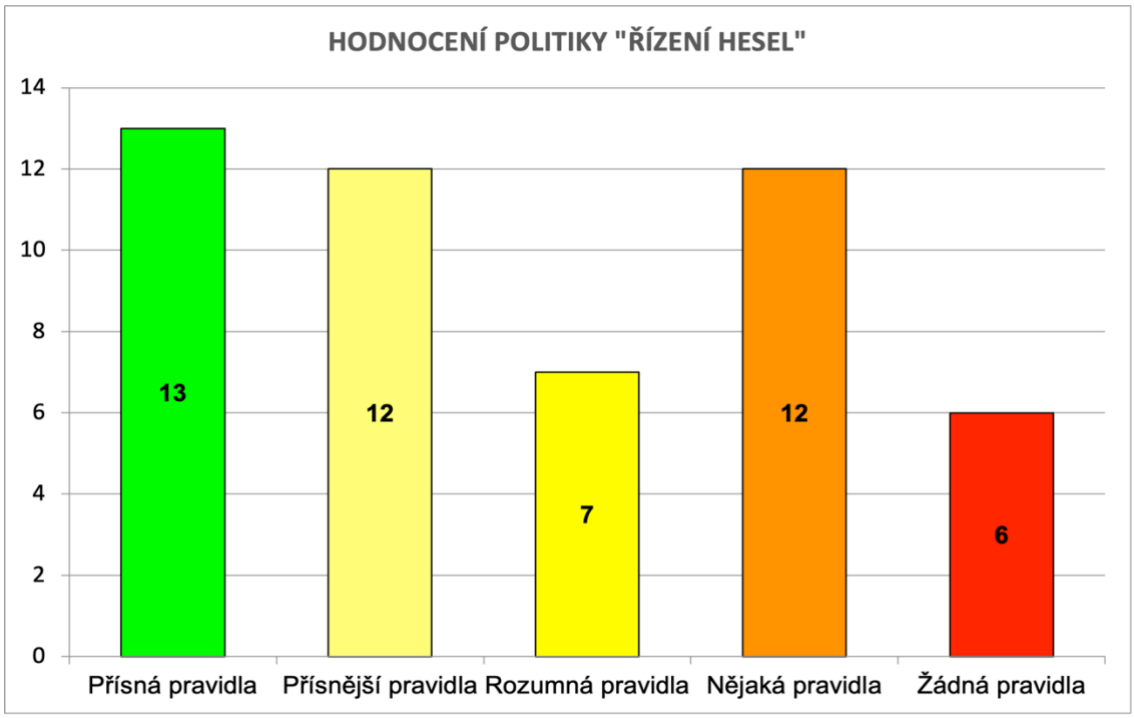
Obrázek 18 - IT hodnocení politiky "Vzdálený přístup"

Jedná se hlavně o využití full-tunnel VPN, které umožňuje se z jakékoli sítě připojit do společnosti s iluzí, že zařízení je přímo na firemní síti, včetně bezpečnostních pravidel.

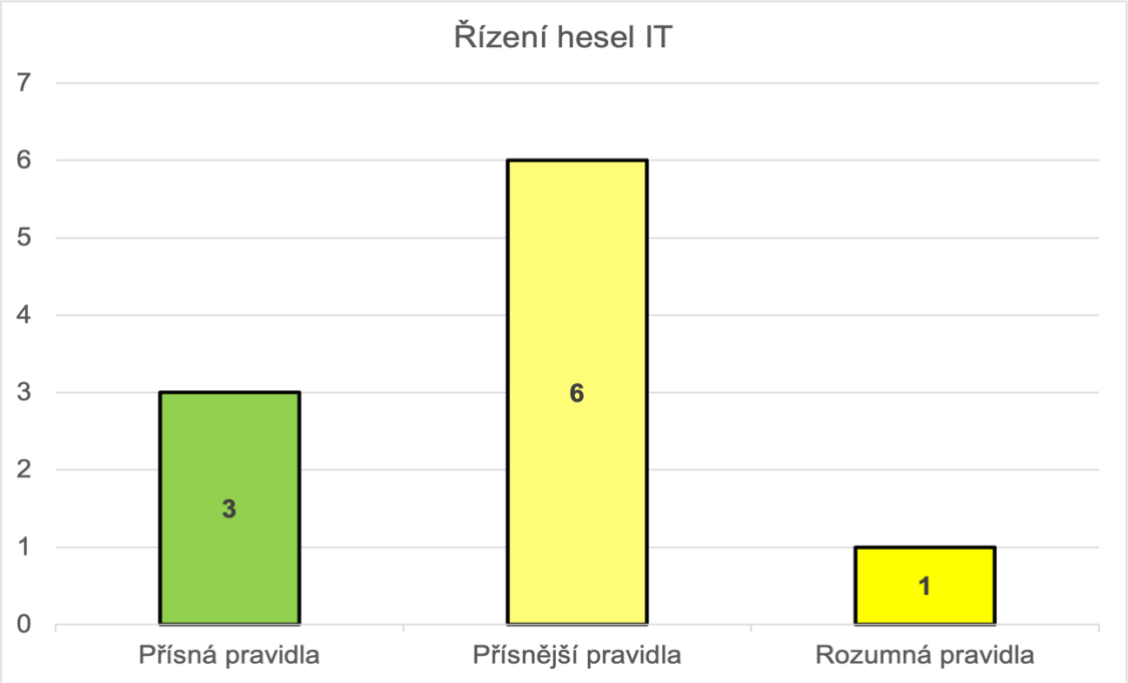
Na základě výsledků obou kategorií jsem navrhl politiku vzdáleného přístupu tak, aby minimalizovala potenciální riziko poškození, ke kterému může dojít v důsledku neoprávněného použití zdrojů. Tato politika je zaměřena na všechny zaměstnance a zahrnuje ustanovení pro odesílání a přijímání e-mailů a intranetových zdrojů. Zásady také zahrnují požadavky na přístup k VPN a šifrování disku.

Požadavky na vzdálený přístup by měly být podobné požadavkům na místní přístup. Zaměstnanci mají přísný zákaz zapojovat se do nelegální činnosti na svém vzdáleném přístupu a také nesmí dovolit neoprávněným uživatelům používat jejich pracovní zařízení. Zásady prosazují silné přístupové fráze, odhlašování se a zakazují připojování zařízení k jiným sítím ve chvíli, kdy jsou připojeni k interní síti. Vyžaduje, aby uživatelé zajistili, že používají nejaktuálnější antimalwarový software a operační systém.

Dalším velkým tématem v mém dotazníku byla hesla. Hesla jsou důležitým tématem v každé společnosti. Dnes se pomalu přechází na přihlašování bez hesla pomocí různých metod jako například biometrika, bezpečnostní klíče nebo propojené zařízení. Zkoumaná společnost si v tomto ohledu vede velmi dobře. To vychází i z výsledků dotazníku. Zaměstnanci jsou spokojeni s metodami řízení hesel (viz obr. 18 a 19).



Obrázek 19 - Uživatelské hodnocení politiky "Řízení hesel"



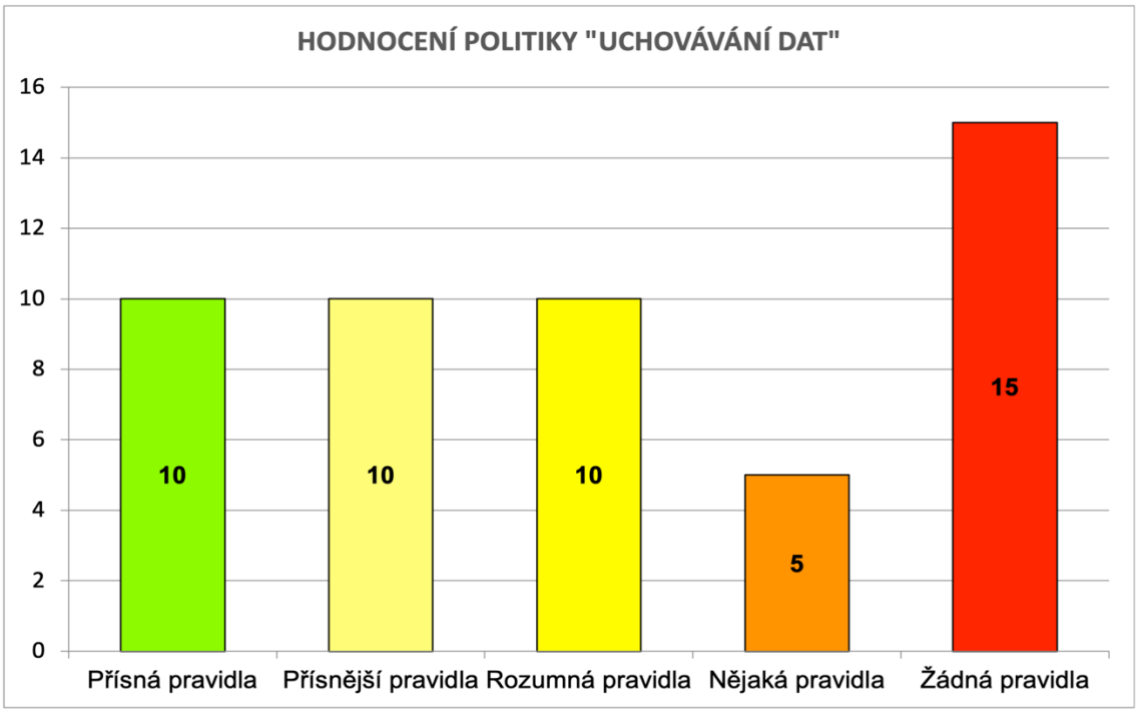
Obrázek 20 - IT hodnocení politiky "Řízení hesel"

Zkoumaná společnost používá technologie vyvinuté společností Microsoft. Jedná se zde o propojení biometrických dat s přihlašovacími informacemi zkombinované s podmíněným přístupem. Jedná se o technologii nazvanou Windows Hello. Hesla si zde uživatelé vytváří a aktualizují na základě standardu NIST 800-63b. Předchozí pokyny NIST doporučovaly nutit uživatele měnit hesla každých 90 dní (180 dní u přístupových frází). Změna hesel však příliš často dráždí uživatele a obvykle je nutí opakovaně používat stará hesla nebo používat jednoduché vzorce, což poškozuje pozici v oblasti bezpečnosti informací. I když lze implementovat strategie zabraňující opětovnému použití hesla, uživatelé je stále najdou kreativními způsoby.

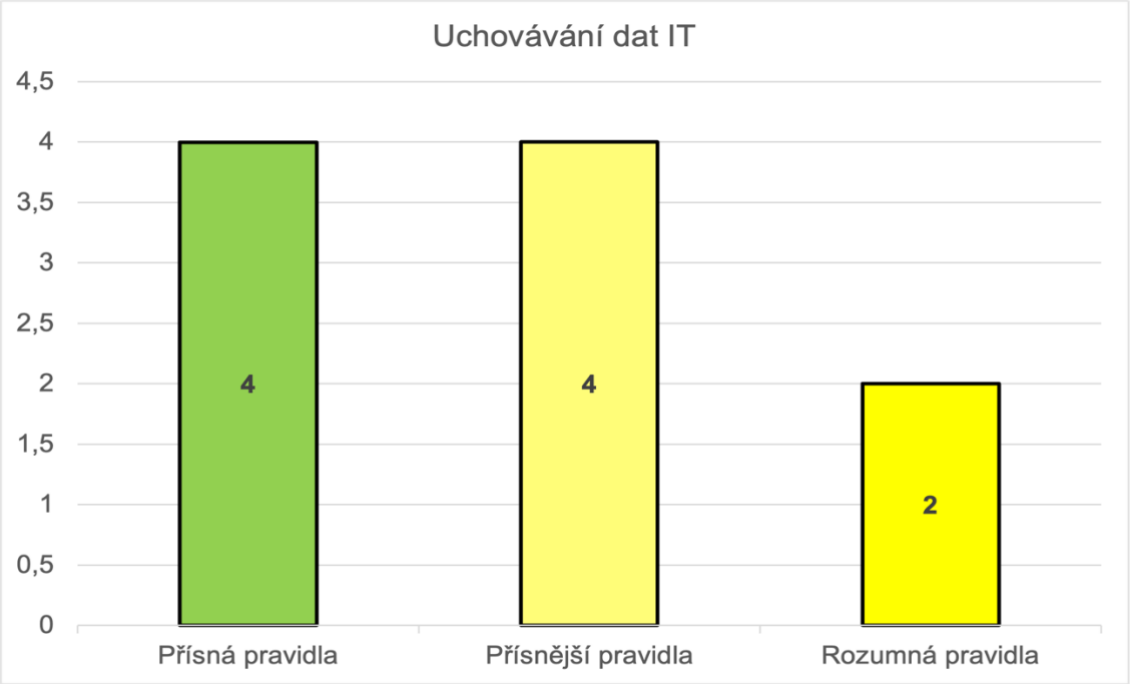
Současné doporučení NIST ohledně maximálního věku hesla je proto žádat zaměstnance, aby si nové heslo vytvořili pouze v případě potenciální hrozby nebo podezření na neoprávněný přístup. Délka hesla se také odvíjí od stejného standardu. Mnoho organizací vyžaduje, aby hesla obsahovala různé symboly, jako je alespoň jedno číslo, velká i malá písmena a jeden nebo více speciálních znaků. Přínos těchto pravidel však není zdaleka tak významný, jak se očekávalo, a uživatelé si díky nim mnohem hůře hesla pamatují.

Na druhé straně bylo zjištěno, že délka hesla je primárním faktorem síly hesla. V souladu s tím NIST doporučuje povzbuzovat uživatele, aby volili dlouhá hesla nebo přístupové fráze o délce až 64 znaků (včetně mezer).

Uchovávání dat je poslední politikou řešenou v mém dotazníku. Jak jsem již zmínil v KI – Běžné užití IT a KII – Údaje o zákaznicích, uchovávání dat podléhá právním úpravám v zákoně. Každý podnikatelský subjekt má povinnost zálohovat účetní doklady a smlouvy po dobu pěti let. Výsledek z dotazníku naznačuje nesprávnou práci se zálohováním důležitých souborů podléhající velké důležitosti (viz obr. 20). Nicméně z pohledu IT je zde vše v pořádku (viz obr. 21). Z pohledu správní rady a právního oddělení společnost zálohuje veškerá důležitá data, které podléhají právní úpravě na několika místech na sobě nezávislých.



Obrázek 21 - Uživatelské hodnocení politiky "Uchovávání dat"



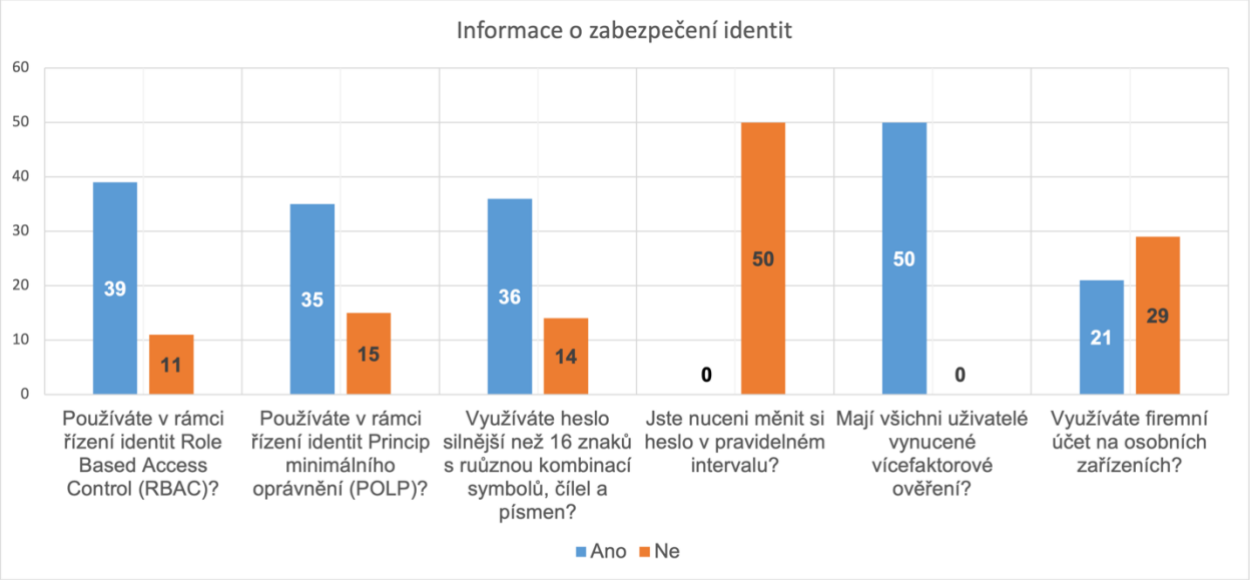
Obrázek 22- IT hodnocení politiky "Uchovávání dat"

Zkoumané společnosti jsem doporučil postupovat pravidlem 3-2-1. Pravidlo 3-2-1 může pomoci v procesu zálohování. Uvádí, že by měly existovat alespoň 3 kopie dat uložené na 2 různých typech paměťových médií a jedna kopie by měla být uchovávána mimo pracoviště na vzdáleném místě (to může zahrnovat cloudové úložiště). Pro eliminaci ztráty dat z různých důvodů by měla být použita 2 nebo více různých médií. Kopie mimo pracoviště chrání před požárem, krádeží fyzických médií (jako jsou pásky nebo disky) a přírodními katastrofami, jako jsou povodně a zemětřesení.

Vytvořil jsem pravidla pro uchovávání dat, která specifikuje typy dat, které musí firma uchovávat a jak dlouho. Pravidla také stanovují, jak budou data uložena a zničena. Tato politika pomůže odstranit zastaralá a duplicitní data a vytvořit více úložného prostoru. Politika uchovávání dat také pomůže uspořádat data, aby je bylo možné použít později. Typy dat zahrnují dokumenty, záznamy o zákaznících, transakční informace, e-mailové zprávy a smlouvy. Vytvoření této politiky bylo nezbytné pro zkoumaný podnik, který uchovává citlivé informace.

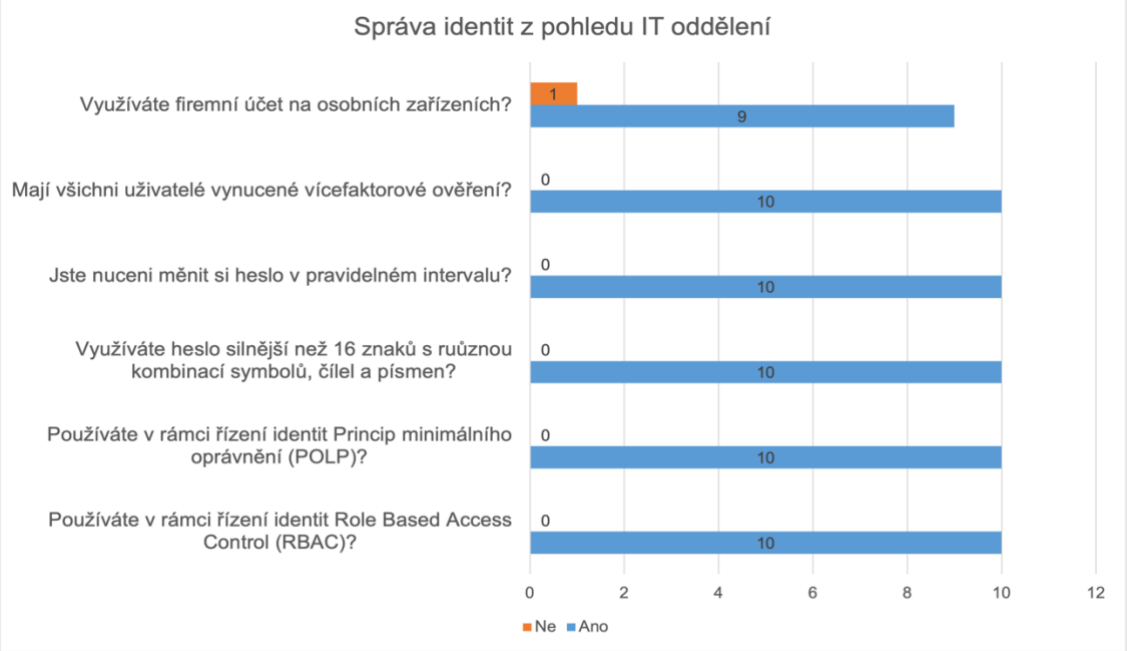
5.2.4 Otázka 4. – 9. Řízení identit

Identita a oprávnění je nejdůležitější technologií v jakékoli společnosti. Oprávnění dává uživateli přístup využívat a upravovat data, soubory, zákazníky, nakládat s finančními prostředky firmy a podobně. Součástí tohoto tématu jsem zvolil šest jednoduchých dotazů na průzkum práce s identitami a oprávněním (viz obr. 22).



Obrázek 23 - Uživatelské informace o zabezpečení identit

Z pohledu IT oddělení výsledek vypadá jednostranně (viz obr. 23).



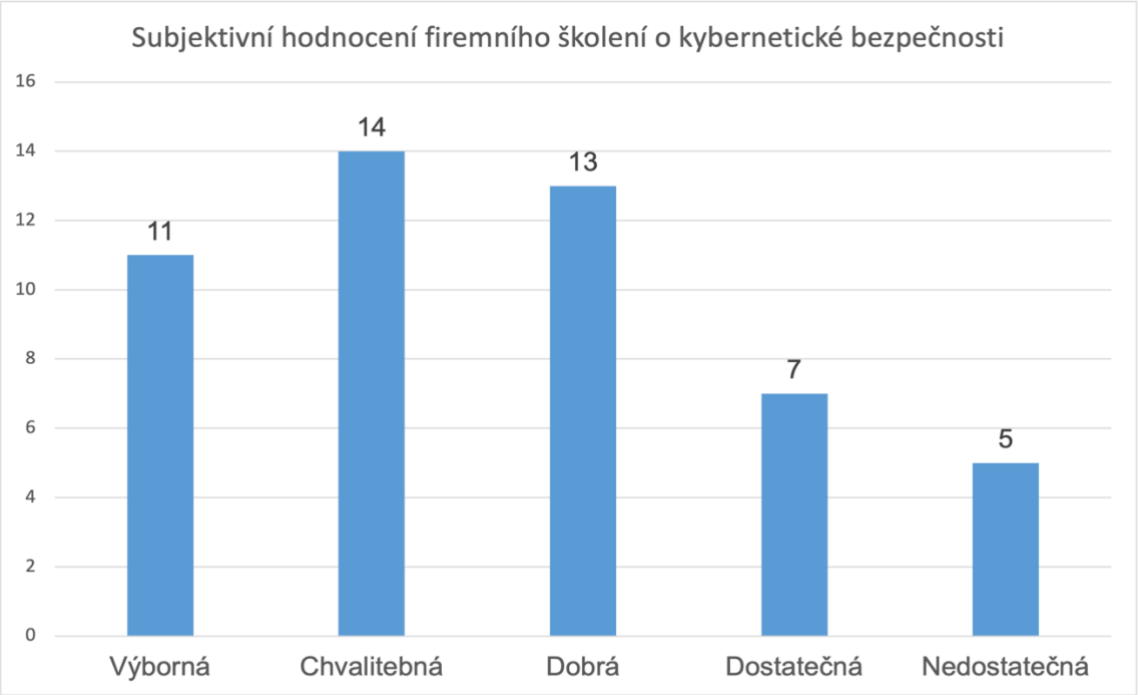
Obrázek 24 - Správa identit z pohledu IT oddělení

Na výsledcích jednotlivých otázek je dokázáno, že zkoumaná společnost přistupuje k identitě velice obezřetně. IT společně s personálním oddělením má vytvořenou sadu rolí napárovanou na hierarchii společnosti – Rozpočtový celek (Business Unit), tým a virtuální role v týmu. Tím společnost docílila integritě oprávnění pro každého zaměstnance, zabezpečila přístupnost novým zaměstnancům z pohledu možnosti práce od prvního dne apod. Zároveň jsou role tvořeny za pomocí principu POLP (principu minimálního oprávnění) - tedy minimálnímu potřebnému oprávnění k plynulému dokončení pracovní náplně.

Zároveň se potvrdilo nasazení pravidel správy hesel, kde všech 50 respondentů není nuceno měnit si heslo v pravidelném intervalu. Identita je pak u všech zaměstnanců chráněna vícefaktorovou autentizací pomocí Azure AD technologiím.

5.2.5 Otázka 10 Jakým způsobem byste ohodnotili firemní školení na téma kybernetická bezpečnost?

Správně zřízené školení kybernetické bezpečnosti je silným základem pro bezpečnost společnosti. Důležité je, aby tato školení byla vedena zábavnou formou s cílem předat co nejvíce informací co možná nejjednodušeji. V mnou zkoumané společnosti je zpětná vazba směrem k těmto školením velice pozitivní. Více než polovina respondentů uvedla, že úroveň školení je nadprůměrná (viz obr. 24).



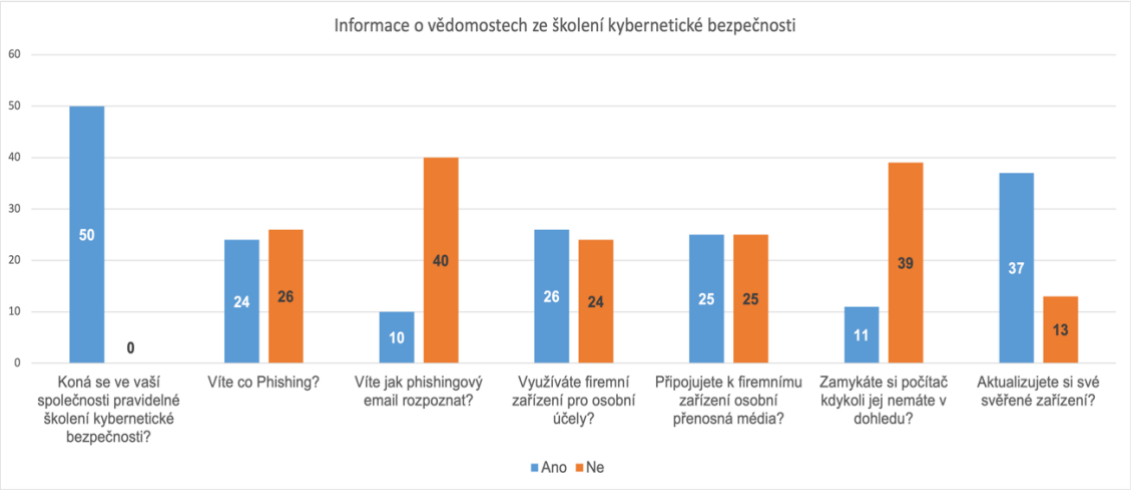
Obrázek 25 - Uživatelské hodnocení školení o kybernetické bezpečnosti

Ve společnosti jsme zavedli školení tzv. „Šokovou formou“ a následnou diskusí. IT oddělení vytvoří program, který se rozšíří mezi uživatele pomocí emailů či komunikační aplikace. K šíření této aplikace se použije phishingový email, který má veškeré náležitosti, kromě nebezpečnosti. Odkaz, který se ukrývá v této zprávě, vede na stránku vytvořenou právě IT oddělením, kde uživatele poučí o chybě, kterou udělal.

Po tzv. „zkoušce ohněm“ společnost vyhlásí tradiční celodenní školení kybernetické bezpečnosti jak pro uživatele, kteří se „chytili“ tak i pro uvědomělé uživatele. Uživatelé si mohou zkusit práci na napadených zařízeních, vidí několik typů útoků a jsou vedeni k vědomostem, pomocí kterých tyto útoky rozpoznají.

5.2.6 Otázka 11. -17. Školení o kybernetické bezpečnosti

K vytvoření nového stylu školení mě dovedli výsledky následujících otázek ohledně školení kybernetické bezpečnosti. Více jak polovina respondentů nebyla schopna popsat co je „Phishing“ (viz obr. 25). 80 % respondentů nevěděla, jak Phishing rozpoznat. Z anonymních výsledků bylo následně zjištěno, že uživatelé porušují pravidla využívání svěřeného hardwaru.



Obrázek 26 - Informace o vědomostech ze školení o kybernetické bezpečnosti

Na základě dalších výsledků byla nastavena nová technologická opatření, které zaručí vyšší bezpečnost uživatelských koncových zařízení. Jedná se tedy o propojení mobilního telefonu se zařízením. Jakmile se uživatel vzdálí od svého zařízení natolik, že se ztratí z dosahu Bluetooth, bude počítač automaticky uzamknut.

Zároveň bylo nastaveno skenování připojených zařízení. Ve chvíli připojení se spustí podprogram bezpečnostního frameworku, který nejdříve prozkoumá připojené zařízení. Pokud jej vyhodnotí, jako bezpečné umožní práci s tímto zařízením.

5.3 Navrhovaná doporučení

Jak již bylo zmíněno, dotazníkovému šetření byly podrobeny dvě skupiny zaměstnanců. Konkrétně šlo o zaměstnance bez IT vzdělání a zaměstnance s IT vzděláním. Celkově dotazník obsahoval 17 otázek, které byli rozděleny do 3 témat. První část dotazníku, konkrétně otázky 1. až 3., měla za cíl zjistit subjektivní pohled na pravidla ohledně kybernetické bezpečnosti ve zkoumané společnosti. Z výsledků první části můžeme konstatovat, že pohled uživatelů na daná pravidla jsou průměrná. Naopak ze strany IT jsou výsledky spíše nadprůměrné. Tím se potvrdila má domněnka, že uživatelé nejsou správně seznámeni s pravidly společnosti nebo jim nerozumí.

Ve druhé části dotazníku, konktrétně otázky 4. až 9., jsem se snažil zjistit pohled na stav zabezpečení uživatelských účtu a přístup k oprávněním ve zkoumané společnosti. Zde výsledky dotazníkového šetření potvrdili vyjádření silných stránek ve SWOT analýze. Zkoumaná společnost je z mého pohledu na velice dobré úrovni správy uživatelských účtů a oprávnění.

Ve třetí části, konkrétně otázky 10. až 17., jsem se zaměřil na interní školení o kybernetické bezpečnosti ve zkoumané společnosti. Navzdory tomu, že většina respondentů hodnotí školení průměrně až nadprůměrně, výsledky následujících otázek prokázaly silné nedostatky ve fyzické bezpečnosti uživatelských pracovních stanic a základních znalostí o bezpečnosti emailů.

Na základě výsledků výzkumu jsme našli společně s experty kybernetické bezpečnosti nejlepší možné řešení pro danou zkoumanou společnost. Doporučení, které jsem popsal ve své bakalářské práci, jsou ve své formě použitelné v jakékoli společnosti bez potřeby speciálních a drahých technologií. Základem silného bezpečnostního štítu společnosti jsou právě pravidla, kterými by se měla řídit každá osoba připojená do interní sítě firmy. Výsledky této práce splňují potřeby standardů ISO/IEC 2700 Systém řízení bezpečnosti informací pro bankovní instituce a standardy popsané v NIST o bezpečnosti hesel.

Na základě výsledků SWOT analýzy a dotazníkového šetření jsme společně s IT oddělením společnosti a personálním oddělením navrhli následující opatření a zlepšení.

- Nasazení pravidel Mail-Flow z pohledu zabezpečení emailové pošty popsané v teoretické části mé práce.
- Udržení opatření v bezpečnosti identit – zdokonalování a monitorování Role Based Access Control, vytváření rolí pomocí Principu minimálního oprávnění.
- Úprava bezpečnostních politik pro používání firemních zařízení, řízení změn, vzdálený přístup, Incident Response a řízení hesel.
- Udržet školení kybernetické bezpečnosti v praktické formě tréninku.
- Monitorovat uživatelská zařízení a zařízení k nim připojená bezpečnostním frameworkem.

6 DISKUSE

Bakalářská práce se zabývá tématem Kybernetické bezpečnosti z pohledu podnikové infrastruktury. Cílem této práce je popsat kybernetické hrozby, jak je rozpoznat, a hlavně jak se jim bránit.

Má bakalářská práce vznikla z důvodu rostoucího počtu kybernetických útoků ve světě. Kybernetické útoky jsou stále sofistikovanější a přesnější. Bohužel v dnešním světě není kybernetická bezpečnost ani z daleka hlavním zájmem většiny společností. Stále se dbá na projektech, které přináší zisk, zatímco kybernetická bezpečnost „jen" chrání před ztrátou. Doporučení popsané v mé bakalářské práci mají poukázat na nebezpečí číhající v kyberprostoru.

Jak popisuje portál www.embroker.com, Kyberkriminalita, která zahrnuje vše od krádeže nebo zpronevěry až po hacking a zničení dat, vzrostla v důsledku pandemie COVID-19 o 600 % (https://www.embroker.com/blog/cyber-attack-statistics/). Téměř každé odvětví muselo přijmout nová řešení, a to donutilo společnosti rychle hledat nová bezpečnostní řešení. Počítačová kriminalita bude stát společnosti po celém světě odhadem 10,5 bilionu dolarů ročně do roku 2025, oproti 3 bilionům dolarů v roce 2015. Při meziročním tempu růstu o 15 procent — Cybersecurity Ventures také uvádí, že počítačová kriminalita představuje největší převod ekonomického bohatství v historii. Podle zprávy Ponemon Institute's State of Cybersecurity Report hlásí malé a střední podniky po celém světě nedávné zkušenosti s kybernetickými útoky:

- Nedostatečná bezpečnostní opatření: 45 % uvádí, že jejich procesy jsou při zmírňování útoků neúčinné.
- Četnost útoků: 66 % zažilo kybernetický útok v posledních 12 měsících.
- Pozadí útoků: 69 % uvádí, že kybernetické útoky jsou stále cílenější.

Mezi nejčastější typy útoků na malé podniky patří:

- Phishing / sociální inženýrství: 57 %
- Kompromitovaná/ukradená zařízení: 33 %
- Krádež pověření: 30 %

Tím, že společnosti porozumí cílům útoků a důsledkům, vedoucí podniku může minimalizovat potenciál, získat hodnotu ve svém úsilí v oblasti kybernetické bezpečnosti, a dokonce zabránit budoucím útokům.

Dle mého názoru je velice zdrcující, že společnosti se doslova „honí“ za penězi místo toho, aby si chránili ty vydělané. Neuvědomují si, že v případě malé ochrany proti kybernetickým hrozbám stačí jeden úspěšný útok ransomwarem a společnosti nezbude nic jiného než opustit trh. Je překvapivé, že i přes to, že konkurence v různých oblastech odpadá právě z důvodu kybernetického útoku, jsou společnosti „v klidu“. Poslední věcí, které bych rád předal společnostem je: *„Obraťte svou pozornost ke kyberprostoru a nenechte svou společnost padnout jen kvůli maximalizaci výdělku. Čas a finance vyhrazené na zlepšení ochrany společnosti před kyberzločinci nejsou zahozené, ale mají svůj význam“*

Doporučení vytvořené v bakalářské práci popisují nejběžnější metody obrany proti takovým útokům. Vzhledem ke stavu kybernetické bezpečnosti ve společnostech po celé České republice jsou doporučení a metody založené více na pravidlech, které prakticky nic nestojí a dokážou snížit riziko útoku o několik procent.

Speciálně samotné zabezpečení uživatelů z technického pohledu nebo z pohledu pravidel a procesů je velkým tématem v téměř každé společnosti využívající IT. Tento výrok je podpořen diplomovou prací s názvem „Kybernetická bezpečnost koncových uživatelů v ČR a jejich ochota se zabezpečit“ od autora Bc. Jana Kleinera z Masarykovy univerzity (Fakulta sociálních studií) z roku 2020, kde autor říká:

„Hackerům stačí jediná zranitelnost, aby získali přístup do systému. Uživatel se však musí bránit všude, a je tudíž v počáteční nevýhodě. K základnímu zabezpečení však stačí pár poměrně jednoduchých a časově a finančně nenáročných kroků jako je vytvoření a management silných hesel, opatrnost při zadávání údajů (zejména s ohledem na phishing), zálohování, aktualizace apod. Skóre kyberbezpečnosti, které se o tyto postupy opírá, však nabývá pro uživatele pesimistických hodnot. Přes 23 % uživatelů je zabezpečeno podprůměrně. Jedná se ale o průměr v základním zabezpečení a „podprůměrně“ zde znamená tři až pět základních zranitelností.“

(https://is.muni.cz/th/xsa0b/Kleiner_Diplomova_prace.pdf)“, což potvrzuje výsledky z mého dotazníku.

Během mé praxe jsem spolupracovat s několika společnostmi na identifikaci kybernetických hrozeb. Bohužel se vyplnily nejhorší obavy a technická vyspělost některých společností (dokonce i poměrně známých) byla velice špatná až žádná. Není zde na místě svádět tyto chyby na nedostatek finančních prostředků či času. Nedostatky v technickém řešení kybernetické bezpečnosti podporuje diplomová práce z vysoké školy podnikání a práva s názvem „Kybernetická bezpečnost ve vybraných organizacích“ od autorky Bc. Venduly Vlčkové z roku 2020, kde zjišťujeme, že z tázaných třinácti společností má více než polovina potíže pokrýt základní technické parametry pro kybernetickou bezpečnost. Příkladem takového základního parametru můžou být pravidelné penetrační testy aplikací od externího dodavatele, Security Information and Event Management (SIEM) tedy bezpečnostní monitoring, chybějící oddělení kybernetické bezpečnosti s patřičnými oprávněními a postavením ve společnosti apod. I navzdory těmto nálezům si tázané společnosti myslí, že jsou připraveni na aktuální kybernetické hrozby. Což sami vyvrací v otázce zaměřující se na proběhlé incidenty tázaných společností, kde oznamují útoky typu malware, phishing, advanced persistent threat (což jsou cílené útoky na společnost), cryptolocker apod. Doporučení v mé bakalářské práci napomáhají se proti takovým útokům autonomně bránit nebo alespoň na ně včas upozornit. Nasadit SIEM nebo bezpečnostní framework není sice levnou disciplínou, ale v porovnání s potencionálními ztrátami stále vyhrávají.

V bakalářské práci zmiňuji standardy ISO 2700 a NIST, které jsou aktuálně společnostmi zabývající se audity společnostní z pohledu IT bezpečnosti vyžadovány. Součástí standardu ISO 2700 jsou podnormy ISO 27001 systém řízení bezpečnosti informací (ISMS), ISO 27002 soubor postupů a opatření, ISO 27003 směrnice pro implementaci ISMS a ISO 27005 řízení rizik na které navazuji ve své bakalářské práci. Stejné doporučení zaměřit se na splnění výše uvedených standardů dává ve své diplomové práci z roku 2015 autor Bc. Tomáš Stránský z Univerzity Hradec Králové s názvem „Bezpečnost podnikové IT infrastruktury a implementace ISO 2700“.

Školení kybernetické bezpečnosti bylo dalším tématem řešené v mé bakalářské práci. Spolupracující společnosti jsem doporučil zavést školení hrou. Zaměstnanci si mohli vyzkoušet práci s napadeným zařízením, hádali, zda prezentované obrázky emailových zpráv jsou nebo nejsou pokusem o phishing, zažili živý telefonát s podvodníkem vydávacího se za pracovníka podpory ze společnosti Microsoft. Do diskuse jsem se rozhodl zahrnout zpětnou vazbu samotných zaměstnanců z proběhlého školení ve formě rozhovoru. Zaměstnanců jsem se ptal na tři otázky:

- Jak jste si užil/a nový způsob školení kybernetické bezpečnosti?
- V porovnání s předchozím stylem školení, odnesl/a jste si více vědomostí?
- Byl/a byste schopen/na předat získané vědomosti dále?

Ze získaných odpovědí jsem vybral tři nejdetailnější.

Zaměstnanec 1 odpovídá: *„Školení jsem si moc užila. Oproti předchozímu školení je tu spoustu věcí, které si můžu na vlastní kůži vyzkoušet. Nejzajímavější pro mě bylo práce na počítači, kde právě probíhalo šifrování dat. V jednu chvíli pracujete, v druhé se vám počítač začne sekat, a nakonec se na vás zasměje čertova tvář s žádostí o zaslání peněz. Velice nepříjemný pocit. Na rozdíl od předchozích školeních, kde bylo zbytečně moc textů a odborných slov, kterým jsem nerozuměla, je nové školení velice příjemné a zábavné. Předávat vědomosti spíše nebudu. Asi bych nebyla schopna odpovědět na nějaké detailnější otázky.“*

Zaměstnanec 2 odpovídá: *„Je super, jak jde ze zdánlivě nudného a povinného školení udělat příjemně strávený den v práci. Nejvíc mě zaujalo, jak mohou vypadat podvodné emaily. Ty, co mi chodí do mé osobní pošty jsou jasně rozeznatelné, ale zprávy, které nám tu dnes ukazovali byly velice promakané a s velkou pravděpodobností bych jim věřil. Ze školení si rozhodně odnáším způsob kontroly podezřelého emailu. Do dnes jsem netušil, že email může mít neviditelnou hlavičku. Předávám informace doma denně dětem. Mám 2 syny pubertálního věku a už se u nás dokonce řešilo odcizení herního účtu, takže jsem rád za každou novinku v této oblasti.*

Většina zaměstnanců, kteří si školením prošli si nový způsob pochvalují a těší se na další možnost se jej zúčastnit. Dostal jsem pár nápadů, které by zaměstnanci rádi

probrali na příštím sezení jako například konverze měny v zahraničí, zabezpečení domácí sítě a další.

Výsledkem práce je, že spolupracující společnost je lépe chráněna před kybernetickými hrozbami. Nové a upravené procesy se nasadili velice rychle a umožnili společnosti začít upravovat aktuální stav domény a sítě dle nových pravidel. Během implementace těchto úprav společnost utratila minimum finančních prostředků k dosažení maximálního potenciálu navrhovaných řešení. Díky navrhnutým aktivitám a výsledkům jsme se domluvili se spolupracující společností na dalších návrzích a implementaci bezpečnostních mechanismů ve společnosti.

7 ZÁVĚR

V bakalářské práci byla zpracována problematika aktuálních hrozeb, podnikatelských subjektů a jejich kategorizace, a popsány aktuální metody pro zabezpečení podnikové infrastruktury.

Na základě sesbíraných informací, výsledků dotazníku a osobních zkušeností z oboru o přímočarém doporučovaném způsobu zabezpečení infrastruktury byla vytvořena doporučení z hlediska organizačních změn, procesních změn a technologických úprav s cílem kybernetickou bezpečnost pozvednout na úroveň ochrany 21. století.

Během zpracovávání této práce byly popisované metody a změny nasazovány a testovány v popisované společnosti ve spolupráci s personálním a IT oddělením s velice pozitivním výsledkem. Cíl práce byl splněn a přímo implementován do společnosti, kde z nejnovějších výsledků bylo dosaženo ke zlepšení kybernetické bezpečnosti.

Zpracování této práce mě obohatilo jak v osobním, tak i v profesním životě a motivovalo mě pokračovat v šíření povědomí o bezpečnostních hrozbách a učit společnosti jakým způsobem se proti nim chránit. Zároveň napomohlo jedné společnosti zdokonalit přístup k řešení problému kybernetické bezpečnosti a pozvedlo její úroveň.

8 SEZNAM POUŽITÝCH ZKRATEK

IT – Informační bezpečnost

BEC – Business Email Compromise

HTML – Hypertext Markup Language

IoT – Internet of Things

IP – Ingress Protection

DNS – Domain Name System

URL – Uniform Resource Locator

PIN – Personal Identification Number

SQL – Structured Query Language

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

AWS – Amazon Web Sevices

QR – Quick Response Code

IAM – Identity and Access Management

POLP – Principle of least privilege

FIPS – Federal Information Processing Standards

GPS – Global Positioning System

OTP – One-Time Password

OS – Operační Systém

SaaS – Software as a service

RaaS – Ransomware as a service

MFA – Vícefaktorové ověření

RBAC – Role Based Access Control

APT – Acceptable Use Policy

VPN – Virtual Private Network

AD – Active Directory

SIEM – Security Information and Event Management

9 SEZNAM POUŽITÉ LITERATURY

[1] ALKHALIL, Zainab, Chaminda HEWAGE, Liqaa NAWAF a Imtiaz KHAN. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science. 2021, 3. ISSN 2624-9898. Dostupné z: doi:10.3389/fcomp.2021.563060

[2] SOOD, Aditya K. a Sherali ZEADALLY. Drive-By Download Attacks: A Comparative Study. IT Professional. 2016, 18(5), 18-25. ISSN 1520-9202. Dostupné z: doi:10.1109/MITP.2016.85

[3] BREWER, Ross. Ransomware attacks: detection, prevention and cure. Network Security. 2016, 2016(9), 5-9. ISSN 13534858. Dostupné z: doi:10.1016/S1353-4858(16)30086-1

[4] ARCE, Daniel G. Malware and market share: detection, prevention and cure. Journal of Cybersecurity. 2018, 4(1), 5-9. ISSN 2057-2085. Dostupné z: doi:10.1093/cybsec/tyy010

[5] LI, He, Qiang LIU a Jiliang ZHANG. A survey of hardware Trojan threat and defense: detection, prevention and cure. Integration. 2016, 55(1), 426-437. ISSN 01679260. Dostupné z: doi:10.1016/j.vlsi.2016.01.004

[6] MALLIK, Avijit, Abid AHSAN, Mhia Md. Zaglul SHAHADAT a Jia-Chi TSOU. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science. 2019, 77-92. ISSN 25618148. Dostupné z: doi:10.5267/j.ijdns.2019.1.001

[7] OSANAIYE, Opeyemi, Kim-Kwang Raymond CHOO a Mqhele DLODLO. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications. 2016, 67, 147-165. ISSN 10848045. Dostupné z: doi:10.1016/j.jnca.2016.01.001

[8] ISHIKURA, Naotake, Daishi KONDO, Vassilis VASSILIADES, Iordan IORDANOV a Hideki TODE. DNS Tunneling Detection by Cache-Property-Aware Features. IEEE Transactions on Network and Service Management. 2021, 18(2), 1203-1217. ISSN 1932-4537. Dostupné z: doi:10.1109/TNSM.2021.3078428

[9] BOSNJAK, L., J. SRES a B. BRUMEN. Brute-force and dictionary attack on hashed real-world passwords. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018,

2018, 1161-1166. ISBN 978-953-233-095-3. Dostupné z: doi:10.23919/MIPRO.2018.8400211

[10] ABIKOYE, Oluwakemi Christiana, Abdullahi ABUBAKAR, Ahmed Haruna DOKORO, Oluwatobi Noah AKANDE a Aderonke Anthonia KAYODE. A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm. EURASIP Journal on Information Security. 2020, 2020(1). ISSN 2510-523X. Dostupné z: doi:10.1186/s13635-020-00113-y

[11] KOLOUCH, Jan a Pavel BAŠTA, CyberSecurity, Praha: CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7

[12] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019, ISBN 978-80-7380-765-8

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

[14] Rising, P., Microsoft 365 Security Administration: MS-500 Exam Guide: Plan and implement security and compliance strategies for Microsoft 365 and hybrid environments, Packt Publishing, 2020, ISBN 978-1838983123

[15] Kybernetická bezpečnost [online]. Národní úřad pro kybernetickou bezpečnost, 2018 [cit. 2022-03-11]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

[16] European Union Agency for Network and Information Security, The SANS Institute

[17] Check Point 2022 Security Report [online]. Check Point Research Center, 2022 [cit. 2022-03-11]. Dostupné z: https://pages.checkpoint.com/cyber-security-report-2022.html

[18] KAMENÍČEK, Lukáš. *Kybernetická bezpečnost z pohledu podnikové informatiky*. Praha, 2016. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Buchalcevová, Alena.

[19] ČESKO. § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů – znění od 1. 7. 2017. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

[20] ČESKO. § 35 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty – znění od 1. 1. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-235#p35-2

[21] ČESKO. § 31 odst. 2 zákona č. 563/1991 Sb., o účetnictví – znění od 1. 1. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1991-563#p31-2

[22] ČESKO. Část 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 1. 9. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#cast1

[23] ČESKO. § 7 zákona č. 586/1992 Sb., České národní rady o daních z příjmů – znění od 1. 1. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1992-586#p7

[24] ČESKO. § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) - znění od 1. 2. 2022. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240#p2

[25] ČESKO. § 504 zákona č. 89/2012 Sb., občanský zákoník – znění od 1. 7. 2021. In: Zákony pro lidi.cz [online]. © AION CS 2010-2022 [cit. 25. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89#p504

[26] *Spotify Hit with a Credential Stuffing Attack with Data from Another Breach* [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://www.bitdefender.com/blog/hotforsecurity/spotify-hit-with-a-credential-studding-attack-with-data-from-another-breach

[27] *Microsoft Exchange Hack: What You Need to Know and How You Can Remain Protected* [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://www.checkpoint.com/latest-cyber-attacks/microsoft-exchange-hack/

[28] *EU Banking Authority Hacked As Microsoft Exchange Attacks Continue* [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://www.forbes.com/sites/daveywinder/2021/03/09/eu-banking-authority-hacked-as-microsoft-exchange-attacks-continue/?sh=20c0b9f2fe06

[29] *Cyberattack Forces a Shutdown of a Top U.S. Pipeline* [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

[30] *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom* [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[31] Black market for fake vaccine certificates booms [online]. 2021 [cit. 2022-03-16]. Dostupné z: https://blog.checkpoint.com/2021/09/14/amid-vaccine-mandates-fake-vaccine-certificates-become-a-full-blown-industry/

[32] National Institute of Standards and Technology [online]. Standards for Security Categorization of Federal Information and Information Systems. 2004. Dostupné z: doi:10.6028/NIST.FIPS.199

[33] Journal of International Social Research. 10. 2017. ISSN 1307-9581. Dostupné z: http://sosyalarastirmalar.com/cilt10/sayi51_pdf/6iksisat_kamu_isletme/gurel_emet.pdf

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK

12 SEZNAM PŘÍLOH

12.1 Příloha A – Dotazník

Informace o zabezpečení

Jakým způsobem byste ohodnotili zabezpečení emailů ve vaší společnosti?

- 1
- 2
- 3
- 4
- 5

Jakým způsobem byste ohodnotili zabezpečení identit ve vaší společnosti?

- 1
- 2
- 3
- 4
- 5

Jakým způsobem byste ohodnotili firemní pravidla z pohledu kybernetické bezpečnosti?

- Používání firemních zařízení
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla
- Řízení změn
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla

    - Žádná pravidla
- Incident Response
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla
- Vzdálený přístup
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla
- Řízení obchodních partnerů
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla
- Řízení hesel
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla
- Uchovávání dat
    - Přísná pravidla
    - Přísnější pravidla
    - Rozumná pravidla
    - Nějaká pravidla
    - Žádná pravidla

Zabezpečení z pohledu identit / uživatelských účtů

Používáte v rámci řízení identit Role Based Access Control (RBAC)?
Oprávnění na základě role

- Ano
- Ne

Používáte v rámci řízení identit Princip minimálního oprávnění (POLP)?
Oprávnění ne vetší, než pracovní náplň vyžaduje

- Ano
- Ne

Využíváte heslo silnější než 16 znaků s různou kombinací symbolů, čísel a písmen?

- Ano
- Ne

Jste nuceni měnit si heslo v pravidelném intervalu?

- Ano
- Ne

Mají všichni uživatelé vynucené vícefaktorové ověření?

- Ano
- Ne

Využíváte firemní účet na osobních zařízeních?
Emaily na osobním mobilním telefonu, vzdálený přístup ze soukromého počítače

- Ano
- Ne

Jste nuceni měnit si heslo v pravidelném intervalu?

- Ano
- Ne

Kvalita školení o kybernetické bezpečnosti

Jakým způsobem byste ohodnotili firemní školení na téma kybernetická bezpečnosti?

- 1
- 2
- 3
- 4
- 5

Koná se ve vaší společnosti pravidelné školení kybernetické bezpečnosti?

- Ano
- Ne

Víte, co je Phishing?

- Ano
- Ne

Víte, jak phishingový útok rozpoznat?

- Ano
- Ne

Využíváte firemní zařízení pro osobní účely?
Sociální sítě, sdílení dat, ukládání osobních dat (fotografie, videa, hudba)

- Ano
- Ne

Připojujete k firemnímu zařízení osobní přenosná média?
Flash Disky, mobilní telefon, přenosný disk

- Ano
- Ne

Zamykáte si počítač kdykoli jej nemáte v dohledu?

- Ano
- Ne

Aktualizujete si své svěřené zařízení?

- Ano
- Ne