UNIVERZITA PARDUBICE

Fakulta ekonomicko – správní

DIPLOMOVÁ PRÁCE

2024 **Bc. Michal Hroch**

UNIVERZITA PARDUBICE

Fakulta ekonomicko – správní

KYBERNETICKÁ BEZPEČNOST A OCHRANA DAT VE VYBRANÉM PODNIKU

Bc. Michal Hroch

Diplomová práce

2024

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michal Hroch**
Osobní číslo:	**E22761**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Kybernetická bezpečnost a ochrana dat ve vybraném podniku**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem diplomové práce je provést analýzu současného stavu kybernetické bezpečnosti a ochrany dat ve vybraném podniku. Navrhnout opatření ke zlepšení bezpečnostní situace vybraného podniku.

Osnova:

- Vymezení pojmů z oblasti kybernetické bezpečnosti.
- Formulace problému.
- Hodnocení zabezpečení v dané firmě.
- Doporučení nápravných opatření.

Rozsah pracovní zprávy: **cca 55 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

BEAVER, Kevin a Ira WINKLER. *Cybersecurity All-in-One For Dummies*. Hoboken, New Jersey, USA: John Wiley, 2023. ISBN 139415285X.
KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti (č. 181/2014)*. Praha 3: Wolters Kluver, 2015. ISBN 978-80-7478-818-5.
SMEJKAL, Vladimír. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. 2. vydání. Praha: Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Vedoucí diplomové práce: **Ing. Kateřina Příhodová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2023**
Termín odevzdání diplomové práce: **30. dubna 2024**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlášení

Prohlašuji:
Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 17. 5. 2024

Bc. Michal Hroch v.r.

PODĚKOVÁNÍ

Chtěl bych poděkovat své vedoucí práce za její pomoc a rady při řešení a spoustě cenných rad při psaní práce. Dále bych chtěl poděkovat své přítelkyni za psychickou podporu.
V neposlední řadě chci poděkovat rodině za podporu v době mého studia.

Bc. Michal Hroch

ANOTACE

Tato diplomová práce se zaměřuje na problematiku kyberbezpečnosti a ochrany dat ve vybraném podniku. V průběhu práce byla provedena analýza kybernetické bezpečnosti s pomocí metodologie, která zahrnovala analýzu ochrany dat, ochranu proti phishingu a ransomwaru, osobní rozhovory se zaměstnanci, simulaci phishingového útoku a skenování zranitelností. Práce identifikovala nedostatky v bezpečnostním systému a navrhla konkrétní nápravná opatření. Výsledky této práce přinášejí nejenom nové poznatky o kybernetické bezpečnosti v konkrétním podniku, ale také metodiku pro zlepšení bezpečnostních opatření v podobných organizacích.

KLÍČOVÁ SLOVA

Kyberbezpečnost, ochrana dat, phishing, ransomware

TITLE

CyberSecurity and data protection in business

ANNOTATION

This diploma thesis focuses on the issue of cyber security and data protection in the selected company. During the work, a cyber security analysis was carried out using a methodology that included data protection analysis, phishing and ransomware protection, personal interviews with employees, phishing attack simulation and vulnerability scanning. The work identified deficiencies in the security system and proposed specific corrective measures. The results of this work bring not only new knowledge about cyber security in a specific company, but also a methodology for improving security measures in similar organizations.

KEYWORDS

CyberSecurity, data protection, phishing, ransomware

OBSAH

SEZNAM ZKRATEK

IT	Informační Technologie
ISO/IEC	International Organization for Standardization/International Electrotechnical commission (Mezinárodní organizace pro normalizaci/Mezinárodní elektrotechnická komise)
ISMS	Information Security Management Systém (Systém řízení bezpečnosti informací)
CSF	CyberSecurity Framework (Rámec kybernetické bezpečnosti)
NIST	National Institute of Standards and Technology (Národní institut standardů a technologie)
NIS	Network and Information Security (Síťová a informační bezpečnost)
EU	Evropská Unie
ČR	Česká republika
DDoS	Distributed Denial-of-Service (Distribuované odepření služby)
USB	Universal Serial Bus (Univerzální sériová sběrnice)
IDS/IPS	Intrusion Detection System/Intrusion Prevent Systém (Systém pro detekci/prevenci průniku)
UDP	User Datagram Protocol (Protokol pro přenos datagramů)
ICMP	Internet Control Message Protocol (Internetový protokol pro služební informace)
SYN	Synchronize (Synchronizace)
HTTP	HyperText Transfer Protokol (HyperTextový transportní protokol)
MitM	Man in the Middle (Člověk uprostřed)
DNS	Domain Name Systém (Systém doménových jmen)
ARP	Address Resolution Protocol (Protokol pro získání linkové adresy)
HTTPS	HyperText Transfer Protokol Secure (Zabezpečený hypertextový transportní protokol)
SSL	Secure Sockets Layer (Vrstva bezpečnostních socketů)
Wi-Fi	Wireless Fidelity (Bezdrátová síť)
VPN	Virtual Private Network (Virtuální soukromá síť)
ICT	Information and Communication Technologies (Informační a komunikační technologie)
BMS	Building Management Systém (Systémy řízení budov)

HD	Hard Drive (Pevný disk)
DMARC	Domain-based Message Authentication, Reporting and Conformance (Ověřování, hlášení a shoda zpráv v dooméně)
CVSS	Common Vulnerability Scoring Systém (Společný systém hodnocení zranitelností)
IP	Internet Protocol (Internetový protokol)
DKIM	DomainKeys Identified Mail (email podepsaný doménovým klíčem)
SPF	Sender Policy Framework (Rámec pro ochranu proti spamu)
NÚKIB	Národní Úřad pro Kybernetickou a Informační Bezpečnost
KB	Kybernetická bezpečnost

SEZNAM ILUSTRACÍ

SEZNAM TABULEK

ÚVOD

Rozvoj digitálních technologií a internetu v posledních letech přinesl mnoho pozitivních změn do našich životů. Díky nim jsme schopni rychleji a efektivněji komunikovat, sdílet informace a řešit složité problémy. Nicméně, s tímto růstem digitálního světa se zvyšuje i potenciál pro kybernetické útoky a hrozby, které mohou ohrozit naši bezpečnost a integritu na internetu.

Kybernetická bezpečnost a ochrana dat se tak stávají neodmyslitelnou součástí našeho digitálního života. Každý den se setkáváme s novými technologiemi a digitálními platformami, které usnadňují naše každodenní činnosti, ale zároveň otevírají nové možnosti pro kybernetické útoky. Od bankovních účtů po sociální média a firemní sítě, žádný sektor není imunní vůči těmto hrozbám.

Důvodem, proč je kybernetická bezpečnost tak důležitá, je ochrana našeho soukromí a bezpečnost jednotlivců. V digitálním světě, kde se naše osobní údaje neustále sbírají a zpracovávají, je klíčové zajistit, aby tyto informace zůstaly v bezpečí a nebyly zneužity k nekalým účelům. Navíc, v korporátním prostředí, kde jsou firemní data kritickým aktivem, je nezbytné chránit tyto informace před kybernetickými útoky a zabezpečit integritu a spolehlivost firemní infrastruktury.

Každý úspěšný kybernetický útok může mít katastrofální následky nejen na finanční stabilitu a pověst organizace, ale také na důvěru zákazníků a obchodní partnery. Ztráty způsobené kybernetickými útoky mohou být enormní, ať už jde o finanční prostředky, důvěrné informace nebo důvěru veřejnosti. Proto je klíčové, abychom se aktivně věnovali prevenci a ochraně proti kybernetickým hrozbám a zajistili, že naše digitální prostředí zůstane bezpečné a spolehlivé.

Cílem této práce je analyzovat a zhodnotit současné zabezpečení firemní infrastruktury a navrhnout opatření pro jeho zlepšení. Tato analýza bude zahrnovat identifikaci slabých míst a zranitelností v systémech a procesech firmy, stejně jako provedení metodiky, která zahrnuje skenování zabezpečení, testování zranitelností a další diagnostické postupy. Na základě zjištěných nedostatků budou navržena konkrétní bezpečnostní opatření a doporučení pro zlepšení ochrany firemních aktiv a citlivých dat. Tato práce bude také poskytnout firmě komplexní přehled o stavu jejího zabezpečení a navrhnout konkrétní kroky k zajištění bezpečnosti a ochrany před současnými i budoucími hrozbami v kybernetickém prostředí.

1 Vymezení pojmů z oblasti kybernetické bezpečnosti

Kybernetická bezpečnost se zabývá ochranou systémů, sítí a programů před digitálními útoky. Tyto útoky jsou často zaměřeny na přístup, změnu nebo zničení citlivých informací, vyvádění uživatelů z provozu a vydírání peněz od uživatelů. Kybernetická bezpečnost je tedy klíčová pro ochranu integrity, důvěrnosti a dostupnosti informací. Vzhledem k rostoucímu počtu uživatelů, zařízení a programů v moderním podnikání, stejně jako kvůli stále se zvyšujícímu objemu citlivých dat, která se stále častěji ukládají, stává se kybernetická bezpečnost stále důležitější. [1], [2]

Na druhé straně, informační bezpečnost se zaměřuje na ochranu citlivých informací před neoprávněným přístupem a zneužitím, a to bez ohledu na to, zda jsou tyto informace digitální nebo fyzické. Zahrnuje řadu procesů a metod, které jsou navrženy tak, aby ochránily osobní údaje, duševní vlastnictví, datové protokoly a informace o zařízeních a službách. [1], [2]

Hlavní rozdíl mezi kybernetickou a informační bezpečností spočívá v rozsahu ochrany. Kybernetická bezpečnost se soustředí primárně na digitální bezpečnost, tj. ochranu proti útokům přes internet nebo jiné formy sítí. Naopak, informační bezpečnost je širší pojem, který zahrnuje ochranu informací ve všech formách, včetně fyzické ochrany dokumentů, telefonních hovorů a dalších forem i ne-digitální komunikace. [1], [2]

Kybernetická hrozba je potenciální nebezpečí nebo riziko, které vychází z možného úmyslného či neúmyslného poškození, zneužití, nebo narušení informačních systémů, sítí, dat či služeb prostřednictvím kybernetických útoků. Tato hrozba může vzniknout ze strany jednotlivců, skupin nebo organizací, kteří se snaží získat neoprávněný přístup k citlivým informacím, narušit fungování systémů nebo způsobit škody prostřednictvím různých technik. Kybernetické hrozby mohou mít širokou škálu dopadů, včetně finančních ztrát, porušení soukromí, narušení důvěryhodnosti a integrity dat, a mohou postihnout jednotlivce, organizace, nebo dokonce celé národy. [1], [2]

Kybernetický útok je úmyslná akce nebo série akcí, které jsou zaměřeny na narušení, poškození, nebo zneužití informačních systémů, sítí, dat nebo služeb. Tyto útoky mohou být prováděny jednotlivci, skupinami, nebo organizacemi a mohou mít různé cíle, včetně získání neoprávněného přístupu k citlivým informacím, poškození systémů, nebo způsobení finančních ztrát. Existuje mnoho druhů kybernetických útoků, včetně malware, phishing, ransomware,

útoků typu Distributed Denial of Service (DDoS), úniků dat, a mnoho dalších. Tyto útoky se často vyvíjejí a mění se spolu s technologickým vývojem a jsou jedním z hlavních rizik, kterým čelíme v digitálním prostředí. [1], [2]

Jedním z klíčových aspektů kybernetické bezpečnosti je ochrana proti kybernetickým hrozbám a útokům, jako jsou malware, phishing, ransomware, a další typy útoků, které se snaží proniknout do sítí a systémů. Ochrana před těmito hrozbami vyžaduje neustálé monitorování a aktualizaci bezpečnostních opatření, jako jsou firewally, antivirové programy a další technologie pro detekci a prevenci. [1], [2]

Informační bezpečnost, na druhou stranu, zahrnuje řadu politik a postupů, které mají za cíl udržet informace v bezpečí před jakýmkoli druhem neoprávněného přístupu nebo zneužití. To zahrnuje opatření jako je správa přístupových práv, šifrování dat, fyzické zabezpečení datových center a bezpečnostní školení zaměstnanců. [1], [2]

V kontextu moderních podniků se obě oblasti, tedy kybernetická a informační bezpečnost, vzájemně doplňují. Efektivní strategie bezpečnosti vyžaduje integraci obou těchto aspektů, aby se zajistila komplexní ochrana proti širokému spektru hrozeb. Podniky a organizace se musí zaměřit nejen na technologické aspekty bezpečnosti, ale také na aspekty lidské a procesní, aby byly schopny čelit různým formám hrozeb a zabezpečit tak svá data a systémy na všech úrovních. [3]

2 Přehled relevantních standardů

Standardy v oblasti kybernetické bezpečnosti jsou zásadní pro ochranu informací a IT infrastruktur v digitálním světě. Využívání těchto standardů umožňuje organizacím vytvořit, implementovat a udržovat efektivní systémy ochrany proti neustále se vyvíjejícím kybernetickým hrozbám. Standardy poskytují rámec pro nejlepší postupy a procedury, pomáhají identifikovat a řídit rizika, a zároveň usnadňují dodržování právních a regulačních požadavků. S jejich pomocí mohou organizace zvýšit důvěru zákazníků a partnerů v jejich schopnost ochránit citlivá data.

2.1 ISO/IEC 27000

Mezinárodní standardy ISO/IEC 27000 jsou klíčové pro efektivní management a ochranu informačních aktiv v kybernetickém prostředí. Série ISO/IEC 27000, která se skládá z několika navzájem souvisejících standardů, nabízí komplexní rámec pro nastavení, implementaci, udržování a neustálé zlepšování systémů managementu informační bezpečnosti (ISMS). Tyto standardy jsou navrženy tak, aby byly aplikovatelné v různých organizacích, bez ohledu na jejich velikost nebo odvětví. [3]

Hlavním pilířem této série je ISO/IEC 27001, který poskytuje požadavky pro zavedení, provoz a udržování ISMS. Standard klade důraz na identifikaci a řízení rizik, která souvisí s informačními aktivy, a zajišťuje, že organizace systematicky řeší bezpečnostní otázky. Klíčovým prvkem ISO/IEC 27001 je proces hodnocení rizik, který vyžaduje, aby organizace prováděla pravidelnou analýzu hrozeb a zranitelností, na jejichž základě pak stanoví adekvátní bezpečnostní kontroly. [3]

ISO/IEC 27002, který funguje jako doprovodný standard k ISO/IEC 27001, poskytuje soubor nejlepších postupů a doporučení pro implementaci bezpečnostních kontrol. Tyto kontrolní mechanismy pomáhají organizacím chránit se před širokým spektrem kybernetických hrozeb a zajišťují ochranu důvěrnosti, integrity a dostupnosti informačních systémů. [3]

Pro cloudové služby jsou relevantní standardy ISO/IEC 27017 a ISO/IEC 27018. ISO/IEC 27017 poskytuje pokyny pro bezpečnostní aspekty cloud computingu, včetně řízení přístupu, operací, virtualizace a incident managementu. ISO/IEC 27018 se pak zaměřuje na ochranu osobních údajů uložených v cloudu, což je klíčové pro organizace, které zpracovávají osobní data svých klientů. [3]

Implementace a certifikace podle ISO/IEC 27000 umožňuje organizacím demonstrovat závazek k ochraně informací, což je nezbytné v dnešním digitálním světě. Nejenže pomáhá v budování důvěry u zákazníků a obchodních partnerů, ale také usnadňuje dodržování právních a regulačních požadavků v oblasti ochrany dat. Význam těchto standardů je pak dán jejich globálním uznáním a adaptabilitou. Organizace po celém světě je považují za zlatý standard pro nastavení a udržování bezpečnostních politik a procedur. Implementace ISO/IEC 27000 znamená pro organizace nejen zvýšení bezpečnosti, ale i zlepšení celkového managementu a efektivity operací. Certifikace podle ISO/IEC 27001 a dalších standardů v rámci série ISO/IEC 27000 vyžaduje systematický přístup, který zahrnuje interní audit, řízení dokumentace, neustálé vzdělávání a školení zaměstnanců a průběžnou revizi a zlepšování bezpečnostních procesů. Toto vyžaduje značné úsilí a zdroje, ale výsledný přínos v podobě lepší ochrany informací a zvýšené důvěryhodnosti organizace je neocenitelný. [3]

2.2 NIST Cybersecurity Framework

NIST Cybersecurity Framework (CSF) je jeden z klíčových standardů pro řízení a minimalizaci kybernetických rizik v organizacích. Vyvinutý Národním institutem pro standardy a technologie (NIST) ve Spojených státech, tento rámec poskytuje sadu průmyslově uznávaných nejlepších postupů a pokynů, které pomáhají organizacím lépe porozumět, řídit a snižovat kybernetická rizika. NIST CSF je navržen tak, aby byl flexibilní a snadno přizpůsobitelný různým typům organizací, včetně těch v soukromém sektoru, vládních agenturách a vzdělávacích institucích.

NIST CSF je strukturován do pěti hlavních funkcí: Identify, Protect, Detect, Respond a Recover. Tyto funkce poskytují široký přehled o tom, jak organizace může řídit a minimalizovat kybernetická rizika na všech úrovních.

- **Identify** – funkce pomáhá organizacím rozpoznat a pochopit své prostředí a kybernetická rizika, která jim hrozí. Zahrnuje identifikaci aktiv, obchodního prostředí, zranitelností a souvisejících hrozeb.
- **Protect –** zaměřuje se na vývoj a implementaci vhodných ochranných opatření, aby zabezpečila kritická aktiva. Zahrnuje přístupovou kontrolu, ochranu dat, informační ochranu a školení zaměstnanců.

- **Detect –** popisuje potřebné aktivity pro identifikaci výskytu kybernetického incidentu. To zahrnuje monitorování sítí, detekci anomálií a událostí, a hodnocení bezpečnostního stavu.
- **Respond –** funkce definuje akce, které je třeba podniknout v případě kybernetického incidentu, včetně řízení incidentů, analýzy a mitigace dopadů.
- **Recover –** zaměřuje se na obnovu schopností a služeb po kybernetickém incidentu, včetně plánů obnovy a komunikace s veřejností a zúčastněnými stranami.

NIST CSF je ceněn pro svou flexibilitu a schopnost být přizpůsoben individuálním potřebám organizace. Jeho využití může pomoci organizacím nejen v řízení a minimalizaci rizik, ale také ve zlepšení celkové bezpečnostní kultury a v dodržování regulatorních a legislativních požadavků.

Při porovnání NIST CSF s ISO/IEC 27000, je důležité si uvědomit, že oba tyto rámce mají podobné cíle, ale odlišují se ve svém přístupu a struktuře. Zatímco série ISO/IEC 27000 poskytuje více preskriptivní přístup s podrobnými specifikacemi pro systémy managementu informační bezpečnosti a je zaměřena na globální použití, NIST CSF je více flexibilní a poskytuje široký rámec pro různé typy organizací. ISO/IEC 27000 se zaměřuje především na procesy a politiky, zatímco NIST CSF nabízí širší pohled na celkové řízení rizik a bezpečnostní praxi.

Výběr mezi těmito rámci závisí na konkrétních potřebách a cílech organizace, stejně jako na jejím regulačním a obchodním prostředí. Mnoho organizací zjistí, že kombinace obou přístupů nabízí nejlepší řešení pro komplexní a efektivní kybernetickou bezpečnost. [4]

2.3 NIS (2)

Směrnice o bezpečnosti sítí a informací (NIS), která byla přijata Evropskou unií, představuje základní legislativní rámec pro zvýšení úrovně kybernetické bezpečnosti v členských státech. Cílem této směrnice je zajistit vysokou úroveň ochrany sítí a informačních systémů, které jsou klíčové pro fungování vnitřního trhu a pro ochranu občanů EU před kybernetickými hrozbami. Směrnice NIS se vztahuje především na poskytovatele základních služeb v klíčových sektorech, jako jsou energetika, doprava, bankovnictví, infrastruktura finančního trhu,

zdravotnictví a dodávka pitné vody, stejně jako na digitální služby, jako jsou cloudové služby, online tržiště a vyhledávače. [5]

Podstatou směrnice NIS je stanovení společných bezpečnostních požadavků pro tyto klíčové operátory a poskytovatele služeb. Směrnice vyžaduje, aby dotčené subjekty přijaly vhodná technická a organizační opatření k řízení rizik pro bezpečnost svých sítí a informačních systémů. Kromě toho musí být schopny nahlásit závažné kybernetické incidenty příslušným národním úřadům. Důraz je kladen na zajištění, že sítě a systémy jsou odolné proti incidentům, a že v případě incidentu jsou k dispozici efektivní reakční plány. [5]

NIS 2, která je revizí a rozšířením původní směrnice, zahrnuje řadu významných aktualizací a změn. Jedním z hlavních rozšíření NIS 2 je zahrnutí dalších sektorů a typů organizací, včetně veřejné správy a dalších odvětví, považovaných za důležité pro ekonomiku a společnost, jako jsou potravinářství, výroba léčiv, a chemický průmysl. Tato změna reflektuje rostoucí závislost společnosti na široké škále digitálních služeb a potřebu rozšířit oblast působnosti kybernetické bezpečnosti. Dále NIS 2 posiluje bezpečnostní požadavky, přičemž klade větší důraz na řízení rizik a zavádí přísnější dohled a sankční režim pro porušení bezpečnostních požadavků. Zvýšená pozornost je věnována také přeshraniční spolupráci a výměně informací mezi členskými státy EU, což je klíčové pro efektivní reakci na kybernetické incidenty a pro zajištění vysoce účinné a koordinované obrany proti hrozbám. [5]

Porovnáme-li NIS a NIS 2 s ISO/IEC 27000 a NIST CSF, je zřejmé, že zatímco ISO a NIST poskytují flexibilní rámce pro organizační kybernetickou bezpečnost a nejlepší postupy, NIS a NIS 2 jsou zaměřeny na stanovení a vynucování minimálních bezpečnostních standardů a požadavků na hlášení na úrovni států EU. Směrnice NIS a NIS 2 přinášejí dodatečnou vrstvu regulace a standardizace, která doplňuje organizačně orientované přístupy ISO a NIST, a zároveň zvyšuje povědomí o důležitosti ochrany sítí a informací v širším, mezinárodním kontextu. [3], [4], [5]

2.4 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti v České republice představuje klíčový legislativní prvek v rámci národní bezpečnostní strategie. Tento zákon byl přijat s cílem posílit obranu proti kybernetickým hrozbám a zabezpečit klíčové informační systémy a služby, které jsou nezbytné

pro fungování státu a společnosti. Jeho hlavním účelem je zajistit vysokou úroveň ochrany proti kybernetickým útokům, a tím přispět k celkové kybernetické odolnosti země. [6]

Zákon definuje povinnosti a zodpovědnosti různých subjektů, včetně provozovatelů základních služeb, poskytovatelů důležitých služeb a orgánů veřejné moci. Provozovatelé základních služeb, jako jsou energetika, doprava, zdravotnictví, bankovnictví a další klíčové sektory, jsou povinni zavést a udržovat adekvátní bezpečnostní opatření pro ochranu svých sítí a informačních systémů. Tyto požadavky zahrnují přijetí efektivních bezpečnostních politik, implementaci technických a organizačních opatření pro prevenci a detekci kybernetických útoků, a vytvoření plánů pro reakci na incidenty a obnovu po nich. Kromě toho, zákon stanovuje povinnost hlásit významné kybernetické incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) nebo jinému příslušnému orgánu. Toto hlášení je klíčové pro efektivní reakci na kybernetické hrozby a pro koordinaci mezi různými subjekty a vládními orgány. NÚKIB hraje centralizovanou roli v kybernetické bezpečnosti v ČR, poskytuje směrnice a podporu pro subjekty podle zákona a monitoruje dodržování bezpečnostních standardů a požadavků. [6]

Zákon také zavádí systém certifikace a akreditace pro poskytovatele kybernetických bezpečnostních služeb. Tento systém zajišťuje, že služby a produkty používané pro zabezpečení klíčových sítí a systémů splňují určité bezpečnostní standardy a jsou spolehlivé. [6]

Porovnáme-li český zákon o kybernetické bezpečnosti se standardy jako ISO/IEC 27000 nebo NIST CSF, je zřejmé, že zákon představuje více regulativní a přikazující přístup, zatímco ISO a NIST poskytují flexibilní rámce pro organizační bezpečnostní řízení. Zatímco ISO a NIST se zaměřují na nejlepší postupy a doporučené strategie pro řízení informační bezpečnosti, český zákon stanovuje konkrétní požadavky a povinnosti pro subjekty působící v různých sektorech. Tento zákon je tedy významným nástrojem pro zajištění národní kybernetické bezpečnosti a poskytuje rámec pro ochranu klíčové infrastruktury a služeb proti kybernetickým hrozbám. Zákon o kybernetické bezpečnosti v ČR představoval důležitý krok k posílení národní obrany proti kybernetickým útokům a je klíčovým prvkem v celkové strategii kybernetické bezpečnosti země. Jeho implementace a dodržování jsou zásadní pro ochranu klíčových informačních systémů a služeb, což je nezbytné pro funkčnost a bezpečnost moderní společnosti. [3], [4], [6]

2.5 Časový kontext norem a zákonů

Abychom porozuměli vývoji a vzájemnému postavení standardů a legislativy v oblasti kybernetické bezpečnosti, je důležité zvážit, jak postupně vznikaly a jak se navzájem doplňují. Zde je přehled, jak se tyto standardy a právní předpisy vyvíjely a jak spolu souvisí:

- **Standardy rodiny ISO/IEC 27000**

  Jedná se o mezinárodně uznávanou sérii standardů pro správu informační bezpečnosti, která byla vyvíjena postupně od počátku 21. století. Série ISO/IEC 27000 poskytuje rozsáhlý rámec pro nastavení, implementaci, monitorování a zlepšování systémů managementu informační bezpečnosti (ISMS) v organizacích. Tyto standardy jsou založeny na nejlepších postupech a nabízejí flexibilní přístup, který organizace mohou přizpůsobit svým specifickým potřebám. Tento standard se stále vyvíjí a zlepšuje. [3]

- **NIST Cybersecurity Framework**

  Vyvinutý Národním institutem pro standardy a technologie USA a poprvé publikovaný v roce 2014, tento rámec nabízí soubor průmyslově uznávaných nejlepších postupů pro zlepšení kybernetické odolnosti organizací všech velikostí, sektoru a rizikového profilu. NIST CSF se zaměřuje na pět hlavních funkcí – Identify, Protect, Detect, Respond a Recover – a je široce využíván jak v soukromém sektoru, tak vládními organizacemi. Tento standard se stále vyvíjí. [4]

- **Směrnice o bezpečnosti sítí a informací (NIS)**

  Přijatá EU v roce 2016, tato směrnice představuje první významný právní předpis EU zaměřený na zlepšení kybernetické bezpečnosti napříč členskými státy. Zaměřuje se na poskytovatele základních služeb a digitálních služeb, kterým ukládá povinnosti v oblasti bezpečnostních opatření a hlášení kybernetických incidentů. [5]

- **Zákon o kybernetické bezpečnosti v ČR**

  Tento zákon, který byl přijat v reakci na požadavky a doporučení na evropské úrovni, je specifický pro Českou republiku a zaměřuje se na ochranu národní infrastruktury. Stanovuje specifické požadavky pro různé organizace v ČR, včetně povinnosti hlásit významné kybernetické incidenty a zavést vhodná bezpečnostní opatření. [6]

- **NIS 2**

  Jako aktualizace a rozšíření původní směrnice NIS, NIS 2, která je v procesu přijímání a implementace v rámci EU, přináší rozšířený rozsah působnosti, zahrnující více sektorů a zvyšující požadavky na bezpečnostní opatření a hlášení incidentů. [5], [7]

Vývoj a vzájemné propojení těchto standardů a legislativy ukazují na rostoucí globální uznání důležitosti kybernetické bezpečnosti a potřebu koordinovaného přístupu jak na mezinárodní, tak na národní úrovni. Zatímco ISO/IEC a NIST poskytují obecné rámce a směrnice, evropská legislativa (NIS a NIS 2) a národní zákony jako je český zákon o kybernetické bezpečnosti představují specifické právní požadavky a povinnosti. Tyto různé přístupy se vzájemně doplňují a poskytují komplexní pohled na správu a ochranu kybernetické bezpečnosti v různých kontextech.

3 Hrozby a útoky

Kybernetické hrozby a rizika představují neustále se vyvíjející výzvu pro organizace v dnešní digitální době. S rostoucí závislostí na digitálních technologiích a internetu se zvyšuje i rozsah a složitost potenciálních kybernetických útoků, které mohou mít závažné důsledky na provoz, finanční stabilitu, důvěryhodnost a právní postavení organizací. [8]

Kybernetická hrozba je jakékoli možné nebezpečí nebo riziko, které může ohrozit bezpečnost informačních systémů, sítí, dat nebo služeb. Tato hrozba může být vytvořena jak úmyslně, tak neúmyslně, a může mít různé formy, včetně malware, phishingu, ransomwaru, sociálního inženýrství a mnoho dalších. Kybernetický útok pak představuje konkrétní akci nebo sérii akcí, které jsou zaměřeny na narušení, poškození nebo zneužití informačních systémů, sítí, dat nebo služeb. Tyto útoky mohou být prováděny různými subjekty, jako jsou jednotlivci, skupiny nebo organizace, a mohou mít různé cíle, včetně získání neoprávněného přístupu k citlivým informacím, poškození reputace organizace nebo způsobení finančních ztrát.[1], [2]

Tyto útoky jsou jedny z nejběžnějších útoků vůbec[9]:

- Malware
- DoS/DDoS
- Phishing
- Spoofing
- Útoky založené na krádeži identity
- Útoky pomocí vkládání kódu
- Útoky na dodavatelský řetězec
- Sociální inženýrství
- Vnitřní hrozby
- DNS tunelování
- Útoky na zařízení IoT

V další kapitole jsem vybrané z nich více rozebral.

3.1 Malware

Malware je škodlivý software navržený k narušení, poškození nebo neoprávněnému přístupu k počítačovým systémům a sítím. Jeho hlavními cíli jsou krádež citlivých dat, narušení operací a poškození systémových komponent. Malware se může dostat do sítě různými způsoby, včetně phishingových e-mailů se škodlivými přílohami nebo odkazy, exploitace zranitelností v softwaru nebo operačním systému, stahování infikovaného softwaru z neověřených zdrojů, nebo pomocí USB a jiných vyměnitelných médií. Jakmile je malware v síti, může se rychle šířit mezi zařízeními a způsobit širokou škálu problémů. Tyto problémy zahrnují krádež citlivých informací, jako jsou finanční údaje a osobní identifikační údaje, poškození nebo úplné smazání dat, zneužití systémových zdrojů pro těžbu kryptoměn nebo provedení DDoS útoků, narušení nebo úplná ztráta přístupu k systémovým funkcím a službám a exfiltrace dat do vzdálených serverů řízených útočníkem.[10]

Detekce malware vyžaduje kombinaci antivirového softwaru, firewallových systémů, systémů pro detekci a prevenci průniku (IDS/IPS) a pravidelného monitorování a analýzy síťového provozu. Antivirový software je zásadní pro skenování, identifikaci a odstraňování známého malware. Firewally pomáhají zabránit neoprávněným přístupům, zatímco systémy IDS/IPS mohou detekovat a blokovat podezřelý provoz a potenciální hrozby. Důležitá je také schopnost

rychle reagovat na incidenty, což zahrnuje izolování infikovaných systémů, analýzu povahy a rozsahu útoku a obnovení čistých verzí systémů a dat. [10]

Prevence vstupu malware do sítě zahrnuje řadu opatření, jako je používání bezpečnostního softwaru a jeho pravidelné aktualizace, implementace bezpečnostních zásad a postupů, včetně silné autentizace a minimálních oprávnění uživatelů, školení zaměstnanců v oblasti kybernetické bezpečnosti k posílení povědomí o phishingových a sociálně inženýrských taktikách, udržování aktuálních bezpečnostních záplat a aktualizací pro všechny softwarové produkty a operační systémy a pravidelné zálohování důležitých dat. [10]

3.1.1 Ransomware

Ransomware je specifický typ malware, který v Česku zarezonoval především díky útoku na benešovskou nemocnici a Ředitelství silnic a dálnic. Ransomware šifruje data na infikovaném zařízení a vyžaduje od oběti zaplacení výkupného za jejich dešifrování. Tento typ útoku se stal běžným a významným problémem v kybernetické bezpečnosti, jelikož útočníci cílí jak na jednotlivce, tak na organizace včetně nemocnic, škol a vládních institucí. Ransomware obvykle proniká do systému prostřednictvím phishingových e-mailů se škodlivými přílohami, využíváním bezpečnostních zranitelností v softwaru nebo prostřednictvím drive-by downloading, kde je malware stáhnut při návštěvě infikované webové stránky. Jakmile je ransomware spuštěn, šifruje data na pevném disku nebo síťových úložištích a obvykle zobrazuje výzvu s pokyny k zaplacení výkupného, často ve formě kryptoměny kvůli zachování anonymity útočníka. Důsledky ransomware útoku mohou být devastující – od ztráty cenných osobních nebo firemních dat, přes významné finanční ztráty spojené s platbou výkupného, až po narušení běžného provozu a služeb. Navíc, platba výkupného nezaručuje, že útočník skutečně poskytne klíč pro dešifrování dat, a může povzbudit další útoky.[11]

Detekce ransomware se opírá o podobné bezpečnostní nástroje a postupy jako detekce jiného typu malware, včetně antivirového softwaru, firewalů, systémů pro detekci a prevenci průniku a pravidelného monitorování sítě. Mnoho antivirových řešení nyní zahrnuje specifické moduly pro detekci ransomware. [11]

Prevence ransomware útoků vyžaduje komplexní přístup. Důležitá je nejen technická ochrana, ale i školení uživatelů, aby rozpoznali phishingové pokusy a vyhýbali se návštěvě podezřelých nebo neověřených webových stránek. Organizace by měly pravidelně aktualizovat všechny své systémy a aplikace, aby se minimalizovalo riziko exploitace zranitelností. Dále je nezbytné

provádět pravidelné zálohování důležitých dat na oddělených systémech, což umožňuje obnovu dat v případě útoku. V případě, že dojde k infekci ransomwarem, měly by mít organizace připravený plán reakce na incidenty, který by obsahoval postupy pro izolaci infikovaných systémů, analýzu rozsahu útoku, odstranění ransomware, obnovení dat ze záloh a komunikaci s dotčenými stranami. Celkově ransomware představuje jednu z největších hrozeb v kybernetické bezpečnosti dneška. Jeho rostoucí sofistikovanost a škodlivost vyžadují pečlivou a komplexní strategii prevence, připravenosti a reakce. [11]

3.2 Metoda útoku DDoS

DDoS, neboli Distributed Denial of Service, je typ kybernetického útoku, jehož cílem je znemožnit přístup k webovým stránkám, serverům nebo sítím tím, že je zahlcuje nadměrným množstvím internetového provozu. Útoky DDoS jsou prováděny pomocí sítí infikovaných počítačů, známých jako botnety, které jsou řízeny útočníkem. Každý počítač v botnetu posílá požadavky na cílový server nebo síť, což vede k jejich přetížení a následnému výpadku služby.[12]

Technicky DDoS útoky mohou být kategorizovány do několika typů na základě metody, kterou používají k zahlcení cíle. Mezi tyto typy patří:

- **Volumetrické útoky**
  Tyto útoky generují obrovské množství provozu, aby zaplnily šířku pásma cílového serveru. Příkladem je UDP flood nebo ICMP (Ping) flood. [12]
- **Protokolové útoky**
  Útočí na zdroje serveru a vybavení síťové infrastruktury, jako jsou firewally a load balancery. Příkladem je SYN flood, kde útočník zahltí cíl požadavky na navázání spojení. [12]
- **Aplikační vrstvové útoky**
  Tyto útoky cílí na konkrétní aplikace nebo služby na serveru a jsou často těžší detekovat. Příkladem je HTTP flood. [12]

Při DDoS útoku se útočníci často spoléhají na velký počet počítačů, které byly infikovány malware a staly se součástí botnetu. Tito "boti" jsou roztroušeni po celém světě, což útoku dodává anonymitu a komplikuje jeho odhalení a potlačení. [12]

Detekce a obrana proti DDoS útokům vyžaduje pokročilé monitorovací a mitigovací nástroje. Mezi běžné obranné strategie patří:

- **Síťové chování a analýza provozu**
  Použití systémů pro detekci a prevenci průniku (IDS/IPS) a dalších nástrojů pro monitorování a analýzu síťového provozu, aby byly identifikovány neobvyklé vzorce, které mohou naznačovat DDoS útok. [12]
- **Mitigace prostřednictvím poskytovatelů služeb**
  Mnoho poskytovatelů internetových služeb a specializovaných firem nabízí služby mitigace DDoS, které mohou pomoci rozptýlit nebo filtrovat nežádoucí provoz. [12]
- **Redundance a škálovatelnost**
  Zajištění, že síťová infrastruktura a servery jsou dostatečně robustní a schopné zvládnout náhlý nárůst provozu. [12]
- **Cloudové založené řešení**
  Některé cloudové služby nabízí flexibilitu a škálovatelnost potřebnou k absorbování nárůstu provozu a snížení dopadu DDoS útoků. [12]

Je důležité si uvědomit, že úplné zabránění DDoS útoků je extrémně obtížné, zejména vzhledem k rostoucí velikosti a sofistikovanosti těchto útoků. Proto je klíčové mít kromě preventivních opatření také efektivní plán reakce na incidenty a obnovy, aby se minimalizoval dopad na operace v případě útoku. [12]

3.3 Sociální inženýrství

Sociální inženýrství je forma manipulace, která využívá lidské chyby k získání důvěrných informací, přístupu k systémům nebo k narušení bezpečnostních protokolů. Na rozdíl od jiných kybernetických hrozeb, které využívají technické zranitelnosti, sociální inženýrství cílí na psychologické slabiny lidí. Útočníci používají řadu technik, aby přiměli oběti k tomu, aby poskytly citlivé informace nebo provedly akce, které by jinak neprováděly. [13]

Tyto techniky můžou zahrnovat:

- **Phishing**

  Phishing je pravděpodobně nejrozšířenější formou sociálního inženýrství. Útočníci posílají podvodné e-maily nebo zprávy, které se zdají pocházet z důvěryhodného zdroje, s cílem získat citlivé informace jako jsou přihlašovací údaje nebo finanční informace. [13]
- **Spear Phishing**

  Jedná se o cílenější formu phishingu, kde útočník má konkrétního cíle a často využívá personalizované informace získané o oběti, aby útok byl přesvědčivější. [13]
- **Pretexting**

  Zde útočník vytvoří falešný příběh (pretext) k získání důvěry oběti a vyžádání citlivých informací. Například mohou předstírat, že jsou bankovním úředníkem, který potřebuje ověřit informace o účtu. [13]
- **Baiting**

  Tato technika využívá lákavé návnady, jako jsou zdarma nabízené softwarové programy, které obsahují malware, nebo USB flash disky s škodlivým softwarem, které jsou "náhodně" zanechány na místech, kde je pravděpodobné, že je oběť najde a použije. [13]
- **Tailgating/Piggybacking**

  Tato technika zahrnuje následování zaměstnance do kontrolovaných nebo bezpečnostních oblastí. Útočník může například předstírat, že je novým zaměstnancem nebo dodavatelem, který zapomněl přístupovou kartu. [13]
- **Reverse Social Engineering**

  Zde útočník vytvoří situaci, ve které je oběť vedená k tomu, aby sama vyhledala útočníka, obvykle pro poskytnutí pomoci nebo řešení problému, který útočník vytvořil. [13]

Sociální inženýrství je tak účinné, protože využívá přirozené tendence lidí důvěřovat a pomáhat. Obrana proti sociálnímu inženýrství vyžaduje školení a osvětu zaměstnanců, aby byli schopni rozpoznat podvodné taktiky a správně reagovat. Důležité je také vytvoření bezpečnostních politik a procedur, které pomáhají minimalizovat rizika, jako jsou pravidla pro ověřování totožnosti a postupy pro zacházení s neznámými zařízeními nebo požadavky. Kromě

toho je důležité posílit bezpečnostní kulturu organizace a podporovat otevřenou komunikaci o bezpečnostních hrozbách a incidentech. [13]

3.4 MitM útoky

Man-in-the-Middle (MitM) útoky jsou forma kybernetické hrozby, při které útočník tajně odposlouchává a někdy upravuje komunikaci mezi dvěma stranami, aniž by si toho byly obě strany vědomy. Cílem těchto útoků může být krádež citlivých informací, manipulace s daty nebo narušení komunikace. MitM útoky lze provádět různými způsoby a mohou se zaměřit na různé typy komunikace, včetně e-mailů, webového prohlížení nebo jakékoli jiné formy digitální komunikace.[14]

Techniky používané v MitM útocích:

- **Interceptace sítě**
  Útočník může odposlouchávat síťovou komunikaci, například na nezabezpečených Wi-Fi sítích. To může být provedeno pomocí nástrojů pro odposlech, jako jsou paketové snifery, které zachycují a analyzují síťový provoz. [14]
- **DNS Spoofing**
  Tato technika zahrnuje manipulaci s Domain Name System (DNS), což vede oběti k připojení na falešné webové stránky, které útočník kontroluje, místo na legitimní stránky. [14]
- **ARP Spoofing**
  V této technice útočník posílá falešné ARP (Address Resolution Protocol) zprávy do sítě s cílem asociovat svou MAC adresu s IP adresou jiného hostitele, jako je výchozí brána, což mu umožňuje odposlouchávat nebo manipulovat s provozem mezi hostitelem a sítí. [14]
- **SSL Stripping**
  Útočník zde může přimět webový prohlížeč oběti k používání nezabezpečeného HTTP spojení místo šifrovaného HTTPS, což umožňuje odposlech komunikace. [14]

- **Session Hijacking**
  V této technice útočník ukradne platné session tokeny, které umožňují přístup k zabezpečeným účtům nebo webovým službám. [14]

Obrana proti Man-in-the-Middle (MitM) útokům vyžaduje komplexní přístup, který zahrnuje několik klíčových aspektů, včetně používání šifrování, bezpečnostních certifikátů a silných bezpečnostních protokolů, stejně jako vzdělávání uživatelů. Jedním z nejdůležitějších kroků je zajištění, že veškerá komunikace, zejména ta, která probíhá přes internet, je šifrována. To se děje prostřednictvím použití HTTPS na webových stránkách, což zaručuje, že veškerá data přenášená mezi uživatelem a webovým serverem jsou šifrována. Kromě toho je užitečné používat virtuální privátní sítě (VPN), které poskytují bezpečné spojení a šifrování dat, zejména když jsou uživatelé připojeni k veřejným nebo nezabezpečeným Wi-Fi sítím. Dalším důležitým opatřením je ujištění se, že webové stránky používají platné bezpečnostní certifikáty. Toto je klíčové pro ověření pravosti webových stránek a ochranu před útoky, jako je SSL stripping, kde se útočník snaží oběti vnutit nezabezpečené spojení. Uživatelé by měli být vedeni k tomu, aby vždy kontrolovali bezpečnostní certifikáty webových stránek, zejména při zadávání citlivých informací, jako jsou přihlašovací údaje nebo finanční informace. [14]

Je také důležité používat silné bezpečnostní protokoly na síťových zařízeních, jako jsou Wi-Fi routery, a pravidelně je aktualizovat. To totiž pomáhá zabránit útokům, jako je ARP spoofing, kde útočník může manipulovat sítí a odposlouchávat komunikaci. Bezpečnostní protokoly a pravidelné aktualizace firmwaru zajistí, že síťová infrastruktura je odolná proti nejnovějším známým hrozbám. Dalším slabým článkem jsou samozřejmě lidé. Uživatelé by měli být informováni o rizicích spojených s MitM útoky a měli by vědět, jak rozpoznat potenciální nebezpečí. To zahrnuje pochopení rizik spojených s připojováním k neznámým nebo veřejným Wi-Fi sítím a schopnost identifikovat podezřelé e-maily nebo webové stránky, které mohou být součástí phishingového útoku. [14]

3.5 Exploits a Zero-Day útoky

Exploits a zero-day útoky jsou pokročilé formy kybernetických hrozeb, které zneužívají zranitelnosti v softwaru nebo operačních systémech. Tyto typy útoků jsou obzvláště nebezpečné, protože často představují neznámé nebo neopravené bezpečnostní slabiny. [15]

Exploit je kód, nástroj nebo metoda, která využívá zranitelnost v softwaru. Tyto zranitelnosti mohou být způsobeny chybami v programování, nedostatečným zabezpečením nebo jinými nedostatky v návrhu systému. Exploity mohou být použity k neoprávněnému získání přístupu k systému, eskalaci oprávnění, krádeži dat nebo spuštění škodlivého kódu. Existuje mnoho druhů exploitů, od těch, které cílí na specifické aplikace, až po ty, které se zaměřují na síťové protokoly nebo operační systémy. Zero-day útok je specifický typ exploitu, který zneužívá dosud neznámou nebo neopravenou zranitelnost. "Zero-day" odkazuje na skutečnost, že vývojáři mají "nula dní" na opravu chyby, protože útok se odehrává dříve, než je zranitelnost veřejně známa nebo opravena. Zero-day útoky jsou obzvláště nebezpečné, protože proti nim neexistují předem připravené obranné mechanismy nebo opravy. Útočníci, kteří používají exploits a zero-day útoky, často využívají sofistikované techniky a pokročilé malware k dosažení svých cílů. Mohou cílit na jednotlivce, organizace nebo dokonce celé vládní infrastruktury. Následky těchto útoků mohou zahrnovat krádež citlivých informací, dlouhodobé narušení služeb, finanční ztráty a vážné poškození pověsti. [15]

Obrana proti exploits a zero-day útokům vyžaduje víceúrovňový přístup. Prvním krokem je pravidelné aktualizace softwaru a systémů, což pomáhá opravit známé zranitelnosti. Avšak v případě zero-day útoků nemusí být tato metoda dostatečná, protože zranitelnost ještě nebyla identifikována nebo opravena. Proto je důležité mít robustní bezpečnostní systémy, jako jsou pokročilé antivirové programy, firewally a systémy pro detekci a prevenci průniku, které mohou identifikovat a blokovat podezřelé chování nebo neobvyklý síťový provoz. Celkově, zatímco je obtížné zcela eliminovat riziko exploits a zero-day útoků, kombinace neustálého sledování, aktualizací, pokročilých bezpečnostních technologií a osvěty uživatelů může významně snížit riziko a dopad těchto pokročilých kybernetických hrozeb. [15]

4 Formulace problému

4.1 Význam kybernetické bezpečnosti

V dnešní době, kdy se organizace stále více spoléhají na digitální technologie, se kybernetická bezpečnost stává neodmyslitelnou součástí jejich operací a strategií. Pro organizace, které se zabývají ICT a systémovou integrací, je kybernetická bezpečnost zvláště klíčová z několika důvodů. Především, jako poskytovatelé ICT služeb, se organizace neustále setkávají s velkým množstvím citlivých informací, včetně obchodních tajemství, osobních dat zákazníků a interních operativních informací. Jakýkoliv únik nebo kompromitace těchto dat by měl závažné důsledky nejen pro bezpečnost informací, ale také pro důvěryhodnost a reputaci organizací. Z technického hlediska jsou organizace zodpovědné za zajištění bezpečnosti svých systémů a infrastruktury, což zahrnuje ochranu před širokou škálou kybernetických hrozeb, jako jsou malware, DDoS útoky, phishingové kampaně a další sofistikované útoky. Tato odpovědnost vyžaduje nejen pokročilé technické řešení, jako jsou silná šifrování, firewall, antivirové programy a systémy pro detekci a prevenci průniku, ale také pravidelné aktualizace a údržbu systémů, aby byly ochráněny proti nejnovějším hrozbám. Dalším důvodem, proč je kybernetická bezpečnost pro tyto organizace klíčová, je potřeba dodržování přísných regulačních a právních požadavků. V oblasti ICT a systémové integrace je mnoho předpisů a norem, které vyžadují, aby organizace chránila data a infrastrukturu svých klientů. Nedodržení těchto předpisů může vést k závažným právním a finančním sankcím, což dále zvyšuje význam robustní kybernetické bezpečnostní strategie. Kromě toho, v dnešním propojeném světě, kde je pověst organizace stále více závislá na digitální přítomnosti, může jakýkoliv bezpečnostní incident způsobit dlouhodobé poškození reputace organizace. Zákazníci a partneři očekávají, že jejich data budou uchovávána bezpečně, a jakýkoliv selhání v této oblasti může vést k ztrátě důvěry a obchodních příležitostí. V neposlední řadě je klíčové pochopení, že kybernetická bezpečnost ovlivňuje nejen technologickou stránku podnikání, ale všechny jeho aspekty, včetně lidských zdrojů, operací a podnikové strategie. Vytvoření a udržení silné bezpečnostní kultury, včetně pravidelného školení zaměstnanců a vytváření bezpečnostních politik, je nezbytné pro ochranu proti interním i externím hrozbám.[1], [2]

Takto je zřejmé, že kybernetická bezpečnost není jen otázkou IT, ale klíčovou součástí celkového úspěchu a reputace organizace v oblasti ICT a systémové integrace. Přístup k ní vyžaduje komplexní strategii, která zahrnuje technologii, lidi a procesy, aby bylo zajištěno bezpečné a úspěšné podnikání. [1], [2]

4.2 Identifikace hrozeb

V této kapitole se pokusím identifikovat hrozby, které můžou firmu postihnout. Jednou z největších hrozeb v dnešním digitálním prostředí je ransomware, což je forma malware, která šifruje data na infikovaném zařízení a vyžaduje od oběti výkupné za jejich dešifrování. Pro ICT firmu, jejíž operace závisí na spolehlivosti a bezpečnosti jejích systémů a sítí, může útok ransomwarem mít katastrofální důsledky. Ransomware může proniknout do systému různými cestami, včetně phishingových e-mailů, zneužití síťových zranitelností nebo přes infikované webové stránky. Jakmile jsou data šifrována, firma se ocitá v situaci, kdy nemůže přistupovat ke klíčovým datům a systémům, což může vést k zastavení provozu, finančním ztrátám a poškození pověsti. Kromě bezprostředního dopadu na operace může mít útok ransomware dlouhodobé následky v podobě ztráty důvěry ze strany klientů a obchodních partnerů. [11]

Další významnou hrozbou pro ICT firmu jsou DDoS útoky, které mohou přetížit síťovou infrastrukturu a znemožnit přístup k důležitým službám. Pro firmu, která poskytuje služby spojené s optickými spoji a síťovou infrastrukturou, může takový útok vážně narušit služby pro klienty a způsobit významné provozní a finanční problémy. Kromě toho, firma musí čelit hrozbám spojeným s vnitřními zranitelnostmi a zastaralým softwarem. Slabiny v síťové infrastruktuře, nedostatečně aktualizovaný software nebo hardware, který není schopen odolávat nejnovějším typům kybernetických útoků, mohou vést k bezpečnostním poruchám. Tyto poruchy nejen ohrožují bezpečnost dat, ale také mohou mít právní důsledky vzhledem k rostoucím regulačním požadavkům na ochranu dat. [12]

Vzhledem k narůstající složitosti kybernetických hrozeb je důležité nejen prevence, ale i plány obnovy. I když by se firma jistě snažila maximalizovat svoji bezpečnost, není možné být stoprocentně imunní vůči všem možným hrozbám. Proto je klíčové mít plány a strategie pro rychlé a efektivní obnovení provozu v případě bezpečnostního incidentu, a tím minimalizovat škody a výpadky. [16]

Tato opatření zahrnují pravidelná zálohování dat, vytvoření izolovaných zálohovacích systémů, které jsou odpojeny od hlavní sítě, a vypracování konkrétních postupů a procesů pro krizový management a obnovu. Je také důležité pravidelně testovat tyto plány prostřednictvím simulací a cvičení, aby se zajistilo, že jsou aktuální a funkční.

Plány obnovy mohou hrát klíčovou roli v udržení kontinuity provozu firmy a minimalizaci dopadů kybernetických hrozeb. Jsou nedílnou součástí celkové strategie kybernetické bezpečnosti a pomáhají zajistit, že firma bude schopna rychle a efektivně reagovat na nepředvídané situace a zachovat svoji reputaci a konkurenceschopnost na trhu. [17]

4.3 Lidský faktor v kyberbezpečnosti

Lidský faktor v kontextu kybernetické bezpečnosti hraje klíčovou roli ve všech aspektech ochrany organizace před kybernetickými hrozbami. V této kapitole se zaměřím na význam lidského faktoru, analýzu chyb zaměstnanců, nedostatečného školení a interních hrozeb, ale také na strategie, jak tuto oblast zlepšit a snížit rizika spojená s lidským faktorem.

Začnu významem lidského faktoru v kybernetické bezpečnosti. Zaměstnanci a pracovníci ve firmě nejsou pouze uživateli IT systémů, ale také součástí bezpečnostního řetězce. To znamená, že jejich chování, rozhodnutí a povědomí o kybernetických hrozbách mají zásadní vliv na celkovou kybernetickou rezilienci organizace. Správně informovaní a školení zaměstnanci mohou být první linií obrany proti kybernetickým útokům, zatímco neopatrné chování může způsobit zranitelnosti a bezpečnostní incidenty. Analýza chyb zaměstnanců je tak důležitým krokem v identifikaci rizik spojených s lidským faktorem. Chyby mohou zahrnovat nesprávné kliknutí na podezřelý e-mailový odkaz, sdílení citlivých informací s neoprávněnými osobami nebo nedodržení bezpečnostních postupů. Je důležité provádět pravidelné analýzy incidentů a chyb, abychom lépe porozuměli tomu, kde mohou být slabiny a jak je lze řešit. Dále bývá častým problémem nedostatečné školení zaměstnanců, které může vést k bezpečnostním rizikům. Zaměstnanci by měli být informováni o aktuálních kybernetických hrozbách, rozpoznávání phishingových pokusů a správném chování při zacházení s citlivými daty. Školení by nemělo být pouze jednorázovou záležitostí, ale kontinuálním procesem, který udržuje zaměstnance informované a ostražité. [18]

Interní hrozby, které mohou pocházet od aktuálních nebo bývalých zaměstnanců, představují další výzvu. Tyto hrozby zahrnují zneužití přístupových práv, úmyslné poškozování systémů a krádeže citlivých dat. Identifikace a monitorování rizik spojených s interními hrozbami je klíčové pro prevenci a rychlou reakci. Strategie pro zlepšení kybernetické bezpečnosti v oblasti lidského faktoru zahrnují vytváření bezpečnostní kultury, která zdůrazňuje význam bezpečnosti a zahrnuje všechny zaměstnance. K tomu patří pravidelná a cílená školení, vytváření

bezpečnostních politik a postupů, transparentní komunikace a motivace zaměstnanců k dodržování bezpečnostních pravidel.[19]

5 Hodnocená zabezpečení v dané firmě

V této části se zaměřuji na analýzu vlastních zjištění v oblasti kybernetické bezpečnosti ve zkoumané firmě. Soustředím se na problematiku nakládání s daty, zabezpečení přístupu k nim a jejich dostupnost, jakož i na otázky týkající se šifrování, phishingu a ransomwaru. Dále uvádím výsledky osobních rozhovorů se zaměstnanci, které sloužily k lepšímu pochopení bezpečnostní situace v rámci organizace z jejich perspektivy. Následně podrobně popisuji provedený phishingový útok a sken zranitelností, jež pomohly identifikovat konkrétní bezpečnostní nedostatky a potenciální rizika v informačním systému firmy.

5.1 Informace o firmě

Firma, která byla založena v roce 1991, je českou společností v plném vlastnictví českých občanů, bez jakéhokoli zahraničního kapitálu. Je známá svým vlastním vývojem produktů a zároveň zastupuje různé domácí i zahraniční výrobce a dodavatele. Tato rozmanitost umožňuje poskytování široké škály produktů a služeb, které uspokojují různé potřeby klientů. S více než 500 zaměstnanci v České republice disponuje společnost solidní pracovní silou, což jí umožňuje zaručit vysokou kvalitu poskytovaných služeb a rychlou odezvu na požadavky zákazníků. Roční obrat firmy se pohybuje kolem 1 miliardy Kč a má pobočky v několika významných městech, včetně Prahy, Brna, Plzně, Tábora, Ústí nad Labem, Hradce Králové a Ostravy.

Pokud jde o nabízené služby, firma se specializuje na poradenskou a konzultační činnost, dodávky projektů na klíč a speciální projekty zaměřené na ochranu a utajení informací. To zahrnuje širokou škálu aktivit, od průzkumu a detailního plánování až po geodetické práce a provozování dohledového a síťového operačního centra 24/7. Dalšími oblastmi činnosti jsou dodávky komunikační a bezpečnostní techniky, včetně elektronických zabezpečovacích a požárních signalizací, přístupové kontrolní systémy a měřicí přístroje. Firma se také specializuje na návrh, řízení výstavby a provoz datových místností a center a poskytuje kompletní správu a údržbu objektů včetně vnitřní ochrany prostřednictvím systému BMS.

Z uvedeného vyplývá, že důležitost ochrany dat, pracovních postupů, znalost zákazníků a připravovaných projektů je pro firmu klíčová a selhání bezpečnosti informací a kybernetické bezpečnosti může mít značné dopady, v krajním případě způsobit i zánik firmy.

Při jednání se zástupci firmy jsem nabídl možné poskytnutí metodicky a objektivně provedeného posouzení stavu kybernetické bezpečnosti v oblastech, které jsou z jejich pohledu významné. Výsledkem byla shoda na provedení zhodnocení jejich situace v oblasti kybernetické bezpečnosti, zejména v ochraně proti phishingu a ransomwaru, a návrhu možného řešení.

5.2 Metodika zhodnocení

K realizaci jsem si vybral metodiku interního auditu kybernetické bezpečnosti aplikovanou na část bezpečnostních opatření – ochrana dat v ICT firmy, nastavení přístupu k datům, zavedená bezpečnostních opatření, nasazení detekčních nástrojů a zjištění souladu s požadavky a využití „best practices“.

Metodika interního auditu kybernetické bezpečnosti (auditu KB), stejně jako audit ČSN EN ISO/IEC 27001:2022 vycházejí ze společného postupu definovaného mezinárodním standardem ČSN EN ISO 1911:2018 Směrnice pro auditování systémů managmentu. Při zhodnocení stavu jsem se rozhodl přihlížet k této směrnici, kdy programem hodnocení (auditu) bylo v úvodu zmíněné ověření stavu ochrany dat na jedné z poboček firmy v daném časovém rozmezí a plán zahrnoval provedení vzájemně odsouhlasených kroků se zaměřením jak na organizační opatření, definující pravidla ochrany dat, tak na nastavení technických opatření. Oblast zjištění skutečné úrovně bezpečnostního povědomí a znalostí zaměstnanců jsem se rozhodl zajistit využitím rozhovorů na bázi jednotné sady otázek a prostřednictvím testovacího e-mailu obsahujícího metody phishingu, technická opatření jsem ověřoval formou skenování zranitelností ve spolupráci s IT firmy. V obou případech jsem využil postup posuzování shody stanoveného (očekávaného) stavu se stavem skutečným, a to na základě seznamu opatření, který je označován jako Prohlášení o aplikovatelnosti, a to v rozsahu jen domluvených oblastí, které jsou obsahem této části.

Realizace využívá zejména získání důkazů o pravdivosti anebo existenci nálezů v kontextu kritérií určených pro hodnocení, v tomto případě stanovené bezpečnostní politiky firmy a zavedených bezpečnostních opatření a znalostí zaměstnanců. Metodicky jsem provedl hodnocení znalostí bezpečnostních pravidel a opatření zaměstnanci firmy na bázi sady dotazů, jejichž výsledky jsem dále zpracoval pro získání objektivních důkazů. Tuto část hodnocení jsem se rozhodl rozšířit o testování citlivosti zaměstnanců na phishingové útoky pro objektivní ověření míry citlivosti zaměstnanců na phishingový e-mail nesoucí sebou riziko potenciálního

ohrožení firmy. V oblasti technických opatření jsem vybral metodu testování zranitelností, která umožňuje získat důkazy pro vyhodnocení shody s opatřeními stanovenými firmou pro ICT.

Při plánování jsem zvažoval, že by organizační a technická část proběhly souběžně, nicméně konečné rozhodnutí respektovalo jak dostupnost personálních zdrojů, tedy zaměstnanců a specialistů ICT, tak i časovou náročnost obou kroků ověření a byly provedeny postupně v návaznosti na sebe. Výsledky obou částí jsem poté vyhodnotil formou tabulek a grafů tak, aby reporting vůči vedení firmy usnadnil orientaci ve zjištěném stavu a formuloval jsem doporučení ke zlepšení. V rozsahu působnosti zákona o kybernetické bezpečnosti se tedy jedná o formu auditu vybraného systematického celku (VKB § 16,) a následné použití testování (VKB v rozsahu §11, odst.3 a §25) souvisejících nastavení prostředí ICT firmy.

Obrázek 1 – Postup auditu

5.3 Analýza stávajícího zabezpečení

Domluvené činnosti jsem zahájil analýzou stávajícího nastavení bezpečnostních opatření pro ochranu dat tak, aby bylo možné posoudit soulad mezi požadavky, jako jsou uvedeny dále, a skutečností, která bude reflektovat jak moje vlastní zjištění, tak výsledky osobního šetření mezi zaměstnanci firmy.

Kapitola 3.3.1 až 3.3.7 popisují stav nakládání s daty ve firmě, přístup k nim s ohledem na důvěrnost a jejich ochranu s ohledem na zajištění jejich integrity pomocí šifrování. Část 3.3.8. následně popisuje možné navazující riziko pro ochranu šifrováním. Dostupnost dat je popsána v části 3.4.2 a 3.4.3.

Komplex požadavků a zejména jejich vazba na bezpečnostní povědomí zaměstnanců se stal vstupem pro formulování otázek na osobní pohovory v části 3.5.

5.3.1 Definování oblasti

Při zajišťování bezpečnosti dat je zásadním krokem přesně definovat oblast, ve které se data nacházejí. Tento proces zahrnuje identifikaci všech míst, kde jsou uložena data, a jejich klasifikaci podle úrovně citlivosti. Data mohou být umístěna na interních serverech, cloudových platformách, zařízeních zaměstnanců nebo jiných místech. Po identifikaci míst, kde jsou data uložena, je nezbytné provést analýzu rizik spojených s každou oblastí a zabezpečit je odpovídajícím způsobem. Tímto způsobem je možné zajistit, že každá oblast dat je chráněna v souladu s její úrovní důvěrnosti a s potřebami zabezpečení.

Dále je důležité zjistit, kdo má přístup k těmto datům a jakým způsobem. Tím lze lépe určit, jakými způsoby mohou být data ohrožena a jaké bezpečnostní opatření je třeba přijmout.

Klasifikace dat do různých kategorií podle jejich citlivosti je klíčovým prvkem v ochraně dat. Mezi běžné kategorie patří vyhrazená, soukromá a veřejná data. Každá kategorie vyžaduje odlišná bezpečnostní opatření a postupy ochrany dat.[3]

5.3.2 Kategorizace dat

V případě této firmy lze pozorovat značné nedostatky v kategorizaci dat, zejména v prostředí pobočkových serverů. Na pobočkových serverech je situace daleko od ideálního stavu, kdy veškerá data jsou umístěna na neřízeném serveru bez jasného rozdělení nebo organizace. Tento přístup způsobuje zmatek a nejistotu ohledně toho, kde jsou uložena důležitá data a jak jsou chráněna.

Naopak, na centrálním serveru je situace podstatně lepší, kde jsou data rozdělena a organizována podle jednotlivých oddělení, jako je HR, finanční oddělení a další. Tento přístup umožňuje jasnou a strukturovanou správu dat, což výrazně usnadňuje jejich ochranu a zabezpečení. Je zjevné, že nedostatečné řízení a kategorizace dat na pobočkových serverech představuje vážné riziko pro bezpečnost a integritu dat ve firmě.[20]

5.3.3 Umístění dat

Ve firmě poskytují zaměstnancům firemní notebooky a mobilní zařízení. Každá pobočka má svá vlastní úložiště dat, která zahrnují servery umístěné přímo na dané pobočce. Tato decentralizovaná architektura poskytuje určitou míru flexibility a snižuje zátěž na centrálním

úložišti. Veškeré zálohy se odehrávají také na tomto úložišti. Na centrální úložiště se přenáší pouze zlomek dat, která jsou potřeba přístupná pro zaměstnance z jiných poboček.

Decentralizace však přináší i specifická rizika. Například, přístup k datům na pobočkách může být obtížněji řízen a spravován, což může zvýšit riziko nesprávného používání dat nebo jejich zneužití. Dále existuje riziko fyzického poškození serverů na pobočkách, například v důsledku přírodních katastrof, vandalismu nebo krádeže.

Kromě pobočkových serverů existuje také centrální úložiště dat na hlavní centrální pobočce. Tato centrální infrastruktura může být zasažena různými riziky, včetně kybernetických útoků, jako jsou phishing, ransomware nebo útoky typu Distributed Denial of Service (DDoS).

Dalším rizikem je možnost ztráty nebo odcizení firemních notebooků a mobilních zařízení zaměstnanců. Pokud nejsou tato zařízení správně chráněna hesly nebo šifrována, může dojít k neoprávněnému přístupu k citlivým datům uloženým na těchto zařízeních. To by mohlo vést k úniku důvěrných informací nebo porušení předpisů o ochraně osobních údajů. Dále je nutné brát v úvahu riziko spojené s mobilními zařízeními, která jsou často vystavena většímu nebezpečí ztráty nebo odcizení než klasické stolní počítače. Tyto zařízení mohou být také cílem sofistikovaných kybernetických útoků, které využívají zranitelnosti mobilních operačních systémů nebo aplikací. [9]

5.3.4 Přístupová práva

V rámci zabezpečení dat ve firmě je klíčové řádně spravovat přístupová práva, zejména v kontextu umístění dat a infrastruktury. Zatímco na centrálním serveru, řízeném interním IT týmem, jsou přístupová práva pečlivě spravována a monitorována, situace na pobočkách vyžaduje zvýšenou pozornost.

Na pobočkových serverech není řízení přístupových práv, což znamená, že každý zaměstnanec na pobočce má de facto neomezený přístup k datům. Toto nastavení může představovat značné riziko, zejména pokud se nezajistí adekvátní ochrana dat a kontrola přístupu. Nedostatečné řízení a monitorování přístupových práv na pobočkách může vést k možnosti neoprávněného přístupu k citlivým informacím, zneužití dat nebo úniku důvěrných informací. Aby firma minimalizovala tato rizika, je nezbytné provést revizi a aktualizaci politik a postupů týkajících se správy přístupových práv na všech úrovních organizace.

5.3.5 Podmíněný přístupy

V této firmě je patrný závažný nedostatek v oblasti řízení přístupu, který představuje vážné riziko pro bezpečnost dat. Jednou z hlavních slabin je absence podmíněného přístupu, což znamená, že zaměstnanci a další uživatelé mají neomezený přístup k datům bez ohledu na kontext, jako je jejich poloha, čas přístupu nebo zařízení, ze kterého se přihlašují.

Nepřítomnost podmíněného přístupu vytváří ideální podmínky pro možné útoky a neoprávněný přístup k citlivým informacím. Například, pokud zaměstnanec přistupuje k důvěrným datům z neznámého zařízení nebo z jiné země, měly by být vyvolány varovné signály a uplatněny další bezpečnostní opatření. Absence těchto kontrolních mechanismů však umožňuje potenciálním útočníkům snadněji proniknout do systému a získat neoprávněný přístup k důvěrným informacím.[21]

Dalším výrazným nedostatkem je nepoužívání dvoufázové autentizace, což je jedna z nejzákladnějších ochranných opatření v kybernetické bezpečnosti. Dvoufázová autentizace poskytuje dodatečnou vrstvu zabezpečení tím, že požaduje od uživatele potvrzení své identity pomocí dvou nezávislých faktorů, jako je heslo a jednorázový kód. Bez použití tohoto opatření jsou uživatelské účty zranitelné vůči různým útokům, jako jsou phishingové útoky nebo útoky na hesla.

Celkově lze říci, že absence podmíněného přístupu a nedostatek dvoufázové autentizace ve firmě představují značné riziko pro bezpečnost dat a vyžadují naléhavou pozornost a kroky k jejich nápravě a zlepšení. Bez těchto základních bezpečnostních opatření je firma vystavena vysokému riziku úniku, zneužití nebo poškození důvěrných informací. [21]

5.3.6 Doménová zařízení

Dalším závažným nedostatkem v bezpečnosti dat této firmy je možnost přístupu do firemní sítě prostřednictvím VPN i z nedoménových počítačů. Tento nedostatek představuje vážné riziko pro bezpečnost a integritu sítě, neboť umožňuje potenciálně neověřeným zařízením, která nemusí splňovat bezpečnostní standardy firmy, připojit se k firemní síti a získat přístup k citlivým datům a systémům.

Tím, že je umožněno připojení k VPN z nedoménových počítačů, jsou firemní systémy vystaveny zvýšenému riziku útoků a neoprávněného přístupu. Taková zařízení mohou být náchylná k různým bezpečnostním hrozbám, jako jsou malware, spyware nebo neoprávněné

přístupy třetích stran. Bez adekvátních bezpečnostních opatření a kontroly je možné, že se do firemní sítě dostanou útočníci, kteří by mohli způsobit značné škody a ztráty.

5.3.7 Šifrování

Ve firmě je patrná vážná mezera v ochraně dat, zejména pokud jde o šifrování uložených informací. Všechna data uložená na firemních notebookách a mobilních zařízeních nejsou šifrována, aniž by byl využíván nějaký nástroj jako BitLocker pro šifrování disků v notebookách. Tato situace výrazně zvyšuje riziko ztráty nebo zneužití citlivých informací v případě krádeže nebo ztráty těchto zařízení.[22]

Co se týče dat uložených na serveru, také nejsou šifrována a není použit ani žádný specifický šifrátor či šifrovací nástroj. Tento nedostatek systematického šifrování dat na serveru znamená, že existuje potenciální riziko, že citlivé informace mohou být ohroženy v případě neoprávněného přístupu k serverovým úložištím. [22]

5.3.8 Q day

Vzhledem k hypotetické budoucnosti, kdy by kvantové počítače mohly být dostatečně vyspělé na prolomení běžně používaných šifer, jako je RSA, se stává nevyužívání šifrátorů firmou akutním bezpečnostním rizikem. Avšak dokonce i nyní existuje potenciál, že někdo odposlouchává zašifrované informace s cílem pozdějšího prolomení na kvantovém počítači. Tento scénář by mohl umožnit útočníkům získat přístup k citlivým informacím, které byly považovány za bezpečné. Takové chování by mohlo způsobit závažné narušení důvěrnosti a integrity dat firmy a mít vážné důsledky pro její pověst a obchodní zájmy.[23]

Tato situace zdůrazňuje naléhavou potřebu proaktivního přístupu k zabezpečení dat a implementaci pokročilých šifrovacích opatření. Firmy, které nevyužívají šifrování nebo zůstávají na starších šifrovacích standardech, by mohly být vystaveny vysokému riziku úniku důvěrných informací a ztrátě důvěryhodnosti vůči svým zákazníkům a obchodním partnerům.

5.3.9 Phishing

V současné době je phishing nejpoužívanější formou kybernetického útoku, který může vážně poškodit firmu. Útočníci se snaží získat citlivé informace od zaměstnanců, jako jsou hesla, bankovní údaje nebo osobní identifikační údaje, vydávajíce se za legitimní entitu nebo kolegu. Tento druh útoku může vést k finančním ztrátám, krádeži důvěrných firemních informací,

včetně strategických dat o klientech a obchodních tajemstvích. Existuje také riziko, že by firma mohla být cílem ransomwarového útoku, kde by útočníci šifrovali data a požadovali výkupné za jejich uvolnění.

Aktuálně je ochrana firmy proti phishingovým útokům velmi nedostatečná a riskantní. Pouze spoléhání na implementovaný firewall s filtrováním e-mailů a jediné školení zaměstnanců o rozpoznání phishingu za posledních 5 let není dostatečné pro ochranu firmy. Tato minimální ochranná opatření vystavují firmu vážnému nebezpečí. Zaměstnanci mohou být snadnými terči pro rafinované phishingové útoky, které mohou vést k úniku citlivých firemních informací, krádeži identity zaměstnanců, finančním ztrátám a poškození pověsti firmy. Bezpečnostní rizika jsou v této situaci vysoká a může dojít k vážným důsledkům pro firmu, včetně ztráty důvěryhodnosti u klientů, ztráty obchodu a potenciálně i sankcí ze strany regulačních orgánů. Je naléhavě nutné zvážit vylepšení bezpečnostních opatření a zvýšení investic do bezpečnostních technologií a školení zaměstnanců, aby se minimalizovala rizika spojená s phishingovými útoky.

5.3.10 Ransomware

Firma v současnosti využívá antivirový a antimalwarový software jako součást své obrany proti ransomware, avšak existují významné nedostatky v provádění bezpečnostních opatření. Aktualizace koncových zařízení jsou ponechány na koncových uživatelích, což vytváří značnou nejednotnost a riziko zastaralých zabezpečovacích opatření. Navíc, přestože je školení zaměstnanců o nebezpečích ransomware součástí strategie firmy, provádí se nedostatečně a nesystematicky, což snižuje jeho účinnost. Zaměstnanci nemají žádné omezení přístupu k serverům poboček, což zvyšuje pravděpodobnost šíření ransomware po síti v případě úspěšného útoku. Tento nedostatek řízení a kontroly přístupu představuje závažnou bezpečnostní trhlinu a zvyšuje riziko pro celou firmu.

5.3.11 Zálohování

Zálohování dat je nedílnou součástí strategie ochrany dat firmy před potenciálními hrozbami, jako je ransomware. Bohužel, stávající postup zálohování dat vykazuje několik kritických nedostatků, které značně zvyšují riziko bezpečnostních incidentů. Bylo zjištěno, že zálohy serverů poboček jsou uloženy na tom samém serveru, což vytváří bod selhání, který může být snadno zneužitý útočníky. Navíc, absence zálohování dat na oddělených úložištích (centrální server) mimo hlavní síťovou infrastrukturu vystavuje firmu zvýšenému riziku ztráty dat

v případě útoku. Další závažnou chybou je uložení zálohovaných dat na online serveru, což může vést k jejich kompromitaci v případě, že by útočník získal přístup k tomuto serveru. Nepřítomnost důkladně ověřených a testovaných zálohovacích procesů dále zhoršuje situaci, jelikož nelze zaručit kompletnost a použitelnost zálohovaných dat v případě potřeby obnovy. Tato závažná bezpečnostní díra v procesu zálohování dat vystavuje firmu značnému riziku a vyžaduje okamžitou revizi a aktualizaci zabezpečovacích opatření.[24]

5.3.12 Obnova po ransomware

Proces obnovy po ransomware útoku je klíčovou součástí celkové strategie zabezpečení firmy a ochrany dat. Bohužel, stávající postupy obnovy dat vykazují značné nedostatky, které mohou vážně ohrozit schopnost firmy rychle se vzpamatovat po útoku ransomware. Jedním z hlavních nedostatků je absence izolovaného „read- only Hard Drive (HD) repository“, ve kterém by byla uchována zálohovaná data chráněna před možnými útoky ransomware. Tento nedostatek zvyšuje riziko, že zálohovaná data budou také infikována a znehodnocena. Další závažnou chybou je nedostatečné pravidelné testování procesů obnovy dat z různých bodů v čase, což komplikuje zajištění účinnosti zálohovacího a obnovovacího plánu v případě skutečného útoku. Provozování dvou serverů, které jsou zabezpečeny a mimo provoz kromě dobu záloh, je krok správným směrem, nicméně nedostatečné opatření k minimalizaci pravděpodobnosti jejich infekce ransomwarem. Používání páskových knihoven pro dlouhodobé uchování záloh může poskytnout spolehlivý způsob uchovávání dat, nicméně je třeba zajistit, aby byla tato data řádně chráněna před riziky ransomware útoků. Celkově tyto nedostatky v procesu obnovy po ransomware představují závažnou bezpečnostní trhlinu a vyžadují okamžitou revizi a aktualizaci zabezpečovacích opatření firmy.[25]

5.4 Rozhovory se zaměstnanci

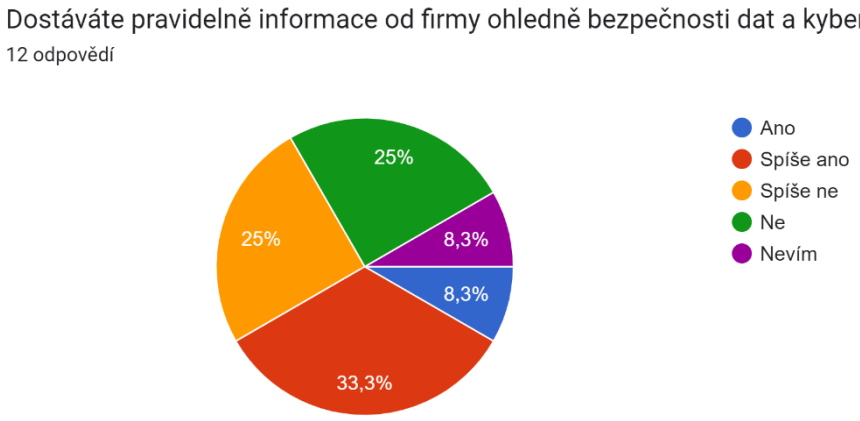
V průběhu mého hodnocení zabezpečení ve firmě jsem se rozhodl zahrnout i sběr dat pomocí osobního rozhovoru o deseti otázkách přímo na pobočce, abych získal hlubší vhled do aktuální situace. Tato část analýzy se zaměřila na pobočku, kde jsem prováděl hodnocení. Ve firmě bylo celkem 13 zaměstnanců oprávněných přistupovat do sítě v této pobočce. Právě s nimi jsem vedl osobní rozhovory.

V průběhu dne se mi podařilo vyzpovídat 12 pracovníků ze třinácti. Tento vysoký podíl odpovědí mi umožnil získat rozsáhlý soubor dat a názorů od zaměstnanců, kteří přímo pracují v této lokalitě. Jedna osoba se rozhovoru nezúčastnila, protože byla nemocná a nedostal jsem

se k němu. Přestože tato jedna absence snížila celkový počet odpovědí, stále jsem byl schopen získat významný vhled do situace z více než 90% účastí zaměstnanců pobočky.

5.4.1 Pravidelné informace od vedení

Na základě odpovědí na otázku týkající se pravidelných informací od firmy o bezpečnosti dat a kybernetických hrozbách lze vidět, že zaměstnanci mají různorodé názory a zkušenosti. Ze 100 % respondentů odpovědělo 25 % s "Ne", 25 % "Spíše ne", 33 % s "Spíše Ano", 8 % s "Ano" a 8 % s "Nevím". Tento rozdíl ve vnímání může být způsoben nedostatečnou komunikací ze strany managementu ohledně bezpečnostních hrozeb a opatření. Zaměstnanci, kteří nejsou pravidelně informováni, mohou být méně obeznámeni s aktuálními bezpečnostními trendy a postupy, což může vést ke zvýšenému riziku kybernetických útoků. Naopak, zaměstnanci, kteří mají pravidelný přístup k informacím o bezpečnosti, jsou pravděpodobněji informováni a připraveni na řešení potenciálních hrozeb. Tento rozdíl ve vnímání zdůrazňuje důležitost efektivní komunikace a vzdělávání v oblasti kybernetické bezpečnosti ve firmě.

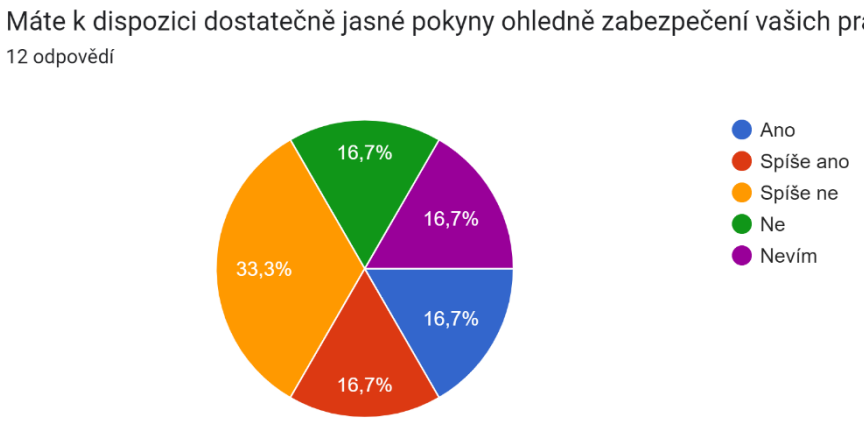


Obrázek 2 – Pravidelné informace od vedení

Zdroj: Vlastní zpracování

5.4.2 Zabezpečení zařízení

Na základě odpovědí na otázku týkající se dostupnosti jasných pokynů ohledně zabezpečení pracovních zařízení lze pozorovat různé úrovně povědomí a informovanosti zaměstnanců. Z celkového vzorku 33 % respondentů odpovědělo s "Spíše ne", zatímco 17 % odpovědělo s "Spíše Ano", stejně jako 17 % odpovědělo "Ano". Dále 17 % odpovědělo s "Nevím", a stejně tak 17 % odpovědělo s "Ne". Tato variabilita odpovědí může být způsobena nekonzistentními komunikačními kanály a nedostatečnými školicími programy, které by zaměstnancům poskytly jasné pokyny ohledně zabezpečení pracovních zařízení. Ti, kteří odpověděli negativně, mohou čelit zvýšenému riziku kybernetických útoků z důvodu nedostatečného povědomí o bezpečnostních postupech. Naopak zaměstnanci, kteří mají k dispozici jasné pokyny, jsou pravděpodobněji lépe vybaveni k ochraně svých pracovních zařízení a citlivých dat. Tento rozdíl ve vnímání zdůrazňuje potřebu konzistentních a dostupných zdrojů informací o bezpečnostních postupech ve firmě.



Obrázek 3 – Zabezpečení zařízení

Zdroj: Vlastní zpracování

5.4.3 Změna hesel

Na základě odpovědí na otázku o četnosti změny hesel k pracovním účtům a systémům lze identifikovat značné nedostatky v bezpečnostních postupech zaměstnanců. Až 25 % respondentů uvádí, že hesla mění pouze jednou za čtvrt roku, což je interval, který se pohybuje na hraně bezpečnostních doporučení. Tento časový rámec není dostatečně častý na to, aby poskytoval adekvátní ochranu důležitých účtů a dat před potenciálními kybernetickými hrozbami. Dokonce 42 % zaměstnanců deklaruje, že hesla mění jednou za půl roku, což představuje ještě menší ochranu a zvýšené riziko pro bezpečnost firemních systémů. Je alarmující, že se 33 % respondentů hlásí k tomu, že hesla mění jednou ročně, což je nebezpečně dlouhá doba, během které by mohla dojít k úniku citlivých informací nebo kybernetickému útoku. Tento trend jasně ukazuje na naléhavou potřebu zlepšení povědomí zaměstnanců o významu časté změny hesel a důslednějším vynucením dodržování bezpečnostních standardů ve firmě.

Obrázek 4 – Změna hesel

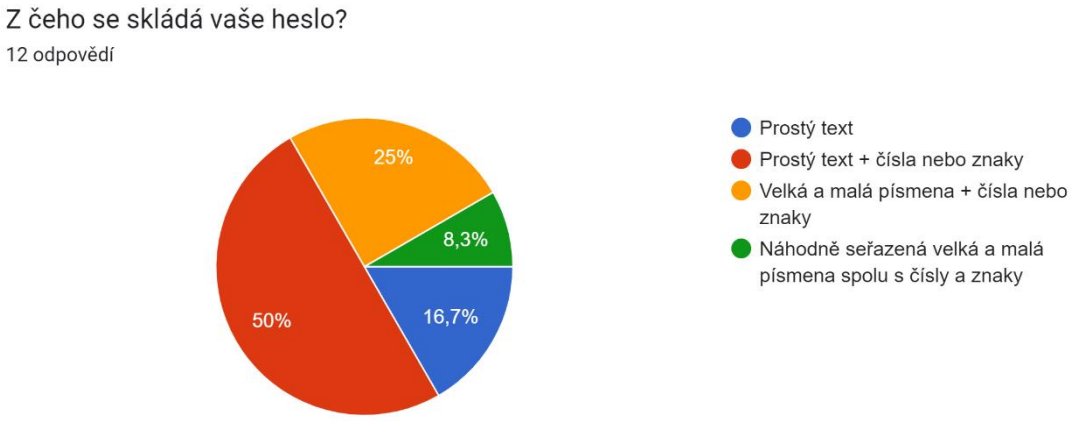
Zdroj: Vlastní zpracování

5.4.4 Složení hesel

Na základě odpovědí na otázku o složení hesel lze identifikovat rozdílné přístupy mezi zaměstnanci. Přestože pouze jeden zaměstnanec uvedl, že jeho heslo obsahuje kombinaci velkých a malých písmen spolu s čísly a speciálními znaky, což je preferovaná forma pro zvýšení bezpečnosti hesel. Tato skutečnost neodpovídá převažujícímu trendu, kdy 17 % respondentů uvádí, že jejich hesla jsou pouze v podobě prostého textu, což je nejrizikovější varianta. Navíc 50 % respondentů používá hesla, která obsahují prostý text doplněný o čísla

nebo speciální znaky, což stále představuje nedostatečnou úroveň ochrany. Dalších 25 % respondentů uvádí, že používá kombinaci velkých i malých písmen a znaků nebo čísel dohromady, což stále není dost pro maximalizaci zabezpečení hesel.

Je alarmující, že 11 z 12 respondentů má nedostatečně silné heslo, což je důležité zejména v kontextu předchozí otázky, kde jsem zjistil, že 75 % respondentů nemění svá hesla dostatečně často. Toto zjištění znamená vážnou bezpečnostní hrozbu pro firmu, protože slabá hesla zvyšují riziko úspěšného prolomení účtů a potenciální ztráty citlivých dat či dokonce podnikových prostředků. Je naléhavě nutné, aby zaměstnanci byli lépe informováni o významu silných hesel a pravidelné změny hesel, aby se snížilo riziko kybernetických útoků a ochránily se důležité firemní informace.



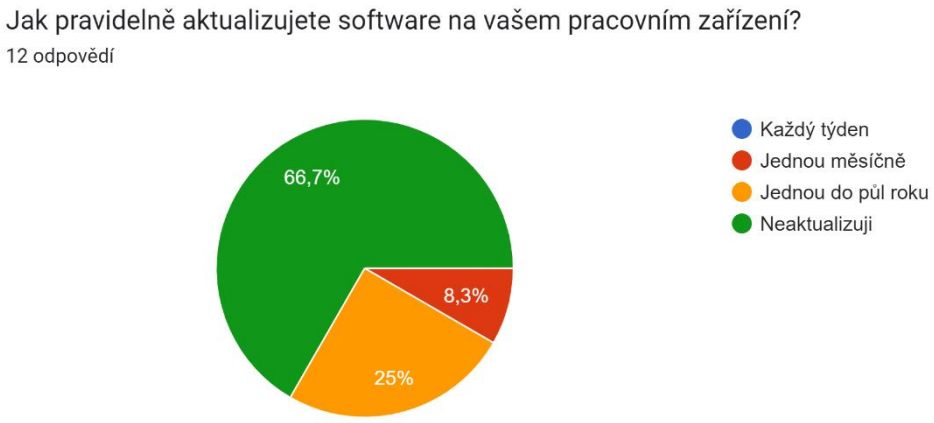
Obrázek 5 – Složení hesel

Zdroj: Vlastní zpracování

5.4.5 Aktualizace softwaru

Na otázku ohledně pravidelnosti aktualizace softwaru na pracovních zařízeních odpověděli respondenti různě. Jedna osoba uvedla, že aktualizuje software jednou měsíčně, což je povzbudivé z hlediska bezpečnosti. Nicméně většina respondentů (11 z 12) odpověděla negativně. Tři respondenti uvedli, že aktualizují software pouze jednou do půl roku, zatímco osm respondentů přiznalo, že svůj software vůbec neaktualizuje. Tato situace představuje značné bezpečnostní riziko pro firmu, protože neaktualizovaný software může obsahovat zranitelnosti, které mohou být využity kybernetickými útočníky k infikování systémů ransomwarem, krádeži dat nebo jiným útokům. Navíc tato skutečnost ještě umocňuje dřívější

zjištění, že většina respondentů nezmění svá hesla dostatečně často, což dále zvyšuje rizika pro bezpečnost dat a systémů v organizaci.



Obrázek 6 – Aktualizace softwaru

Zdroj: Vlastní zpracování

5.4.6 Speciální opatření

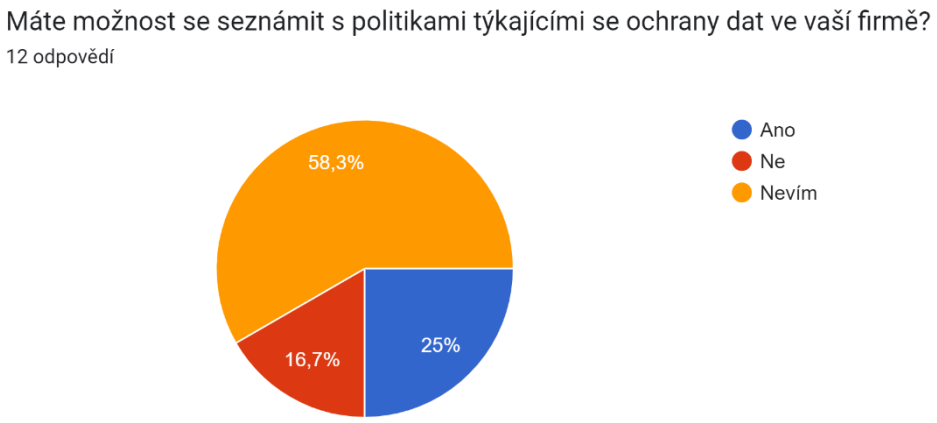
Je znepokojující, že většina respondentů nepoužívá žádná speciální opatření pro zabezpečení svých pracovních zařízení mimo pracovní dobu, přičemž většina z nich často cestuje po stavbách, kde jsou rizika krádeží a ztrát vyšší než v uzamčené kanceláři. Neochráněný notebook v autě, na veřejném místě nebo doma může být snadným cílem pro zloděje nebo útočníka. Jediný jednotlivec, který tuto praxi uplatňuje, je zcela osamocen. Tímto opomenutím se zvyšuje riziko zneužití dat nebo útoků na osobní informace zaměstnanců. Jelikož existují bezplatné nástroje jako BitLocker, které mohou poskytnout alespoň základní ochranu v případě ztráty nebo odcizení pracovních zařízení, je tato absence speciálních opatření nejen nevhodná, ale také zbytečně zvyšuje rizika pro celou organizaci.

Obrázek 7 – Speciální opatření

Zdroj: Vlastní zpracování

5.4.7 Politiky firmy

Je značně znepokojivé, že 16 % respondentů nemá jasnost ohledně možnosti se seznámit s politikami týkajícími se ochrany dat ve firmě, přičemž z toho většina (58 %) dokonce neví, zda takové politiky existují. Tato skutečnost může být způsobena nedostatečnou transparentností společnosti v oblasti komunikace politik a postupů v oblasti kybernetické bezpečnosti. Nedostatek informací může mít za následek nízkou informovanost zaměstnanců ohledně důležitých zásad a pravidel, což může vést k neuvědomělým chybám nebo chybějící spolupráci při dodržování bezpečnostních standardů. Je nezbytné, aby firma zlepšila svou komunikační strategii a zajistila, aby všichni zaměstnanci byli řádně informováni o politikách a postupech týkajících se ochrany dat.

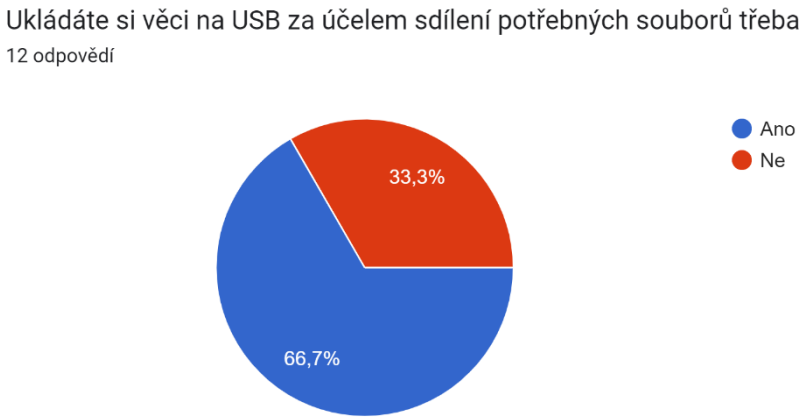


Obrázek 8 – Politiky firmy

Zdroj: Vlastní zpracování

5.4.8 Sdílení souborů

Bylo pro mě absolutně alarmující, že většina respondentů (67 %) pravidelně ukládá důležité soubory na USB za účelem sdílení s jinými stranami, jako jsou subdodavatelé. Toto chování přináší značná bezpečnostní rizika pro společnost. Představte si situaci, kdy dojde ke ztrátě nebo odcizení flash disku. To by mohlo vést k úniku citlivých dat, což by zase ohrozilo důvěrnost a integritu informací společnosti. Co je ještě horší, existuje vysoké riziko, že USB zařízení může být nakaženo škodlivým softwarem při připojení k nezabezpečenému počítači. To by mohlo způsobit šíření malware do firemní sítě, což by mohlo způsobit ještě větší škody. Dalším nebezpečím je vynášení citlivých dat nezabezpečenou cestou, což může být v rozporu se zákony a může vést k právním následkům pro společnost. Je nezbytné, aby zaměstnanci byli lépe poučeni o nebezpečích spojených s používáním USB zařízení pro sdílení důležitých dat a byli motivováni k dodržování bezpečnostních postupů.

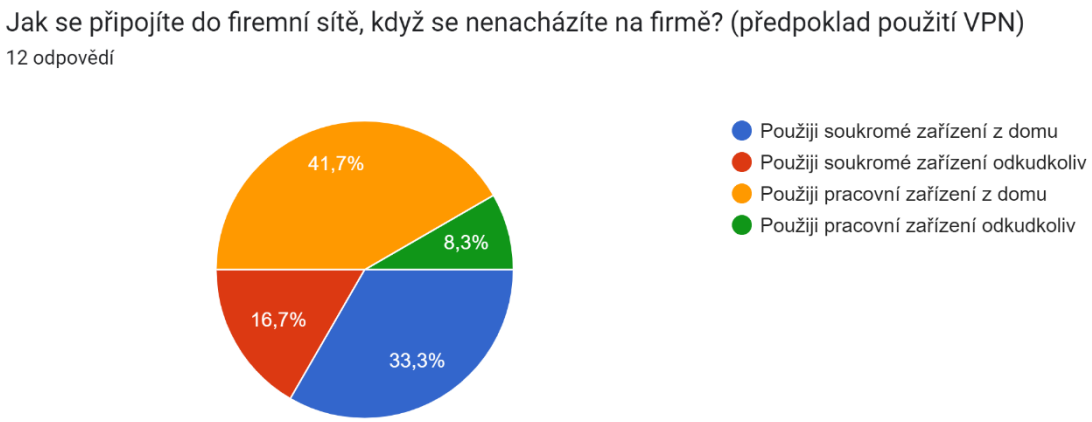


Obrázek 9 – Sdílení souborů

Zdroj: Vlastní zpracování

5.4.9 Připojení k síti

Je zjevné, že existuje rozmanitost postupů při připojování do firemní sítě mimo kancelářské prostředí. Zatímco 42 % respondentů volí použití pracovních zařízení z domova, což je v souladu s bezpečnostními směrnicemi a představuje nejbezpečnější možnost, zbytek respondentů se uchyluje k různým riskantním postupům. Například 33 % respondentů používá soukromá zařízení z domova, což představuje značné bezpečnostní riziko, protože tyto zařízení nejsou pod správou IT oddělení a mohou být náchylná k infekcím malwarem nebo útokům hackerů. Dokonce 17 % respondentů se připojuje k firemní síti pomocí soukromých zařízení odkudkoliv, což je nejhorší možná varianta z hlediska bezpečnosti. Taková zařízení mohou být vystavena různým kybernetickým hrozbám na veřejných nezabezpečených sítích, což může ohrozit citlivá firemní data. Kromě toho 8 % respondentů se připojuje k firemní síti pomocí pracovních zařízení na neznámých sítích, což opět představuje zvýšené bezpečnostní riziko. Je nezbytné zdůraznit důležitost používání pouze ověřených a spravovaných pracovních zařízení při připojování k firemní síti mimo pracoviště.

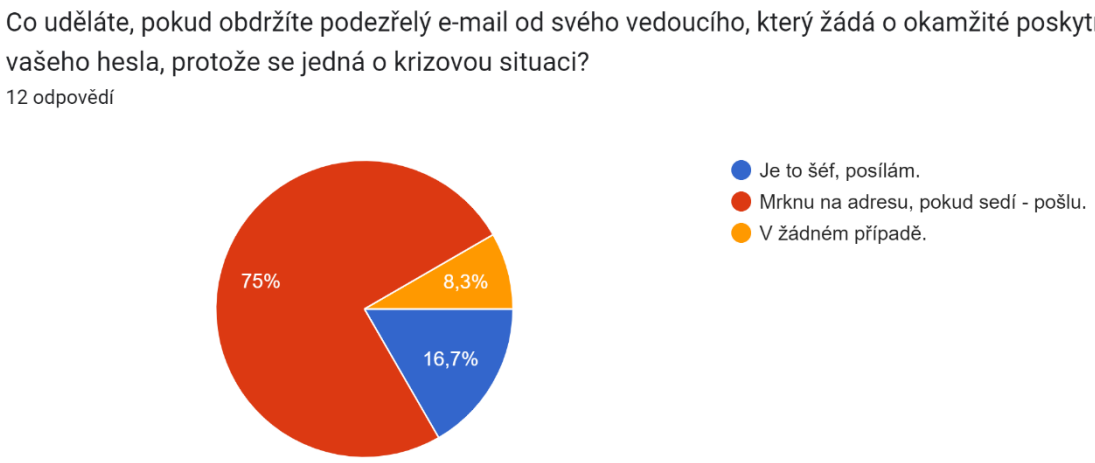


Obrázek 10 – Připojení k síti

Zdroj: Vlastní zpracování

5.4.10 Podezřelý email

Z odpovědí na tuto otázku je patrné, že většina respondentů nedodržuje základní bezpečnostní postupy při zacházení s podezřelými e-maily. Až devět respondentů uvedlo, že by se podívalo na adresu odesílatele a heslo následně zaslalo, což je velmi nebezpečné chování. I když se adresa zdá být legitimní, může se jednat o sofistikovaný phishingový útok, který má za cíl získat citlivé informace. Dvě osoby uvedly, že by heslo okamžitě poslaly, pokud by e-mail přišel od jejich nadřízeného. Toto je zcela nepřijatelné chování, které vystavuje firemní síť závažnému riziku. Šéf by nikdy neměl žádat o heslo prostřednictvím e-mailu, a tímto způsobem může dojít k vážnému ohrožení bezpečnosti dat a systémů organizace. Jedna osoba správně uvedla, že by heslo nikdy neposkytla, což je jedině správná reakce v této situaci. Možná rizika díky chybám respondentů zahrnují možnou ztrátu citlivých informací, kompromitaci firemní sítě a systémů, a možnou finanční škodu způsobenou kybernetickým útokem.



Obrázek 11 – Podezřelý email

Zdroj: Vlastní zpracování

5.4.11 Závěry z rozhovorů

Respondenti poskytli informace, které ukazují na několik klíčových oblastí, kde by mohlo dojít k bezpečnostním rizikům. Mezi ně patří nedostatečně silná hesla, nedostatečná aktualizace softwaru a nesprávné zacházení s podezřelými e-maily. Tyto nedostatky představují potenciální hrozbu pro důvěrnost a integritu firemních dat a systémů.

Je důležité si uvědomit, že výsledky těchto rozhovorů nejsou nezvratnými skutečnostmi, ale spíše ukazateli, které je třeba brát s rezervou. Existuje možnost, že někteří respondenti mohli své odpovědi poskytnout bez dostatečné vážnosti nebo s nízkou úrovní uvědomělosti o rizicích kybernetické bezpečnosti. Navzdory této rezervě jsou však identifikovaná rizika důležitá a vyžadují pozornost.

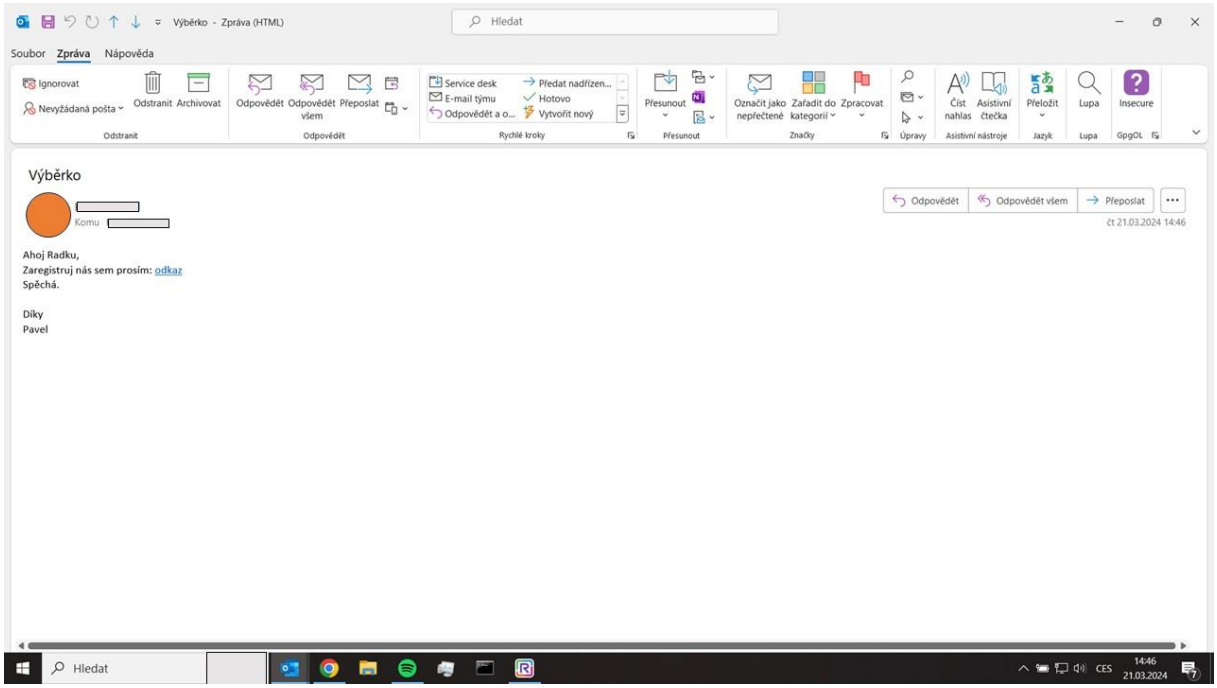
5.5 Phishingový útok

Jelikož mám výsledky prezentovat vrcholovému managementu a vedoucímu oblasti, rozhodl jsem se pro phishingový útok, abych potvrdil vážnost chyb zjištěných z rozhovorů. Vzhledem k malému počtu obětí jsem se rozhodl k cílenému útoku pomocí podvržení odesílatele. Jak již bylo zmíněno, firma se spoléhá v ochraně proti phishingu jen na firewall a nemá implementovaný DMARC. To znamená, že mi stačí vytvořit takový email, který projde firewallem a bude vypadat jako odesílatel, kterého chci. V tomto případě je ideální vytvořit

odesílatele, který bude vypadat jako vedoucí pobočky a bude chtít, aby se zaměstnanci někam proklikli a něco udělali. Každý email je personalizovaný. Tím si ulehčím trochu práce, protože než by se reálný útočník dostal ke všem jménům, tak by mu to zabralo déle času. Jedná se o 12 lidí, kteří dostali do své schránky tento útok, který je bude odkazovat na mou webovku. [26], [27]

5.5.1 Počáteční fáze útoku

Celkem bylo odesláno 12 emailů. V tomto kroku jsem vynechal ředitele pobočky. Využil jsem tohoto útoku v den, kdy se na pobočce nenacházel, a tudíž potencionálně takový útok dával smysl. Každý email byl stejný jako na obrázku dole. Lišil se jen v oslovení. Stačilo využít toho, že firma nepoužívá DMARC, a tudíž příchozí adresa byla ve formě bigboss@organizace.cz, stejně jako je adresa ředitele. Schválně jsem odkaz schoval pouze pod „odkaz“ a následně pod bit.ly, aby to alespoň někoho odradilo. [26], [27]



Obrázek 12 - Vzhled přijatého emailu

Zdroj: Vlastní zpracování

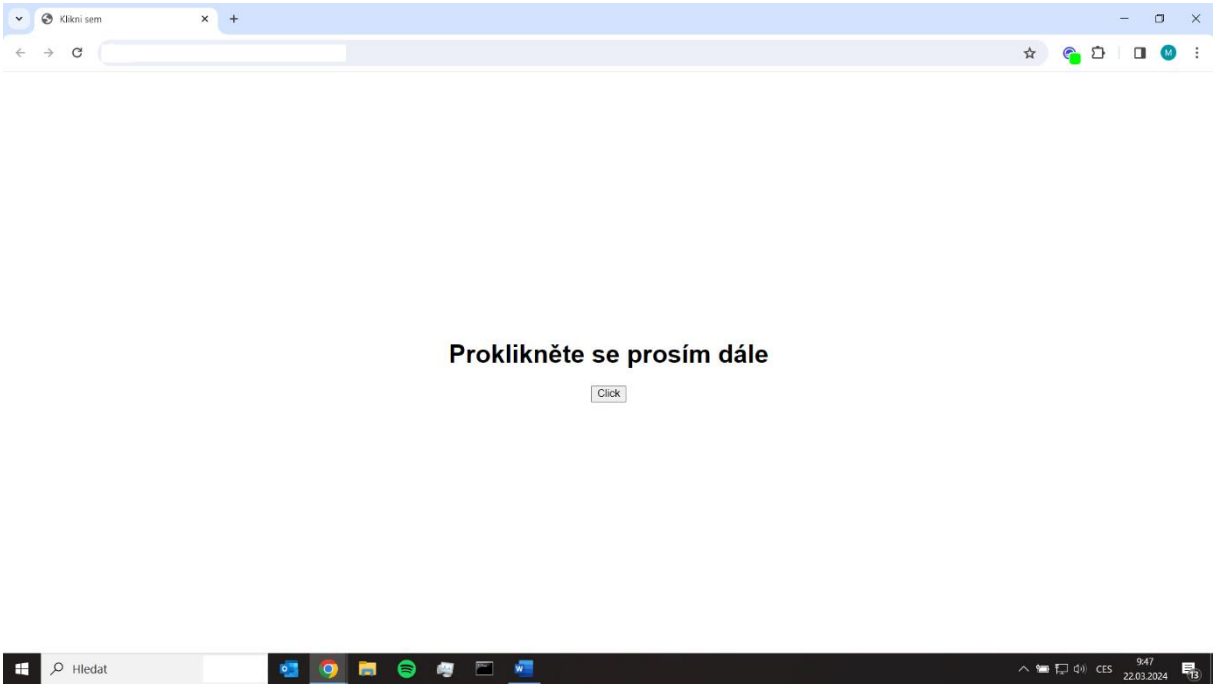
5.5.2 Konečná fáze útoku

V druhé fázi tohoto útoku již mohlo být cokoliv. V moment, kdy se oběť proklikne, může přistoupit na jakoukoliv stránku nebo server, na který jsem odkázal. Mohly tu být falešné firemní stránky a já na nich mohl chtít přihlášení, nebo jsem třeba mohl chtít přihlášení

bankovní identitou. Mohl jsem na otevření stránky pustit škodlivý skript, v podstatě cokoliv. V mém případě mi ovšem stačilo pouze zaregistrovat, že někdo na danou stránku vkročil. Proto jsem si vytvořil pro každou oběť jednu stránku na testovacím serveru, který jsem zpřístupnil z internetu. Poté mi už stačilo jen spárovat stránky s lidmi a zjistit, zda se mi na nich někdo objevil. [26], [27]

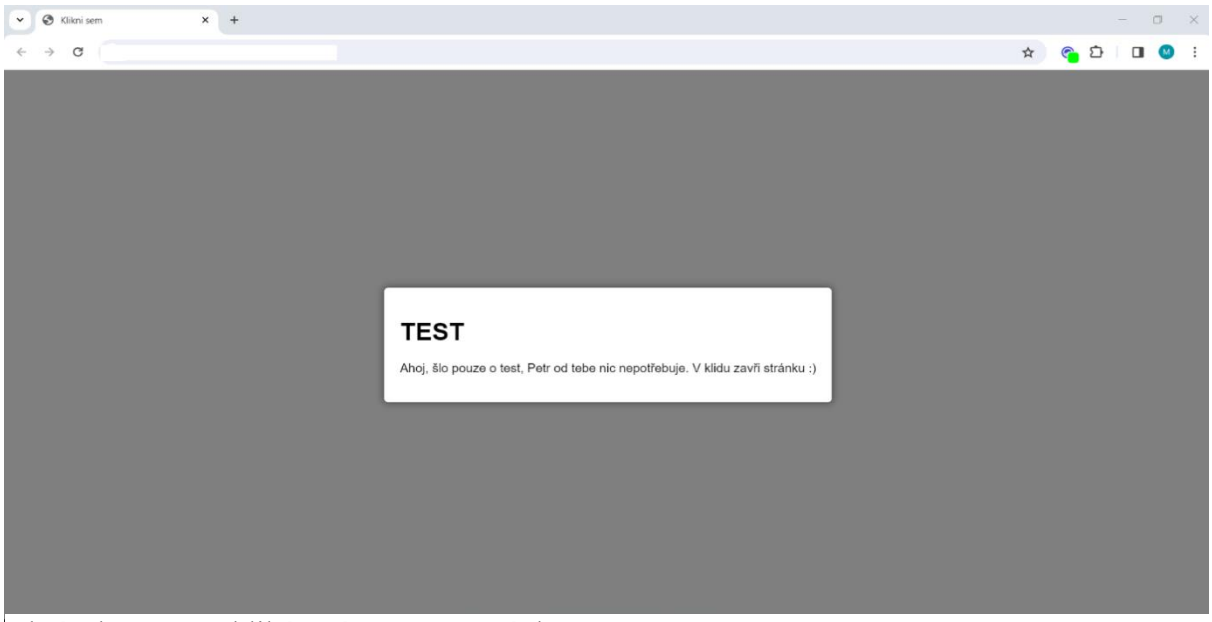
Napsal jsem si pro to tuto stránku. Od pohledu velmi podezřelá, neprofesionální, dokonce s požadavkem na další proklik. Stačil mi samotný přístup na stránku a proklik byl trošku navíc, ale vsadil jsem na lidskou zvědavost.

Věřil jsem totiž, že zvědavost a pocit spěchu je donutí na to kliknout, a následně pak nebudou volat řediteli, že to vypadá divně (případně mě nahlašovat IT). [26], [27]



Obrázek 13 - Stránka připravená na proklik

Zdroj: Vlastní zpracování



Obrázek 14 - Rozklikávací možnost stránky

Zdroj: Vlastní zpracování

5.5.3 Výsledky útoku

Tento test jsem provedl, abych si potvrdil výsledky předchozích osobních rozhovorů, případně je vyvrátil s tím, že to není „tak zlé“. Byl jsem velmi překvapen, jak extrémně úspěšně tento útok dopadl. Jak jsem na začátku uvedl, na pobočce se nachází 13 lidí s přístupem do sítě. Vedoucí odjel a jeho se test netýkal. Bohužel další člověk byl během toho nemocný, takže maximum, co jsem mohl získat bylo 11 prokliků.

Tabulka 1 - Výsledky útoku (Zdroj: Vlastní)

Pozice	ID	Proklik	Čas od odeslání (min)
Sekretářka 1	1	Ano	12
Sekretářka 2	2	Ano	17
Technik 1	3	Ano	50
Technik 2	4	Ano	35
Stavbyvedoucí 1	5	Ano	28
Stavbyvedoucí 2	6	Ano	37
Stavbyvedoucí 3	7	Nemocen	-
Stavbyvedoucí 4	8	Ano	23
Stavbyvedoucí 5	9	Ano	115
Stavbyvedoucí 6	10	Ano	186
Vedoucí sekce 1	11	Ne	-
Vedoucí sekce 2	12	Ano	8
Vedoucí pobočky	13	Nebyl zahrnut v testu	-

Z tabulky lze vyvodit, že úspěšnost útoku byla obrovská. Každého účastníka jsem si označil ID, abych byl schopen dohledat, zda prokliknul, či ne. Z celkem 13 lidí, kteří mají přístup prokliklo 10 z nich. Z toho jeden byl nemocen a vedoucí nebyl zahrnut. To z toho dělá naprosto neuvěřitelné číslo, skoro 91 % účastníků by prošlo dále. Průměrně se proklikli až za dobu 50 minut, nicméně je vidět, že „kancelářské“ pozice jako je sekretářka nebo vedoucí sekce, mají značně kratší dobu prokliku. Bohužel to potvrzuje výsledek z rozhovorů, kde v desáté otázce také všichni až na jednu výjimku podlehli. Z toho lze vyvodit, že se pravděpodobně snažili zaměstnanci při rozhovoru odpovídat pravdivě, a to dává velmi realistický pohled na kyberbezpečnost ve firmě s notnou dávkou důvěryhodnosti.

5.6 Sken zranitelností

Na infrastruktuře firmy jsem provedl tři testy zranitelností pomocí systému Nessus. První test byl venkovní, bez jakékoliv autorizace. Druhým testem byl vnitřní ale také bez autorizace. Posledním testem byl vnitřní test s právy administrátora. Výsledkem testování jsou reporty s ohodnocenými riziky podle CVSS (Common Vulnerability Scoring Systém) v3.1. Rizika mají následující určení: [28]

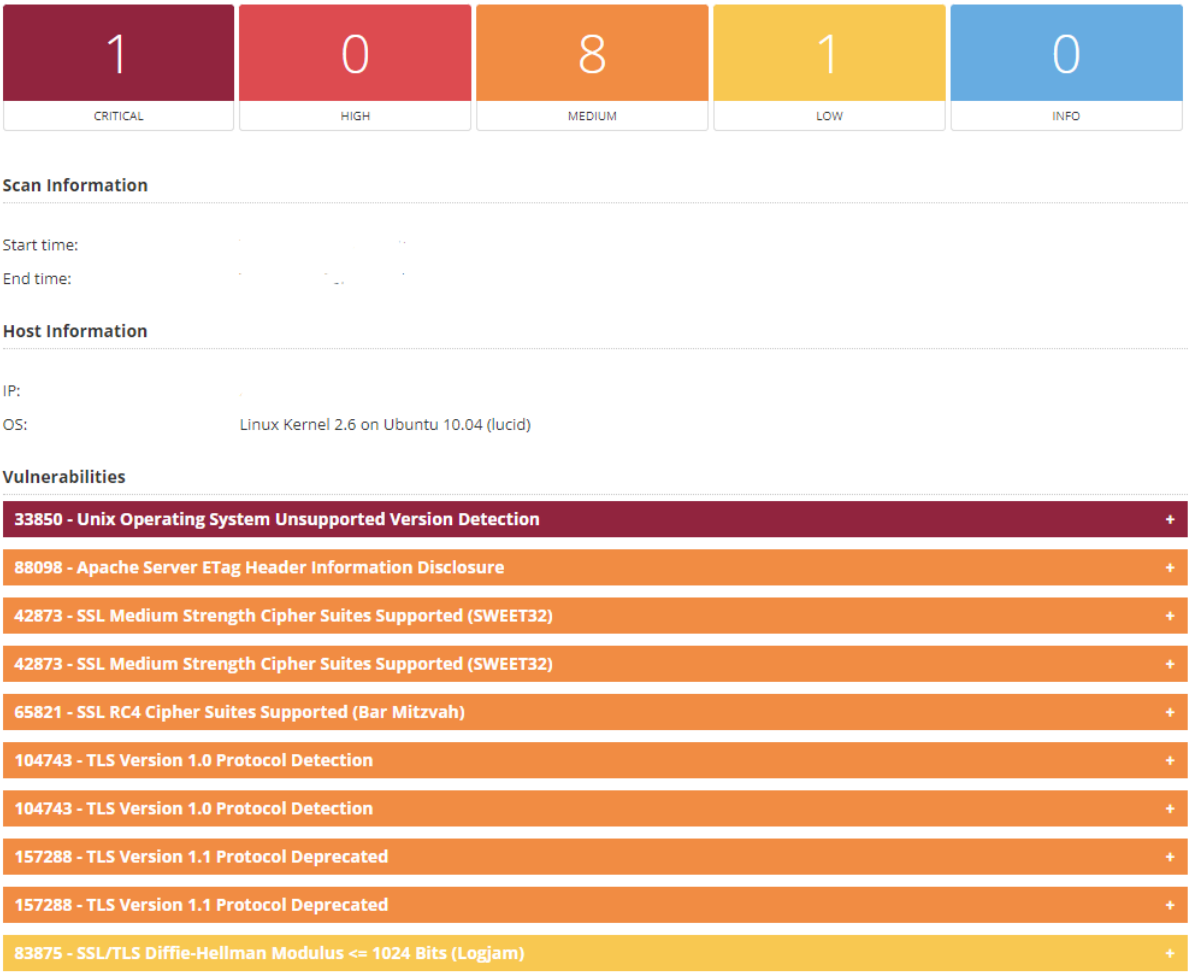
Tabulka 2 - Dělení podle CVSS (Zdroj: Tenable)

Riziko	**Popis**
KRITICKÉ	CVSS skóre zranitelnosti je 10.
VYSOKÉ	CVSS skóre zranitelnosti je mezi 7.0 a 9.9.
STŘEDNÍ	CVSS skóre zranitelnosti je mezi 4.0 a 6.9.
NÍZKÉ	CVSS skóre zranitelnosti je mezi 0.1 a 3.9.
INFORMATIVNÍ	CVSS skóre zranitelnosti je 0 nebo se nejedná o zranitelnost.

Kvůli bezpečnosti firmy jsou některé údaje vymazány a výsledky testu nebudou součástí příloh.

5.6.1 Externí test

Prvním testem byl externí test. Ten probíhá tak, že Nessus proskenuje dané vnější IP adresy a snaží se najít jakékoliv slabé místo pro zneužití. Výsledkem testu je následný report se zjištěnými zranitelnostmi. Je důležité si uvědomit, že tento test byl veden z venku, bez jakýchkoliv oprávnění. Test byl veden pouze na zadanou IP adresu, na kterou mi bylo povoleno sken spustit. Na výsledku vidíme, že nám sken našel dokonce kritickou chybu, kterou je starý operační systém. Chyba je zařazena do kritických chyb a měla by být neprodleně odstraněna. Méně závažné chyby nevyžadují bezodkladné vyřešení, ale je i přesto důležité je nevynechat a snažit se je opravit v rozumném časovém horizontu. [28]

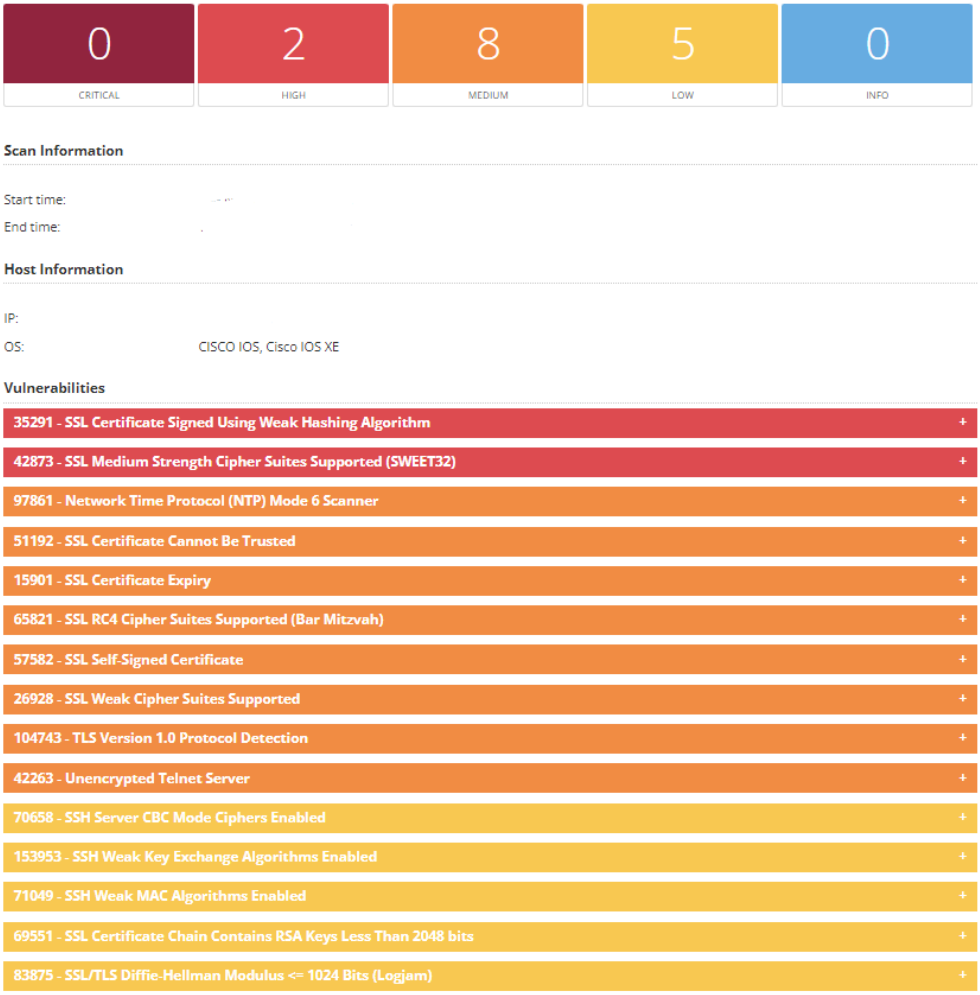


Obrázek 13 - Externí sken zranitelností

Zdroj: Vlastní zpracování

5.6.2 Interní test

Interní test probíhal napojením do interní sítě testované firmy, nicméně stále bez práv. Nutno zdůraznit, že tento test našel na níže zveřejněném obrázku dvě zranitelnosti s vysokou váhou skóre. Tyto chyby by se měli opravit ihned po kritických chybách a zesílit hashovací algoritmus. Nutno dodat, že test našel v dalších zařízeních mnohem víc chyb, nicméně žádné důležitější. Jediné kritické chyby v tomto ohledu byly nalezeny na zařízeních AXIS. Tato zařízení jsou kamery, na kterých nebyl proveden upgrade firmwaru a zůstaly tam zranitelnosti. Díky těmto zranitelnostem by v krajním případě mohlo jít získat kontrolu nad těmito kamerami.



Obrázek 14 - Neautorizovaný sken zranitelností

Zdroj:Vlastní pracování

5.6.3 Interní test s právy administrátora

Poslední test byl proveden z interní sítě s plnými právy administrátora. Jedná se o poslední verzi testu, která simuluje to, co uvidí útočník v moment, kdy dokáže eskalovat svá práva až na administrátorskou úroveň. Výsledky testu jsou značně horší a množství kritických zranitelností by mělo být řešeno.

KRITICKÉ ZRANITELNOSTI	
Identifikátor	Označení zranitelnosti
33850	Nepodporované verze operačních systémů (Unix)
20007	Zastaralé verze protokolu SSL verze 2 a 3 se známými slabostmi
22024	Zranitelný software development kit (SDK) pro UPnP zařízení
117882	Zranitelný firmware systémů společnosti AXIS (ACV-128401)
93650	Zranitelný Dropbear SSH Server
137702	Zranitelnosti v implementaci TCP/IP knihovně společnosti Treck (Ripple20)
55786	Zjištěna Oracle Databáze v nepodporované verzi
58327	Heap-Based Buffer Overflow zranitelnost ve službě Samba
34460	Detekována nepodporovaná verze webového serveru
108797	Nepodporované verze operačních systémů (Windows)
125313	RCE zranitelnost v Microsoft RDP
58987	Nepodporovaná verze PHP
138475	Cross-site scripting (XSS) a další zranitelnosti ve VMware ESXi
73756	Zjištěn Microsoft SQL Server v nepodporované verzi
140696	Zranitelná verze serveru CodeMeter
77823	Remote code execution zranitelnost v Bashi (Shellshock)
156032	Detekována nepodporovaná verze protokolu Apache Log4j
103964	Zastaralá verze Oracle Java SE / Java for Business (JRE)
118233	Kritické zranitelnosti v Oracle MySQL
129500	RCE zranitelnost ve Spring frameworku (CVE-2018-1270)
166034	Chybějící security updaty OS Windows
58134	Nepodporovaná verze Microsoft Silverlight
62758	Nepodporovaná verze Microsoft XML Parseru (MSXML) a XML Core Services
21608	Neaktuální databáze antivirového programu Eset NOD32
4732	Nepodporovaná verze OS koncových stanic
111111	Zranitelné aplikace nainstalované na koncových stanicích
38153	Chybějící security updaty OS Windows na koncových stanicích
97997	Nezabezpečené operace při čtení/zápisu Intel Management Engine (zranitelnost INTEL-SA-00075)

Celkový počet KRITICKÝCH zranitelností: 28

Zdroj: Vlastní zpracování

Obrázek 16 - Shrnutí kritických zranitelností ze skenu

Zdroj: Vlastní zpracování

5.6.4 Shrnutí testu

Na konci celého testování Nessus vygeneruje přehled kritických chyb, které je potřeba řešit. Tento přehled je jen souhrn skupin zranitelností. Konkrétní zranitelnosti jsou uvedeny vždy na testovacím reportu. V tomto konci je vidět, že kyberbezpečnost nepatří mezi priority firmy. Veškeré výsledky testování byly předány firmě a nebudou vzhledem k citlivosti údajů, součástí této práce. Proto tato kapitola slouží pouze k ukázce, jak vypadají data z reálné firmy.

6 Doporučení nápravných opatření

V této kapitole jsou shrnuty identifikované nedostatky v oblasti kybernetické. Identifikované nedostatky jsou popsány a podloženy informacemi získanými během auditu. Na základě těchto zjištění jsou navržena konkrétní řešení a doporučení pro zlepšení bezpečnosti organizace. Tato řešení jsou zaměřena na eliminaci identifikovaných nedostatků a posílení celkové kybernetické odolnosti organizace.

6.1 Shrnutí nedostatků

V rámci analýzy bezpečnosti ve firmě byla identifikována řada závažných nedostatků, které vyžadují okamžitou pozornost a nápravu. Jedním z hlavních problémů je nedostatečná ochrana proti phishingovým útokům. Organizace spoléhá v této oblasti výhradně na firewall a neprovádí implementaci technologií jako je DMARC, což značně zvyšuje riziko úspěšných phishingových útoků, které mohou vést ke kompromitaci citlivých informací zaměstnanců.

Dalším klíčovým nedostatkem je nízká úroveň povědomí zaměstnanců o kybernetické bezpečnosti. Zjištění z rozhovorů ukázala, že zaměstnanci mají jen malou informovanost o důležitých bezpečnostních postupech a politikách firmy v této oblasti. Tato nedostatečná uvědomělost může vést k neuvědomělým chybám a chybějící spolupráci při dodržování bezpečnostních standardů, což zvyšuje riziko úspěšných kybernetických útoků. Důležitým aspektem je také nedostatečné zacházení se zabezpečením pracovních zařízení mimo pracovní dobu. Většina zaměstnanců neprovádí žádná speciální opatření pro zabezpečení svých zařízení mimo pracovní dobu, což zvyšuje riziko zneužití dat nebo útoků na osobní informace zaměstnanců, zejména v prostředí s vyšším rizikem krádeží a ztrát. Dále bylo zjištěno nedostatečné dodržování bezpečnostních postupů při zacházení s podezřelými e-maily. Mnoho zaměstnanců bylo náchylných k otevření e-mailů obsahujících podezřelé odkazy, což zvyšuje riziko infikování firemní sítě škodlivým softwarem a kompromitace citlivých dat.

Tyto identifikované nedostatky představují vážnou bezpečnostní hrozbu pro organizaci a vyžadují okamžitou implementaci nápravných opatření k zajištění ochrany dat a systémů firmy.

6.2 Porovnání

Při analýze zjištěných nedostatků v oblasti kybernetické bezpečnosti jsem identifikoval několik klíčových oblastí, které mohou představovat závažná rizika pro organizaci. Přestože jsem sledoval především ochranu proti phishingovým útokům a ransomware, další problémy mohou být stejně závažné či dokonce závažnější.

6.2.1 Nedostatečná ochrana proti phishingu:

Firma se spoléhala především na firewall jako ochranu proti phishingovým útokům, což může být nedostatečné pro detekci sofistikovaných phishingových e-mailů. Absence implementace technologií jako je DMARC zvyšuje riziko úspěšných phishingových útoků, které mohou vést k úniku citlivých informací a finančním ztrátám.

6.2.2 Nedostatečná ochrana před ransomware:

Nedostatečná ochrana pracovních zařízení mimo pracovní dobu zvyšuje riziko zneužití dat nebo útoků na osobní informace zaměstnanců, což může vést k infikování firemní sítě ransomwarem a výpadkům v provozu.

6.2.3 Nedostatečné povědomí zaměstnanců o kybernetické bezpečnosti:

Neuvědomělost zaměstnanců o důležitých bezpečnostních postupech a politikách firmy může vést k neuvědomělým chybám a kompromitaci firemních systémů. Nedostatečná informovanost zaměstnanců může zvýšit úspěšnost phishingových útoků a šíření ransomwaru.

6.2.4 Nedostatečná transparentnost v komunikaci politik a postupů:

Nedostatek informací o politikách a postupech týkajících se ochrany dat může vést k nízké informovanosti zaměstnanců a nedodržování bezpečnostních standardů, což může ohrozit důvěrnost a integritu firemních dat.

6.2.5 Riziko spojené se sdílením důležitých dat pomocí USB zařízení:

Pravidelné ukládání důležitých souborů na USB za účelem sdílení s jinými stranami, jako jsou subdodavatelé, představuje značná bezpečnostní rizika pro společnost, včetně možného úniku citlivých dat a infekce malwarem.

6.2.6 Rozmanitost postupů při připojování do firemní sítě mimo kancelářské prostředí:

Existence rozdílných postupů při připojování k firemní síti mimo pracoviště, včetně používání soukromých nebo neznámých zařízení, představuje zvýšené bezpečnostní riziko a snižuje účinnost ochrany firemních dat.

6.2.7 Nedodržování základních bezpečnostních postupů při zacházení s podezřelými e-maily:

Nedostatečné povědomí o rizicích spojených s phishingovými e-maily může vést k narušení důvěrnosti a integrity firemních dat a systémů, až po finanční škody způsobené kybernetickými útoky.

6.2.8 Přehled závažnosti problémů

Pro hodnocení jsem zvolil čtyřstupňovou škálu pro hodnocení míry závažnosti identifikovaných rizik.

Pro zjednodušení jsem nepoužil komplexní hodnocení míry rizik v souladu s doporučeními NÚKIB a VKB, kdy míra rizika je výsledkem součinu dopadu, míry hrozby a zranitelnosti daného aktiva, v tomto případě lidských zdrojů a technických aktiv v prostředí ICT firmy.

Vzhledem k omezenému rozsahu vybraného systematického celku (data) využívám pouze okrajově výsledky jejich identifikace a hodnocení, nicméně také s ohledem na čtyřstupňovou škálu používanou v rámci jak VKB, tak ISO 27001:2022.

Takže také pro výsledné shrnutí a vyhodnocení zjištěných dat využívám shodný přístup, kdy hodnotím míru uplatnění hrozby s plným dopadem a s přihlédnutím k tomu, že se hrozba uplatní pouze prostřednictvím zranitelnosti, je zohledněno v doporučeních ke zlepšení a v tabulce.

Tabulka 3 - Popis škály hodnocení zjištěných výsledků (Zdroj: Vyhláška č. 82/2018 Sb.)

Míra		Popis
Nízká	**1**	Zranitelnost neexistuje nebo je její zneužití hrozbou málo pravděpodobné. Bezpečnostní opatření jsou aplikována a jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření nebo omylem způsobené snížení bezpečnosti.
Střední	**2**	Existence zranitelnosti anebo možnost jejího zneužití je pravděpodobná. Bezpečnostní opatření jsou aplikována a jejich účinnost je pravidelně kontrolována, nicméně schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena, přesto nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	**3**	Existence zranitelnosti anebo možnost jejího zneužití je velmi pravděpodobná. Bezpečnostní opatření jsou aplikována, ale jejich účinnost nepokrývá všechny potřebné aspekty, není pravidelně kontrolována a jsou snahy o obcházení nastavených pravidel. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	**4**	Existence zranitelnosti anebo možnosti jejího zneužití je téměř jistá až jistá. Bezpečnostní opatření jsou popsána, ale nejsou plně realizována anebo je jejich účinnost značně omezena lidskými a technickými nedostatky. Neprobíhá kontrola účinnosti bezpečnostních opatření a jsou známé opakovaně úspěšné pokusy překonání bezpečnostních opatření.

Ačkoli byla použitá metoda a způsoby ověření reálného stavu ve firmě zaměřena na objektivní posouzení stavu kybernetické bezpečnosti, je výsledné hodnocení jednotlivých nálezů zatížena subjektivním přístupem k posouzení výstupů. Proto jsem použil Tabulka 3 - Popis škály hodnocení zjištěných výsledků (Zdroj: Vyhláška č. 82/2018 Sb.) s popisy škály a zajistil tak jistou míru objektivizace.[29]

Tabulka 4 - Hodnocení závažnosti (Zdroj: Vlastní)

Problém	Hodnocení
Nedostatečná ochrana proti phishingu	4
Nedostatečná ochrana před ransomware	3
Nedostatečné povědomí zaměstnanců o kybernetické bezpečnosti	4
Riziko spojené se sdílením důležitých dat pomocí USB zařízení	3
Rozmanitost postupů při připojování do firemní sítě mimo kancelářské prostředí	3
Nedodržování základních bezpečnostních postupů při zacházení s podezřelými e-maily	4

6.3 Konkrétní doporučení

Vzhledem k nedostatečné ochraně proti phishingovým útokům, která vyplývá z nedávných výsledků testování kybernetické bezpečnosti, je nezbytné, aby organizace přijala okamžitá opatření ke zlepšení svých obranných mechanismů. Phishingové útoky představují jednu z nejčastějších hrozeb pro bezpečnost firemních sítí a úspěšné phishingové útoky mohou vést k vážným důsledkům, včetně úniku citlivých informací, infikace škodlivým softwarem a finanční ztráty. Následující doporučení jsou navržena s cílem posílit ochranu proti phishingu a zajistit, aby organizace byla lépe připravena na potenciální hrozby. Jejich implementace je klíčová pro zajištění bezpečnosti firemních dat a ochranu před kybernetickými útoky:

1. **Školení zaměstnanců:**

   Školení zaměstnanců o technikách phishingu, rozpoznávání podezřelých e-mailů a správných postupech při manipulaci s neznámými odesílateli je nezbytné pro zlepšení kybernetické gramotnosti v organizaci. Pravidelná a systematická školení jsou klíčová, aby zaměstnanci byli informováni o aktuálních hrozbách a bezpečnostních postupech. Doporučuje se školit zaměstnance alespoň jednou ročně a také po výskytu kybernetického incidentu. Školení po bezpečnostním incidentu je důležité, protože může poskytnout zaměstnancům nezbytné znalosti a dovednosti k prevenci podobných událostí v budoucnu. Pokud se stane nějaký incident, na který nebyli zaměstnanci

dostatečně připraveni, je důležité provést analýzu příčin a následně poskytnout specifické školení zaměstnancům, aby se předešlo opakování podobných chyb. Je zásadní, aby školení zaměstnanců bylo pružné a reagovalo na aktuální potřeby a události v oblasti kybernetické bezpečnosti. Tímto způsobem může organizace neustále posilovat svou obranyschopnost a snižovat riziko kybernetických hrozeb.

2. **Implementace DMARC:**

   DMARC (Domain-based Message Authentication, Reporting, and Conformance) je mechanismus, který slouží k zajištění bezpečnosti elektronické komunikace pomocí ověřování e-mailových zpráv. Tento systém využívá kombinaci již existujících metod, jako je SPF (Sender Policy Framework) a DKIM (DomainKeys Identified Mail), a umožňuje majitelům domén lépe chránit své e-maily před nežádoucím doručením.[26]

   Implementace DMARC přináší několik klíčových výhod. Zaprvé, umožňuje majitelům domén kontrolovat, kdo a jak využívá jejich domény k odesílání e-mailů, a poskytuje jim možnost zlepšit důvěryhodnost jejich doručovaných zpráv. Zadruhé, pomocí zasílání reportů o odesílaných zprávách majitelé domén získávají užitečné informace o chování příjemců a o tom, jak jsou jejich e-maily vyhodnocovány. [26]

   Fungování DMARC je založeno na kontrole DKIM alignment a SPF alignment, které porovnávají různé aspekty e-mailových zpráv, jako je doména odesílatele v hlavičce zprávy a v DKIM podpisu. Díky těmto kontrolám je možné identifikovat a odmítnout podezřelé zprávy a minimalizovat riziko doručení nežádoucího obsahu. [26]

   Pro implementaci DMARC je nutné provést příslušné úpravy v DNS záznamech domény, včetně přidání záznamu typu TXT s odpovídajícími parametry. Kromě toho je třeba zajistit správné nastavení DKIM a SPF politiky a zabezpečit pravidelné zasílání reportů o odesílaných zprávách. [26]

   Celkově lze říci, že implementace DMARC představuje účinný způsob, jak zlepšit bezpečnost elektronické komunikace a ochránit se před nežádoucím doručením e-mailových zpráv. Díky této technologii majitelé domén získávají větší kontrolu nad svými e-mailovými komunikacemi a mohou lépe chránit své uživatele před phishingem a dalšími formami kybernetických útoků. [26]

3. **Správa hesel:**

   Správa hesel je klíčovým prvkem bezpečnostních opatření v naší organizaci. Pro zvýšení úrovně ochrany dat a účtů uživatelů je nezbytné provést změny v procesu správy hesel. Proto bude od nynějška vyžadováno, aby uživatelé pravidelně měnili svá hesla každé 3 měsíce. Tato opatření jsou nezbytná pro zajištění bezpečnosti firemních systémů a ochranu citlivých informací před neoprávněným přístupem.

   Současně s tím bude nutné, aby nová hesla obsahovala kombinaci malých a velkých písmen, čísel a speciálních znaků. Tímto způsobem se zajistí větší odolnost hesel proti různým metodám útoků a zvýší se celková bezpečnost firemní infrastruktury.

   Pro usnadnění správy hesel a zvýšení bezpečnosti navrhuji implementovat nástroj pro správu hesel, jako je třeba Keepass. Tento nástroj umožní uživatelům bezpečně ukládat a spravovat svá hesla a přístupové údaje do šifrovaného úložiště, které je chráněno silným hlavním heslem. Takový nástroj představuje efektivní prostředek k ochraně hesel a snižuje riziko jejich zneužití.

   Kromě toho bude součástí těchto změn také pravidelné školení zaměstnanců o správných postupech pro zacházení s hesly a používání nástroje pro správu hesel. Tím se zvýší povědomí o důležitosti silných hesel a bezpečných postupů pro jejich uchování a použití.

4. **Zálohování:**

   V rámci strategie ochrany dat proti ransomware útokům je klíčové implementovat efektivní zálohovací opatření. Jedním z účinných přístupů k minimalizaci rizika infekce ransomwarem je využití read-only zálohovacího úložiště. Tento přístup zajišťuje, že data uložená na zálohovacím úložišti jsou chráněna před jakýmikoli změnami a úpravami, což v podstatě vylučuje možnost infekce ransomwarem a minimalizuje riziko ztráty dat.

   Kromě toho je možné zvážit nasazení redundatních serverů, které jsou aktivní pouze v době zálohování. Tímto způsobem jsou zálohovaná data fyzicky oddělena od hlavní pracovní sítě, což poskytuje další vrstvu ochrany proti ransomware útokům. Tato síťová oddělenost minimalizuje expozici zálohovaných dat k různým hrozbám, včetně škodlivých útoků.

Využití těchto bezpečnostních opatření vytváří robustní zálohovací strategii, která minimalizuje riziko infekce ransomwarem a zajišťuje bezpečnost a dostupnost firemních dat.

5. **Omezení práv a segmentace sítě**

   Omezení práv na serverech, doplněné o segmentaci sítě, tvoří základní kámen v ochraně proti různým hrozbám, včetně ransomware. Důsledně nastavená oprávnění a rozdělení sítě do segmentů pomáhají minimalizovat riziko neautorizovaného přístupu a omezuje šíření škodlivého softwaru napříč firemní infrastrukturou.

   Na pobočkových serverech je vhodné provést segmentaci sítě, což umožňuje izolovat různé skupiny uživatelů a zařízení. To znamená, že každá skupina má přístup pouze k určitým zdrojům a datům, což minimalizuje riziko, že by ransomware mohl způsobit škody na citlivých datech nebo kritických systémech. Současně umožňuje segmentace rychleji a efektivněji reagovat v případě, že dojde k útoku, protože izoluje postiženou část sítě a brání šíření infekce do dalších oblastí.

   V centrální síti je důležité provést podobné opatření. Centralizovaná správa oprávnění a segmentace sítě umožňuje administrátorům pečlivě kontrolovat přístup k datům a zdrojům. Segmentace umožňuje oddělit různé části sítě a aplikovat různá bezpečnostní pravidla na každou z nich, což zvyšuje odolnost sítě proti ransomware útokům a minimalizuje dopad incidentů.

   Omezení práv a segmentace sítě na serverech na pobočkách i v centrální síti poskytuje vysokou úroveň ochrany firemních dat a systémů. Tato opatření minimalizují riziko neoprávněného přístupu a zvyšují schopnost sítě rychle reagovat na hrozby, jako jsou ransomware útoky.

6. **Změna připojování do sítě**

   Zastavení připojování nedoménových počítačů do firemní sítě představuje klíčové opatření pro zajištění bezpečnosti a stability IT infrastruktury. Existuje několik důvodů, proč je povolení těchto zařízení riskantní a proč je jejich omezení nezbytné.

   Zaprvé, nedoménové počítače nejsou spravovány prostřednictvím firemního správcovského nástroje, což znamená, že nemohou být řádně aktualizovány, monitorovány nebo řízeny. To může vést k nebezpečím spojeným

s neaktualizovaným softwarem a zranitelnostmi, které mohou být využity k útokům, včetně ransomware.

Dále, nedoménové počítače mohou přinést do firemní sítě nežádoucí software, malware nebo škodlivé skripty, což může ohrozit bezpečnost celé infrastruktury. Bez příslušných bezpečnostních opatření a správy těchto zařízení může dojít k infekci celé sítě.

Omezit připojování nedoménových počítačů bude prospěšné z hlediska bezpečnosti, stabilitu sítě a dodržování firemních bezpečnostních politik. Zamezení přístupu neautorizovaným zařízením minimalizuje riziko infekce ransomwarem a dalšími hrozbami. Dále to umožňuje lépe sledovat a spravovat všechna zařízení připojená k síti, což zvyšuje účinnost správy a reakci na bezpečnostní incidenty.

Řešení tohoto problému nemusí být nákladné. Použití integrovaných nástrojů pro správu síťových připojení a politik pro správu zařízení může umožnit snadnou implementaci a řízení zásad omezujících přístup nedoménových počítačů. To zahrnuje využití funkcí Active Directory, skupinových politik a síťových firewallů pro definování pravidel a omezení přístupu na základě doménového členství.

Zastavení připojování nedoménových počítačů je tedy nezbytným krokem ke zvýšení bezpečnosti a stability firemní sítě, a to za relativně nízké náklady a s minimálními dopady na běžný provoz organizace.

7. **Aktualizace softwaru**

Zavedení omezení připojování nedoménových počítačů do firemní sítě vyžaduje současně i aktualizaci politik a postupů týkajících se správy aktualizací softwaru. Změna politiky z uživatelské na správcovskou úroveň je klíčová pro zajištění bezpečnosti a správného fungování IT infrastruktury.

Tradiční přístup, kdy uživatelé mají odpovědnost za aktualizaci svého softwaru, může být neúčinný a riskantní, zejména v prostředí, kde jsou povoleny nedoménové počítače. Z tohoto důvodu je vhodné přejít k centralizované správě aktualizací, kterou obvykle zajišťuje správce IT.

Implementace politiky správcovské úrovně zahrnuje nastavení automatických aktualizací softwaru na všech zařízeních v síti. To zajišťuje, že veškerý software je vždy aktuální a chráněný před známými zranitelnostmi. Kromě toho může být

využit automatizační nástroj, který umožní centrální správu aktualizací a jejich distribuci na všechna zařízení v síti.

Tímto způsobem je zajištěna konzistence a efektivita správy aktualizací, což výrazně snižuje riziko bezpečnostních incidentů spojených s neaktualizovaným softwarem. Současně tento přístup zlepšuje ochranu firemní sítě proti různým hrozbám, včetně ransomware.

Změna politiky aktualizací softwaru na správcovskou úroveň je tedy nezbytným doplňkem k omezení připojování nedoménových počítačů a přispívá k celkové bezpečnosti a stabilitě firemní IT infrastruktury.

8. **Podmíněný přístup**

Zavedení podmíněného přístupu na základě polohy nebo času představuje další účinné opatření ke zvýšení bezpečnosti a kontroly ve firemní síti. Tato strategie umožňuje definovat specifické podmínky pro povolení připojení nedoménových počítačů, minimalizuje tak rizika spojená s jejich používáním. [18]

Přístup na základě polohy umožňuje nastavit podmínky, za nichž je doménovým zařízením povolen přístup do firemní sítě pouze z určitých fyzických umístění, například z firemních prostor nebo přes virtuální privátní síť (VPN). Tímto způsobem lze omezit rizika spojená s připojením zařízení z neznámých nebo neautorizovaných míst.

Podobně přístup na základě času umožňuje určit specifické časové intervaly, během nichž je doménovým zařízením povolen přístup do firemní sítě. Toto opatření může být užitečné například pro přístup zaměstnanců na cestách, kteří potřebují přístup ke firemním prostředkům pouze během pracovní doby.

Kombinace obou přístupů umožňuje vytvořit robustní strategii zabezpečení, která zajišťuje, že doménová zařízení mají přístup do firemní sítě pouze za přesně definovaných podmínek, což minimalizuje rizika spojená s jejich používáním. V neposlední řadě je potřeba zavést dvoufázové ověřování.

9. **Zamezení USB**

Implementace opatření proti vynášení USB zařízení s firemními daty je klíčovým prvkem zabezpečení firemní infrastruktury a ochrany citlivých informací. Existuje několik doporučení a řešení, která lze zavést k minimalizaci rizika spojeného s neoprávněným vynášením USB zařízení.

Prvním krokem je nastavení politiky pro správu zařízení, která umožní administrátorům centrálně řídit přístup k USB portům na pracovních zařízeních. Tímto způsobem lze například zakázat přístup k USB portům pro uživatele, kteří nejsou oprávněni pracovat s citlivými daty, nebo povolit pouze určitým skupinám uživatelů práci s externími zařízeními. Kromě výše zmíněných opatření je také vhodné zvážit implementaci síťových úložišť pro sdílení dat, jako je například OneDrive. Tato řešení umožňují zaměstnancům snadný a bezpečný způsob sdílení a ukládání dokumentů a souborů, aniž by bylo nutné používat externí USB zařízení.

OneDrive a podobné platformy poskytují možnost centrálního ukládání dat v cloudu, což zajišťuje jejich dostupnost z libovolného místa a za jakýchkoliv okolností. Zaměstnanci mohou jednoduše nahrávat, sdílet a synchronizovat soubory mezi různými zařízeními, aniž by bylo nutné používat USB flash disky. Implementace síťových úložišť také umožňuje administrátorům efektivně spravovat přístup k datům a nastavovat oprávnění pro jednotlivé uživatele. To znamená, že lze definovat, kdo má přístup, k jakým dokumentům a souborům, a minimalizovat tak riziko neoprávněného přístupu nebo sdílení citlivých dat.

Díky možnosti vytvářet zálohované kopie dat a historii verzí dokumentů lze také zvýšit bezpečnost a spolehlivost uchovávání firemních informací. V případě, že dojde k havárii nebo útoku na jedno zařízení, jsou data stále k dispozici z jiných zdrojů a není nutné spoléhat pouze na fyzická USB zařízení.

Celkově lze tedy implementací síťových úložišť pro sdílení dat, jako je OneDrive, dosáhnout bezpečného a efektivního způsobu práce se soubory a dokumenty, a to bez nutnosti vynášení USB zařízení mimo firemní prostředí. To přispívá k ochraně citlivých informací a minimalizaci rizika spojeného s neoprávněným přístupem k firemním datům.

10. Opravení chyb zjištěných skenem zranitelnosti

Oprava těchto slabých míst je nezbytná pro minimalizaci rizika a ochranu firemních dat. To může zahrnovat instalaci opravných aktualizací a záplat, konfiguraci bezpečnostních politik a pravidel, aktualizaci softwaru a hardwaru na nejnovější verze a implementaci dalších bezpečnostních opatření doporučených výrobci a odborníky na kybernetickou bezpečnost. Proces opravy zranitelností by měl být pravidelný a systematický, s důrazem na prioritizaci

oprav podle závažnosti zjištěných zranitelností. To znamená, že zranitelnosti s vyšším rizikem a potenciálním dopadem by měly být opraveny jako první.

Oprava slabých míst a zranitelností je klíčovým prvkem celkové strategie kybernetické bezpečnosti a přispívá k ochraně firemních aktiv a zachování důvěryhodnosti a integrity IT prostředí.

ZÁVĚR

Cílem této práce bylo zhodnotit současné zabezpečení firmy a navrhnout řešení, které by pomohlo posílit bezpečnostní postupy a ochranu firemní infrastruktury. Analyzoval jsem existující bezpečnostní opatření, identifikoval slabá místa a zranitelnosti prostřednictvím skenování, phishingového útoku a osobních rozhovorů. Na základě této analýzy jsem vypracoval doporučení a návrhy pro zlepšení bezpečnosti, které zahrnovaly implementaci nových technologií, aktualizaci politik a postupů.

Vypracoval jsem komplexní a efektivní opatření, která by minimalizovala rizika spojená s kybernetickými hrozbami a posílila ochranu firemních aktiv a citlivých dat. Zaměřil jsem se na prevenci útoků, detekci potenciálních hrozeb a rychlou reakci v případě bezpečnostních incidentů. Při návrhu řešení jsem také bral v úvahu potřeby a specifika dané firmy, aby byla navržená opatření co nejefektivnější a nejvhodnější pro konkrétní prostředí.

Celkově lze konstatovat, že cíle této práce byly splněny. Na základě provedené analýzy a navržených opatření by měla firma dosáhnout výrazného zlepšení svého zabezpečení a snížení rizika kybernetických útoků. Implementace doporučení by měla vést k posílení odolnosti infrastruktury vůči různým hrozbám a zabezpečit kontinuitu provozu a ochranu citlivých dat. Je důležité, aby firma přistoupila k realizaci navržených opatření s odpovídající prioritou a angažovaností, aby bylo dosaženo očekávaných výsledků a udržena vysoká úroveň kybernetické bezpečnosti v dlouhodobém horizontu.

POUŽITÁ LITERATURA

[1] STEINBERG, J.; BEAVER, K.; WINKLER, I. a COOMBS, T. *All-in-One For Dummies*. Wiley, 2023. ISBN ISBN 139415285X..

[2] SMEJKAL, V. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* 2. vydání. Aleš Čeněk, 2019. ISBN ISBN 978-80-7380-765-8.

[3] ISO. ISO/EIC, *27001*. 2022.

[4] NIST. *The NIST Cybersecurity Framework (CSF) 2.0.* Online. 2024. Dostupné z: https://doi.org/10.6028/NIST.CSWP.29. [cit. 2024-05-17].

[5] EVROPSKÝ PARLAMENT. *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).* Online. 2022. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.CES. [cit. 2024-05-17].

[6] PARLAMENT ČESKÉ REPUBLIKY. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* Online. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/181_2014_Sb.%20Platn%20znn.pdf. [cit. 2024-05-17].

[7] *Co přináší nová směrnice EU o síťové a informační bezpečnosti?* Online. 2016. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf. [cit. 2024-05-17].

[8] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC, 2019. ISBN ISBN 978-80-88168-31-7.

[9] CROWDSTRIKE. *10 most common types of cyber attacks*. Online. 2024. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/. [cit. 2024-05-17].

[10] PALO ALTO NETWORKS. *Malware | What is Malware & How to Stay Protected from Malware Attacks*. Online. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-malware. [cit. 2024-05-17].

[11] MICROSOFT. *Co je ransomware?* Online. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-ransomware. [cit. 2024-05-17].

[12] FORTINET. *What Is DDOS Attack?* Online. Dostupné z: https://www.fortinet.com/resources/cyberglossary/ddos-attack. [cit. 2024-05-17].

[13] CROWDSTRIKE. *10 types of social engineering attacks and how to prevent them.* Online. 2023. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/. [cit. 2024-05-17].

[14] RAPID7. *Man in the Middle (MITM) Attacks*. Online. 2023. Dostupné z: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/. [cit. 2024-05-17].

[15] CROWDSTRIKE. *What is a zero-day exploit?* Online. 2022. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit/. [cit. 2024-05-17].

[16] CRASHPLAN. *Think Your Small Business is Immune to Cyber Attacks? Think Again.* Online. 2023. Dostupné z: https://www.crashplan.com/resources/guide/think-your-small-business-is-immune-to-cyber-attacks/. [cit. 2024-05-17].

[17] CHECK POINT SOFTWARE TECHNOLOGIES LTD. [17] *How to Create a Cybersecurity Disaster Recovery Plan.* Online. Dostupné z: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/how-to-create-a-cybersecurity-disaster-recovery-plan/. [cit. 2024-05-17].

[18] AO KASPERSKY LAB. *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable form Within*. Online. Dostupné z: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. [cit. 2024-05-17].

[19] OPEN TEXT CORPORATION. *What is an Insider Threat*? Online. Dostupné z: https://www.opentext.com/what-is/insider-threat. [cit. 2024-05-17].

[20] PALO ALTO NETWORKS. *What Is Data Classification?* Online. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/data-classification. [cit. 2024-05-17].

[21] MICROSOFT. *Co je podmíněný přístup?* Online. 2024. Dostupné z: https://learn.microsoft.com/cs-cz/entra/identity/conditional-access/overview. [cit. 2024-05-17].

[22] THALES. *Thales Luna HSMs*. Online. Dostupné z: https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms. [cit. 2024-05-17].

[23] BUSINESS INSIDER. *Brace yourself for 'Q-Day,' a global cybersecurity event that could expose our most important secrets*. Online. 2023. Dostupné z: https://www.businessinsider.com/q-day-2025-cybersecurity-quantum-computing-data-security-privacy-china-2023-12. [cit. 2024-05-17].

[24] TECHTARGET. *The 7 critical backup stratégy best practices to keep data safe.* Online. 2023. Dostupné z: https://www.techtarget.com/searchdatabackup/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe. [cit. 2024-05-17].

[25] MICROSOFT. *Disaster recovery best practices and strategies for SharePoint search*. Online. 2023. Dostupné z: https://learn.microsoft.com/en-us/sharepoint/search/best-practices-of-disaster-recovery-for-search. [cit.2024-05-17].

[26] SEZNAM.CZ A. S. *DMARC.* Online. Dostupné z: https://napoveda.seznam.cz/cz/dmarc-zaznam/. [cit. 2024-05-17].

[27] CANIPHISH. *How To Spoof An Email Address In 5 Steps.* Online. 2024. Dostupné z: https://caniphish.com/blog/how-to-spoof-an-email-address. [cit. 2024-05-17].

[28] TENABLE, INC. *Scans.* Online. 2024. Dostupné z: https://docs.tenable.com/nessus/Content/Scans.htm. [cit. 2024-05-17].

[29] PARLAMENT ČESKÉ REPUBLIKY. *Vyhláška č.82/2018.* Online. 2018. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#f6228905. [cit. 2024-05-17].