UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

DIPLOMOVÁ PRÁCE

2024 Bc. Monika Oberfalcerová

Univerzita Pardubice

Fakulta ekonomicko-správní

Kybernetická bezpečnost a ochrana dat

Diplomová práce

2024 Bc. Monika Oberfalcerová

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Monika Oberfalcerová**
Osobní číslo:	**E22764**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Kybernetická bezpečnost a ochrana dat**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cíl práce: Zhodnoťte situaci z hlediska kybernetické bezpečnosti a ochrany dat ve vybraném podniku.

- vytvořte ucelený přehled o aktuálních bezpečnostních hrozbách
- zhodnoťte situaci z hlediska kybernetické bezpečnosti a ochrany dat ve vybraném podniku.
- Navrhněte opatření pro vybraný podnik ke zlepšení bezpečnostní situace, např. zálohování, metod kryptografie, GDPR, ochrany počítačových systémů před neoprávněným přístupem, útoky, škodlivým softwarem a dalších.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
SMEJKAL, Vladimír. Kybernetická kriminalita. 2., rozš. a aktualiz. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80--88168-31-7.
KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
DOUCEK, Petr. Řízení bezpečnosti informací. 2., rozš. a aktualiz. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

Vedoucí diplomové práce: **prof. Ing. Jan Čapek, CSc.**
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.
děkan

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

V Pardubicích dne 1. září 2023

Prohlašuji:

Práci s názvem Kybernetická bezpečnost a ochrana dat jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, 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. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne

Bc. Monika Oberfalcerová

PODĚKOVÁNÍ

Chtěla bych poděkovat vedoucímu práce, panu prof. Ing. Janu Čapkovi, CSc., za cenné rady, odbornou pomoc a doporučení, které mi pomohly při zpracování diplomové práce.

ANOTACE

Tato diplomová práce se věnuje problematice kybernetické bezpečnosti a ochrany dat ve vybraném podniku. Úvodní část práce představuje základní pojmy a principy v oblasti kybernetické bezpečnosti. Na základě konzultací s IT managementem dané společnosti byla provedena SWOT analýza a na jejím základě jsou dále navržena specifická opatření ke zlepšení kybernetické bezpečnosti, včetně organizačních, procesních a technologických doporučení. Práce poskytuje praktická doporučení, která mohou významně přispět k ochraně citlivých dat a zvýšení celkové bezpečnosti podniku. Výsledky práce nabízejí nejen nové poznatky o kybernetické bezpečnosti v konkrétním podniku, ale také metodiku pro zlepšení bezpečnostních opatření v podobných organizacích.

KLÍČOVÁ SLOVA

kybernetická bezpečnost, kybernetické útoky, ochrana dat, bezpečnostní opatření, organizační bezpečnost

ANNOTATION

This thesis addresses the issues of cybersecurity and data protection in a selected company. The introductory part of the thesis presents basic concepts and principles in the field of cybersecurity. SWOT analysis was conducted based on consultations with the IT management of the company, and specific measures to improve cybersecurity, including organizational, procedural, and technological recommendations, were proposed based on this analysis. The thesis provides practical recommendations that can significantly contribute to the protection of sensitive data and the overall security of the company. The results of the thesis offer not only new insights into cybersecurity in a specific company but also a methodology for improving security measures in similar organizations.

KEYWORDS

Cybersecurity, Cyber attacks, Data Protection, Security Measures, Organizational Security

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

AI – Artificial intelligence (umělá inteligence)

APT - Advanced Persistent Threat (pokročílá trvalá hrozba)

ARP – (Address Resolution Protocol (služení protokol v počítačových sítích)

BCP – Business Continuity Plan (plán kontinuity činností)

BEC - Business E-mail Compromise (emailové útoky)

DDoS - Distributed Denial-of-Service (Distribuované odepření služby)

DHCP - Dynamic Host Configuration Protocol (protokol z rodiny TCP/IP)

DMZ – Demilitarized zone (demilitarizovaná zúona)

DNS – Domain Name System (systém doménových jmen)

DRP – Disaster Recovery Plan (plán obnovy)

IAM – Identity and Access Management (Správa identit a přístupu)

ICT – Information and Communication Technologies (informační a komunikační technologie)

IDS – Intrusion Detection System (systém pro odhalení průniku)

IPS – Intrusion Prevention System (systém prevence narušení)

IP – Internet Protocol (protokol propojení sítí)

IS – Information System (informační systém)

ISMS - Systém řízení bezpečnosti informací **(**Information Security Management Systém)

IT - Information Technology (informační technologie)

IoT – Internet of Things (internet věcí)

HTTP – HyperText Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

LAN – Local Area Network (lokální síť)

LLM – Large Language Model

MD5 - Algoritmus Message Digest 5

MFA – Multi-Factor Authentication (vícefaktorová autentizace)

NAC – Network Access Control (řízení přístupu)

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PDCA – Plan-do-check-act (naplánuj-proveď-ověř-jednej)

PoLP - Principle of least privilege (princip minimálního oprávnění)

RAM – Random Access Memory (paměť s náhodným přístupem)

RBAC - Role-based access kontrol (RBAC)

SCADA – Supervisory Control and Data Acquisition (dohledové řízení a získávání dat)

SIEM - Security Information and Event Management (systém pro správu bezpečnostních informací a událostí)

SoD – Segregation of Duties (segregace povinností)

SQL- Stuctured Query Language (strukturovaný dotazovací jazyk)

SSO – Single sign on

SWOT – zkratka, kde S = Strengths (Silné stránky), W = Weaknesses (Slabé stránky), O = Opportunities (Příležitosti), T = Threats (Hrozby)

TLS – Transport Layer Security

VLAN – Virtual Local Area Network (virtuální lokální síť)

VPN – Virtual Private Network (virtuální privátní síť)

ZTNA – Zero Trust network access (přístup k síti Zero Trust)

2FA – Two-factor authorization (dvoufaktorová autentizace)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Kybernetická bezpečnost a ochrana dat se stávají stále důležitějšími pro všechny podniky v dnešním digitálním věku. S rostoucí digitalizací a závislostí na informačních technologiích roste počet kybernetických hrozeb a útoků a proto účinná ochrana dat a robustní kybernetická bezpečnost jsou nezbytné pro zajištění kontinuity podnikání, ochranu reputace a zachování důvěry klientů.

Tato diplomová práce se zaměřuje na analýzu problematiky kybernetické bezpečnosti a ochrany dat. V první části se věnuje základním principům kybernetické bezpečnosti, včetně rozboru různých druhů kybernetických útoků a jejich dopadů. Zkoumá techniky jako malware, DDoS útoky, sociální inženýrství, skenování portů, zero day útoky, DNS tunneling a další pro poskytnutí uceleného přehledu o hrozbách, kterým čelí moderní informační systémy.

Práce je následně zaměřena na vývoj kybernetické bezpečnosti jak ve světě, tak v České republice a analyzuje současný stav a trendy v této oblasti. Seznamuje o organizačních opatřeních, která jsou nezbytná pro efektivní řízení bezpečnosti informací, včetně systému řízení bezpečnosti informací a bezpečnostní politiky organizací v souladu se zákonnými povinnostmi. Technická opatření jsou dalším klíčovým aspektem této práce a zabývá se konkrétními bezpečnostními opatřeními, ochranou sítí a služeb, aplikační bezpečností a zabezpečením vzdáleného přístupu k počítačovým systémům.

Praktická část práce zahrnuje analýzu současného stavu kybernetické bezpečnosti v organizaci, kde je provedena detailní SWOT analýza, která identifikuje silné stránky, slabé stránky, příležitosti a hrozby spojené s kybernetickou bezpečností podniku. Tato analýza poskytne komplexní pohled na interní a externí faktory, které ovlivňují bezpečnostní postavení organizace. Informace ke SWOT analýze jsou na základě odpovědí IT managementu podniku. Zjištění ze SWOT analýzy budou základem pro formulaci konkrétních návrhů a doporučení.

Cílem této diplomové práce je poskytnout komplexní pohled na kybernetickou bezpečnost a ochranu dat, identifikovat hlavní hrozby a navrhnout efektivní opatření pro jejich zmírnění. Diplomová práce má přispět k lepšímu pochopení důležitosti kybernetické bezpečnosti a pomoci organizacím lépe chránit své informace a data před stále sofistikovanějšími kybernetickými hrozbami.

1 KYBERNETICKÁ BEZPEČNOST

Pro pojem bezpečnost existuje mnoho definic. Cílem bezpečnosti je ochrana něčeho před poškozením, zničením, nebo odcizením. Dle Výkladového slovníku kybernetické bezpečnosti je kybernetická bezpečnost souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.[1] Kyberprostorem rozumíme prostor, kde se odehrává komunikace prostřednictvím počítačových sítí a ze kterého může přijít kybernetický útok. Kybernetickou bezpečnost můžeme definovat jako určitou ochranu počítačů, sítí a dalších připojených zařízení před kybernetickými útoky vedenými z kyberprostoru. Kyberzločinci se snaží narušit základní atributy bezpečnosti. Jedná se o ohrožení dostupnosti počítačů a počítačových sítí, důvěrnosti a integrity dat, která jsou uložena na počítačích a jejich sítích, zpracovávána anebo přes ně přenášena. Kybernetické útoky se snaží zneužít nějaké zranitelnosti, která může být vlastnost nějakého informačního aktiva, nebo absencí či nedostatečnosti bezpečnostních opatření, která by měla být v organizaci zavedena.

Informační aktiva jsou data, informace, znalosti, software, hardware, uložiště dat a IT zařízení, která mají pro firmu hodnotu. Jelikož bez nich nemohou fungovat procesy a probíhat rozhodování a řízení, jejich ztráta, odcizení, nebo zneužití přestavují pro firmu problém.

Jednotlivá kybernetická rizika by měla být analyzována a následně by mělo být rozhodnuto o jejich zvládání. Měly by být zavedeny jisté sady bezpečnostních opatření. Kybernetická bezpečnost je poměrně mladý obor a je součástí informační bezpečnosti, jež se zabývá ochranou informací zpracovávaných, uchovávaných a přenášených v jakékoli podobě a na jakémkoliv médiu. Neprobíhá pouze v elektronické podobě mezi počítači, ale může mít i podobu na papíře, nebo mít formu ústní výměny informací mezi lidmi, kteří jsou také součástí informačního systému.[2]

1.1 Dopady kybernetických útoků

Kybernetický útok představuje snahu o anonymní infiltraci a neoprávněný přístup k počítači, výpočetnímu systému, počítačové síti nebo jiné technologii s cílem způsobit škodu, nebo ubohacení útočníka. Cílem kybernetického útoku může být neoprávněné odcizení či zničení dat a informací, využití prolomeného počítačového nebo informačního systému k provedení dalších útoků, ovládnutí výpočetního prostředí či infrastruktury, deaktivace počítače, a podobně. Mohou být iniciativou jednotlivců či skupin, známých jako hackeři nebo hacktivisté, a mohou být součástí politicky motivovaných kybernetických válek mezi státy nebo kyberterorismu ze strany nestátních aktérů a teroristů. Hackerům často jde o vydírání a vymáhání výkupného,

přičemž preferovanou formou platby je většinou kryptoměna, což umožňuje útočníkům udržet svou anonymitu. Kybernetické útoky jsou stále sofistikovanější, což představuje rostoucí hrozbu pro národní bezpečnost. Důvody a motivace těchto útoků jsou rozmanité a zahrnují aktivity jako sabotáže, špionáž, krádeže, podvody, hacktivismus a další.[3]

Dopady kybernetických útoků se vždy projeví negativně na zisku společnosti, jejího tempa růstu, ale i může vést ke krachu nebo nucené likvidaci společnosti. Závažnost útoku se odvíjí od úrovně zavedených opatření. Po úspěšném útoku je nutné vynaložit určité náklady na uvedení systému do původního stavu a je potřeba přijmout opatření k zamezení stejné situace. Společnost může utrpět okamžitou ztrátu z důvodu nemožnosti poskytovat své služby. Dále ji může klesnout tržní podíl, klesnout počet klientů pro ztrátu důvěry, může dostat pokutu, čelit sankcím a platit soudní výlohy. Rovněž je ohrožen zájem potenciálních klientů.**Chyba! Nenalezen zdroj odkazů.**

1.2 Druhy kybernetických útoků

Kybernetické útoky představují závažnou hrozbu pro jednotlivce, podniky i státní instituce. Existuje celá řada druhů kybernetických útoků, které se liší svou technikou, cíli a následky.

1.2.1 Hacking

Pojem hacker vznikl v 50. letech 20. století a označuje technicky nadanou osobu, která je schopná nalézt nová řešení problému. Hacking lze označit jako proniknutí do počítačového systému nestandartním způsobem, většinou obejitím, nebo prolomením jeho bezpečnostního systému. Cílem tohoto jednání je dokázání si hackerovy intelektuální převahy a schopnosti, aniž by měl hacker zájem na zisku, anebo zničení informací v systému. Hacker také může využívat své znalosti ve prospěch počítačových systémů, odstraňováním programovacích chyb, diagnostikou vadného hardware. Ne každá aktivita hackerů je legální, protože dochází k porušení základních lidských práv a svobod.

1.2.2 Cracking

Cracker má podobné schopnosti jako hacker, ale je označen za osobu slídící a snažící se odhalit citlivé informace, s cílem jejich následného neoprávněného užití. Poškozuje počítačové sítě a počítače pro vlastní zviditelnění a pro zisk. Jeho znalosti počítačových systému a programování nejsou většinou na tak vysoké úrovni jako u hackera a většinou pracuje ve skupině.

Password cracking slouží k zjištění přístupového hesla licencovaného systému, nebo programu. Crackerem je vytvořen keygen, anebo crack, který umožní následné užití programu. Upravené programy tímto způsobem bývají sdíleny na warez fórech a P2P sítích.[4][4]

1.2.3 Malware

Malware označuje jakýkoli software úmyslně navržený k poškození počítače, serveru, klienta nebo počítačové sítě. Může mít různé podoby:

Phishing probíhá prostřednictvím e-mailů, webů, textových zpráv či jiných forem elektronické komunikace, kdy se kyberzločinec vydává za důvěryhodný zdroj s cílem odcizit citlivé informace. Kyberzločinec se může vydávat za banku a poslat příjemci varovný email, že jeho účet byl z důvodu podezřelé aktivity zablokován. Po kliknutí uživatele na odkaz v emailu se nainstaluje do počítače uživatele malware. Cílem phishingových metod je odcizení hesel, uživatelských jmen, údajů o platebních kartách a bankovních údajů, krádeže identity a odcizení peněz přímo z osobního bankovního účtu, nebo platební karty.

Spyware bývá nainstalován bez vědomí uživatele. Může monitorovat chování online, snižovat výkon zařízení a měnit jeho nastavení, shromažďovat citlivé informace.

Adware je taktéž nainstalován bez vědomého souhlasu uživatele. Cílem je zobrazování agresivní reklamy v automaticky otevíraných oknech, aby generovaly zisky díky kliknutím. Adware často zpomalují výkon zařízení a mohou instalovat další software a měnit nastavení prohlížeče, čímž zvyšuje zranitelnost zařízení vůči jiným malwarovým útokům.

Viry narušují normální provoz zařízení zaznamenáváním, poškozováním a odstraňováním jeho dat. Často jsou do jiných zařízení šířeny otevřením škodlivého souboru.

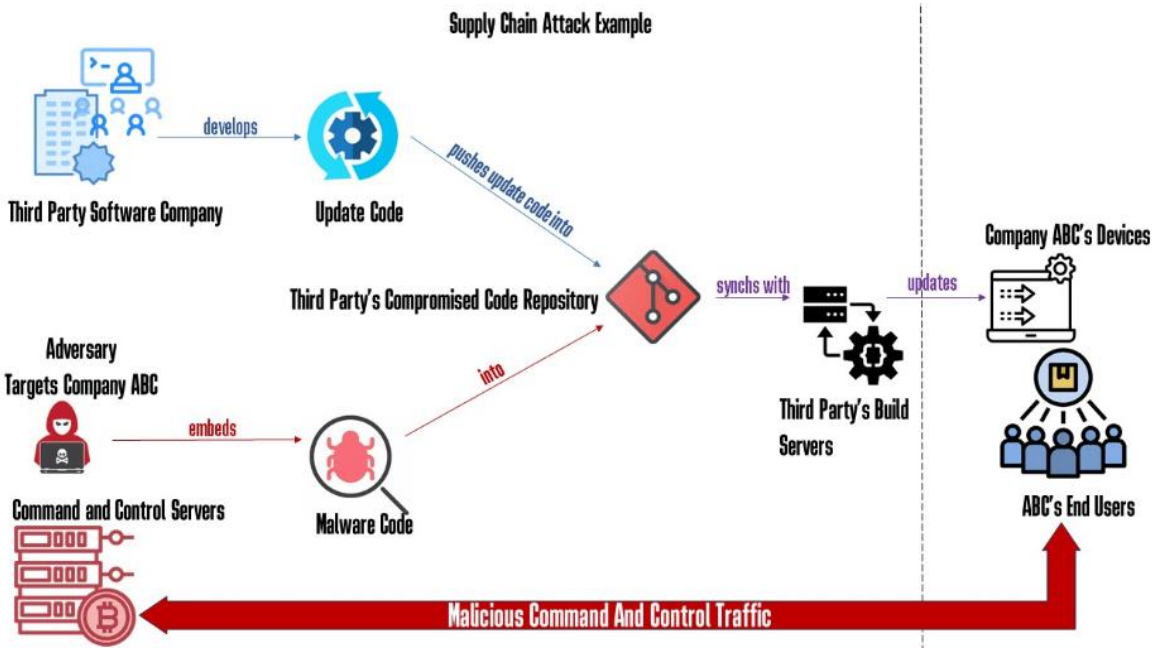
Programy pro zneužití slabých míst a jejich sady zneužívají slabá místa a jsou také označované jako exploit a využívají zranitelnosti v softwaru. Obchází bezpečnostní opatření počítače a následně infikují zařízení. Hackeři s nekalými úmysly aktivně vyhledávají zastaralé systémy, která mají ohrožené zabezpečení a využívají je k nasazení malwaru. Integrací kódu prostředí do programu s cílem využít tato slabá místa, mohou kyberzločinci stáhnout další malware, který následně napadne další zařízení a infiltruje organizaci. Programy pro zneužití slabých míst se mohou ukrývat v reklamách na legitimních webech bez tušení provozovatelů, jako emailová příloha, nebo na škodlivých webech. Jako příklad potenciálně infikovaného softwaru lze uvést Adobe Flash Player, Adobe Reader, webové prohlížeče, Oracle Java a Sun Java. Mezi běžné sady tohoto typu patří Angler/Axpergle, Neutrino a Nuclear.

Bezsouborový malware je obtížné najít a odstranit, jelikož většina antivirových programů není navržena, aby kontrolovala firmware. Bezsouborový malware může například přijít prostřednictvím škodlivých síťových paketů, které následně zneužijí ohrožení zabezpečení.

Malware využívající makra se ukrývá v infikovaných e-mailových přílohách a souborech ZIP, které jsou maskované jako právní dokumenty, účtenky a faktury, aby uživatelé byly nuceni k jejich otevření. V posledních verzích Microsoft Office jsou ve výchozím nastavení makra zakázaná a proto kyberzločinci musí uživatele donutit k jejich zapnutí, aby šlo tímto způsobem zařízení infikovat.

Ransomware - útočník vyhrožuje obětem zničením nebo zablokováním dat, pokud nezaplatí výkupné. Při útocích s využitím ransomwaru vedených lidmi je organizace napadena chybami v konfiguraci systému a zabezpečení, což umožňuji infiltrace malwaru. Často bývá doprovázena zašifrováním dat v organizaci, kdy útočník má data a organizace se k vlastním datům nedostane. Útočníci cílí na velké organizace, protože jsou schopné zaplatit výkupné v řádech milionů dolarů. Často získávají přístup k sítím prostřednictvím krádeže přihlašovacích údajů zaměstnance. Mnoho organizací volí placení výkupného, než by nechaly uniknout citlivá data a riskovaly další kyberútoky, i přes nejistotu úplné ochrany dat.

Útoky na dodavatelské řetězce – kybernetické útoky na dodavatelské řetězce se zaměřují na slabá místa u dodavatelů, jako jsou poskytovatelé softwaru, služeb nebo komponent, aby získali přístup k větším cílovým společnostem. Útočníci mohou infiltrovat dodavatelský řetězec prostřednictvím škodlivého softwaru, kompromitovaných aktualizací softwaru nebo zranitelných systémů dodavatelů.



Obrázek 1: Útok na dodavatelský řetězec

Zdroj: CovertSwarm

Podvody spojené s technickou podporou - kyberzločinec může přímo zavolat uživateli a vydávat se za pracovníka softwarové společnosti. Jakmile si získá důvěru, naléhá na instalaci aplikace, nebo poskytnutí vzdáleného přístupu k uživatelovu zařízení. Cílem je přimět uživatele zaplatit za nepotřebné služby technické podpory z důvodu zfalšovaného problému se zařízením, platformou nebo softwarem, nebo přimět uživatele naistalovat malware.

Trojský kůň může být samostatný program, nebo bývá ukryt v jiných souborech a programech, které navenek působí legitimně. Uživatel může stáhnout trojského koně ve víře, že stahuje nějaký prospěšný program do počítače. Například když stahuje z nedůvěryhodného serveru, může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou. Trojský kůň může stahovat a instalovat další malware, zneužívat infikované zařízení k podvodným kliknutím, zaznamenávat stisknutí kláves, zaznamenávat informace o navštívených webech, odesílat hackerovi informace jako hesla a přihlašovací údaje, nebo poskytnout kyberzločinci kontrolu nad zařízením.

Červi se mohou nacházet v přílohách e-mailů, programech pro sdílení souborů, na sociálních sítích, vyměnitelných jednotkách, v síťových sdílených složkách a textových zprávách. Červ se kopíruje a může měnit nastavení zabezpečení zařízení, bránit k přístupu k souborům a krást citlivé informace.

Programy pro těžbu kryptoměn zneužívají výpočetní kapacitu zařízení. Nakažení tímto typem malwaru často bývá prostřednictvím e-mailové přílohy, nebo pomocí webu, který zneužije chyby zabezpečení ve webových prohlížečích, nebo využitím výpočetního výkonu počítače. Programy na těžbu kryptoměn využívají složité matematické výpočty k udržení blockchainového registru, což umožňuje těžařům generovat nové mince.[5]

Rootkit je sada nástrojů, která kyberzločinci poskytuje nejvyšší oprávnění (administátorská práva) v systému. Je obzvláště nebezpečný, protože je navržený tak, aby ukryl svoji přítomnost v zařízení. Na rozdíl od jiných typů malwaru hluboce skrytý rootkit nevykazuje mnoho příznaků a proto může obejít bezpečnostní software. Může být ukryt ve firmware, v RAM, pod operačním systémem. Často se může rootkit dostat do počítače prostřednictvím phisingového e-mailu, stažením nakaženého programu, sady exploitů a dalších. Může provádět akce jako deaktivace antivirového softwaru, sledování aktivity, zaznamenávat stisknuté klávesy, ukrást citlivá data, přihlašovací a finanční údaje, deaktivovat bezpečnostní protokoly, anebo spuštění jiného malwaru na zařízení.[6]

1.2.4 DDoS útoky

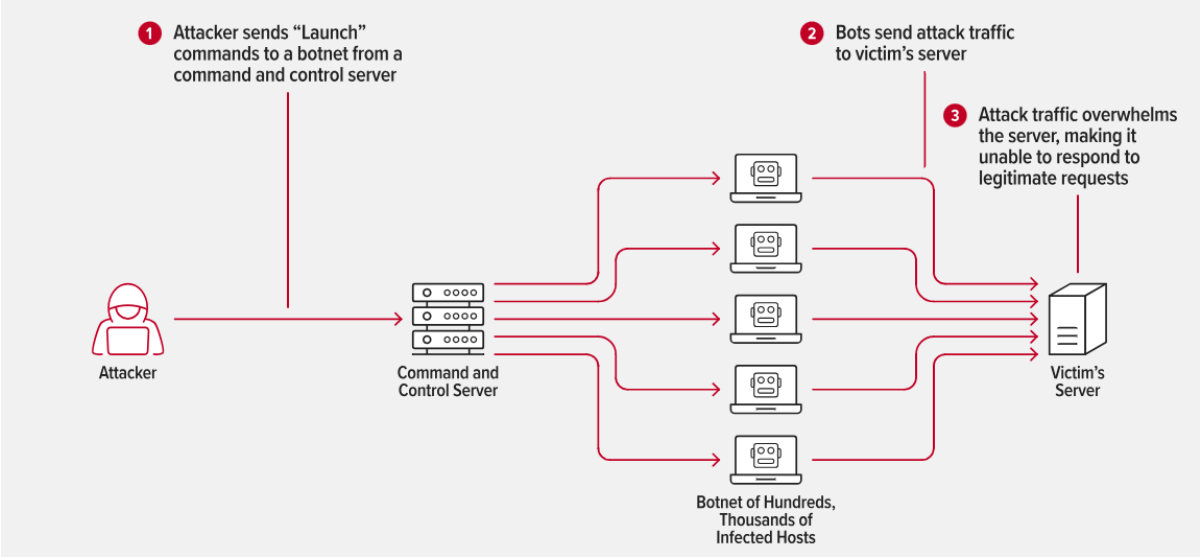
Zkratka DDoS znamená „Distributed Denial of Service“ a cílem tohoto útoku je odepřít, znepřístupnit nebo zpomalit uživatelům nějakou službu. Služba může představovat webovou stránku, e-shop, nebo aplikaci. K útoku je využívána síť infikovaných počítačů („zombie“) z celého světa a s využitím řídících serverů jsou posílány nevyžádané požadavky, s cílem vytížit kapacitu linky dané služby. Pozornost je zaměřena na síťové prvky systémů, navazující na internetové připojení, případně na webové stránky, servery či databáze a ta se vlivem přetížení znepřístupní.

Kyberzločinci nejčastěji provádějí útoky na objednávku a motivem může být:

- vydírání, kdy kyberzločinec požaduje výkupné, výměnou za ukončení útoku
- politický hacktivismus
- snaha poškodit konkurenci
- kamufláž, pro odvedení pozornosti od jiné, závažnější aktivity.[7]

Botnet je schopen kromě počítačů a telefonů infikovat nové technologie, jako jsou zařízení internetu věcí v domácnostech, veřejných prostorech a zabezpečených oblastech, IP kamery, směrovače, linuxové systémy a mohou ohrozit ještě více nic netušících uživatelů. Nejběžnějším způsobem, jak se stát součástí botnetu, je tajná infekce botnetovým agentem. K infekci může dojít například otevřením škodlivé přílohy, nebo návštěvou stránky, která poskytuje škodlivý

obsah prostřednictvím exploit kit. Většina botnetů má extrémně malou stopu, takže je obtížné rozpoznat, kdy počítač ovládá kyberzločinec ke škodlivým účelům.[8]



Obrázek 2: DDoS útok

Zdroj: NGINX

1.2.5 Sociální inženýrství

Člověk je nejslabším článkem každého bezpečnostního řešení. Techniky sociálního inženýrství spoléhají na zvědavost, strach, lidskou závist a chamtivost. Tvůrci podvodných emailových zpráv se snaži donutit uživatele k předem promyšlené akci a získat práva do počítačového systému, nebo získat určité informace.

Mezi nejrozšířenější metody patří:

Baiting, kde si uživatel stáhne infikovaný soubor, například v podobě falešného přehrávače za účelem přehrání oblíbeného filmu.

Phishing, kde se útočník snaži vylákat osobní údaje podvodnými emailovými zprávami.

Pretexting, kde za účelem získání přístupu k utajeným informacím se kyberzločinec vydává za někoho jiného.

Scareware, kde pomocí falešného upozornění na nebezpečí napadení škodlivým softwarem si uživatel na doporučení nainstaluje infikovaný antivir.[9]

1.2.6 Skenování portů

Skenování portů je technika průzkumu sítě určená k identifikaci otevřených portů v počítači. Skener identifikuje aplikace spuštěné v systému, protože určité programy naslouchají na

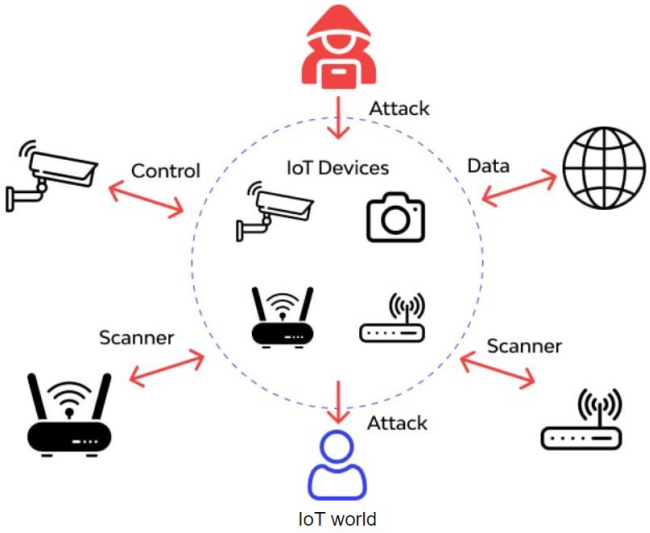
určitých portech a reagují na provoz. Například port 80 je používán u HTTP, port 53 u DNS a port 22 u SSH. Jedná se o průzkumnou fázi, která předchází skutečnému útoku.

1.2.7 Zero Day útok

Zero day útok (útok nultého dne) je kybernetický útok nebo hrozba využívající doposud neznámé zranitelnosti v systému, pro kterou zatím neexistuje obrana. Zranitelnost může být zneužita pomocí zero day exploitu, kterou může být software, nebo řada příkazů využívající programátorské chyby k proniknutí do systému. Tato doposud neobjevená chyba je útočníky využívána k infikování systémů spywarem, ransomwarem, keylogerem, trojským koněm, nebo jiným malwarem. V důsledku mohou být odcizena data, nebo může být převzata kontrola nad cílovým zařízením. Nultý den označuje skutečnost, že je uživatel ohrožen až do vydání aktualizace autora vadného software. Doba ohrožení zero day exploitem může být několik dní, týdnů i delšího časového období.[10]

1.2.8 Útoky zaměřené na IoT

Přestože zařízení Internetu věcí (IoT) mohou působit jako příliš malá nebo příliš specializovaná na to, aby představovala hrozbu, tak i ty nejobyčejnější zařízení mohou být rizikem, pokud jsou napadena přes internet. Může se jednat například o špehování přes dětskou elektronickou chůvičku až po narušení funkce zdravotního přístroje pro udržování životních funkcí. Jakmile útočník převezme řízení, může krást data, odepřít poskytování služeb nebo spáchat jiný kybernetický zločin, který je možný pomocí počítače. Útoky na infrastrukturu IoT způsobují škody, které nejsou omezeny jen na úniky dat a nespolehlivost provozu, ale mohou mít za následek i fyzické poškození zařízení nebo i osob, které tato zařízení používají nebo na nich závisejí.[11]



Obrázek 3: IoT útok

Zdroj: Wallarm

1.2.9 DNS Tunneling

Útok na DNS (Domain Name System) je typ útoku, který cílí na infrastrukturu DNS, což je základní systém pro překlad doménových jmen na IP adresy a naopak. Cílem útoku na DNS může být přerušení provozu webových stránek, krádež citlivých informací, šíření malware, phishing, podvržení dat nebo jednoduše destabilizace a vyřazení DNS infrastruktury.

Existuje několik forem útoků na DNS, z nichž některé zahrnují:

DNS spoofing: Tento útok zahrnuje odesílání falešných DNS odpovědí na dotazy klientů. Útočník zkresluje data v DNS odpovědích tak, aby uživatelé byli přesměrováni na škodlivé webové stránky nebo jiné neautorizované servery.

DNS amplification: Při tomto typu útoku útočník zneužívá otevřené DNS servery k odesílání malého dotazu s falešnou zdrojovou adresou, která je cílem útoku. DNS servery odpovídají na tento dotaz s velkou odpovědí, což umožňuje útočníkovi zvýšit objem provozu směřujícího na cílový systém, což může vést k přetížení a výpadkům.

DNS cache poisoning: Při tomto typu útoku útočník znečistí mezipaměť DNS serveru falešnými informacemi. To může vést k tomu, že uživatelé budou přesměrováni na nelegitimní webové stránky, což může být využito k phishingu, šíření malware nebo dalším útokům.

Distributed Denial of Service (DDoS) útoky na DNS: Tyto útoky zahrnují zaplavení DNS serverů obrovským objemem dotazů, čímž se přetíží jejich kapacita a znemožní legitimním uživatelům získat odpovědi na své dotazy.[12]

2 STAV KYBERNETICKÉ BEZPEČNOSTI

Malé a střední podniky jsou vůči kybernetickým útokům zranitelnější, protože jim obvykle chybí povědomí o kybernetické bezpečnosti, interní IT pracovníci a kybernetický postoj, aby se jim bránily. Zatímco 43 % kybernetických útoků je zaměřeno na malé podniky, pouze 14 % je považováno za připravené, vědomé a schopné bránit své sítě a data.

Než se objevila umělá inteligence, byly tyto útoky byly méně detekovatelné. Společnost Positive Technologies provedla řadu penetračních testů firem, které působí v několika velkých sektorech, jako jsou finance, oblast paliv a energetiky, vládních orgánů, průmyslových podniků a dokonce i IT společností. Bylo prokázáno, že v 93 procentech testovacích případů by útočník mohl prolomit ochranu sítě organizace a získat přístup k místní síti. Lidé jsou stále zneužíváni jako nejslabší článek v kybernetické bezpečnosti. E-mailový phishing, spear-phishing a sociální inženýrství jsou i nadále trendem jako nejběžnější a nejspolehlivější způsob nelegálního přístupu k síti. Další důležitou hrozbou, se kterou se podniky musí vypořádat je zabezpečení koncových bodů, ransomwarové útoky, které jsou každoročně na vzestupu a útoky na cloud.[13]

2.1 Kybernetická bezpečnost ve světě

Cílem kyberzločinců jsou často malé podniky, jelikož mají obvykle méně zabezpečené sítě a jejich opatření v oblasti kybernetické bezpečnosti jsou méně účinné než u velkých korporátních společností. Malé podniky jsou atraktivním cílem z důvodu dostatku citlivých informací a proto kyberzločinci vyvíjí neustále nové metody k infiltraci. Každoročně stoupá počet útoků a za rok 2023 jsou odhadovány ztráty za kybernetické zločiny na 8 biliónů dolarů.[14] Očekává se, že ztráty v roce 2024 vzrostou na 9,5 bilionů dolarů a v roce 2025 na 10,5 biliónů. Zpráva společnosti IBM odhaluje, že průměrný kybernetický útok na narušení dat má za následky ztráty dosahující 4,45 milionů dolarů a ve zdravotnictví je nejvyšší průměrná ztráta v důsledku narušení dat 10,93 milionů dolarů ročně.[15]

Kybernetické útoky se mohou zaměřovat na podniky, finanční instituce i na jednotlivce, aby ukradly citlivé informace, jako jsou údaje o kreditní kartě, přihlašovací údaje, nebo osobní údaje, které lze prodat na černém trhu nebo využít k podvodům. Mohou být finančně motivované, nebo mohou být vedeny k narušení soupeřících národů nebo organizací jako forma moderní války.[16]

Tabulka 1: Země, kde se nejčastěji vyskytují kybernetické útoky

Země	Zastoupení
Čína	18,83%
Spojené státy	17,05%
Brazílie	5,63%
Indie	5,33%
Německo	5,10%
Vietnam	4,23%
Thajsko	2,51%
Rusko	2,46%
Indonésie	2,41%
Nizozemsko	2,20%

Zdroj: GBHackers

Nejběžnější typy kybernetických útoků v roce 2023:

- Malware
- Phishing
- Denial-of-Service (DoS) Attacks
- Code Injection Attacks
- IoT-Based Attacks
- Identity-Based Attacks
- Supply Chain Attacks
- Spoofing
- Insider Threats
- DNS Tunneling[17]

Největší kybernetické útoky 2023

Každým rokem narůstá počet kybernetických útoků o desítky procent a škody jsou vyčísleny na biliony korun. Ransomware gangy v minulém roce útočily na menší a méně chráněné organizace, ale ohrozili i mnoho významných podniků. Trendem minulého roku byl dvojitý ransomware útok, kde útočníci kromě zašifrování dat a odepření přístupu ke složkám. Také hrozili zveřejněním citlivých dat. Útok nultého dne (Zero day exploit) dokázal po celém světě ohrozit bezpečnost téměř 2000 organizací a neustále se objevují nové případy.[18]

Tabulka 2: Příklady největších kybernetických útoků v roce 2023

Měsíc a společnost	Incident a jeho následek
Leden, 2023 Royal Mail	Kybernetický útok na společnost Royal Mail spojený s LockBit Ransomware**.** Kvůli vážnému narušení služeb způsobeným kybernetickým útokem musela společnost Royal Mail musela zastavit své mezinárodní doručovací služby.Bylo požádováno výkupné v milionech, které Royal Mail odmítla zaplatit. Musela se uchýlit k manuálním procesům, které výrazně prodloužily čekací doby jejích zákazníků.
Leden, 2023 Yum! Vlastník KFC, Taco Bell a Pizza Hut fast foodů	Ransomware gang ukradl data společnosti Yum!Brands. Firma původně uvedla, že nic nenasvědčuje tomu, že by byly odcizeny informace o zákaznících. Dle tvzení byla kompromitována pouze firemní data. Útok donutil Yum! dočasně uzavřít 300 míst ve Spojeném království.O tři měsíce později Yum! uvedl, že některá data zaměstnanců nakonec unikla a poté musela společnost čelit hromadné žalobě v souvislosti s únikem osobních údajů zákazníků.
Leden & březen 2023 T-Mobile	T-Mobile byla hacknuta a ukradena data z 37 milionů účtů prostřednictvím jednoho ze svých API. T-Mobile byl v roce 2023 napaden dvakrát. Po útoku v lednu společnst odhalila další útok v březnu, kde mohli útočníci přistupovat k T-Mobile účtům a zjistit čísla PiN, čísla sociálního zabezpečení. osobním údaje a další data.
Březen, 2023 Acer	Útočníci (údajně známí jako IntelBroker) napadli server hostující soukromé dokumenty používané servisními techniky. Útočníci nabourali servery a získali 160 GB ukradených dat obsahujících technické manuály, softwarové nástroje, detaily back-end infrastruktury, dokumentace k produktům pro telefony, tablety a notebooky, obrazy systému BIOS, soubory ROM i ISO a náhradní digitální produktové klíče (RDPK).
Březen, 2023 AT&T	AT&T musela varovat 9 milionů zákazníků o narušení dat po hacknutí dodavatele. Prodejce, kterého AT&T využívá k marketingu, zažil bezpečnostní incident, při kterém hackeři odhalili informace o 9 milionech zákazníků. Útočníci přistupovali z bezdrátových účtů k informacím o zákaznících související se sítí, jako je počet linek na účtu nebo bezdrátovém tarifu a dalších.
Květen, 2023 Intel	Vyděračský gang Money Message ukradl soukromé klíče Intel Boot Guard po porušení MSI.Výrobce počítačového hardwaru MSI tvrdil, že během útoku útočníci ukradli 1,5 TB dat, včetně firmwaru, zdrojového kódu a databází. Gang požadoval výkupné ve výši 4 000 000 dolarů a poté, co nebylo zaplaceno, začali unikat ukradená data MSI, včetně zdrojového kódu firmwaru používaného základními deskami společnosti.
Červenec, 2023 Microsoft	Microsoftu byl údajně ukradeno 30 milionů zákaznických účtů. Hacktivisté, Anonymous Sudan, tvrdili, že úspěšně hackli Microsoft a přistoupili k velké databázi obsahující více než 30 milionů účtů Microsoft, e-mailů a hesel. Útočnici nabídli, že tuto databázi prodají zájemcům za 50 000 USD, a vyzvali zájemce, aby se spojili s jejich telegramovým robotem k zajištění nákupu dat.
Září, 2023 MGM Resorts & Caesars Entertainment	Casino & Entertainment Giants MGM Resorts & Caesars Entertainment ovlivněny masivními útoky Scattered Spider. Po útoku byly ovlivněny některé systémy společnosti, včetně hlavních webových stránek, online rezervací a služeb v kasinech, jako jsou bankomaty , hrací automaty a automaty na kreditní karty. Pro Caesars vedl kybernetický útok ke kompromitaci citlivých informací mnoha členů věrnostního programu. Některé zprávy naznačují, že Caesars zaplatil polovinu obrovského výkupného, které hackeři požadovali, aby zabránili úniku ukradených informací.
Září, 2023 Sony	K hacknutí společnosti Sony se přihlásili k zodpovědnosti různí hackeři. K útoku na systémy Sony se původně přihlásila vyděračská skupina s názvem RansomedVC. Tato skupina tvrdila, že během útoku narušila sítě Sony a ukradla 260 GB da a snažila se je prodat za 2,5 milionu dolarů. Jiná hackerské skupině MajorNelson unikl zdarma 2,4 GB komprimovaný archiv, který obsahuje 3,14 GB nekomprimovaných dat, o kterých tvrdí, že také patří Sony.
Září, 2023 Airbus	Společnosti Airbus unikla data, která se údajně týkala tisíců dodavatelů. Hacker zveřejnil informace o 3 200 dodavatelích společnosti Sony na dark webu. Aktér používající přezdívku „USDoD“ zveřejnil na BreachForums, že získal přístup k webovému portálu Airbus poté, co kompromitoval účet zaměstnance turecké letecké společnosti.
Říjen, 2023 Boeing	Gang LockBit tvrdil, že ukradl obrovské množství citlivých dat leteckému gigantovi, který chtěl zveřejnit online, pokud by Boeing nezaplatil výkupné do 2. listopadu. 2023. Podle zpráv, LockBit nakonec zveřejnil ukradená data. Boeingu uniklo více než 43 GB souborů poté, co odmítla zaplatit výkupné.
Prosinec, 2023 Toyota Financial Services (TFS)	Toyota Financial Services (TFS) potvrdila, že při útoku byly odhaleny citlivé osobní a finanční údaje. Aktéři hrozeb požadovali platbu ve výši 8 000 000 dolarů za vymazání ukradených dat a dali Toyotě 10 dní na to, aby na jejich požadavek reagovala. Toyota s kyberzločinci nakonec nevyjednala výkupnéa všechna data zřejmě unikla na vyděračském portálu Medusa na dark webu.

Zdroj: Cyber Management Alliance

2.2 Kybernetická bezpečnost v České republice

Navzdory tomu, že množství kyberhrozeb neustále roste, Česká republika v oblasti kybernetické bezpečnosti oproti dalším evropským zemím zaostává. Na základě analýzy společnosti Logicworks, opírající se o data Eurostatu, silná hesla při autentizaci používá 86,5 % českých firem, což je čtyři procentní body nad průměrem EU. Avšak ve Finsku je to skoro 94 %. Biometrickou autentizaci využívá pouze 18 % českých podniků, avšak v Nizozemsku dosahuje 24 %. U biometrické autentizace unijní průměr představuje 13,5 %. V oblasti šifrování dat a komunikace má Česká republika podíl 32 %, což představuje zhruba čtyři body méně než průměr. Pouze 12 % českých firem má pojistku proti incidentům v oblasti informačních a komunikačních technologií (ICT), což je polovina evropského průměru. V porovnání s Dánskem, kde je tato míra 71 %, je český stav v této oblasti výrazně nižší.

Pokud se zaměříme na výdaje na ICT bezpečnost v přepočtu na HDP na obyvatele, investice do kyberbezpečnosti v Česku patří mezi nižší v Evropě. S narůstajícím počtem kyberhrozeb je stále důležitější sledovat, jak jednotlivé ekonomiky reagují na tyto výzvy. Vzhledem k častým diskusím o digitalizaci státního aparátu má Česká republika v oblasti IT bezpečnosti značný prostor pro zlepšení.[19]

V České republice existuje několik institucí a organizací, které se zabývají kybernetickou bezpečností a poskytují podporu, poradenství a koordinaci v této oblasti. Mezi nejdůležitější patří:

- **Národní úřad pro kybernetickou a informační bezpečnost (NUKIB):**

Národní úřad, který má za úkol koordinovat činnosti v oblasti kybernetické bezpečnosti v České republice, poskytovat bezpečnostní doporučení a informace a spolupracovat s ostatními institucemi a organizacemi v této oblasti.

- **CERT-CSIRT teamy:**

V České republice působí několik CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) týmů, které se zabývají reakcí na bezpečnostní incidenty a poskytují podporu organizacím při řešení kybernetických hrozeb a útoků.

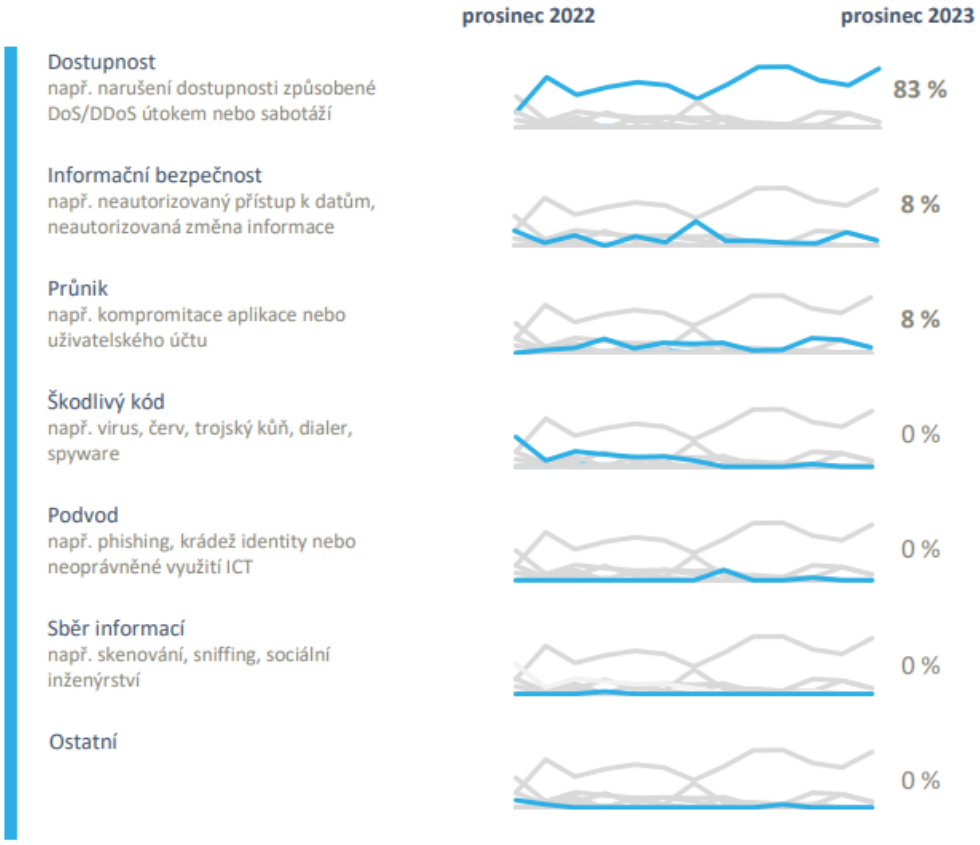
Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB**)** v roce 2023 evidoval 262 kybernetických incidentů, což je rekordní počet. V porovnání s rokem 2022 je to téměř dvojnásobný nárůst. Příčinou jsou hlavně opakované vlny DDoS útoků vedené zejména

proruskými hacktivistickými skupinami. Dva incidenty byly klasifikovány jako velmi významné a byly zařazeny do nejvyšší kategorie závažnosti. Týkaly se významné strategické státní instituce a druhý neregulovaného subjektu z obranného sektoru. Nejzastoupenější jsou DDoS útoky. Útočníci operovali také s velkým počtem účtů vytvořených pomocí botů, čímž podkopali důvěryhodnost oficiálních postižených účtů a způsobilo to jejich nefunkčnost. Oblast umělé inteligence (AI) a chatbotů na bázi LLM (Large Language Model) byla zneužita ke generování phishingu a psaní škodlivého kódu. U této oblasti se předpokládá, že útoky budou stále sofistikovanější, jelikož umělá inteligence a stále větší využívaní chobotů na bázi velkých jazykových modelů dávají útočníkům lepší možnosti.[20]

Předpokládá se, že stále větší komplikace bude působit komplexnost aplikací ve firmách, množství zastaralých aplikací a různorodá úroveň „vendor locku“.[1] Příkladem může být zero day útok i sofistikované útoky přes dodavatelské řetězce. Každá firma musí kontrolovat a přemýšlet nad tím, zda v jejích byznysových procesech má nějaké subdodavatele. Co se stane, pokud v softwaru dodavatele bude nějaký backdoor a jak dobře dodavatel chrání svoje vlastní procesy. Jaké má firma vlastní řešení, pokud bude dodavatel napaden? Příkladem může být útok z roku 2022 na společnost Okta, která je dodavatelem autentizačního softwaru. Hackerská skupina Lapsu$ měla za cíl se dostat přes Oktu ke koncovým firemním zákazníkům. Útočníci narušili systém přes subdodavatele tohoto gigantu.[21]

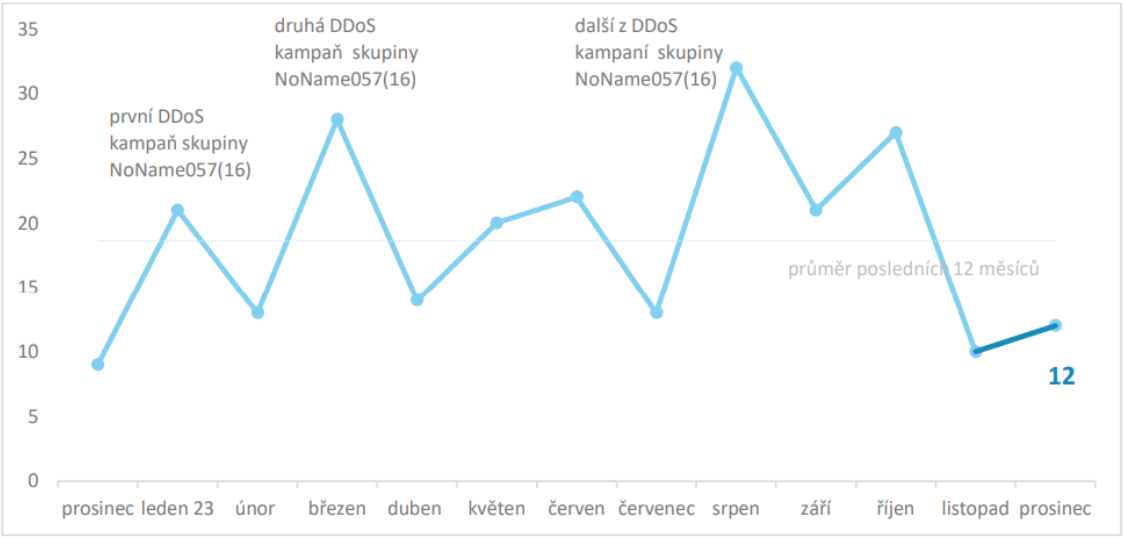
Pokud se zaměříme na zprávu Kybernetické incidenty pohledem NÚKIB, vydávanou Národním úřadem pro kybernetickou a informační bezpečnost, zjistíme, že v České republice nejvíce útoků cílí na dostupnost serverů, kde byly tyto útoky v měsíci prosinci 2023 zastoupeny z 83%. Z 8 % došlo k neautorizovanému přístupu k datům, nebo k neautorizované změně informace a z 8 % došlo k průniku, například kompromitací aplikace nebo uživatelského účtu.

[1] Vendor lock-in je situace, v nichž se zadavatel svým předchozím postupem při zadávání veřejné zakázky v oblasti IT dostal do pozice, kdy se při potřebě změny či úpravy systému nemůže vymanit ze závislosti na konkrétním dodavateli a jeho řešení.



Obrázek 4: Klasifikace incidentů nahlášených NÚKIB

Zdroj: NÚKIB



Obrázek 5: Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Zdroj: NÚKIB

3 ORGANIZAČNÍ OPATŘENÍ

Organizační opatření se zaměřují na vytváření a implementaci procesů, politik a postupů, které řídí lidské chování a fungování organizace. Zahrnují například vytváření bezpečnostních politik a postupů, definování rolí a odpovědností v oblasti bezpečnosti, provádění školení zaměstnanců, zavedení kontroly přístupu a správu hesel, monitorování a řízení dodavatelských vztahů. Cílem organizačních opatření je vytvoření kultury bezpečnosti a zajištění dodržování stanovených pravidel a postupů v celé organizaci.

3.1 Kategorizace podnikatelských subjektů

Donedávna byly hlavním cílem kybernetických útoků hlavně finanční firmy a vlády. Z důvodu vyšší potřeby využití IT technologií se stávají i ostatní potencionálním cílem útoku. Ve většině průmyslových odvětví se přechází na nové technologie, jako například umělá inteligence, pokročilá analytika, internet věcí (IoT), které přinesou několik výhod, ale také vystaví společnost a její zákazníky novým druhům kybernetických rizik.

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

a. Subjekty používající IT pro práci s dokumenty, účetnictví, archivování

Do této kategorie spadá většina podnikatelských subjektů využívající IT technologii pro usnadnění podnikání nebo potřeby plnit povinné evidence. Potřeba využití IT vyplývá ze zákona o uchovávání dokumentů, potřeba využívat komunikační služby, plánování služeb, archivace dat a faktur, správa jednoduchého účetnictví apod. Do této kategorie spadají manufaktury, řemeslníci, maloobchodníci, subjekty poskytující služby. Tyto subjekty nejsou hlavním zájmovým cílem pro útočníky. Neopatrné používání internetu může způsobit nechtěné stažení škodlivého softwaru. Hlavním rizikem jsou pro tyto subjekty interní zaměstnanci a hrozby jako Adware, Phishing, Malware a Ransomware.

b. Subjekty uchovávající údaje o zákaznících

Do druhé kategorie spadají subjekty užívající IT zpracovávající osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, kde se osobním údajem rozumí jakákoli informace týkající se konkrétního jedince, kterou je možné přímo nebo nepřímo identifikovat pomocí čísla, kódu nebo dalších prvků spojených s jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitou. Podnikatelský subjekt uchovávající

osobní údaje o zákaznících, případně o vlastních zaměstnancích, je ohrožen o něco více než malé subjekty. Hrozí rizika jako SQL Injection, Brute Force a Man-in-the-middle útoky, ale i také sofistikovanější útoky typu Phishing.

c. Subjekty používající průmyslové řídicí systémy (typu ICS/SCADA)

ICS (Industrial Control System) je zkratka obecně pro všechny průmyslové řídicí systémy. Pod tuto obecnou kategorii můžeme zařadit prvky SCADA, distribuované kontrolní systémy, programované logické obvody a jiné prvky používané převážně ve výrobě a infrastruktuře. „SCADA“ je zkratka pro „Supervisory Control And Data Acquisition“, v překladu „dozorčí řízení a sběr dat“. Znamená to, že například průmyslová výroba nebo distribuce je řízena jednotlivými technickými prvky a člověk provádí jenom dohled (často vzdálený) nebo případnou změnu nastavení. Řídící prvky jsou používány především v oblastech strojní výroby, energetiky (distribuce plynu, tepla, elektřiny a ropy), vodního hospodářství (čističky, zásobárny, distribuce vody) a dopravy (dopravní signalizace, semafory, větrání v tunelech). Rozvoj těchto řídících prvků a jejich automatizace je spojen s pojmem „Průmysl 4.0“, který umožňuje kompletní propojení a automatizaci výrobních procesů a služeb. Subjekty kritické infrastruktury jsou často terčem sofistikovaných kybernetických útoků, které hrozí kybernetickou sabotáží.

Poskytovatelé online obsahu nebo služeb

Každým rokem přibývají služby, které lidem poskytují zábavu, ale také jsou nedílnou součástí pracovní náplně. Podstatou pro zařazení do této kategorie je, že nedostupnost jimi provozovaného internetového portálu způsobí zásadní finanční ztráty, jelikož na poskytování online obsahu nebo služeb jsou závislí. Příkladem mohou být e-mailové a cloudové služby, poskytovatelé streamované hudby (Spotify, Apple Music), pracovních nástrojů (Adobe, SAP apod.), zpravodajské portály, elektronické obchody a další. Ve většině případů jsou útoky na tyto weby objednávány konkurencí těchto subjektů. Jedná se především o útoky s cílem způsobit nedostupnost služeb nebo obsahu.

Subjekty chránící si know-how

Tato kategorie zahrnuje subjekty uchovávající neveřejné duševní vlastnictví. Jsou často terčem špionážních kampaní ze zahraničí za účelem ekonomické špionáže. Zejména se jedná o oblasti výzkumného nebo akademického sektoru, energetický, petrochemický nebo plynový průmysl, telekomunikace a zbrojní a obranný průmysl.[22]

3.2 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System – ISMS) představuje soubor pravidel s cílem zachování důvěrnosti, integrity a dostupnosti informací uplatněním procesu řízení rizik a ujistit zainteresované strany, že jsou rizika přiměřeně řízena. V rámci ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací a kontrolována zavedená opatření. ISMS je integrován do systémů organizace a je součástí celkového systému a procesů.[23]

3.2.1 Triáda CIA

Triáda CIA je nejznámější a nejpoužívanější triádou kybernetické bezpečnosti. Název vznikl ze slov:

- Confidentiality (důvěrnost)
- Integrity (celistvost)
- Availability (dostupnost)

Obrázek 6: Triáda CIA

Zdroj: SecurityMadeSimple

Triáda CIA je vztahována především k informacím. Informační bezpečnost je definována řadou norem ISO 27000. Patří sem základní normy informační bezpečnosti:

- ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní požadavky
- ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

Triáda CIA by se měla uplatňovat nejen na informace samotné, ale i na další prvky jako jsou data, počítačové systémy a jiné.

Důvěrnost (Confidentiality)

K informacím, datům a informačním systémům by měli přistupovat pouze autorizované (oprávněné) subjekty. Z hlediska kybernetické bezpečnosti lze aplikovat některou z klasifikací informací.

Příklady klasifikačních schémat:

1. Klasifikace informací dle zákon 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti:
    - **Přísně tajné (Top secret) –** neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážnou újmu zájmům České republiky.
    - **Tajné (Secret) -** neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu zájmům České republiky.
    - **Důvěrné (Confidential) –** neoprávněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republiky.

Klasifikace informací využívaná v komerční sféře:

- **Chráněné –** Neoprávněné nakládání s informacemi by mohlo způsobit závažné poškození či zničení organizace (např. únik strategických informací, zdrojových kódů, schémat zabezpečení, hesel aj.).
- **Interní –** neoprávněné nakládání s informacemi by mohlo způsobit poškození organizace (např. únik osobních údajů, smluv aj.).
- **Citlivé –** neoprávněné nakládání s informacemi by mohlo mít negativní dopad na společnost (např. dosud nezveřejněné informace o projektech, plánovaných akcích aj.).
- **Veřejné –** neoprávněné nakládání s informacemi by nemělo nikoho poškodit a nemělo by mít jakýkoliv dopad na společnost (např. veřejně dostupné kontakty, prezentace projektů aj.).

Integrita

Intergritou rozumíme nemožnost zásahu do dat, informací, počítačových systémů a jejich nastavení jinou osobou, než je k tomuto úkonu oprávněna. Je to záruka neporušenosti dat, informací a systému. V případě porušení integrity může dojít ke změně dat a může uplynout značná doba, než je narušení integrity zjištěno.

Tabulka 3:Hodnocení integrity dle vyhlášky o kybernetické bezpečnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standartní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí šifrování.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu.).

Zdroj: [23]

Dostupnost

Dostupnost je definována jako vlastnost přístupnosti k informacím, datům nebo počítačovému systému a jejich použitelnosti na žádost oprávněné osoby.

Tabulka 4: Stupnice pro hodnocení dostupnosti dle vyhlášky o kybernetické bezpečnosti

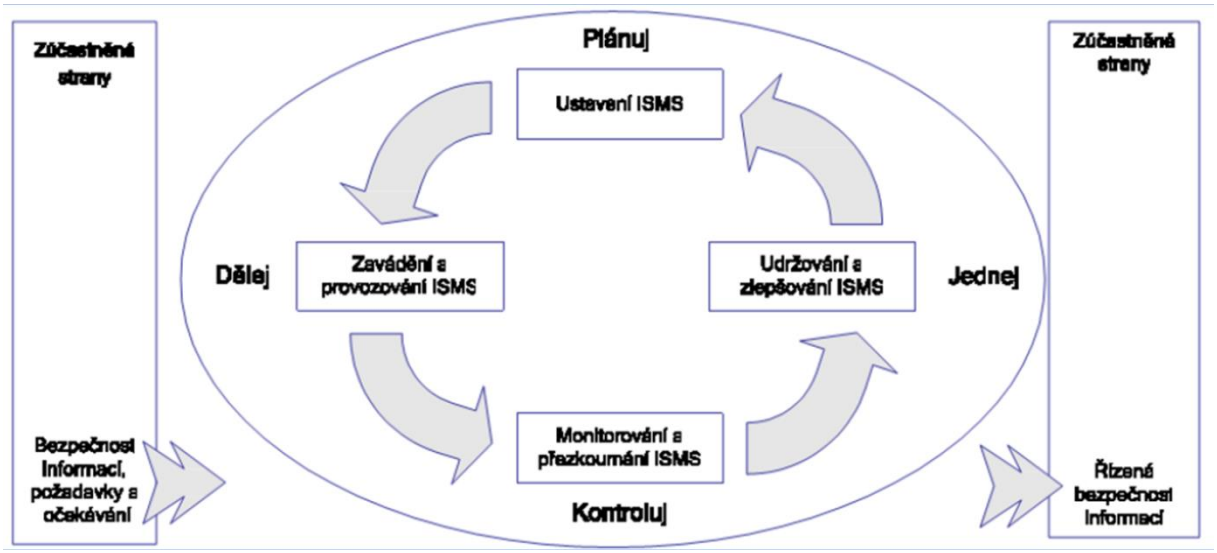
Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (Cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může výt podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Zdroj: [23]

Triáda CIA bývá častokrát znázorňována graficky pro lepší pochopení jejích jednotlivých atributů a vztahů. Triáda bývá doplněna i o prvky, jako jsou technologie, lidé a procesy.[23]

3.2.2 PDCA cyklus

Systém řízení bezpečnosti informací vyžaduje systémový a kompletový přístup, který respektuje principy a prvky celého životního cyklu kybernetické bezpečnosti. Je založen na PDCA cyklu, neboli taktéž zvaného Demingově cyklu. PDCA se skládá z počátečních písmen Plan-Do-Check-Act, neboli Plánuj-Dělej-Kontroluj-Jednej. PDCA cyklus má více variant a v oblasti kyberbezpečnosti je vhodná OPDCA, která je rozšířena o Observe (Pozoruj/Poznamenej), která předchází fázi plánování.



Obr. č. 2 - PDCA model aplikovaný na procesy ISMS

Zdroj: ISO 27 001:2006

3.3 Bezpečnostní politika a zákonné povinnosti organizace

Dle § 2 písm. c) VoKB se bezpečnostní politikou rozumí soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.

Ustanovení §30 VoKB stanovuje povinnosti subjektů uvedených v §3 písm. c) až f) a h) ZoKB:

Tabulka 5: Vyhláška č. 82/2018 Sb

Vyhláška č. 82/2018 Sb.
1.1. Politika systému řízení bezpečnosti informací
1.2. Politika řízení aktiv
1.3. Politika organizační bezpečnosti
1.4. Politika řízení dodavatelů
1.5. Politika bezpečnosti lidských zdrojů
1.6 Politika řízení provozu a komunikací
1.7. Politika řízení přístupu
1.8. Politika bezpečného chování uživatelů
1.9. Politika zálohování a obnovy a dlouhodobého ukládání
1.10. Politika bezpečného předávání a výměny informací
1.11. Politika řízení technických zranitelností
1.12. Politika bezpečného používání mobilních zařízení
1.13. Politika akvizice, vývoje a údržby
1.14. Politika ochrany osobních údajů
1.15. Politika fyzické bezpečnosti
1.16. Politika bezpečnosti komunikační sítě
1.17. Politika ochrany před škodlivým kódem

Zdroj: Vlastní zpracování

Vyhláška o kybernetické bezpečnosti dále stanovuje obsah bezpečnostní dokumentace a co musí zahrnovat. Dále je nutné přezkoumávat bezpečnostní politiku a bezpečnostní dokumentaci v pravidelných intervalech.[24]

Bezpečnost v organizaci

Ustanovení organizační bezpečnosti je zásadní pro zvládání případných kybernetických útoků a hrozeb.

Řízení aktiv

V rámci řízení aktiv povinná osoba stanovuje metodiku pro identifikaci a klasifikaci aktiv organizace. Dále hodnotí důležitost a hodnotu aktiv a určuje garanta aktiv. Hodnotí primární a podpůrná aktiva z hlediska důvěrnosti, integrity a dostupnosti a stanovuje pravidla ochrany aktiv. Povinná osoba také určuje přípustné způsoby používání a likvidace aktiv, zohledňuje při tom různé faktory jako osobní údaje a právní povinnosti.

Řízení rizik

Vyhláška o kybernetické bezpečnosti popisuje proces řízení rizik povinné osoby v souvislosti s ochranou informačních aktiv. Povinná osoba stanovuje metodiku pro hodnocení rizik a identifikuje relevantní hrozby a zranitelnosti. Hodnocení rizik se provádí pravidelně a zohledňuje významné změny, přičemž výsledky jsou zaznamenány ve zprávě. Na základě výsledků se vypracovává prohlášení o aplikovatelnosti a plán zvládání rizik, který obsahuje cíle a plán realizace bezpečnostních opatření.

Bezpečnost lidských zdrojů

Povinná osoba vypracuje plán rozvoje bezpečnostního povědomí, který zahrnuje formu, obsah a rozsah školení a poučení pro uživatele, administrátory, osoby zastávající bezpečnostní role a dodavatele, a to v souladu se stavem a potřebami systému řízení bezpečnosti informací. Určuje odpovědné osoby za realizaci činností v plánu a zajišťuje poučení a pravidelná školení ve shodě s tímto plánem. Zajišťuje pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní a kontroluje dodržování bezpečnostní politiky. Požaduje předání odpovědností při ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role. Hodnotí účinnost plánu rozvoje bezpečnostního povědomí a řeší případy porušení stanovených bezpečnostních pravidel ze strany zaměstnanců.

Stanovení bezpečnostních požadavků pro dodavatele

Povinná osoba, jako organizace nebo firma, musí stanovit pravidla pro dodavatele týkající se systému řízení bezpečnosti informací a udržovat seznam svých významných dodavatelů. Dodavatele musí informovat o jejich zařazení do seznamu a pravidlech. Povinná osoba je

povinna řídit rizika spojená s dodavateli a pravidelně přezkoumávat smlouvy s významnými dodavateli z hlediska bezpečnosti informací. Před uzavřením smlouvy musí provést hodnocení rizik spojených s plněním výběrového řízení a stanovit způsoby realizace bezpečnostních opatření ve smluvních vztazích s významnými dodavateli. Dále musí pravidelně hodnotit rizika a kontrolovat zavedená bezpečnostní opatření a reagovat na zjištěné nedostatky. Informace o zařazení do seznamu významných dodavatelů a obsahu pravidel musí být jasně poskytnuta dodavatelům a obsahovat identifikaci správce, provozovatele, informačního systému a konkrétního dodavatele.

Zvládání kybernetických bezpečnostních incidentů

Povinná osoba implementuje proces detekce a vyhodnocování kybernetických bezpečnostních událostí a incidentů, včetně přidělení odpovědností a stanovení postupů pro detekci, vyhodnocování a zvládání incidentů. Definuje postupy pro identifikaci, sběr a uchování relevantních dat nutných pro analýzu incidentů a zajistí detekci kybernetických bezpečnostních událostí podle stanovených postupů. Uživatelé, administrátoři a další zaměstnanci jsou povinni hlásit neobvyklé chování informačního systému a podezření na zranitelnosti, a povinná osoba zajistí posuzování těchto událostí a jejich klasifikaci jako incidenty podle specifikací zákona. Provádí zvládání incidentů, přijímá opatření pro odvrácení a zmírnění jejich dopadů, a hlásí je dle příslušných právních ustanovení. Záznamy o incidentech a jejich řešení jsou pečlivě vedeny a provádí se vyšetření a určení příčin incidentů, na základě kterých jsou přijímána bezpečnostní opatření k prevenci opakování podobných událostí.

Kontrola a audit kritické informační infrastruktury a významných informačních systémů

Při auditu kybernetické bezpečnosti povinná osoba provádí a dokumentuje kontrolu dodržování bezpečnostní politiky a technické shody. Výsledky auditu se následně zohledňují v plánech rozvoje bezpečnostního povědomí a zvládání rizik. Dále je prováděno posouzení souladu bezpečnostních opatření s nejlepší praxí, právními předpisy a dalšími relevantními předpisy. V případě zjištění nesouladu jsou určena nápravná opatření pro zajištění souladu. Audit je prováděn pravidelně alespoň každé 3 roky pro povinné osoby uvedené v zákoně, přičemž v odůvodněných případech může být prováděn průběžně po systematických částech. Výsledky auditu musí být posouzeny osobou vyhovující podmínkám stanoveným v zákoně.[25]

4 TECHNICKÁ OPATŘENÍ

Technická opatření a organizační opatření spolu představují základní prvky bezpečnostních opatření. Organizační opatření se zaměřují na lidi a procesy, zatímco technická opatření se zaměřují na technologie a infrastrukturu. Technická opatření jsou zaměřena na technické aspekty ochrany systémů, sítí a dat. Zahrnují implementaci různých technických mechanismů a nástrojů, jako jsou firewall, antivirové programy, šifrování dat, identifikace a autentizace uživatelů, zálohování dat, monitorování síťového provozu apod.

4.1 Bezpečnostní opatření

Cílem je minimalizovat rizika spojená s technologiemi a infrastrukturou a chránit systémy před hrozbami, malwarem a neoprávněným přístupem.

Tabulka 6: Technická opatření zakotvená ve vyhlášce č. 82/2018 Sb.

	Technická opatření zakotvená ve vyhlášce č. 82/2018 Sb.
§ 17 Fyzická bezpečnost	Stanovuje opatření pro ochranu fyzických aktiv a prostor, ve kterých jsou uloženy informace. Povinná osoba je povinna přijmout nezbytná opatření k zamezení neoprávněného vstupu a poškození aktiv.
§ 18 Bezpečnost komunikačních sítí	Stanovuje požadavky na segmentaci komunikačních sítí a zabezpečení dat pomocí kryptografie. Povinná osoba musí aktivně blokovat nežádoucí komunikaci a zajistit ochranu integrity komunikační sítě.
§ 19 Správa a ověřování identit	Stanovuje povinnost používat nástroje pro správu a ověřování identity uživatelů a aplikací. Je vyžadováno použití vícefaktorové autentizace a ukládání autentizačních údajů ve formě odolné proti offline útokům.
§ 20 Řízení přístupových oprávnění	Stanovuje povinnost používat centralizovaný nástroj pro řízení přístupových oprávnění. Je vyžadováno řízení přístupu k jednotlivým aktivům a čtení, zápisu a změn oprávnění.
§ 21 Ochrana před škodlivým kódem	Ukládá povinnost používat nástroje pro ochranu před škodlivým kódem na koncových stanicích, serverech a dalších zařízeních. Povinná osoba je též povinna monitorovat a řídit používání výměnných zařízení a datových nosičů.
§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	Vyžaduje zaznamenávání bezpečnostních a provozních událostí důležitých aktiv informačního a komunikačního systému. Povinná osoba musí také zaznamenávat přihlašování a odhlašování ke všem účtům a další relevantní události.

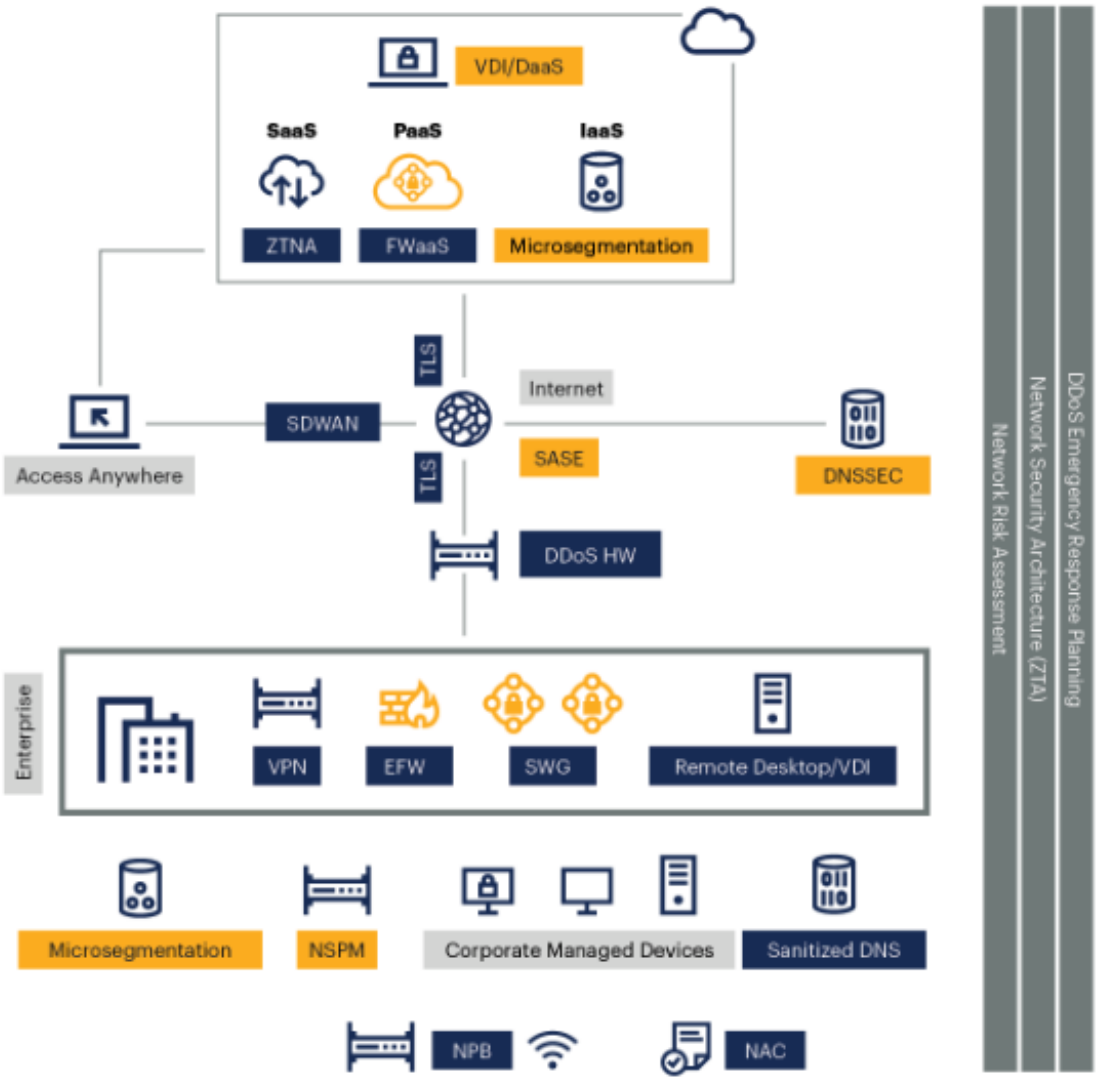
	Technická opatření zakotvená ve vyhlášce č. 82/2018 Sb.
§ 23 Detekce kybernetických bezpečnostních událostí	Požaduje používání nástroje pro detekci kybernetických bezpečnostních událostí v rámci komunikační sítě. Je vyžadována kontrola přenášených dat a blokování nežádoucí komunikace.
§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí	Ukládá povinnost používat nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí. Povinná osoba musí také zajistit vyhledávání souvisejících záznamů a využití informací pro nastavení bezpečnostních opatření.
§ 25 Aplikační bezpečnost	Vyžaduje provádění penetračních testů informačního a komunikačního systému. Povinná osoba musí trvale chránit aplikace, informace a transakce před neoprávněnou činností.
§ 26 Kryptografické prostředky	Stanovuje povinnost používat aktuálně odolné kryptografické algoritmy a klíče. Je též vyžadováno používání systému správy klíčů a certifikátů.
§ 27 Zajišťování úrovně dostupnosti informací	Stanovuje opatření pro zajištění dostupnosti informačního a komunikačního systému. Povinná osoba musí zajistit odolnost systému vůči kybernetickým bezpečnostním incidentům.
§ 28 Průmyslové, řídicí a obdobné specifické systémy	Ukládá povinnost používat nástroje a opatření pro zajištění kybernetické bezpečnosti průmyslových a řídicích systémů. Povinná osoba musí též zajistit obnovení chodu těchto systémů po bezpečnostním incidentu.
§ 29 Digitální služby	Stanovuje bezpečnostní opatření pro poskytovatele digitálních služeb. Povinná osoba musí dodržovat pravidla pro uplatňování směrnice Evropského parlamentu a Rady týkající se řízení bezpečnostních rizik.
§ 30 - Bezpečnostní politika a bezpečnostní dokumentace	Ukládá povinnost stanovit bezpečnostní politiku a vést bezpečnostní dokumentaci. Povinná osoba musí pravidelně přezkoumávat a aktualizovat bezpečnostní politiku a dokumentaci.

Zdroj: Zákony pro lidi

Jedním ze základních prvků kybernetické bezpečnosti je zajištění bezpečnosti počítačových sítí. Bez účinné ochrany počítačových sítí by nebylo možné zajistit ochranu počítačových systémů a uložených dat.

4.1.1 Ochrana sítí

Z pohledu kybernetické bezpečnosti je důležité rozdělit počítačovou síť, kde se zaměřujeme na oddělení systémů se zvýšeným rizikem kompromitace od zbytku sítě (DMZ) a pro oddělení provozu např. jednotlivých oddělení, informačních systémů aj. Rozdělování provozu sítě se obvykle aplikuje pomocí Virtuální LAN (VLAN).



Obrázek 7: Ochrana sítí

Zdroj: Gartner

DMZ (Demilitarized Zone):

DMZ je oddělená síťová zóna mezi vnitřní sítí organizace a veřejnou internetovou sítí. Je určena pro umístění veřejně přístupných serverů a služeb, jako jsou webové servery, e-mailové servery, DNS servery atd. Cílem DMZ je oddělit veřejně dostupné servery od vnitřní sítě, aby se snížilo riziko útoků z internetu na citlivé interní systémy.

VLAN (Virtual Local Area Network):

VLAN je logické oddělení fyzické sítě na jednotlivé virtuální sítě na základě potřeb a požadavků organizace. Umožňuje segmentaci sítě na různé skupiny nebo oddělení, jako jsou oddělení nákupu, oddělení IT, oddělení prodeje apod. Cílem VLAN je izolovat a zabezpečit provoz mezi různými skupinami uživatelů nebo zařízeními na síti. Zatímco VLAN může být implementována v rámci vnitřní sítě a umožňuje organizaci efektivně spravovat a zabezpečovat interní síťový provoz.[23]

Ochrana sítě LAN

Ochrana sítí a protokolů je klíčovým prvkem pro zajištění bezpečnosti a integrity dat v síťovém prostředí. Zde je stručný popis ochrany pro každý z uvedených protokolů a technologií:

DHCP (Dynamic Host Configuration Protocol):

Ochrana DHCP spočívá v prevenci proti neoprávněnému přidělování IP adres a dalších konfiguračních informací. Použití metody jako DHCP snooping, což je funkce ve správě switchů, která umožňuje filtrovat a monitorovat DHCP zprávy mezi klienty a DHCP serverem. Autentizace DHCP pomocí metod jako DHCPv6 Authentication zabraňuje neoprávněným klientům v připojení k síti.

ARP (Address Resolution Protocol):

Ochrana proti ARP spoofingu, což je technika, při které útočník posílá falešné ARP zprávy s cílem ovládnout komunikaci mezi zařízeními v síti. Použití technologií jako statické ARP záznamy nebo dynamické ARP inspekce (DAI), která umožňuje switchům kontrolovat a filtrovat ARP zprávy na základě ověřených záznamů.

DNS (Domain Name System) v bezdrátových sítích:

Implementace DNSSEC (DNS Security Extensions) pro zajištění integrity a autenticity DNS záznamů. Zabezpečení komunikace DNS pomocí DNS over TLS (DoT) nebo DNS over HTTPS (DoH), což jsou protokoly, které šifrují DNS komunikaci, čímž brání útočníkům ve sledování a manipulaci s DNS provozem. Monitorování a detekce DNS útoků jako DNS cache poisoning nebo DNS reflection amplification pomocí specializovaných bezpečnostních nástrojů.

IEEE 802.1X: Je framework navržený pro zajištění autentizace zařízení přistupujících do sítě LAN resp. WLAN.

IPv6: Obsahuje integrovanou podporu IPSec pro šifrování a autentizaci komunikace.[26]

4.1.2 Ochrana na rozhraní sítí

ACL (Access Control Lists):

ACL slouží k řízení přístupu k síťovým zdrojům z různých bodů sítě, což pomáhá minimalizovat rizika útoků od neoprávněných uživatelů nebo zařízení. Správné nastavení ACL může zabránit neoprávněnému přístupu k citlivým datům nebo službám a snížit riziko útoků typu DoS (Denial of Service) nebo DDoS (Distributed Denial of Service).

Firewall:

Firewall je klíčovým prvkem kyberbezpečnosti, který zajišťuje ochranu sítě před neoprávněným síťovým provozem a škodlivými útoky. Správně konfigurovaný firewall může filtrovat a blokovat nebezpečný síťový provoz, jako jsou pokusy o neoprávněný přístup, zneužití zranitelností a škodlivý malware.[27]

Proxy server:

Proxy server může být využit k monitorování a filtrování síťového provozu, což umožňuje organizacím sledovat a kontrolovat internetovou aktivitu svých uživatelů. Tím, že filtruje internetový obsah a blokuje přístup k potenciálně nebezpečným stránkám, může proxy server snížit riziko infikování sítě škodlivým softwarem a chránit uživatele před phishingem a jinými kybernetickými hrozbami.[28]

IDS a IPS (Intrusion Detection System a Intrusion Prevention System):

IDS monitoruje síťový provoz a identifikuje podezřelé aktivity a hrozby, zatímco IPS reaguje na tyto hrozby a aktivně brání síťovou infrastrukturu před útoky.[29]

SIEM (Security Information and Event Management):

SIEM umožňuje organizacím sledovat a analyzovat události a informace z různých zdrojů v síti, což pomáhá identifikovat kybernetické hrozby a reagovat na ně v reálném čase. Integrace SIEM do kybernetické bezpečnostní strategie umožňuje organizacím získat celkový přehled o bezpečnostním stavu své sítě a efektivně reagovat na incidenty a hrozby.

Antivir a Antispam:

Antivirový a antispamový software jsou nezbytnými prvky kybernetické bezpečnosti, které pomáhají chránit uživatele a síťovou infrastrukturu před škodlivým softwarem a nevyžádanou poštou. Tím, že detekují a blokují malware a spamové e-maily, tyto nástroje pomáhají snížit riziko infikování sítě a ztrátu citlivých dat.[30]

4.1.3 Aplikační bezpečnost

Aplikační bezpečnost zahrnuje ověřování uživatelů, hesla, logování řízení přístupů, šifrovanou komunikaci, zranitelnosti a jiné.

Řízení přístupů

Řízení přístupů v aplikační bezpečnosti zahrnuje správu oprávnění uživatelů, autentizaci, autorizaci a sledování aktivit uživatelů. To zahrnuje kontrolu přístupu k aplikacím a datům na základě rolí, oprávnění nebo individuálních povolení. Důležitým prvkem je také správa uživatelských účtů a monitorování jejich aktivit za účelem detekce možných bezpečnostních hrozeb. Šifrování dat se využívá k ochraně citlivých informací a zajištění integrity a soukromí dat. Řízení přístupů je klíčové pro prevenci neoprávněného přístupu a zneužití v aplikacích, což přispívá k celkové bezpečnosti systému.

Ověřování uživatelů

Nejprve musí být ověřena identita uživatele, až poté může dojít řízení uživatelských přístupů. Ověření uživatele probíhá v podobě hesla. Dále je uživatel ověřen na základě vlastnictví určitého tokenu (čipová karta, klíče, mobilní telefon). Ověření může probíhat i na základě toho, čím je, a tím se zabývá biometrie pomocí rozpoznávání jedinečných biologických charakteristik (otisk prstů, hlasu, dynamiky psaní).

Vícefaktorová autentizace je zabezpečovací metoda, která vyžaduje od uživatele předložení alespoň dvou či více faktorů pro získání přístupu k webové stránce nebo aplikaci. Těmito

faktory jsou znalost (např. heslo), vlastnictví (např. bezpečnostní token) a inherence (např. otisk prstu). Tato forma autentizace chrání uživatelská data před neoprávněným přístupem, který by mohl vzniknout například odhalením jediného hesla.

Jedním z typů vícefaktorové autentizace je dvoufaktorové ověření, které obvykle zahrnuje zobrazení náhodně generovaného kódu, který uživatel použije pro ověření, v kombinaci s heslem.. Autentizace probíhá, když se uživatel snaží přihlásit k určitému počítačovému zdroji, jako jsou sítě, zařízení nebo aplikace.

Použití více autentizačních faktorů, jako jsou fyzické předměty, znalosti, biometrie nebo poloha, zvyšuje bezpečnostní úroveň autentizace tím, že snižuje pravděpodobnost neoprávněného přístupu. Například kombinace bankovní karty a PINu při výběru peněz z bankomatu je dobrým příkladem dvoufaktorové autentizace.

Autentizační aplikace třetích stran, jako Google Authenticator nebo Microsoft Authenticator, poskytují další vrstvu zabezpečení tím, že generují neustále se měnící kódy, které uživatelé používají k ověření, často bez nutnosti připojení k internetu.[23]

IAM – Identity Access Management

Správa identit a přístupu (IAM) je rámec obchodních procesů, politik a technologií, který usnadňuje správu elektronických nebo digitálních identit. Se zavedeným rámcem IAM mohou manažeři informačních technologií řídit přístup uživatelů ke kritickým informacím v rámci svých organizací. IAM zahrnuje systémy jednotného přihlašování, dvoufaktorové ověřování, vícefaktorové ověřování a správu privilegovaného přístupu. Tyto technologie umožňují bezpečné ukládání údajů o identitě a profilu, a zajišťují, že jsou sdílena pouze nezbytná a relevantní data.

IAM lze nasadit v místní síti, poskytovat dodavatel třetí strany pomocí cloudového modelu nebo nasadit v hybridním modelu. Základními komponentami IAM jsou identifikace jednotlivců v systému, identifikace a přidělování rolí, správa jednotlivců a rolí v systému, a přidělování úrovní přístupu jednotlivcům nebo skupinám jednotlivců.

Vedoucí představitelé podniků a IT oddělení jsou pod zvýšeným regulačním a organizačním tlakem, aby chránili přístup k podnikovým zdrojům. IAM automatizuje tyto úkoly, umožňuje granulární řízení přístupu a auditování všech podnikových aktiv v prostorách i v cloudu.

IAM se rozšiřuje o nové funkce, včetně biometrie, analýzy chování a umělé inteligence, a je vhodný pro náročné podmínky nového bezpečnostního prostředí. Princip minimálního oprávnění je klíčovým principem při přípravě IAM, omezuje přístupová práva uživatelů pouze na to, co je nezbytně nutné k výkonu jejich práce. Tímto způsobem se předchází vytvoření "Super uživatele", který by měl neomezená oprávnění v síti. IAM je dostupný pro společnosti všech velikostí.[31]

Obrázek 8: Správa identit a přístupu

Zdroj: TÜV Rheinland

Hesla

Hesla jsou tajné údaje, které uživatelé používají k ověření své identity při přihlašování do aplikací. Hashovací funkce jsou algoritmy, které převádějí hesla na jedinečné řetězce znaků, tzv. hashové hodnoty, které jsou ukládány v databázi. Tyto hashové hodnoty jsou těžko zpětně převoditelné na původní heslo, což zvyšuje bezpečnost uživatelských účtů. Heslo může být kybernetickým útokem odchyceno v provozu v počítačové síti, vylákáno sociálním inženýrstvím, získáno pomocí malwaru, uhádnuto nebo „lámáno“. V praxi je požadováno v organizacích dostatečně silné heslo používající malá a velká písmena, čísla, speciální znaky a s požadavkem na minimální možnou délku hesla.

Počet znaků	Pouze čísla	Malá písmena	Malá a velká písmena	Čísla, malá a velká písmena	Čísla, malá a velká písmena, speciální znaky
4	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
5	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
6	okamžitě	okamžitě	okamžitě	okamžitě	okamžitě
7	okamžitě	okamžitě	1 s	2 s	4 s
8	okamžitě	okamžitě	28 s	2 min	5 min
9	okamžitě	3 s	24 min	2 h	6 h
10	okamžitě	1 min	21 h	5 dní	2 týdny
11	okamžitě	32 min	1 měsíc	10 měsíců	3 roky
12	1 s	14 h	6 let	53 let	226 let
13	5 s	2 týdny	332 let	3 tis. let	15 tis. let
14	52 s	1 rok	17 tis. let	202 tis. let	1 mil. let
15	9 min	27 let	898 let	12 mil. let	77 mil. let
16	1 h	713 let	46 mil. let	779 mil. let	5 mld. let
17	14 h	18 tis. let	2 mld. let	48 mld. let	380 mil. let
18	6 dní	481 tis. let	126 mld. let	2 bil. let	26 bil. let

Obrázek 9: Čas na prolomení hesla hrubou silou

Zdroj: ESET

Logy a logování

Logy jsou záznamy událostí a aktivit, které se odehrávají v systému, aplikaci nebo síti. Logování je proces zaznamenávání těchto událostí do logovacích souborů pro účely sledování, diagnostiky, bezpečnosti a auditu. Tyto záznamy mohou obsahovat informace o přístupech uživatelů, chybách systému, změnách konfigurace a dalších událostech, které jsou důležité pro správu a monitorování IT prostředí.

Zabezpečení důvěrnosti a integrity přenášených dat

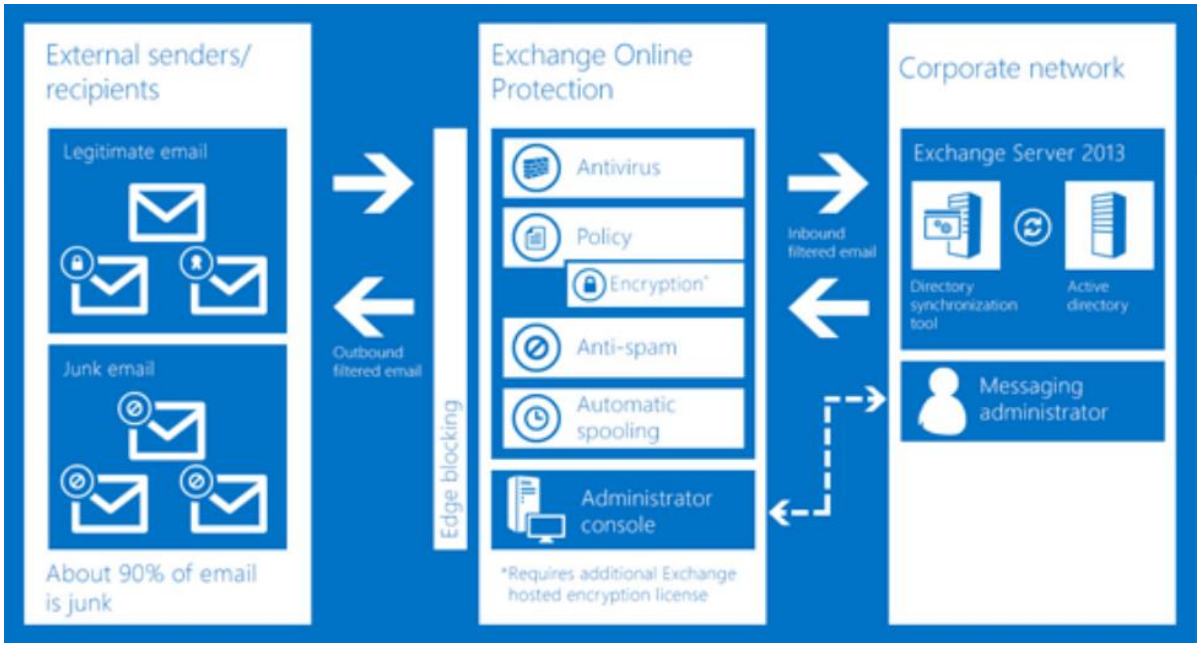
Zabezpečení důvěrnosti a integrity přenášených dat je klíčovým prvkem aplikační bezpečnosti, který zajišťuje, že data přenášená mezi klientem a serverem zůstávají utajena a nejsou narušena během přenosu. Protokol TLS (Transport Layer Security) je kryptografický protokol, který poskytuje šifrování dat a autentizaci spojení mezi klientem a serverem, což zajišťuje bezpečný přenos dat přes internet. Použití TLS umožňuje ochranu citlivých informací, jako jsou hesla, platební údaje nebo osobní údaje, před neoprávněným odposlechem a útoky typu "man-in-the-middle". TLS využívá asymetrickou šifrovací technologii a certifikáty pro ověření identity serveru, což posiluje důvěru v bezpečnost přenášených dat.

Mail-flow

Emailová komunikace je jedním z hlavních kanálů, skrze který mohou společnosti být napadeny škodlivým softwarem. Nebezpečí útoku se odvíjí od velikosti a důležitosti společnosti, ačkoliv i malé firmy nejsou imunní vůči hrozbám. Moderní poskytovatelé emailových řešení nabízejí širokou škálu bezpečnostních mechanismů, jako je AntiSpam, Zero-Trust CDR, vzdálená izolace či spuštění v sandboxu. Doporučuje se automatizovat a přísně kontrolovat tok emailů, nicméně mnohé společnosti se potýkají s tím, že i legitimní pošta může být mylně označena jako podezřelá.

Pro středně velké společnosti se doporučuje zavedení jednoduchých mechanismů, které odstraňují nevyžádanou poštu, ale zachovávají i možnost přijímat legitimní emaily z populárních platforem, jako jsou osobní emailové účty s doménami Google, Microsoft, Yahoo, iCloud, nebo Seznam.

Exchange Online Protection (EOP) poskytuje několik ochranných prvků pro správu pošty. Prvním krokem je kontrola důvěryhodnosti odesílatele a porovnání s databází známých podvodných domén. Poté probíhá skenování zpráv na přítomnost škodlivého kódu a následuje kontrola pravidel vytvořených správci prostředí. Skenování obsahu zajistí, že spamové nebo phishingové zprávy nebudou doručeny. Tyto mechanismy lze doplnit nebo nahradit řešeními třetích stran, v závislosti na zkušenostech a potřebách společnosti v oblasti IT bezpečnosti.[31]



Obrázek 10: Exchange Online Protection (EOP)

Zdroj: Red Level

Zranitelnosti

V aplikační bezpečnosti znamenají zranitelnosti slabá místa nebo nedostatky v softwaru, která mohou být zneužita k útokům nebo neoprávněnému přístupu. Tyto zranitelnosti se mohou týkat chybného kódu, nedostatečného ověřování uživatelů, neodpovídajícího zabezpečení dat a dalších faktorů.

Zranitelnosti můžeme z praktického hlediska rozdělit do dvou skupin:

a) Zranitelnosti, pro něž nebyly vydány opravné záplaty

Těmto zranitelnostem se říká zranitelnosti nultého dne (Zero-Day Vulnerabilities) a jsou pro útočníky nejvíce cenné. Chyby nebyly výrobcem softwaru, nebo poskytovatelem služby identifikovány a tedy ještě nebyly oficiálně opraveny. To znamená, že softwarový systém má stále tuto slabou stránku, která může být zneužita, aniž by byla poskytnuta ochrana nebo opravná akce.

b) Zranitelnosti pro něž ji byly vydány záplaty

I když je dostupná záplata, může zůstat množství systémů a aplikací, kde ještě záplaty nebyly implementovány.[23]

4.1.4 Vzdálený přístup k počítačovým systémům

Zabezpečený vzdálený přístup je souborem bezpečnostních opatření, navržených s cílem ochránit digitální aktiva organizace a zabránit úniku citlivých dat. Mezi možné prvky tohoto přístupu patří VPN, ověřování multifaktorů a ochrana koncových bodů. Vzhledem k rychle se měnícímu prostředí hrozeb a rostoucímu počtu vzdálených pracovníků je zabezpečený vzdálený přístup klíčovým prvkem současného IT prostředí. Jeho úspěšné provádění vyžaduje neustálé vzdělávání uživatelů, posílení politik kybernetické bezpečnosti a rozvoj osvědčených postupů v oblasti bezpečnostní hygieny.

Bezpečný vzdálený přístup není jedinou technologií, ale kombinací různých technologií, které společně poskytují potřebnou úroveň bezpečnosti pro práci z domova nebo jiných vzdálených míst. Mezi tyto technologie patří:

- Zabezpečení koncového bodu: včetně antivirového softwaru a správy bezpečnostních politik pro vzdálená zařízení.

- Virtuální soukromá síť (VPN): šifrovaný tunel pro bezpečné připojení vzdálených uživatelů k firemní síti.
- Přístup k síti Zero Trust (ZTNA): technologie, která nevytváří žádné předpoklady o důvěryhodnosti připojení a vyžaduje opětovné ověření před každou transakcí.
- Řízení přístupu k síti (NAC): kombinace nástrojů pro zajištění bezpečného přístupu k síti, včetně dvoufaktorové autentizace a politického vzdělávání.
- Jednotné přihlášení (SSO): jednotné přihlašování umožňuje uživatelům používat jednu sadu přihlašovacích údajů pro přístup ke všem aplikacím a zdrojům.

5 ANALÝZA SPOLEČNOSTI

5.1 Popis organizace

Jelikož je pro společnosti nepříjemné veřejně mluvit o procesech v oblasti informační bezpečnosti, bylo s managementem IT dohodnuto, že identita společnosti zůstane utajena. Společnost působí v oblasti pojištění a na trhu je více jak 30 let. Její pobočky jsou po celé České republice. Společnost využívá informační technologie k různým účelům, které zefektivňují její činnost. K hlavním činnostem využívající IT patří správa klientských dat, ukládaní informací o pojištěncích a pojistných smlouvách, zpracování pojistných událostí a vyplácení plnění, poskytování zákaznického servisu prostřednictvím e-mailu, telefonických center, online chatů a zákaznických portálů. Také jsou systémy využívány pro interní správu a řízení, jako je podpora interních procesů, řízení lidských zdrojů, účetnictví a plánování.

5.2 Analýza stávajícího stavu zabezpečení

Původním záměrem bylo provést dotazníkové šetření mezi zaměstnanci firmy, aby byly získány relevantní informace o bezpečnostních procesech, postupech a znalostech o kyberbezpečnosti zaměstnanců. Vedení společnosti však vyjádřilo obavy, že by tato metoda mohla nadměrně zatížit zaměstnance a z tohoto důvodu byla ke zhodnocení společnosti zvolena metoda přímých otázek na IT management. Vedoucímu pracovníkovi IT bylo položeno celkem 16 otázek. Vytvořený dotazník, který byl původně určen pro dotazníkové šetření pro zaměstnance, je přiložen v příloze této diplomové práce a může sloužit jako podklad pro další společnosti ke zjištění vědomostí o kyberbezpečnosti svých zaměstnanců. Pokud by úspěšnost znalostí byla pod 80 % procent, doporučila bych přeškolení zaměstnance. Pro porovnání znalostí zaměstnanců a výsledků dotazníku, lze vycházet ze zákona o kyberbezpečnosti.

1) **Má organizace zpracovány postupy a procesy pro vyhodnocování kybernetických bezpečnostních událostí?**

Společnost se řídí zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, který vstoupil v platnost 29. srpna 2014 a účinnosti nabyl 1. ledna 2015. Tento zákon upravuje práva a povinnosti osob a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, transponuje směrnici NIS a zajišťuje bezpečnost sítí elektronických komunikací a informačních systémů.

Hlavní cíle zákona:

- Stanovit základní úroveň bezpečnostních opatření
- Zlepšit detekci a hlášení kybernetických incidentů
- Zavést opatření k reakci na kybernetické incidenty
- Upravit činnost dohledových pracovišť

Dále se řídí vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Tato vyhláška upravuje obsah a strukturu bezpečnostní dokumentace, rozsah bezpečnostních opatření a způsob likvidace dat pro informační a komunikační systém. Tento systém zahrnuje kritickou informační infrastrukturu, komunikační systém, významné informační systémy a sítě elektronických komunikací. Dále stanovuje typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů a náležitosti hlášení těchto incidentů. Taktéž upravuje postupy pro reaktivní opatření a likvidaci dat, provozních údajů a informací.

2) Jsou ve společnosti stanoveny postupy při vzniku nestandardní situace?

Ano, ve společnosti jsou stanoveny postupy při vzniku nestandardní situace. Společnost se nejčastěji potýká s phishingovými emaily, které tvoří zhruba 80 procent všech incidentů, zatímco přibližně 20 procent tvoří ostatní druhy útoků, jako jsou malware, ransomware a útoky na webové aplikace. Při detekci phishingového emailu jsou zaměstnanci instruováni, aby jej okamžitě nahlásili bezpečnostnímu odboru. Bezpečnostní odbor následně provádí analýzu incidentu, která zahrnuje ověření zdroje a obsahu emailu, analýzu potenciálních škod a identifikaci dalších zaměstnanců, kteří mohli být cílem útoku. Kromě toho společnost pravidelně organizuje školení a simulace phishingových útoků pro své zaměstnance, aby zlepšila jejich povědomí o kybernetických hrozbách a posílila jejich schopnost rychle a správně reagovat na nestandardní situace. Tento preventivní přístup pomáhá minimalizovat rizika a zvyšuje celkovou bezpečnostní kulturu ve společnosti. Veškeré incidenty a postupy při jejich řešení jsou dokumentovány a pravidelně revidovány, aby byla zajištěna jejich aktuálnost a efektivnost.

3) **Jsou zaměstnanci obeznámeni s tím, co mají hlásit a mají k dispozici konkrétní kontakty? Hlásí organizace bezpečnostní incident CSIRT týmu?**

Ano, zaměstnanci jsou důkladně informováni o tom, co mají hlásit v případě kybernetického útoku. Mají k dispozici specifické kontakty na odpovědné osoby, které řeší bezpečnostní incidenty. Společnost se postarala o to, aby každý zaměstnanec věděl, jaké kroky má podniknout při detekci potenciální hrozby, což zahrnuje okamžité nahlášení incidentu.

Bezpečnostní incidenty jsou hlášeny Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který funguje jako centrální bod pro koordinaci a řešení kybernetických incidentů v České republice. Zaměstnanci jsou proškoleni nejen na to, jak rozpoznat různé typy kybernetických útoků, ale také na to, jak efektivně komunikovat tyto incidenty kompetentním autoritám.

V minulosti se společnost setkala s různými typy kybernetických útoků, včetně phishingových SMS zpráv, které odkazovaly na falešné webové stránky a útoků zaměřených na odcizení citlivých dat. Tyto zkušenosti vedly k implementaci robustnějších bezpečnostních opatření a postupů, které zahrnují nejen technická řešení, ale i důkladnou přípravu zaměstnanců na podobné situace.

Organizace také zajišťuje, že všechny bezpečnostní incidenty jsou pečlivě dokumentovány a analyzovány, což umožňuje neustálé zlepšování a aktualizaci bezpečnostních protokolů. Díky této komplexní strategii je společnost schopna rychle a efektivně reagovat na kybernetické hrozby, minimalizovat potenciální škody a chránit citlivá data.

4) **Má organizace vypracován plán kontinuity činností (Business Continuity Plan – BCP), plán obnovy (Disaster Recovery Plan – DRP) a havarijních plány, aby v případě mimořádné situace (havárie, živelné pohromy nebo úspěšného kybernetického útoku) byla organizace schopna obnovit svoji funkčnost?**

Vyhláška 82, §15 o kybernetické bezpečnosti se zaměřuje na řízení kontinuity činností. Povinná osoba v rámci tohoto řízení stanoví práva a povinnosti administrátorů a osob v bezpečnostních rolích. Posuzuje a dokumentuje možné dopady kybernetických bezpečnostních incidentů prostřednictvím hodnocení rizik a analýzy dopadů a vyhodnocuje možná rizika pro kontinuitu činností.

Na základě těchto analýz stanovuje cíle řízení kontinuity, které zahrnují definování minimální úrovně poskytovaných služeb, dobu obnovení po incidentu a bod obnovení dat. Dále formuluje politiku řízení kontinuity činností, která tyto cíle zahrnuje. Vypracovává, aktualizuje a

pravidelně testuje plány kontinuity a havarijní plány, které se týkají provozu informačního a komunikačního systému a přidružených služeb.

Navíc provádí opatření ke zvýšení odolnosti informačního a komunikačního systému proti kybernetickým bezpečnostním incidentům a omezení dostupnosti, přičemž se řídí požadavky podle § 27.

5) Jak organizace zajišťuje ochranu informací a kyberbezpečnost

Organizace klade velký důraz na ochranu informací při zacházení s údaji. Cílem zajištění informační bezpečnosti je zabránit neoprávněnému nakládání s informacemi ve všech formách jejich výskytu v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a ve znění pozdějších předpisů, a také v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech a dalších náležitostech v oblasti kybernetické bezpečnosti.

Informační bezpečnost je chápána jako komplexní proces ochrany aktiv, který zahrnuje personální bezpečnost, fyzickou bezpečnost, bezpečnost informačních technologií, plánování kontinuity činností a zajištění souladu s legislativními požadavky a normami. Na všech úrovních organizace za ni odpovídají vedoucí zaměstnanci jednotlivých útvarů.

Zavádění informační bezpečnosti je v souladu se zákonem o kybernetické bezpečnosti a s doporučeními norem ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 27002:2023. Důraz je kladen na:

- stanovení cílů a zásad informační a kybernetické bezpečnosti,
- určení odpovědností a pravomocí k realizaci těchto cílů a zásad,
- zavedení a dodržování opatření vycházejících z bezpečnostních cílů a zásad,
- monitorování a přehodnocování funkčnosti a efektivnosti systému managementu bezpečnosti informací,
- neustálé zlepšování systému managementu bezpečnosti informací založené na výsledcích revizí a auditů.

Organizace, jako správce osobních údajů, zpracovává osobní údaje na základě právních předpisů za účelem zajištění plnění veřejných povinností. To zahrnuje údaje klientů, plátců a jejich zástupců, a to zejména na základě specifických zákonů, které upravují činnost organizace a veřejné služby, které poskytuje. Subjekty údajů jsou povinny poskytovat osobní údaje v

souladu s těmito právními normami pro výkon veřejných povinností. Dále organizace zpracovává osobní údaje v souladu s národními právními předpisy v oblasti účetnictví a finanční kontroly. Také zpracovává informace prostřednictvím kamerového systému, který slouží k ochraně majetku a osob, a zajištění bezpečnosti zaměstnanců a klientů. Tyto kamerové systémy krátkodobě ukládají obrazové záznamy osob pohybujících se v blízkosti nebo uvnitř budov organizace, které jsou řádně označeny. Navíc organizace zpracovává osobní údaje poskytnuté dobrovolně klienty za účelem zefektivnění komunikace a pro přímý marketing, jako je zasílání newsletterů nebo informativních e-mailů i osobní údaje pro zřízení a provozování služby zabezpečené elektronické komunikace prostřednictvím specifických aplikací a pro plnění závazků vůči externím dodavatelům. Osobní údaje na základě souhlasu subjektu údajů jsou zpracovávány po dobu trvání souhlasu subjektů, nebo do jeho odvolání. Ochrana informací a kyberbezpečnost je zabezpečována prostřednictvím implementace robustních bezpečnostních protokolů a pravidelných bezpečnostních auditů. Proti neoprávněnému přístupu a kybernetickým útokům je využíváno šifrování dat, firewally a antivirové programy.

6) **Je pravidelně aplikována kontrola prostředí včetně instalace bezpečnostních aktualizací používaného software serverů i klientských stanic?**

Ano, společnost pravidelně provádí kontroly prostředí a dbá na aktualizaci softwaru jak na serverech, tak na klientských stanicích. Bezpečnostní aktualizace jsou aplikovány systematicky a dle stanoveného plánu, aby byla zajištěna maximální ochrana před potenciálními hrozbami. Jakmile je vydána nová aktualizace nebo patch, je tento software automaticky distribuován a instalován na všech relevantních zařízeních v rámci organizace. Technické oddělení společnosti pravidelně monitoruje stav všech softwarových instalací a ověřuje, že všechny bezpečnostní záplaty byly aplikovány bez problémů.

7) **Je společností aplikováno skenování sítě, portů, případně další jiné metody pro získání důležitých informací o úrovních zabezpečení? Jsou využívány systémy IDS?**

Společnost používá SIEM (Security Information and Event Management) systémy, které jsou klíčové pro monitorování a analýzu logů a anomálií v reálném čase a v případě zjištění anomálie jsou eskalovány podle protokolu.

SIEM systémy shromažďují a analyzují data z různých zdrojů, jako jsou firewally, antivirové programy, servery a síťová zařízení. Tato data jsou pak korelována, aby bylo možné identifikovat neobvyklé aktivity, které by mohly naznačovat kybernetické útoky nebo

bezpečnostní incidenty. SIEM systémy umožňují bezpečnostním týmům rychle reagovat na incidenty tím, že automaticky generují upozornění a eskalují je podle předem definovaných protokolů. Tímto způsobem mohou bezpečnostní odborníci okamžitě zasáhnout a minimalizovat dopad potenciálních hrozeb. SIEM také podporuje dodržování právních a regulačních požadavků, což je důležité, protože společnost je povinna provádět pravidelné bezpečnostní analýzy a monitorování podle zákona o kybernetické bezpečnosti.

Pravidelné skenování sítě, využívání SIEM systémů a dodržování bezpečnostních protokolů jsou klíčové komponenty bezpečnostní strategie společnosti. Tyto postupy umožňují společnosti nejen chránit svá data a systémy před kybernetickými hrozbami, ale také plnit zákonné požadavky.

8) Využívá organizace zálohování pomocí cloudových služeb nebo jinou metodou? Jsou na poskytovatele cloudových služeb uplatněna stejná pravidla jako pro ostatní dodavatele?

Společnost se rozhodla nevyužívat cloudové služby pro zálohování dat, protože jí to neumožňují interní směrnice a bezpečnostní politika. Místo toho spoléhá na své vlastní servery pro ukládání a zálohování dat. V současné době má firma dva fyzické servery. První server je umístěn v centrále společnosti a druhý server je umístěn na jiném fyzicky odděleném místě, aby se zajistila vyšší bezpečnost dat v případě jakékoliv poruchy nebo havárie v hlavním sídle. Vzhledem k tomu, že firma nevyužívá cloudové služby, není potřeba uplatňovat pravidla a bezpečnostní opatření pro poskytovatele cloudových služeb, která by byla jinak aplikována na ostatní dodavatele externích služeb.

9) Je kontrolována příchozí pošta zaměstnanců společnosti antispamem či antivirem?

Ano, příchozí pošta zaměstnanců společnosti je kontrolována antivirovým programem. Tento program prochází veškerou příchozí poštu a hledá potenciální hrozby, jako jsou viry, malware nebo jiné škodlivé kódy. Když antivirový program detekuje jakoukoliv anomálii nebo podezřelý obsah, automaticky označí daný e-mail jako spam a přesune jej do složky nevyžádané pošty. Tento proces pomáhá chránit zaměstnance před škodlivými útoky a minimalizovat riziko nakažení firemních počítačů nebo sítě. Kromě toho zajišťuje, že zaměstnanci mají bezpečnější prostředí pro práci s e-mailem a snižuje pravděpodobnost, že budou vystaveni phishingovým útokům nebo jiným typům kybernetických hrozeb.

10) Bývá pravidelně pořádáno školení zaměstnanců v oblasti kyberbezpečnosti?

Školení zaměstnanců na kybernetickou bezpečnost je povinné pro každého zaměstnance při jeho nástupu na novou pozici v rámci společnosti. Toto počáteční školení je navrženo tak, aby zaměstnance seznámilo se základními principy a postupy kybernetické bezpečnosti, které jsou nezbytné pro ochranu firemních dat a systémů. Po úvodním školení musí každý zaměstnanec absolvovat opakovací školení každé dva roky. Tato pravidelná opakovací školení jsou důležitá pro udržení povědomí o aktuálních bezpečnostních hrozbách a pro osvěžení znalostí o bezpečnostních opatřeních a protokolech.

11) Jakou má organizace politiku hesel? (Jsou vyžadována po zaměstnancích silná hesla (vyšší počet znaků, kombinace čísel, velkých písmen a symbolů)? Jak v pravidelných intervalech požadována změna? Je využíván správce hesel)?

Společnost vyžaduje, aby všichni zaměstnanci používali silná hesla pro přístup k firemním systémům a datům. Tato hesla musí být složena ze čtrnácti znaků a musí obsahovat kombinaci velkých a malých písmen, čísel a speciální symboly, jako jsou například vykřičníky, otazníky, zavináče nebo jiné znaky. Tato kombinace různých typů znaků zajišťuje, že hesla jsou nejen dlouhá, ale také obtížně uhodnutelná nebo prolomitelná prostřednictvím útoků hrubou silou nebo jiných metod kybernetických útoků

12) Je používáno v rámci řízení identit Princip minimálního oprávnění (POLP)?

Ano, v rámci řízení identit je ve společnosti používán Princip minimálního oprávnění (POLP). To znamená, že každý zaměstnanec má přístup pouze k těm datům a systémům, které jsou nezbytné pro výkon jeho pracovní pozice. Pokud zaměstnanec potřebuje přistupovat k dalším datům nebo systémům, které nejsou standardně zahrnuty v jeho oprávnění, musí si podat formální požadavek. Tento požadavek musí obsahovat jasné odůvodnění, proč zaměstnanec tento přístup potřebuje. Žádost je pak předložena zodpovědnému týmu, který vyhodnotí, zda je tento přístup skutečně nutný a zda jsou splněny všechny bezpečnostní požadavky. Na základě tohoto hodnocení se rozhodne, zda bude přístup žadateli udělen, či nikoliv. Tímto způsobem společnost zajišťuje, že každý zaměstnanec má jen nezbytné minimální oprávnění, což snižuje riziko neoprávněného přístupu a zvyšuje celkovou bezpečnost firemních dat a systémů.

13) Je používáno v rámci řízení identit Přístup na základě role (RBAC)?

Ano, ve společnosti je přiřazování uživatelských oprávnění založeno na roli, kterou daný uživatel zastává. Když je přijat nový zaměstnanec, nebo když se změní jeho pracovní pozice, je přiřazen do specifické skupiny, která odpovídá jeho roli. Tato skupina má definována konkrétní oprávnění k přístupu k různým datům a systémům. Oprávnění mohou zahrnovat různé úrovně přístupu, jako je čtení, zápis nebo mazání dat.

Vedoucí zaměstnanec má možnost zadat formální požadavek na přidělení nebo úpravu těchto oprávnění podle konkrétních potřeb zaměstnance. Tento požadavek je poté předán oddělení, které je ve společnosti odpovědné za posuzování a schvalování přístupových práv. Toto oddělení posoudí žádost na základě bezpečnostních pravidel a zásad společnosti a rozhodne, jaká oprávnění jsou pro daného zaměstnance nezbytná vzhledem k jeho pracovní pozici.

Každý zaměstnanec má pouze ta oprávnění, která potřebuje pro svou práci, aby byla minimalizována rizika spojená s neoprávněným přístupem k citlivým datům a systémům.

14) Aplikuje společnost simulaci phishingových emailů na své zaměstnance z důvodu osvěty a vzdělávání zaměstnanců?

Společnost občas praktikuje simulaci phishingových emailů jako součást vzdělávacích aktivit pro své zaměstnance. Tyto simulace jsou prováděny přibližně jednou ročně. Cílem těchto simulovaných útoků je zvýšit povědomí zaměstnanců o potenciálních hrozbách, které představují phishingové e-maily, a posílit jejich schopnost rozpoznat a správně reagovat na podezřelé zprávy.

15) Je využívána vícefaktorová autentizace a podmíněný přístup?

Jelikož se společnost řídí zákonem o kybernetické bezpečnosti, musí splňovat požadavek na vícefaktorovou autentizaci (MFA). Minimálně je tedy zavedena dvoufaktorová autentizace (2FA), která zajišťuje vyšší úroveň zabezpečení přístupu k firemním systémům a datům. Tento systém autentizace vyžaduje, aby zaměstnanci při přihlašování použili nejen své uživatelské jméno a heslo, ale také další ověřovací faktor, například kód zaslaný na mobilní telefon nebo generovaný autentizační aplikací. Někteří zaměstnanci mají povoleno pracovat z home office a tento přístup je zabezpečen pomocí virtuální privátní sítě (VPN). VPN poskytuje bezpečné a šifrované spojení mezi vzdáleným pracovníkem a firemní sítí, čímž zajišťuje ochranu přenášených dat a minimalizuje riziko neoprávněného přístupu.

16) Mají zaměstnanci umožněn volný přístup na veřejném internetu?

Zaměstnanci společnosti mají přístup na veřejný internet, ale tento přístup je omezený. I když mohou navštěvovat určité internetové stránky, existuje seznam konkrétních webů, které jsou blokovány. Toto omezení je zavedeno z důvodu zvýšení bezpečnosti a produktivity práce. Blokované stránky obvykle zahrnují ty, které jsou považovány za bezpečnostní riziko, jako jsou stránky s nelegálním nebo škodlivým obsahem. Společnost takto chrání své systémy a data před potenciálními hrozbami, které by mohly přijít z nedůvěryhodných zdrojů na internetu. Tento omezený přístup je řízen pomocí firemních bezpečnostních protokolů a softwarových řešení, která monitorují a filtrují internetový provoz. Tím je zajištěno, že přístup na internet je využíván efektivně a bezpečně, v souladu s firemními politikami a bezpečnostními standardy.

5.3 SWOT analýza

SWOT analýza je metoda používaná k hodnocení vnitřních a vnějších faktorů, které ovlivňují organizaci. Zahrnuje čtyři hlavní prvky: silné stránky, slabé stránky, příležitosti a hrozby. Silné stránky identifikují, v čem je společnost před konkurencí a cílem je maximalizace silných stránek. Slabé stránky jsou oblasti, kde organizace zaostává a kde je prostor pro zlepšení. Příležitosti jsou externí faktory, které mohou organizaci pomoci růst a rozvíjet se. Hrozby jsou externí výzvy nebo rizika, které mohou negativně ovlivnit výkon organizace. Analýza umožňuje organizacím strategicky plánovat a rozhodovat se na základě komplexního pohledu na jejich situaci. SWOT analýza je často prvním krokem v procesu strategického plánování. Pomáhá identifikovat klíčové oblasti, na které by se organizace měla zaměřit. Výsledky SWOT analýzy poskytují cenné informace pro rozvoj efektivních strategií a zlepšení celkového výkonu organizace.

	Pomocné dosažení cíle	Škodlivé dosažení cíle
Vnitřní původ (atributy organizace)	**Silné stránky** Pokročilá bezpečnostní infrastruktura Kvalifikovaný personál Přísné regulační normy Systém řízení bezpečnosti informací (ISMS) Kontrola a aktualizace softwaru Přístupová politika a řízení identit	**Slabé stránky** Starší technologie Neexistence cloudového zálohování Nedostatečné využívání pokročilých technologií Lidský faktor
Vnější původ (atributy prostředí)	**Příležitosti** Investice do nových technologií Zlepšení školení zaměstnanců Partnerství s bezpečnostními firmami Externí audity a certifikace	**Hrozby** Zvyšující se sofistikovanost útoků Rostoucí počet útoků na pojišťovny Regulační sankce Právní a regulační změny

Obrázek 11: SWOT analýza společnosti

Zdroj: Vlastní zpracování

5.3.1 Silné stránky (Strengths)

Pokročilá bezpečnostní infrastruktura: Moderní bezpečnostní technologie, jako jsou firewally, šifrování, a řešení zabezpečení, pomáhají organizaci detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy. Systém SIEM (Security Information and Event Management) poskytuje komplexní přehled o bezpečnostních událostech a umožňuje rychlou reakci na incidenty. Tato technologie zajišťuje vysokou úroveň ochrany proti různým typům kybernetických útoků, jako jsou DDoS útoky nebo pokusy o průnik do systémů.

Kvalifikovaný personál: Pojišťovna zaměstnává školené odborníky na kybernetickou bezpečnost a IT, kteří jsou dobře vybaveni k detekci a reakci na hrozby. Tito odborníci pravidelně aktualizují své znalosti a dovednosti prostřednictvím školení a certifikací. Díky jejich odborným znalostem a zkušenostem je organizace schopna efektivně řešit bezpečnostní incidenty a minimalizovat riziko narušení bezpečnosti.

Přísné regulační normy: Dodržování přísných zákonů a předpisů týkajících se ochrany osobních údajů, jako je GDPR, zajišťuje vysokou úroveň ochrany citlivých dat. Tato legislativa

vyžaduje přísná opatření na ochranu dat a pravidelné audity, což pomáhá udržovat bezpečnostní standardy na vysoké úrovni.

Systém řízení bezpečnosti informací (ISMS): Implementace ISMS umožňuje systematické řízení a zlepšování bezpečnosti informací. Tento systém zahrnuje pravidelné hodnocení rizik, definování bezpečnostních politik a postupů a sledování jejich dodržování, což zvyšuje celkovou odolnost organizace vůči kybernetickým hrozbám. ISMS také zajišťuje, že všechny bezpečnostní aktivity jsou dokumentovány a sledovány, což usnadňuje identifikaci a řešení potenciálních problémů. Pravidelné audity a revize ISMS zajišťují, že systém zůstává efektivní a odpovídá aktuálním hrozbám a rizikům.

Kontrola a aktualizace softwaru: Aktualizace zahrnují bezpečnostní záplaty a nové verze softwaru, které eliminují známé zranitelnosti a zajišťují, že systémy jsou chráněny před novými typy útoků.

Přístupová politika a řízení identit: Používání principu minimálního oprávnění (POLP) a přístup na základě role (RBAC) zajišťuje, že zaměstnanci mají přístup pouze k datům a systémům, které jsou nezbytné pro jejich práci, což minimalizuje riziko neoprávněného přístupu. Tyto politiky také zajišťují, že přístupová práva jsou pravidelně revidována a aktualizována podle aktuálních potřeb a rolí zaměstnanců. Implementace vícefaktorového ověřování (MFA) dále zvyšuje úroveň bezpečnosti tím, že vyžaduje více forem ověření identity před udělením přístupu.

5.3.2 Slabé stránky (Weaknesses)

Starší technologie: Mít nejnovější počítače a informační technologie je pro velkou pojišťovnu zásadní pro zajištění kybernetické bezpečnosti. Moderní technologie poskytují pokročilou ochranu proti novým a vyvíjejícím se kybernetickým útokům díky lepším bezpečnostním funkcím, jako je integrované šifrování a pokročilé firewally. Vylepšený výkon a spolehlivost moderních technologií umožňují efektivnější běh bezpečnostních aplikací, rychlejší zpracování dat a rychlou reakci na bezpečnostní incidenty. V průměru společnost modernizuje své IT každých 7 let.

Neexistence cloudového zálohování: Společnost nevyužívá cloudové služby pro zálohování dat, což může omezit její schopnost rychle obnovit data v případě katastrofického selhání serverů. Cloudové zálohování poskytuje vyšší dostupnost a odolnost proti ztrátě dat díky geografické redundanci a automatizovaným procesům zálohování.

Nedostatečné využívání pokročilých technologií: I když jsou implementována základní bezpečnostní opatření, společnost zaostává v nasazování pokročilých technologií, jako jsou umělá inteligence a strojové učení pro detekci hrozeb. Tyto technologie by mohly výrazně zlepšit schopnost organizace identifikovat a reagovat na nové a neznámé typy útoků.

Lidský faktor: Chyby zaměstnanců a nedostatečné povědomí o bezpečnostních hrozbách mohou vést k narušení bezpečnosti. I přes existenci bezpečnostních politik a postupů, lidská chyba, jako je kliknutí na phishingový odkaz nebo nesprávná konfigurace systému, může mít vážné důsledky pro bezpečnost organizace. Zvyšování povědomí a pravidelnější školení zaměstnanců mohou pomoci minimalizovat riziko lidských chyb.

5.3.3 Příležitosti (Opportunities)

Investice do nových technologií: Zavádění nejmodernějších bezpečnostních řešení, jako je umělá inteligence a strojové učení pro detekci hrozeb, může výrazně zlepšit schopnost organizace předcházet a reagovat na kybernetické útoky. Tyto technologie mohou automatizovat mnoho aspektů kybernetické bezpečnosti a zvýšit efektivitu ochranných opatření. Například strojové učení může analyzovat velké množství dat a identifikovat vzory, které naznačují potenciální hrozby, což umožňuje rychlejší a přesnější reakci na incidenty. Umělá inteligence může také pomoci při automatizaci rutinních bezpečnostních úkolů, což uvolňuje lidské zdroje pro řešení složitějších problémů.

Zlepšení školení zaměstnanců: Zvýšení povědomí a dovedností zaměstnanců prostřednictvím pravidelných školení o kybernetické bezpečnosti může snížit riziko lidských chyb. Školení by mělo zahrnovat aktuální hrozby, bezpečnostní postupy a simulace kybernetických útoků, aby zaměstnanci byli připraveni na různé scénáře. Zvýšená informovanost a připravenost zaměstnanců mohou výrazně přispět k celkové bezpečnosti organizace.

Partnerství s bezpečnostními firmami: Spolupráce s externími experty a firmami specializujícími se na kybernetickou bezpečnost může přinést nové znalosti a technologie, které posílí bezpečnostní opatření organizace. Tato partnerství mohou také poskytnout přístup k pokročilým nástrojům a službám, které by byly jinak pro organizaci nedostupné.

Externí audity a certifikace: Získání dalších certifikací v oblasti kybernetické bezpečnosti a provádění pravidelných externích auditů může posílit důvěru klientů a zlepšit celkové bezpečnostní postavení společnosti. Audity a certifikace potvrzují, že organizace dodržuje

nejlepší postupy a standardy v oblasti kybernetické bezpečnosti. Pravidelné audity mohou také pomoci identifikovat a opravit slabá místa v bezpečnostních opatřeních.

5.3.4 Hrozby (Threats)

Zvyšující se sofistikovanost útoků: Nové a pokročilé kybernetické útoky, které mohou obejít tradiční bezpečnostní opatření, představují stále větší hrozbu. Hackeři využívají stále složitější techniky, jako je ransomware, spear-phishing, a útoky typu zero-day, které mohou snadno překonat starší nebo neaktualizované bezpečnostní systémy. Organizace musí neustále inovovat a zlepšovat své bezpečnostní postupy, aby čelily těmto stále se měnícím hrozbám. Zvyšující se sofistikovanost útoků také znamená, že organizace musí investovat více prostředků do monitorování a reakce na incidenty.

Rostoucí počet útoků na pojišťovny: Pojišťovny spravují velké množství osobních informací. Únik těchto dat může mít závažné následky jak pro jednotlivce, tak pro organizace. Útoky typu ransomware, kde útočníci šifrují data a požadují výkupné za jejich dešifrování, mohou být pro útočníky velmi lukrativní. Pojišťovny totiž často disponují značnými finančními zdroji, což z nich činí atraktivní cíl pro kybernetické zločince.

Regulační sankce: Pojišťovny musí dodržovat přísné zákony a předpisy týkající se ochrany osobních údajů, jako je GDPR. Nedodržení těchto předpisů může vést k vysokým pokutám a právním následkům. Sankce mohou mít vážné finanční dopady a poškodit reputaci organizace. Organizace musí pravidelně provádět audity a revize svých bezpečnostních politik a postupů, aby zajistily soulad s platnými zákony a předpisy.

Právní a regulační změny: Rychlé změny v právních a regulačních požadavcích mohou vyžadovat časté úpravy bezpečnostních opatření a procesů, což může být časově náročné. Organizace musí být schopna rychle se přizpůsobit novým požadavkům, což může vyžadovat významné investice do aktualizací systémů a školení zaměstnanců. Neustálé změny v legislativě a regulacích také mohou vytvářet nejistotu a komplikovat dlouhodobé plánování bezpečnostních strategií. Flexibilita a schopnost rychlé adaptace jsou klíčové pro udržení souladu s měnícími se právními a regulačními požadavky.

5.4 Navrhovaná doporučení

Na základě rozhovoru s vedoucím IT pracovníkem a podrobně provedené SWOT analýzy se podařilo identifikovat silné stránky a slabé stránky společnosti. Tato kapitola se zaměřuje především na slabiny společnosti, které byly odhaleny během této analýzy, a také doporučením, jak tyto slabiny efektivně řešit. Slabiny v oblasti kybernetické bezpečnosti mohou vést k vážným následkům, které mohou ohrozit nejen chod společnosti, ale také její důvěryhodnost a finanční stabilitu. Je klíčové věnovat těmto problémům dostatečnou pozornost a podniknout kroky k jejich odstranění nebo minimalizaci.

Školení zaměstnanců:

Školení zaměstnanců v oblasti kybernetické bezpečnosti probíhá při nástupu na pozici a následně každé dva roky. Jsou doporučována raději menší a pravidelná školení v kratších intervalech než jedno velké školení za dva roky. Pravidelné připomínání zajišťuje, že si zaměstnanci lépe zapamatují informace a zásady kybernetické bezpečnosti. Efektivní školení reaguje na nejnovější trendy v kyberbezpečnosti. Hackeři neustále vymýšlejí nové metody útoků. Například phishingové útoky jsou na vzestupu, což může být způsobeno rostoucím využíváním umělé inteligence, která dokáže vytvářet podvržené e-maily bez gramatických chyb. Phishingové e-maily bývaly často plné gramatických nebo stylistických chyb, což je dnes už méně obvyklé. Některé klíčové znaky však stále mohou pomoci takové e-maily rozpoznat. Je důležité důkladně analyzovat rizika specifická pro konkrétní společnost. Taková analýza pomáhá určit, na co by se školení mělo zaměřit. Každá firma má jiná rizika. Například některé firmy nemusejí své zaměstnance školit na USB útoky, pokud mají USB porty zcela zakázané. Jiné firmy se mohou zaměřit na školení týkající se ochrany osobních údajů, protože často pracují s citlivými informacemi. Bezpečnostní školení by mělo odpovídat potřebám jednotlivých pracovníků. Lidé z IT oddělení by měli absolvovat školení zaměřené například na ransomware, zatímco obchodní oddělení se může zaměřit na BEC útoky (Business E-mail Compromise), při kterých podvodníci vylákají z firmy peníze prostřednictvím falešných faktur nebo vydáváním se za management. U běžných zaměstnanců by společnost měla rozvíjet povědomí o phishingových hrozbách a dalších metodách sociálního inženýrství.

Hesla

V současnosti si průměrný člověk musí pamatovat až 100 hesel, přičemž jejich počet neustále roste. Studie ukazují, že lidé si obvykle pamatují pouze kolem pěti hesel a často si práci zjednodušují vytvářením snadno uhodnutelných hesel, která používají napříč různými online účty. Někteří z nich nahradí písmena číslicemi a speciálními znaky (například "heslo" se změní na "P4??WØrd"), ale i tak jsou tato hesla snadno prolomitelná. V posledních letech významné organizace, jako je The Open Web Application Security Project (OWASP) a National Institute of Standards and Technology (NIST) posunuly své zásady k uživatelsky přívětivějším přístupům, které zároveň zvyšují bezpečnost hesel. Technologičtí giganti jako Microsoft a Google vybízejí k úplnému přechodu na bezheslové přihlašování. Místo kratších, ale složitých hesel je lepší používat heslové fráze. Takové heslo je delší a složitější, ale stále snadno zapamatovatelné. Například celá věta, která vám utkvěla v paměti, doplněná velkými písmeny a speciálními znaky. Před několika lety byla minimální délka silného hesla osm znaků, skládající se z malých a velkých písmen, speciálních znaků a čísel. Dnes automatizované nástroje dokážou takové heslo prolomit během několika minut, zejména pokud je zabezpečeno hashovací funkcí MD5. Naopak prolomení jednoduchého hesla dlouhého 18 znaků trvá mnohem déle. Delší hesla zvyšují počet možných kombinací exponenciálně, což ztěžuje jejich prolomení. Každé heslo by mělo být jedinečné pro každý účet – pokud by totiž útočník získal klíč, má poté přístup ke všemu. Heslové fráze jsou výrazně bezpečnější než jednotlivá slova a snadnější na zapamatování, sestávající z celé věty nebo sady slov. Například místo "HkfJ#525cJLMS" lze použít "MojePrvníPráceBylaVRychlemObcerstveni@2009", což je delší, bezpečnější a snáze zapamatovatelné. Mnemotechnické pomůcky, jako jsou akronymy, substituce znaků nebo heslové fráze, pomáhají vytvářet silná a snadno zapamatovatelná hesla. Akronymy využívají první písmena slov ve frázi, například "V létě miluji turistiku na horách" na "VLmtnh". Substituce znaků mění některá písmena na čísla nebo speciální znaky, jako například "heslo" na "h35l0" Heslové fráze mohou být například "MojePrvníAutoByloČervenyMercedesAMělo100Koní!". Použití textu písně, básně nebo rýmu, který si snadno zapamatujete, jako například střídání malých a velkých písmen s číslicemi, také pomáhá. Například dětská básnička "kočka leze dírou pes oknem"

Kočka	leze	dírou	pes	oknem
Ko1	Le2	Dí3	Pe4	Ok5

může být převedena na heslo "Ko1Le2Dí3Pe4Ok5".

Posílení lidských zdrojů

Společnost trpí nedostatkem kvalifikovaných odborníků na kybernetickou bezpečnost. Ve firmě s více než tisíci zaměstnanci jsou pouze čtyři IT architekti a několik vývojářů. Tito architekti jsou pracovně přetížení a nemají dostatek času na monitorování detekčních nástrojů, což může omezit schopnost firmy reagovat na incidenty. Pojišťovna by měla investovat do náboru a školení odborníků na kybernetickou bezpečnost a zvýšit počet kvalifikovaných specialistů v týmu.

Zamezení USB

Nejslabším článkem v kyberbezpečnosti je vnímán lidský faktor. Jak již bylo zmíněno v teoretické části, USB útok je typ kybernetického útoku, při kterém se zneužívá USB zařízení k šíření škodlivého softwaru nebo k získání neoprávněného přístupu k datům v cílovém počítači nebo síti. Společnost nevyužívá cloudové služby a spoléhá na vlastní zálohování, což může vést k častějšímu používání USB zařízení a tím se zvýšit riziko kybernetických útoků. Pro ochranu před těmito hrozbami je vhodné zavést několik opatření. Například lze omezit přístup k USB portům pro uživatele, kteří nejsou oprávněni pracovat s citlivými daty, nebo povolit pouze určitým skupinám zaměstnanců práci s externími zařízeními.

Implementace pokročilých technologií

I když společnost používá základní bezpečnostní opatření, měla by zvážit nasazení pokročilých technologií, jako jsou systémy využívající umělou inteligenci (AI) a strojové učení (ML) pro detekci anomálií a potenciálních hrozeb.

Umělá inteligence je dnes klíčovým nástrojem v oblasti kybernetické bezpečnosti. Využívá se zde jak tradiční AI pro lokální analýzu, tak pokročilé AI systémy, které prohledávají obrovská množství dat a hledají podezřelé signály. Vývoj technologií v oblasti kybernetické obrany se neustále přizpůsobuje novým hrozbám. V dnešní době útočníci využívají AI k maskování svých činností a k vytváření velkého množství variant škodlivého kódu, které tradiční obranné nástroje nedokáží zachytit. Navíc útočníci systematicky hledají zranitelnosti v softwaru a aplikacích dostupných z internetu, tzv. zero-day zranitelnosti, o kterých dosud nikdo neví, což jim přináší zisky.

Umělá inteligence pomáhá odhalovat kybernetické útoky tím, že sbírá data z různých zdrojů, jako jsou servery, síťové prvky (routery, switche), bezpečnostní zařízení (firewally, systémy prevence průniku, load ballancery, ochrany proti DDoS útokům, ochrana a monitoring koncových zařízení a jiné) a aplikace (přihlašování uživatelů, přístupy k datům, atd.). K těmto

lokálním datům jsou přidávány informace z globální sítě a informace o známých zranitelnostech. Centrální AI engine analyzuje toto obrovské množství dat a odhaluje vektory útoků, které by jinak unikly lidským operátorům. Tyto principy jsou základem téměř všech moderních bezpečnostních produktů a řešení, jako jsou Next-Gen a XDR. Čím více dat tato řešení mají k dispozici, tím větší je šance na odhalení dlouhodobých útoků (APT), které probíhají v mnoha krocích a mohou se zdát nevýznamné, pokud se na ně podíváme izolovaně.

Příklad takového útoku může zahrnovat škodlivý kód v e-mailu, který vytvoří zadní vrátka, a teprve po týdnech nebo měsících dojde k dalším fázím útoku, jako je stahování admin kitu, k ovládnutí dalších strojů v síti a exfiltrace dat. Po exfiltraci může dojít k úplnému odstranění stop, nebo naopak třeba k zašifrování dat a požadavku na výkupné. Útoky rozložené do dlouhého časového období mohou uniknout pozornosti bezpečnostního týmu a být obtížně odhalitelné nebo vyšetřitelné, pokud mezitím došlo k výmazu záznamů o starších aktivitách.

Efektivní obranou proti AI-řízeným útokům je opět využití AI. AI pomáhá odhalovat podvody, deepfake videa, pokusy o krádež identity a další útoky. Moderní ochrana proti phishingu se často neobejde bez prvků AI, které reagují na aktuální formy a metody útoků.

Udržování citlivých dat ve vlastním datovém centru pod dohledem vlastních expertů je stále nejbezpečnější, ale pro mnoho organizací je to finančně náročné. Proto se často volí kombinace AI a spravovaného cloudu. Řešení od společností jako Microsoft, Google nebo Amazon nabízejí pokročilé nástroje využívající AI, které se neustále učí, jak se bránit proti novým hrozbám. Tato řešení poskytují vysokou úroveň bezpečnosti s minimální potřebou vlastních odborníků, protože experty dodává poskytovatel cloudu.

Zálohování

Lokální zálohování dat nabízí několik výhod. Především, kontrola nad daty zůstává plně v rukou pojišťovny, což může zajišťovat vyšší úroveň bezpečnosti a ochrany citlivých informací. Lokální zálohování na dvou oddělených místech navíc poskytuje jistotu, že v případě fyzického poškození jednoho místa, jako například požáru nebo povodně, budou data stále dostupná z druhé lokality. Lokální zálohy také nevyžadují závislost na internetovém připojení, což znamená, že obnova dat může být rychlá a nezávislá na dostupnosti síťových služeb. Na druhou stranu, lokální zálohování má i své nevýhody. Náklady na hardware, údržbu a fyzickou bezpečnost mohou být značné. Pojišťovna musí také zajistit dostatečné kapacity a pravidelnou aktualizaci zálohovacích systémů, což vyžaduje značné lidské i finanční zdroje. Lokální

zálohování může být zranitelné vůči katastrofickým událostem, pokud nejsou zálohy dostatečně geograficky odděleny. Poskytovatelé cloudových služeb často nabízejí robustní bezpečnostní opatření a možnosti rychlé obnovy dat z jakéhokoli místa s internetovým připojením. Cloudová řešení mohou být také nákladově efektivní, protože eliminují potřebu investic do vlastního hardwaru a umožňují platit pouze za skutečně využívané kapacity. Flexibilita a možnost snadného rozšíření úložiště bez nutnosti fyzických úprav jsou dalšími významnými benefity. Nevýhodou cloudového zálohování je závislost na internetovém připojení, což může znamenat, že v případě výpadku sítě jsou data nedostupná. Navíc, i když cloudoví poskytovatelé investují do zabezpečení, data uložená mimo interní infrastrukturu mohou představovat vyšší riziko úniku nebo kybernetického útoku. Společnost nevyužívá cloudové služby pro zálohování dat, ale lokální zálohování na dvou oddělených místech. Lokální zálohování může omezit schopnost rychle obnovit data v případě katastrofického selhání serverů. Pojišťovna by měla zvážit zavedení hybridního zálohovacího řešení, které kombinuje lokální zálohování s cloudovým zálohováním. Cloudové zálohování poskytuje vyšší dostupnost a odolnost proti ztrátě dat díky geografické redundanci a automatizovaným procesům zálohování. Implementace cloudového zálohování by mohla výrazně zlepšit schopnost organizace obnovit data a minimalizovat dopady případných selhání. Cloudové služby také často nabízejí pokročilé bezpečnostní funkce. Dle zákona č. 181/2004 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), kterým se řídí pojišťovna, mohou orgány veřejné moci mohou využívat cloud computing, pokud před uzavřením smlouvy s poskytovatelem zařadí požadované cloudové služby do odpovídající bezpečnostní úrovně na základě povahy dotčeného informačního nebo komunikačního systému dle prováděcího právního předpisu. Orgány musí zajistit dodržování bezpečnostních pravidel stanovených Úřadem pro poskytování cloudových služeb. Dále musí mít orgány na základě své žádosti okamžitý přístup k informacím a datům uchovávaným poskytovatelem, včetně možnosti kontrolovat tato data v reálném čase.

Bezpečnost IoT

Vzhledem k tomu, že pojišťovna používá kamery, je zásadní pravidelně udržovat a aktualizovat tato zařízení. IoT zařízení, která nejsou správně udržována, představují významné bezpečnostní riziko, protože mohou být snadno zneužita útočníky. Pravidelné aktualizace zabezpečení pomáhají chránit zařízení před známými zranitelnostmi a zajišťují, že software zůstává odolný proti novým hrozbám. Neudržovaná zařízení mohou být použita jako vstupní bod pro útoky na síť. Je nutné zvážit oddělení IoT zařízení od hlavní firemní sítě pomocí segmentace sítě. Tento krok minimalizuje možnost, že kompromitované IoT zařízení může být použito jako brána k dalším citlivým částem infrastruktury.

Segregace povinností (SoD)

Segregace povinností, známá také jako "segregation of duties" (SoD), je klíčový princip v oblasti interního řízení a zabezpečení, který zajišťuje, že kritické úkoly a procesy jsou rozděleny mezi různé jednotlivce nebo týmy. Cílem této praxe je zabránit potenciálnímu zneužití moci a chybám tím, že se minimalizuje riziko, že jedna osoba nebo skupina bude mít kontrolu nad celým procesem.

V IT oddělení, a zejména v oblasti kybernetické bezpečnosti, je tento princip obzvláště důležitý. Například jedna osoba by neměla mít pravomoc implementovat změny v síťové infrastruktuře a zároveň monitorovat bezpečnostní logy. Pokud by totiž jedna osoba měla obě tyto odpovědnosti, mohla by potenciálně zakrýt své vlastní chyby nebo škodlivé jednání. Dalším příkladem může být situace, kdy správce systému, který má přístup k administrativním účtům, nemá také pravomoc schvalovat přístupová práva pro ostatní zaměstnance. Tento přístup zajišťuje, že žádný jednotlivý správce nemůže bez povšimnutí udělit neoprávněný přístup.

Rozdělením těchto úkolů mezi různé osoby nebo týmy se vytváří systém kontrol a vyvážení, který zajišťuje větší transparentnost a bezpečnost. Tímto způsobem je možné lépe chránit citlivá data, zamezit neoprávněným aktivitám a zajistit, že žádná jednotlivá osoba nemá příliš velkou moc nad kritickými systémy a procesy.

Vendor lock-in

Rozvoj informačních technologií v posledních letech umožňuje podnikům a firmám zvyšovat kvalitu svých služeb. Zatímco soukromý sektor často reaguje rychleji a pružněji na externí i interní změny, ve veřejnosprávních institucích je tento proces obvykle pomalejší. Z historického hlediska se rozvoj informačních systémů (IS) ve veřejné správě často pojí s konkrétním dodavatelem. To může vést k závislosti na jednom dodavateli, což je známé jako vendor lock-in. Vendor lock-in je situace, kdy se organizace stane závislou na jediném dodavateli pro produkty a služby, což ji činí obtížným nebo nákladným přejít k jinému dodavateli. Tato závislost může vzniknout kvůli specifickým technologickým řešením, unikátním softwarovým platformám, nebo dlouhodobým smluvním závazkům. Zpočátku, při budování informačního systému, je výhodné mít dodavatele s velkou kapacitou a vysokou odborností. V této fázi se vytváří nová architektura IS, optimalizují se a centralizují organizační celky, řeší se bezpečnost systémů a flexibilita v reakci na změny v organizaci. Dodavatel v této fázi často nese značnou část rizika neúspěchu. Jakmile však období rozvoje a budování skončí, organizace může zjistit, že je závislá na dodavateli, protože klíčové know-how se přesunulo na jeho stranu. Organizace pak ke všem činnostem souvisejícím s úpravami IS potřebuje součinnost dodavatele. To je případ i pojišťovny, která má dodavatele na správu aplikací a IS.

Aby se předešlo vendor lock-inu, je třeba podniknout kroky k získání zpět strategického know-how. To znamená získat zpět kontrolu nad nastavením, rozsahem a způsobem integrací jednotlivých komponent IS. Pokud je situace již vážná, může být nezbytné realizovat přebudování IS. Je potřeba získat strategické vědomosti a kompetence, ale také sladit stav IS s legislativními a technologickými změnami. Modernizace IS zahrnuje také přípravu na nové požadavky v oblasti kybernetické bezpečnosti a GDPR. Pojišťovna by měla být schopna nový systém nejen rozvíjet, ale také provozovat, což tradičně svěřuje dodavatelům. Nové nastavení by mělo zahrnovat větší zapojení vlastních zaměstnanců do návrhu nových architektonických prvků IS. Cílem by mělo být vybudovat moderní systém podporující flexibilitu a schopnost budovat nové typy služeb, zejména ty, které podporují digitální výměnu informací. Pokud získá společnost zpět strategické know-how a více se zapojí do rozvoje a provozu IS, může snížit závislost na dlouholetém dodavateli a otevřít se pro více dodavatelů, čímž podpoří konkurenční prostředí. Konkurenční prostředí přinese tlak na kvalitu dodávky a moderní způsob vývoje IS. Vendor lock-in představuje významné riziko pro společnosti, které mohou čelit zvýšeným nákladům, ztrátě flexibility a strategického know-how, a potenciálním bezpečnostním

problémům. K minimalizaci těchto rizik jsou klíčovými kroky spolupráce s více dodavateli, využívání technologií založených na otevřených standardech a protokolech usnadňující integraci s různými systémy a poskytovateli, vyjednávání flexibilních smluv a budování interního know-how.

ZÁVĚR

Kybernetická bezpečnost je v dnešní době jedním z nejdůležitějších aspektů pro každou organizaci, zvláště pak pro finanční instituce, jako jsou pojišťovny. Analýza kybernetické bezpečnosti v české pojišťovně ukázala, že i přes pevný právní rámec a zavedené postupy existují oblasti, které je třeba zlepšit a posílit. SWOT analýza odhalila jak silné stránky a příležitosti, tak slabé stránky a hrozby, kterým by se společnost měla věnovat, aby byla zajištěna optimální úroveň bezpečnosti.

Jednou z hlavních silných stránek je důsledné dodržování zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a souvisejících vyhlášek. Tato legislativa poskytuje pevný základ pro zajištění bezpečnosti informačních systémů a sítí. Dále pokročilá bezpečnostní infrastruktura, kvalifikovaný personál a implementace systému řízení bezpečnosti informací (ISMS), poskytují solidní základ pro efektivní ochranu proti kybernetickým hrozbám.

Na základě analýzy odpovědí společnosti a provedené SWOT analýzy byly vypracovány návrhy a doporučení, které vycházely z identifikovaných slabých stránek a hrozeb. Pojišťovna by měla zvážit investice do modernizace své technologické infrastruktury, zavedení cloudového zálohování a nasazení technologií, jako je umělá inteligence a strojové učení, které mohou výrazně zlepšit detekci a reakci na kybernetické hrozby. Důležitým krokem je také potřeba se věnovat aktualizacím a údržbě IoT a školení zaměstnanců, aby se minimalizovalo riziko lidských chyb.

Celkově lze říci, že cíle této práce byly úspěšně naplněny. Díky provedené analýze a navrženým opatřením by měla společnost dosáhnout významného zlepšení své bezpečnosti a snížení rizika kybernetických útoků. Úspěšné zlepšení kybernetické bezpečnosti v pojišťovně vyžaduje komplexní a integrovaný přístup, který kombinuje technologické inovace, lidské zdroje a organizační postupy. Důkladné plánování, testování a školení jsou klíčové pro implementaci těchto doporučení. Pravidelné revize a aktualizace bezpečnostních opatření, spolupráce s externími odborníky a aktivní sledování nejnovějších technologických trendů a hrozeb zajistí, že pojišťovna bude schopna čelit současným i budoucím výzvám v oblasti kybernetické bezpečnosti. Společnost, která je proaktivní a přizpůsobivá v oblasti kybernetické bezpečnosti, má větší šanci nejen přežít, ale také prosperovat v digitálním věku.

POUŽITÁ LITERATURA

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[2] ŠULC, Vladimír, 2018. Kybernetická bezpečnost. Plzeň: Aleš Čeněk. ISBN 978-80-7380-737- 5.

[3] Legislativa.cz. Kybernetický útok (kyberútok). Definice, typy, následky a prevence [online]. ©2022 [cit. 2023-11-14]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok#cap3

[4] Cesnet. Kybernetické útoky. [cit. 2023-12-30]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kybernetické_utoky.pdf

[5] Microsoft. Co je malware? [online]. [cit. 2023-12-30]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-malware

[6] Malwarebytes. Rootkit. [online]. [cit. 2023-12-30]. Dostupné z: https://www.malwarebytes.com/rootkit

[7] ESET. DDoS útoky. [online]. [cit. 2023-12-30]. Dostupné z: https://www.eset.com/cz/ddos-utok/

[8] Kaspersky. What is a Botnet? [online]. [cit. 2023-12-30]. Dostupné z: https://usa.kaspersky.com/resource-center/threats/botnet-attacks

[9] Avast. Sociální inženýrství. [online]. [cit. 2023-12-30]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

[10] ESET. Zero day útok. [online]. [cit. 2024-02-24]. Dostupné z: https://www.eset.com/cz/zero-day/

[11] Microsoft Azure. Přehled zabezpečení IoT. [online]. [cit. 2024-02-25]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-iot/security

[12] BLUECAT. Four DNS attack types and how to mitigate them. [online]. [cit. 2024-02-20]. Dostupné z: https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/

[13] Ninja One. 7 Cybersecurity Statistics You Needs to Know in 2024. [online]. [cit. 2024-07-01]. Dostupné z: https://www.ninjaone.com/blog/smb-cybersecurity-statistics-2023/

[14] Cybercrime Magazine. Cybercrime To Cost The World 8 Trillion Annually In 2023. [online]. [cit. 2024-02-23]. Dostupné z: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[15] Express VPN. The true cost of cyber attacks in 2024 and blond. [online]. [cit. 2024-02-20]. Dostupné z: https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

[16] NordLayer. Most common type sof cyberattacks in 2023. [online]. [cit. 2024-02-10]. Dostupné z: https://nordlayer.com/blog/most-common-types-of-cyber-attacks/

[17] GB Hackers. 10 Most Common Types Of Cyber Attacks In 2023. [online]. [cit. 2024-02-10]. Dostupné z: https://gbhackers.com/types-of-cyber-attacks-in-2023/

[18] Cyber Management Alliance. Biggest Cyber Attackds ě023, Top Data Breaches & Ransomware Attacks. [online]. [cit. 2024-02-19]. Dostupné z https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-2023-top-data-breaches-ransomware-attacks

[19] Novinky.cz. Česko zaostává v kybernetické bezpečnosti proti západní Evropě. [online]. [cit. 2023-12-30]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-cesko-zaostava-v-kyberneticke-bezpecnosti-proti-zapadni-evrope-40440046

[20] OPOJISTENI.CZ. NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů. [online]. [cit. 2024-02-24]. Dostupné z: https://www.opojisteni.cz/technologie/kyberneticka-rizika/nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/c:26621/

[21] Reseller Magazine Online. Co čeká kyberbezpečnost v roce 2020? [online]. [cit. 2024-02-25]. Dostupné z: https://www.rmol.cz/novinky/co-ceka-kyberbezpecnost-v-roce-2023

[22] MIŽENKO, Petr. Kybernetická bezpečnost z pohledu podnikové infrastruktury. Kladno, 2022. Bakalářská práce. České vysoké učení v Praze. Vedoucí práce Navrátil, Václav

[23] KOLOUCH Jan, BAŠTA Pavel a kol. CyberSecurity. 1. Vydání. Praha, 2019. ISBN 978-80-88168-31-7

[24] Wolters Kluwer. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti. [online]. [cit. 2024-02-25]. Dostupné z: https://www.aspi.cz/products/lawText/1/90229/0/2/vyhlaska-c-82-2018-sb-o-bezpecnostnich-opatrenich-kybernetickych-bezpecnostnich-incidentech-

reaktivnich-opatrenich-nalezitostech-podani-v-oblasti-kyberneticke-bezpecnosti-a-likvidaci-dat-vyhlaska-o-kyberneticke-bezpecnosti/vyhlaska-c-82-2018-sb-o-bezpecnostnich-opatrenich-kybernetickych-bezpecnostnich-incidentech-reaktivnich-opatrenich-nalezitostech-podani-v-oblasti-kyberneticke-bezpecnosti-a-likvidaci-dat-vyhlaska-o-kyberneticke-bezpecnosti

[25] Zákony pro lidi. Vyhláška č. 82/2018 Sb. [online]. [cit. 2024-02-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82#cast2

[26] DEV. How Networks Work: Exploring the Fundamentals of Switches, Routers, DNS, DHCP, NAT, VPN, and More. [online]. [cit. 2024-02-28]. Dostupné z: https://dev.to/kaushit/how-networks-work-exploring-the-fundamentals-of-switches-routers-dns-dhcp-nat-vpn-and-more-33d1

[27] Ruijie. What is ACL in Networking? Difference between ACL and Firewall. [online]. [cit. 2024-02-28]. Dostupné z: https://www.ruijienetworks.com/support/faq/what-is-acl-in-networking

[28] SPRÁVA SÍTĚ. Co je proxy server. [online]. [cit. 2024-02-28]. Dostupné z: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

[29] JUPITER. What is IDS and IPS? . [online]. [cit. 2024-02-28]. Dostupné z: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

[30] LinkedIn. Antivirus vs SIEM: Understanding the Differences and Synergies. [online]. [cit. 2024-02-28]. Dostupné z: https://www.linkedin.com/pulse/antivirus-vs-siem-understanding-differences-synergies-raghunathan

[31] MIŽENKO, Petr. Kybernetická bezpečnost z pohledu podnikové infrastruktury. Bakalářská práce. České vysoké učení technické v Praze. Vedoucí práce Navrátil Václav.

PŘÍLOHY

Otázky na IT management

1. Má organizace zpracovány postupy a procesy pro vyhodnocování kybernetických bezpečnostních událostí?
2. Jsou ve společnosti stanoveny postupy při vzniku nestandardní situace?
3. Jsou zaměstnanci obeznámeni s tím, co mají hlásit a mají k dispozici konkrétní kontakty. Hlásí organizace bezpečnostní incident CSIRT týmu?
4. Má organizace vypracován plán kontinuity činností (Business Continuity Plan – BCP), plán obnovy (Disaster Recovery Plan – DRP) a havarijních plány, aby v případě mimořádné situace (havárie, živelné pohromy nebo úspěšného kybernetického útoku) byla organizace schopna obnovit svoji funkčnost?
5. Má organizace nějakou certifikaci v oblasti kybernetické bezpečnosti?
6. Je pravidelně aplikována kontrola prostředí včetně instalace bezpečnostních aktualizací používaného software serverů i klientských stanic?
7. Je společností aplikováno skenování sítě, portů, případně další jiné metody pro získání důležitých informací o úrovních zabezpečení? Jsou využívány systémy IDS?
8. Využívá organizace zálohování pomocí cloudových služeb nebo jinou metodou? Jsou na poskytovatele cloudových služeb uplatněna stejná pravidla jako pro ostatní dodavatele?
9. Je kontrolována příchozí pošta zaměstnanců společnosti antispamem či antivirem?
10. Bývá pravidelně pořádáno školení zaměstnanců v oblasti kyberbezpečnosti?
11. Jakou má organizace politiku hesel? (Jsou vyžadována po zaměstnancích silná hesla (vyšší počet znaků, kombinace čísel, velkých písmen a symbolů)? Jak v pravidelných intervalech požadována změna? Je využíván správce hesel?)
12. Je používáno v rámci řízení identit Princip minimálního oprávnění (POLP)?
13. Je používáno v rámci řízení identit Přístup na základě role (RBAC)?
14. Aplikuje společnost simulaci phishingových emailů na své zaměstnance z důvodu osvěty a vzdělávání zaměstnanců?
15. Je využívána vícefaktorová autentizace a podmíněný přístup?
16. Mají zaměstnanci umožněn volný přístup na veřejném internetu?

DOTAZNÍK

1) Jaký postup zvolíte, když dostanete požadavek na změnu hesla?
   - Okamžitě změním heslo podle pokynů a doporučení
   - Odkládám změnu hesla až do poslední chvíle
   - Ignoruji požadavek na změnu hesla
   - Neprovádím žádné změny hesla

2) Používáte na různých online službách stejná hesla?
   - Ano, všechna moje hesla jsou stejná
   - Ano, ale mám různé hesla pro důležité účty
   - Ne, používám různá hesla pro různé služby
   - Nepoužívám hesla, mám automatické přihlášení

3) Jaké kroky podnikáte pro chránění svých firemních hesel?
   - Používám silná a jedinečná hesla pro každý účet
   - Často používám stejná hesla pro různé účty
   - Nepoužívám hesla nebo je používám pouze sporadicky
   - Nepoužívám žádná hesla

4) Jaké opatření používáte k ochraně svých online účtů?
   - Dvoufaktorová autentizace (2FA)
   - Silná hesla
   - Antivirový software
   - Firewal
   - Virtuální privátní síť (VPN)
   - Jiné (uveďte): _____

5) Dělíte se někdy o své přihlašovací údaje nebo hesla s kolegy?
   - Ano
   - Ne

6) Jak reagujete na výstrahy o bezpečnostních aktualizacích na vašem zařízení?
   - Aktualizace provádím ihned po výstraze
   - Provádím aktualizace, ale často odkládám
   - Ignoruji aktualizace a neprovádím je
   - Neprovedl(a) jsem žádné aktualizace

7) Jak reagujete na neobvyklé aktivity ve vašem účtu (např. podezřelé přihlašování)?
   - Okamžitě informuji IT oddělení o neobvyklých aktivitách
   - Zkouším si vyřešit problém sám(a)
   - Ignoruji neobvyklé aktivity a doufám, že odezní
   - Neuvědomil(a) jsem si žádné neobvyklé aktivity

8) Jaká je vaše zkušenost s podvodnými e-maily nebo phishingovými útoky?
   - Nemám zkušenost
   - Mám minimální zkušenost
   - Mám zkušenost, ale nikdy jsem nebyl(a) obětí
   - Stal(a) jsem se obětí

9) Jak zacházíte s citlivými informacemi, když komunikujete přes veřejné komunikační kanály (např. e-mail, chat)?
   - Dbám na to, aby citlivé informace nebyly sdíleny přes veřejné kanály
   - Sdílím citlivé informace bez ohledu na komunikační kanál
   - Neuvědomil(a) jsem si komunikaci citlivých informací přes veřejné kanály

10) Jak zacházíte s podezřelými e-maily (např. od neznámých odesílatelů, s podezřelými přílohami)?
   - Okamžitě je označím jako spam nebo phishing
   - Otevřu je, ale nekliknu na odkazy nebo otevírám přílohy
   - Otevřu je a klikám na odkazy nebo otevírám přílohy bez obav
   - Ignoruji podezřelé e-maily

11) Jaký postup zvolíte, když dostanete podezřelý e-mail od kolegy?

- Zkontaktuji kolegu osobně nebo telefonicky, abych potvrdil(a) pravost e-mailu
- Okamžitě označím e-mail jako spam nebo phishing
- Otevřu e-mail a kliknu na odkazy nebo otevřu přílohy
- Neuvědomil(a) jsem si žádné podezřelé e-maily od kolegů

12) Jaký máte postup, když pracujete mimo kancelář (např. na veřejné Wi-Fi)?

- Používám VPN a další bezpečnostní opatření
- Nedůvěřuji veřejným sítím, takže se vyhýbám práci na nich
- Pracuji na veřejné Wi-Fi bez dalších bezpečnostních opatření
- Pracuji mimo kancelář, aniž bych zvažoval(a) bezpečnostní rizika

13) Jaké máte postupy pro ochranu svého pracovního zařízení, když opouštíte pracoviště?

- Zamykám zařízení a ukládám ho na bezpečné místo
- Nechávám zařízení nezamčené, ale skryté z pohledu veřejnosti
- Pravidelně zamykám zařízení a udržuji jej ve střeženém prostředí
- Někdy zamykám zařízení, ale často ho nechávám nehlídané
- Zřídka zamykám zařízení a občas ho nechávám nehlídané
- Nezajímám se o ochranu zařízení

14) Jakou pozornost věnujete vytváření a udržování záloh důležitých dat?

- Pravidelně zálohuji důležitá data a ukládám je na bezpečném místě
- Občas zálohuji data, ale nepravidelně
- Nezálohuji důležitá data

15) Jaký postup zvolíte, když narazíte na podezřelý webový obsah?

- Okamžitě uzavřu okno a oznamuji to IT oddělení
- Prozkoumám podezřelý obsah blíže
- Ignoruji podezřelý obsah a pokračuji ve prohlížení
- Neprovádím žádné kroky k řešení podezřelého obsahu
- S touto situací jsem se nesetkal(a)

16) Jaký postup zvolíte, když vám dojde, že jste spáchal(a) chybu, která mohla zvýšit riziko kybernetického útoku?

- Okamžitě informuji odpovědnou osobu nebo IT oddělení
- Snažím se chybu rychle napravit sám(a)
- Neuvědomuji si chybu nebo ji ignoruji
- Nezpůsobil(a) jsem žádné chyby ohledně kyberbezpečnosti

17) Uvědomujete si rizika spojená s používáním veřejných Wi-Fi sítí?

- Ano
- Ne

18) Máte povědomí o politikách kyberbezpečnosti ve vaší organizaci?

- Ano
- Ne

19) Znáte postupy pro nahlášení kybernetického incidentu ve vaší organizaci?

- Ano
- Ne

20) Informuje společnost zaměstnance o kyberbezpečnosti a jakou formou?

- Ano, prostřednictvím online školení
- Ano, prostřednictvím pravidelných prezentací
- Ano, prostřednictvím firemních newsletterů
- Neinformuje