Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Firemní procesy ve vztahu k normě ISO 27001

Bc. Lukáš Matejčík

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lukáš Matejčík

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Firemní procesy ve vztahu k normě ISO 27001

Název anglicky

The ISO 27001 standard in relation to the company processes.

Cíle práce

Cílem diplomové práce je provést návrh a posouzení procesů ve vybrané firmě s ohledem na implementaci požadavků normy ISO 27001, tj. seznámit se s problematikou aplikace tohoto mezinárodně platného standardu, který definuje požadavky na systém managementu bezpečnosti informací, s ohledem na požadavky konkrétní firmy. Na základě poznatků z literatury, vlastní analýzy a měření, provést rozbor jednotlivých možností a navrhnout a doporučit vhodná opatření a řešení pro praktickou aplikaci, která budou posouzena z hlediska technického a ekonomického.

Metodika

Struktura práce

1. Úvod

2. Cíl a metodika práce

3. Současný stav sledované problematiky

4. Vlastní řešení; výsledky a diskuse

5. Závěr a doporučení

6. Seznam použitých zdrojů a přílohy

Metodika práce

I. Teoretická část – norma ISO 27001 a její vztah k procesům ve firmě; zákon o kybernetické bezpečnosti 181/2014 Sb. a jeho vztah k procesům ve firmě; analýza procesu přijímání externistů; analýza potenciálních rizik plynoucích z nedostatků procesu

II. Praktická část – návrh řešení nedostatků procesu; analýza dopadu nápravných opatření; zhodnocení nápravných opatření v celkovém kontextu firmy

Doporučený rozsah práce

45 až 55 stran

Klíčová slova

kybernetická bezpečnost, bezpečnost informací, management bezpečnosti informací, sdílení informací

Doporučené zdroje informací

BOHÁČ, L. a BEZPALEC, P.: Datové sítě – přednášky. 1. vydání. České vysoké učení technické, Praha 2011, 204 s., ISBN 978-80-01-04694-4

Příslušné zákony, nařízení vlády, vyhlášky, ČSN, oborové předpisy a odborné časopisy

SPURNÁ, I.: Počítačové sítě – praktická příručka správce sítě. 1. vydání. Computer Media, Kralice na Hané 2010, 180 s. ISBN 978-80-7402-036-0

STALLINGS, W.: Data and Computer Communications. 10. vydání. Pearson: 2013, 912 s. ISBN-13: 978-0133506488

TRULOVE, J.: Sítě LAN – hardware, instalace a zapojení. 1. vydání. Grada, Praha: 2009, 384 s. ISBN 978-80-247-2098-2

Předběžný termín obhajoby

2023/2024 LS – TF

Vedoucí práce

doc. Ing. Petr Vaculík, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 25. 1. 2023

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 8. 3. 2023

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 31. 03. 2024

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Firemní procesy ve vztahu k normě ISO 2700" jsem vypracoval samostatně pod vedením vedoucího diplomové práce s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Petr Vaculíkovi, Ph.D. za věcné připomínky a rady. Mému dědovi, mamince a snoubence bych chtěl poděkovat za podporu při studiu.

Firemní procesy ve vztahu k normě ISO 27001

Abstrakt

Oblast zaměření této diplomové práce je návrh a hodnocení procesů ve vybrané společnosti s ohledem na implementaci požadavků normy ISO 27001. Práce zahrnuje detailní analýzu vlivu standardu na procesy ve společnosti, včetně vztahu mezi ISO 27001 a procesy ve firmě, a také vlivu zákona o kybernetické bezpečnosti 181/2014 Sb. Specifický důraz je kladen na proces přijímání externistů a identifikaci potenciálních rizik plynoucích z nedostatků v tomto procesu. Práce navrhuje opatření k minimalizaci těchto rizik a posílení bezpečnosti informací přizpůsobené specifickým potřebám společnosti. Doporučení plynoucí z diplomové práce si klade za cíl být technicky proveditelné a ekonomicky výhodné, čímž předkládá komplexní přístup k efektivní implementaci ISO 27001 ve vybrané společnosti.

Klíčová slova: kybernetická bezpečnost, bezpečnost informací, management bezpečnosti informací, sdílení informací, ISMS

Company processes in relation to ISO 27001 standard

Abstract

Field of focus of this thesis is on the design and evaluation of processes in a selected company with respect to the implementation of the ISO 27001 standard requirements. It encompasses a detailed analysis of the standard's impact on company processes, including the relationship between ISO 27001 and the processes within the company, as well as the influence of the Cybersecurity Law 181/2014 Sb. A specific focus is given to the process of onboarding external personnel and the identification of potential risks stemming from deficiencies in this process. The thesis proposes measures to mitigate these risks, enhancing information security tailored to the company's specific needs. The recommendations aim to be both technically feasible and economically advantageous, offering a comprehensive approach to implementing ISO 27001 effectively in the chosen company.

Keywords: cyber security, information security, information security management, information sharing, ISMS

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

ISMS – information security management system

GDPR – General data protection regulation

DDoS – Distributed denial of service
DRP – Disaster recovery plan
BIA – Business impact analysis
BCP – Business continuity plan
EU – Evropská Unie
CMDB – Configuration management database
CIO – Chief information officer
CISO – Chief information security officer
CSIRT – Cyber security incident response team
BCM – Business continuity manager

1 Úvod

V dnešním digitálně propojeném světě, kde informace a jejich bezpečnost hrají klíčovou roli ve všech aspektech firemního působení, se stává implementace efektivního systému managementu bezpečnosti informací (ISMS) nejen významnou, ale často nezbytnou součástí úspěšného podnikání. Tato diplomová práce se zaměřuje na návrh a posouzení procesů ve vybrané firmě s ohledem na implementaci požadavků normy ISO 27001. Tento mezinárodně uznávaný standard definuje požadavky ISMS a je zcela zásadní pro zajištění ochrany a integrity firemních dat.

Teoretická část práce se zabývá teoretickým základem, kde je prozkoumána norma ISO 27001 a její význam pro procesy ve firmě. Tato norma není pouze souborem pravidel, ale představuje holistický přístup k zabezpečení informací, který zahrnuje jak technické, tak organizační aspekty. V návaznosti na to je zkoumán vztah mezi zákonem o kybernetické bezpečnosti č. 181/2014 Sb. a procesy ve firmě. Tento zákon, který je zásadní pro český právní rámec v oblasti kybernetické bezpečnosti, má přímý dopad na způsob, jakým firmy spravují a chrání veškeré své informační zdroje.

Mimo teoretický základ se autor práce věnuje také praktické aplikaci těchto teorií. Analyzován je proces životního cyklu (lifecyclu) externistů a identifikována potenciální rizika spojená s nedostatky tohoto procesu. Výstupem práce je rozbor těchto rizik, návrh opatření pro jejich minimalizaci a zesílení bezpečnosti informací v kontextu konkrétní firmy.

2 Cíl práce

Cílem této diplomové práce je aplikace normy ISO 27001 na ISMS a zákonu o kybernetické bezpečnosti č. 181/2014 Sb. ve vybrané organizaci. Hlavním úkolem je identifikovat, jak mohou být principy normy efektivně integrovány do firemních procesů, zejména v procesu přijímání externistů, a navrhnout opatření pro zlepšení ochrany informací. Dále práce hodnotí identifikovaná rizika a navrhuje kroky pro jejich zmírnění s ohledem na technickou realizovatelnost a ekonomickou efektivitu. Závěrem se práce zaměřuje na praktickou aplikaci navržených řešení v konkrétním podnikatelském prostředí a posuzuje jejich vliv vůči zlepšení bezpečnosti informací ve firmě, čímž přináší ucelený pohled na implementaci ISMS v souladu s normou ISO 27001.

3 Metodika

Metody pro vypracování této diplomové práce zohledňují výše uvedený cíl a jsou následující:

- Popis pojmů a praktik v oblasti bezpečnosti informací
- Analýza stavu bezpečnosti informací ve společnosti a popis rizik s tím souvisejících
- Návrh řešení na rizika spojené s bezpečností informací
- Implementace navržených řešení do organizace
- Vyhodnocení výsledků implementace a její dopady na společnost
- Doporučení pro další postup v ochraně informací organizace

4 Současný stav sledované problematiky

Bezpečnost informací je základní kámen ochrany a správy cenných informačních aktiv každé organizace. V éře digitální transformace, kdy se informace staly jedním z nejcennějších zdrojů firem a společností, je důležitější, než kdy jindy chránit je před širokou škálou hrozeb a zranitelností.

4.1 Základní pojmy a definice bezpečnosti informací

Bezpečnost informací je disciplína, která se zabývá ochranou informací a informačních systémů před neoprávněným přístupem, použitím, zveřejněním, narušením, změnou, prohlížením nebo zničením s cílem zajistit jejich důvěrnost, integritu a dostupnost.

Každý z těchto pěti základních principů je zásadní pro vytvoření a udržení bezpečného a důvěryhodného informačního prostředí v organizaci. Společně tvoří základní rámec, na kterém je postavena strategie bezpečnosti informací.

4.1.1 Důvěrnost

Důvěrnost se týká ochrany informací před neoprávněným přístupem nebo prohlížením. Zajištění důvěrnosti informací znamená, že jsou přístupné pouze těm, kteří mají k tomu oprávnění. Zajištění přístupu oprávněných osob se provádí pomocí různých bezpečnostních mechanismů, jako jsou šifrování, kontroly přístupů a autentizační procesy. Například šifrování dat transformuje citlivé informace do formy, kterou nelze číst bez dešifrovacího klíče (1).

4.1.2 Integrita

Integrita se zabývá ochranou informací proti neoprávněným změnám, to zahrnuje jakýkoliv druh modifikace, včetně vymazání nebo poškození. Zajištění integrity znamená udržení přesnosti a úplnosti informací během celého jejich životního cyklu. Toho je dosahováno prostřednictvím kontrolních součtů, digitálních podpisů a systémů, které monitorují a ověřují změny v datech (1).

4.1.3 Dostupnost

Dostupnost v rámci bezpečností informací znamená, že autorizovaní uživatelé mají vždy, když potřebují, přístup k informacím a přidruženým zdrojům. To zahrnuje ochranu proti útokům typu DDoS (Distributed denial of service), které se snaží zpřístupněné služby vyřadit z provozu. Zajištění dostupnosti informací vyžaduje robustní infrastrukturu, redundanci systémů, pravidelné zálohování a efektivní plány obnovy po havárii (1).

4.1.4 Autentičnost

Autentičnost je zaměřena na ověření, že informace jsou skutečně od jejich deklarovaných zdrojů nebo autorů. To představuje potvrzení identity osob nebo systémů, které spolu komunikují. Autentičnost je zpravidla zajišťována prostřednictvím autentizačních technik, jako jsou hesla, biometrické údaje nebo digitální certifikáty, které pomáhají ověřit identitu uživatele nebo zařízení (1).

4.1.5 Nepopiratelnost

Nepopiratelnost zajišťuje, že jednou provedená akce nebo transakce nemůže být popřena svým autorem. To je klíčové v elektronickém obchodování a online komunikaci, kde je důležité mít důkaz o tom, že určitá komunikace nebo transakce skutečně proběhla. Nepopiratelnosti se dosahuje prostřednictvím digitálního podpisu nebo jiných technologií zaznamenávání, které mohou sloužit jako právně uznatelný důkaz (1).

4.2 Význam bezpečnosti informací v organizacích

Význam bezpečnosti informací pro organizace sahá daleko za rámec jednoduché ochrany dat. Je to základní stavební kámen, který umožňuje organizacím udržet si důvěru svých zákazníků, dodržovat regulační požadavky, chránit svou konkurenční výhodu a zajistit kontinuitu svých interních i externích operací. Tato část práce se bude zabývat klíčovými důvody, proč je bezpečnost informací nezbytná pro úspěch a udržitelnost organizací ve všech sektorech a jak může nedostatečná ochrana informací vést k závažným finančním, právním a reputačním rizikům.

4.2.1 Ochrana citlivých dat

Ochrana citlivých dat je klíčovou součástí bezpečnostní strategie organizace, zahrnující osobní údaje, finanční záznamy a obchodní tajemství. Prvním krokem je identifikace

a klasifikace dat podle jejich citlivosti, což umožňuje efektivní aplikaci ochranných opatření. Klasifikace informací je základem pro správně prováděnou ochranu dat (1).

V souladu s právními a regulačními požadavky, jako je obecné nařízení o ochraně osobních údajů musí organizace zajistit, aby jejich způsoby ochrany dat byly v plném souladu s těmito nařízeními, což pomáhá předcházet potenciálním právním a finančním sankcím (2).

Organizace rutinně zpracovávají a ukládají širokou škálu citlivých dat, která mohou zahrnovat osobní údaje zaměstnanců, zákazníků, finanční záznamy (transakce) a obchodní tajemství. Osobní údaje mohou také obsahovat celá jména, adresy, telefonní čísla a další identifikovatelné informace. Finanční informace zahrnují účetní záznamy, investiční strategie, transakce a výkazy zisků a ztrát, zatímco obchodní tajemství mohou zahrnovat nezveřejněné patenty a byznysové strategie (3).

Důsledky neoprávněného přístupu k těmto datům mohou vést k finančním ztrátám, pokutám od státních orgánů, ztrátě důvěry zákazníků, právním sporům a poškození firemní pověsti. Zabezpečení těchto informací je tedy nezbytné pro zachování konkurenční výhody a dodržování regulačních požadavků (4).

Průměrná cena ztráty dat v roce 2023 byla 4,5 milionu dolarů což představuje 15 % nárůst za uplynulé tři roky (5).

4.2.2 Právní a regulační požadavky

Regulační požadavky na kybernetickou bezpečnost v České republice jsou stanoveny především zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a souvisejícími prováděcími předpisy spolu s nařízením Evropského parlamentu a Rady EU 2016/679, GDPR (General data protection regulation). Tento zákon s jeho předpisy a nařízením EU tvoří základní rámec pro ochranu kybernetického prostoru v České republice, stanovují povinnosti pro poskytovatele základních služeb, poskytovatele digitálních služeb a orgány veřejné moci. Zákon o kybernetické bezpečnosti byl přijat s cílem zvýšit ochranu proti kybernetickým hrozbám a posílit národní bezpečnost.

4.2.3 Identifikace a klasifikace subjektů v rámci kybernetické bezpečnosti

V kontextu zajištění kybernetické bezpečnosti je kritickým prvním krokem identifikace a klasifikace subjektů, které jsou považovány za klíčové pro fungování státu a společnosti. V České republice, podobně jako v mnoha jiných zemích, je tento proces formalizován prostřednictvím legislativy, konkrétně zákona o kybernetické bezpečnosti. Tento zákon rozlišuje mezi dvěma hlavními skupinami subjektů, jejichž role a odpovědnost v kybernetickém prostoru jsou považovány za zásadní (6).

Mezi základní poskytovatele se zahrnují organizace a instituce, které poskytují služby nezbytné pro každodenní fungování společnosti a ekonomiky. Mezi tyto služby se řadí:

- Zajištění stabilního a bezpečného dodávání elektrické energie, plynu a paliv.
- Veškeré aspekty dopravní infrastruktury, včetně železniční, letecké, silniční a vodní dopravy.
- Poskytování zdravotní péče a služeb, včetně nemocnic a dalších léčebných zařízení.
- Banky, pojišťovny a další finanční instituce, které jsou klíčové pro stabilitu finančního systému
- Poskytovatelé digitálních služeb (6).

Skupina poskytovatelů digitálních služeb zahrnuje firmy a organizace, které operují především v digitálním prostředí a nabízejí širokou škálu služeb, jako jsou:

- Cloudové služby a poskytování výpočetních zdrojů, úložiště a softwarových aplikací prostřednictvím internetu.
- Platformy, které umožňují kupujícím a prodávajícím setkávat se a obchodovat produkty nebo služby.
- Služby, které umožňují uživatelům vyhledávat informace na internetu.
- Provoz telekomunikací.

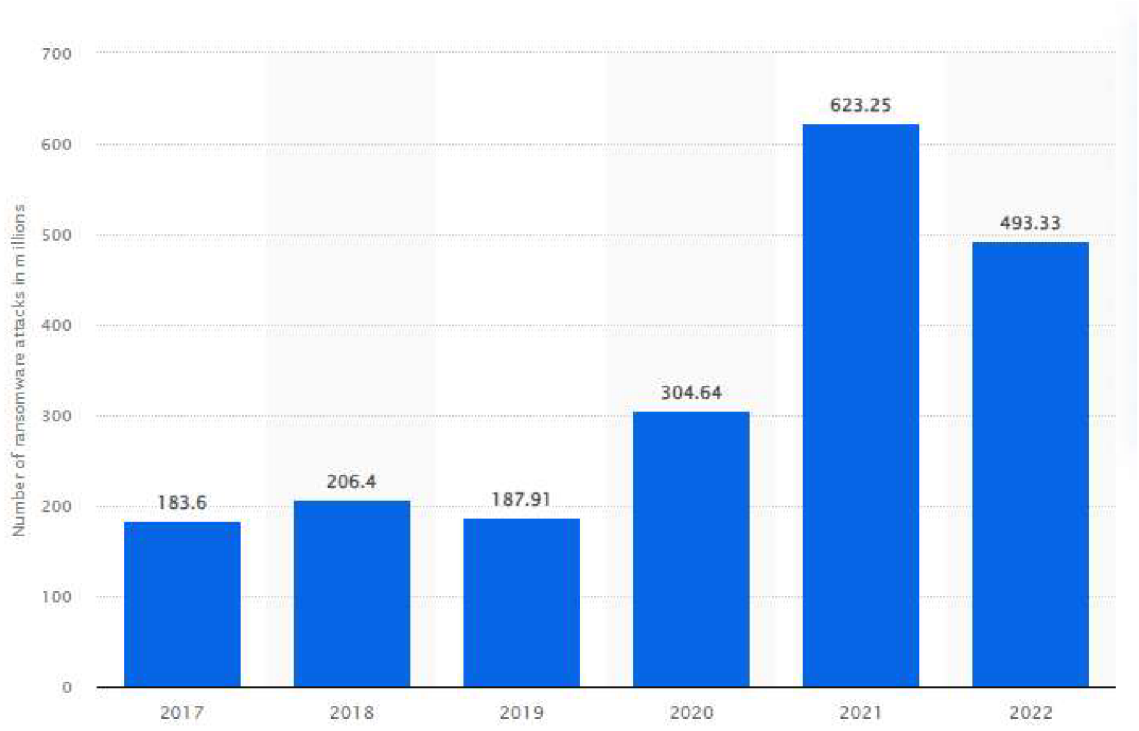
Nedodržení požadavků stanovených v české legislativě a GDPR má vážné důsledky pro organizace. Důsledky mohou představovat:

- GDPR umožňuje uložení pokut až do výše 20 milionů EUR nebo 4 % z celosvětového ročního obratu organizace, v závislosti na tom, která z hodnot je vyšší. Podobně ZKB stanovuje sankce za nedodržení bezpečnostních požadavků.
- Kromě finančních sankcí mohou organizace čelit právním sporům ze strany jednotlivců, jejichž práva byla porušena.
- Bezpečnostní incidenty a nedodržení regulačních požadavků mohou významně poškodit pověst organizace, což může mít dlouhodobý negativní dopad na její poslání a finanční zdraví. Incidenty spojené s kybernetickou bezpečností mohou následně vést k významným operacionálním narušením, včetně ztráty důvěrnosti, integrity a dostupnosti kritických systémů a dat (2).

4.2.4 Kybernetické hrozby a jejich dopad na organizace

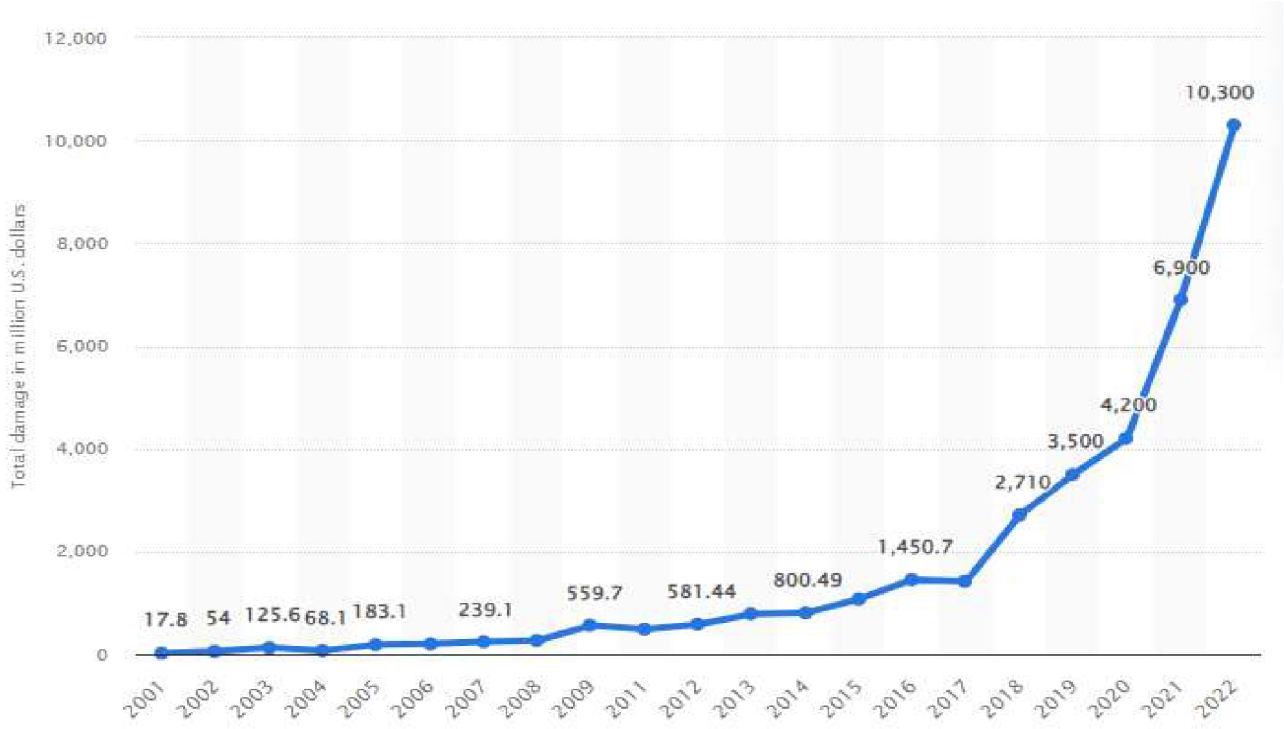
Vzhledem k rostoucímu počtu a komplexnosti kybernetických hrozeb je nutné, aby organizace přijaly komplexní a multidisciplinární přístup k řízení kybernetické bezpečnosti. To zahrnuje nejen technologická opatření, jako je zabezpečení sítí a informačních systémů, ale také školení zaměstnanců, vývoj bezpečnostních politik a procesů, spolupráci s externími partnery a orgány veřejné moci. Kybernetická odolnost se tak stává klíčovým prvkem strategického plánování a řízení rizik v organizacích, umožňující lépe čelit hrozbám a minimalizovat potenciální dopady na jejich operace a zájmy. Mezi nejrozšířenější hrozby se řadí malware, social engineering a jeho formy a insider threat.

Malware, zkratka pro "škodlivý software", je široká kategorie softwaru navrženého s úmyslem infiltrovat, poškodit nebo získat neautorizovaný přístup k informačním systémům. Jeho formy zahrnují viry, červy, trojské koně a ransomware (7). Viry se šíří vkládáním svých kopií do jiných programů nebo souborů, zatímco červi se mohou replikovat a šířit autonomně. Počet útoků formou malwaru se v posledních letech násobně zvedl a je tak čím dál rozšířenějším viz Obrázek 1 (8).



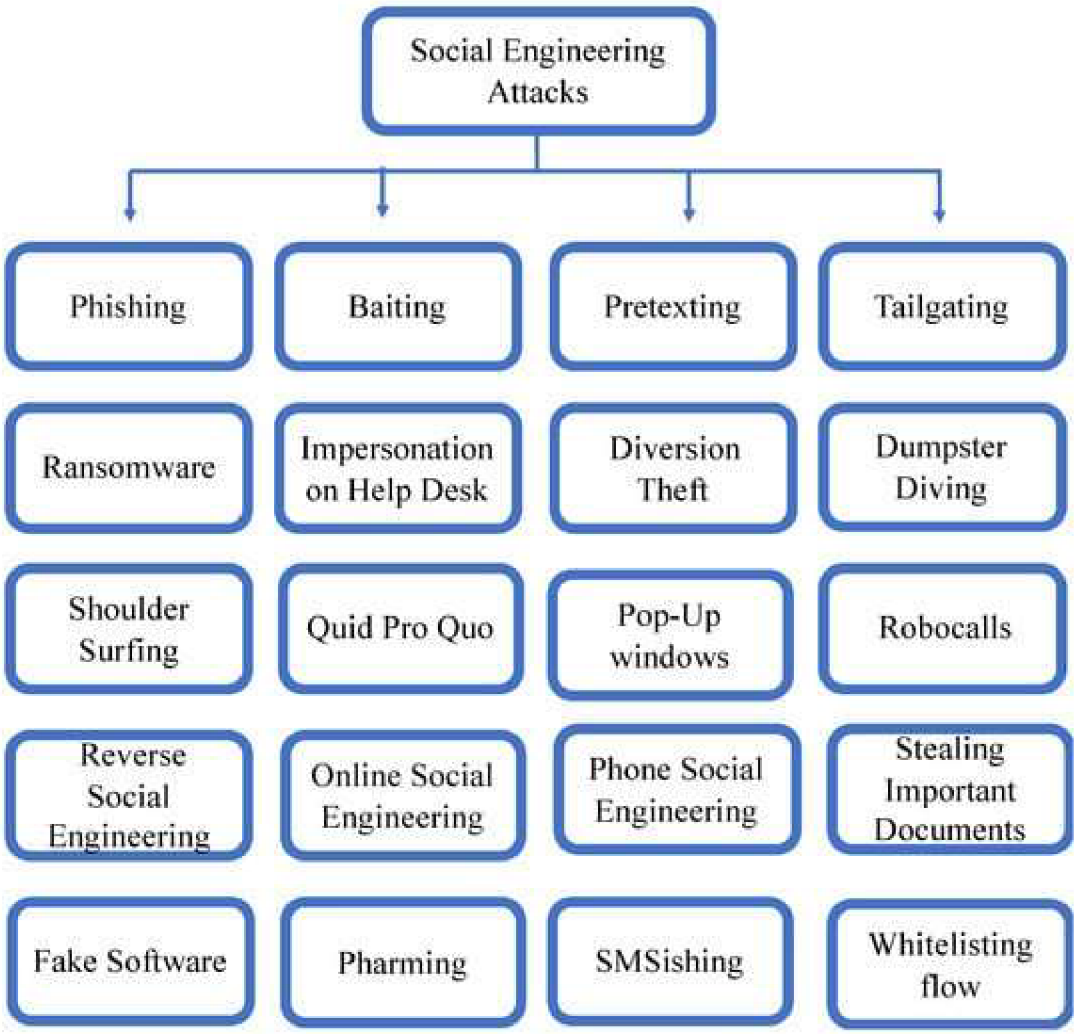
Obrázek 1 Počet pokusů o ransomwarový útok po celém světě 2017-2022 (8)

Malware může způsobit rozsáhlé škody včetně ztráty nebo krádeže citlivých dat, narušení operací a finančních ztrát pro organizace i jednotlivce (9). Malware může také zpomalit nebo úplně vyřadit podniky z provozu a vyžadují často značné náklady na obnovu dat a systémů viz Obrázek 2 (9). Malware rovněž podkopává důvěru uživatelů v digitální služby.



Obrázek 2 Vývoj finančních škod (v mil. USD) způsobený kyberzločinem (9)

Social engineering, neboli sociální inženýrství, je metoda, která využívá lidské faktory a psychologické manipulace k získání důvěrných informací, přístupu k systémům nebo k provádění neoprávněných akcí. Útočníci se často vydávají za důvěryhodné osoby nebo instituce a využívají přesvědčovací taktiky, jako je naléhavost nebo autorita, aby oběť přiměli k akci, která ohrožuje její bezpečnost. Sociální inženýrství představuje vážnou hrozbu pro individuální osoby i organizace, jelikož úspěšné útoky mohou vést k ztrátě citlivých informací, finančním ztrátám a narušení interních procesů. Důvěra mezi zaměstnanci v rámci obchodních vztahů může být vážně poškozena, což může mít dlouhodobé negativní dopady na organizační kulturu a pověst (10). Social engineering má širokou škálu forem viz Obrázek 3 (11).



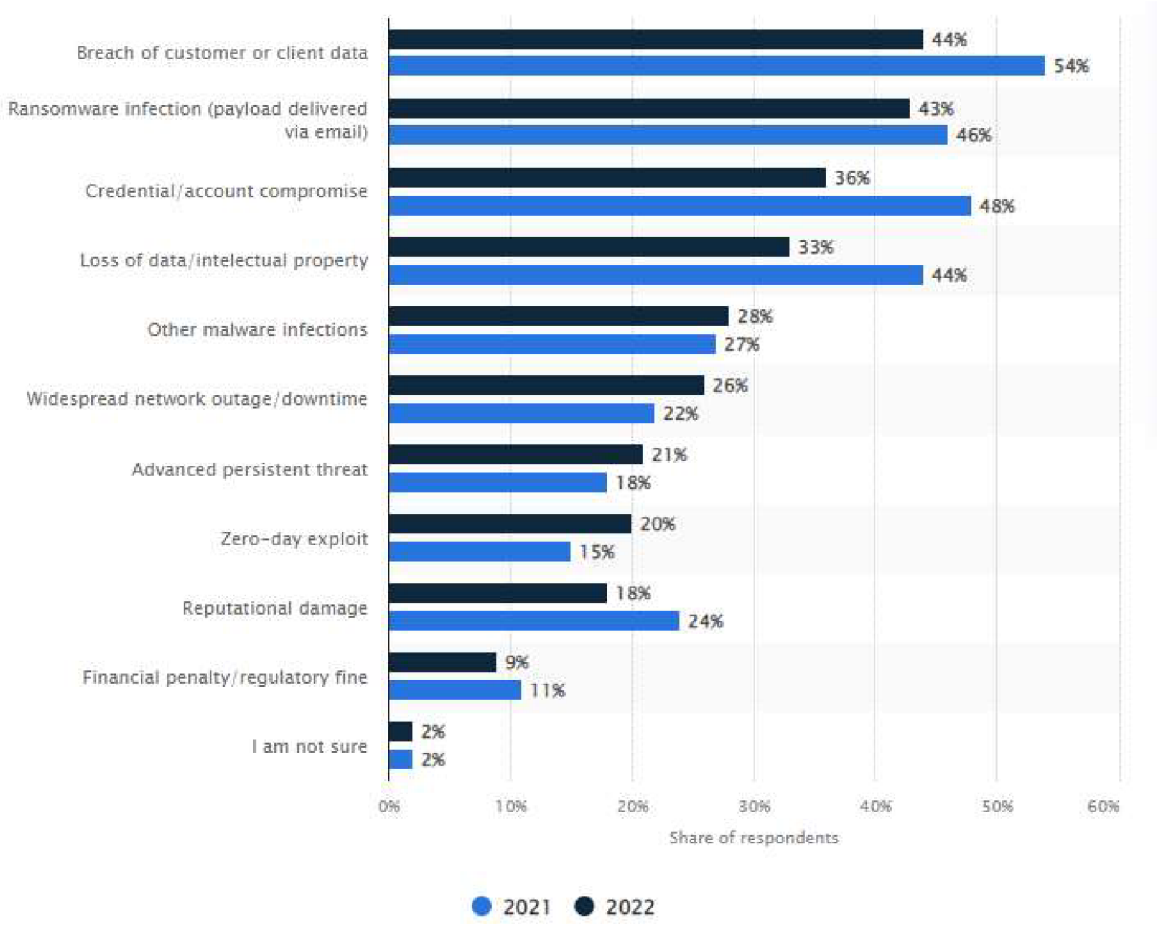
Obrázek 3 Formy social engineeringu (11)

Phishing je forma sociálního inženýrství, při které útočníci využívají podvodné e-maily, zprávy nebo webové stránky k získání citlivých informací, jako jsou přihlašovací údaje a finanční informace. Tato metoda často využívá naléhavé jazykové formulace nebo se vydává za důvěryhodné entity, jako jsou banky nebo známé společnosti, aby přesvědčila oběti k poskytnutí osobních informací. Phishing je díky své časové nenáročnosti pro hackera nejrozšířenějším druhem kybernetické hrozby viz Tabulka 1 (12).

Characteristic	2023	2022	2021	2020
Phishing/Smishing/BEC	438	461	537	383
Ransomware	246	276	357	158
Malware	118	70	141	104
Non-Secured Cloud Environment	14	9	24	50
Credential Stuffing	29	18	14	17
Unpatched Software Flaw	-	-	4	3
Zero Attack Day	110	8	4	1
Other	30	26	426	162
Not Specified	1,380	727	111	-
Total	2,365	1,595	1,613	878

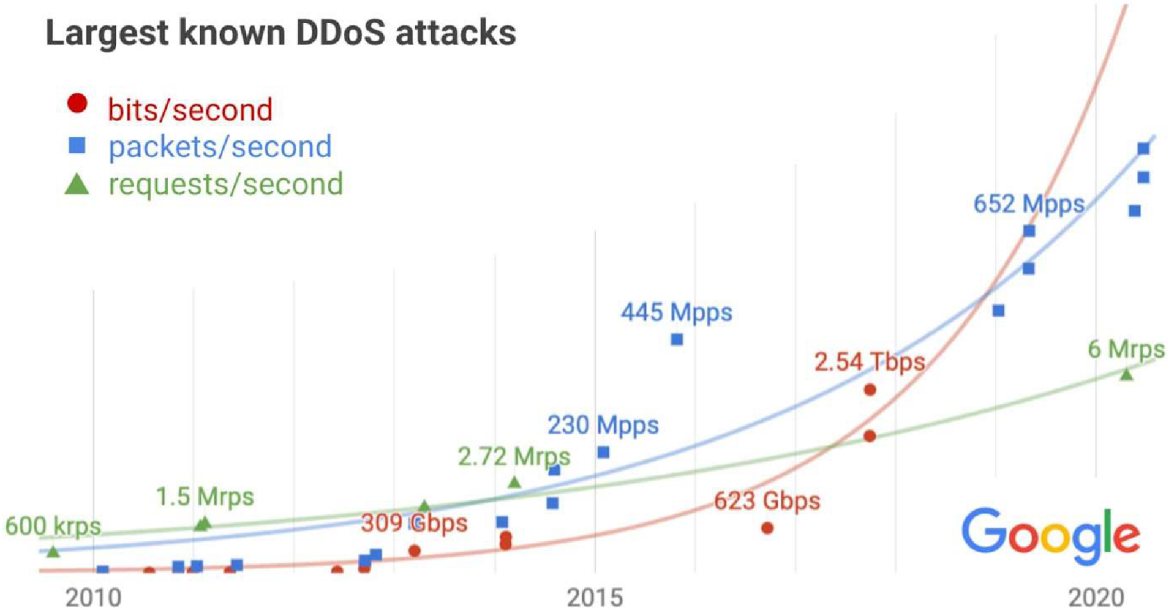
Tabulka 1 Kybernetické útoky vedoucí ke kompromitaci dat dle četnosti (USA 2020-2023) (12)

Phishingové útoky ohrožují osobní i finanční bezpečnost jednotlivců a mohou vést k významným finančním ztrátám, krádežím identity a narušení důvěry v digitální komunikaci. Pro organizace mohou mít útoky dopad na pověst značky, zákaznickou důvěru a mohou způsobit právní důsledky spojené s únikem dat (13).



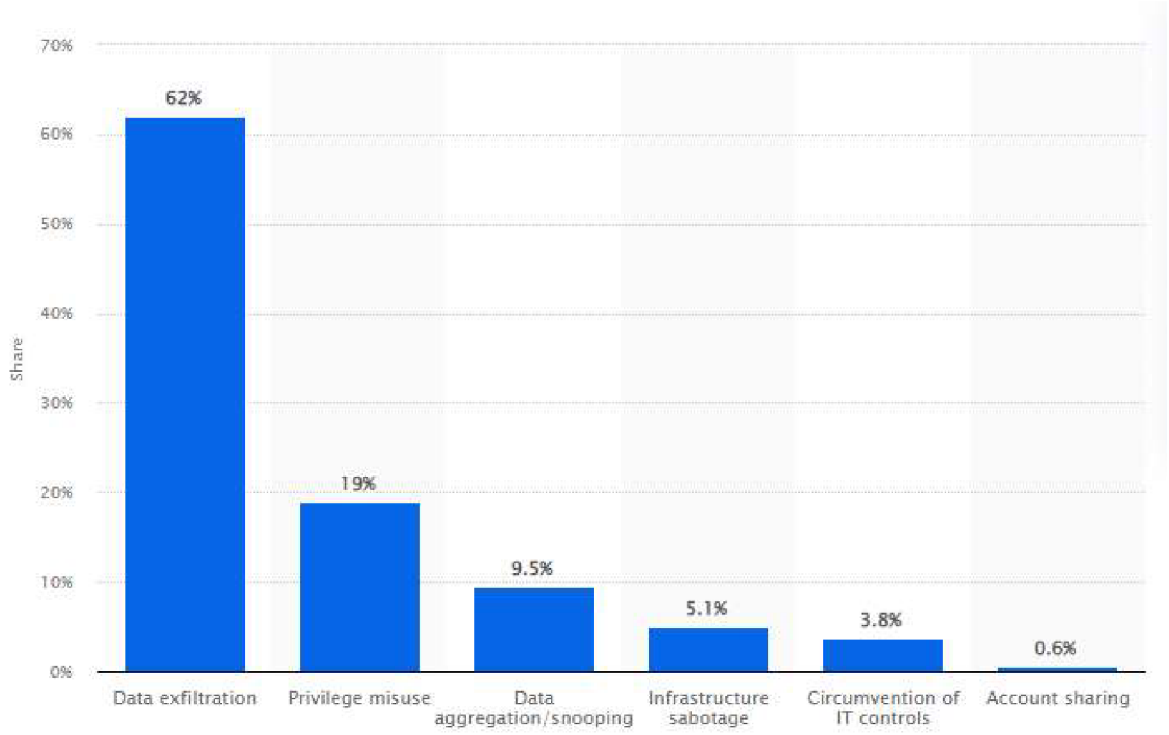
Obrázek 4 Důsledky úspěšných phising útoků na organizace, celosvětově 2021-2022 (13)

DDoS útoky představují přehlcení webového serveru, služby nebo infrastruktury obrovským množstvím požadavků, které přesahují její zpracovatelskou kapacitu. Tím je cílová služba zpomalena nebo úplně vyřazena z provozu. Útoky jsou často prováděny z rozsáhlých sítí kompromitovaných zařízení, známých jako botnety. Útoky pomocí botnetů v průběhu poslední dekády nabývají na své síle, kde největší z nich překročily hranici 2,54 Tbps viz Obrázek 5 (14). DDoS útoky mohou způsobit významné operacionální a finanční dopady na organizace tím, že znemožní přístup k webovým stránkám, online službám nebo kritické infrastruktuře. Pro spotřebitele to znamená přerušení služeb a ztrátu důvěry. Pro společnosti to může znamenat ztrátu příjmů, narušení operací a dlouhodobé poškození pověsti (15).



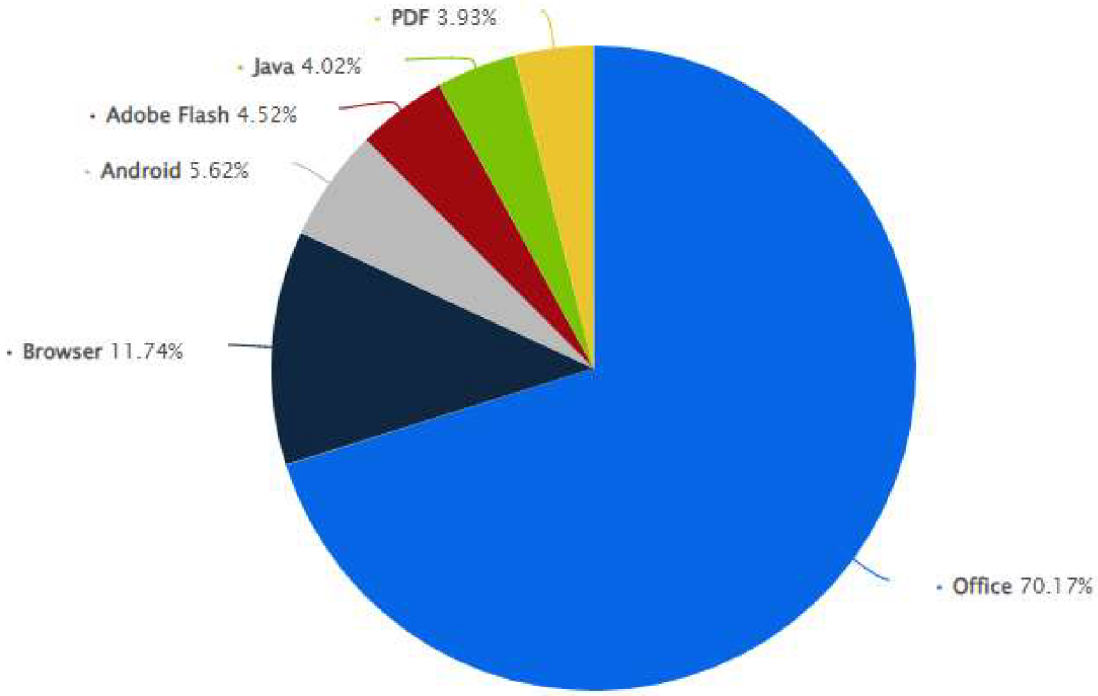
Obrázek 5 Největší známé DDoS útoky (14)

Vnitřní hrozby (insider threats) jsou hrozbou z řad jednotlivců uvnitř organizace, kteří mají legitimní přístup k jejím systémům a datům. Hrozby mohou být úmyslné, jako je krádež citlivých informací nebo sabotáž, nebo neúmyslné, v důsledku nedbalosti a nedostatečného pochopení bezpečnostních protokolů. Nicméně právě hrozby úmyslné jsou nejrozšířenější a patří mezi ně zejména exfiltrace dat, zneužití privilegií (role) a snooping viz Obrázek 6 (16). Vnitřní hrozby představují jedno z největších bezpečnostních rizik pro organizace, jelikož mohou vést k významným ztrátám dat, finančním ztrátám a poškození pověsti. Incidenty mohou také zapříčinit právní postihy spojené s porušením ochrany dat. Zabezpečení proti vnitřním hrozbám vyžaduje komplexní přístup zahrnující technická, organizační a personální opatření.



Obrázek 6 Nejčastější typy insider threats v USA v roce 2020 (16)

Exploit zranitelností jsou škodlivé kódy nebo techniky, které využívají slabiny v softwaru nebo v operačních systémech k získání neoprávněného přístupu, eskalaci privilegií nebo provádění škodlivých akcí. Zranitelnosti mohou být chyby v návrhu, implementaci nebo konfiguraci systémů a aplikací. Právě aplikace využívané k běžné administrativě bývají jedním nejčastějším zdrojem zranitelností, které hackeři využívají viz Obrázek 7 (17). Využití zranitelností může umožnit útočníkům získat kontrolu nad systémy, ukrást citlivá data nebo distribuovat malware. Dopad na organizace zahrnuje ztrátu dat, narušení služeb, finanční ztráty a potenciální právní následky za nedodržení standardů ochrany dat. Proaktivní zabezpečení, včetně pravidelných aktualizací a záplat, je zásadní pro ochranu před těmito hrozbami (18).



Obrázek 7 Aplikace s nejčastěji zneužitou zranitelností celosvětově 11.2021–9.2022 (18)

4.2.5 Důležitost bezpečnostní kultury

Bezpečnostní kultura odkazuje na soubor hodnot, přesvědčení, chování a postojů sdílených mezi členy organizace, které určují, jak je kybernetická bezpečnost vnímána a integrována do jejich každodenních pracovních rutin a rozhodovacích procesů. Efektivní bezpečnostní kultura nejenže podporuje dodržování bezpečnostních politik a procedur, ale také povzbuzuje proaktivní přístup k identifikaci a řešení bezpečnostních rizik.

Důsledek nedostatečného apelu na důležitost bezpečnostní kultury může mít za následek ztrátu dat či jinou kompromitaci informačních systémů organizace a s tím spojené komplikace. Význam správně nastavené a propagované bezpečnostní kultury pochází z datových úniků po celém světě, kde lidský faktor hraje roli ve 74 % známých datových úniků (19).

4.3 Norma ISO 27001

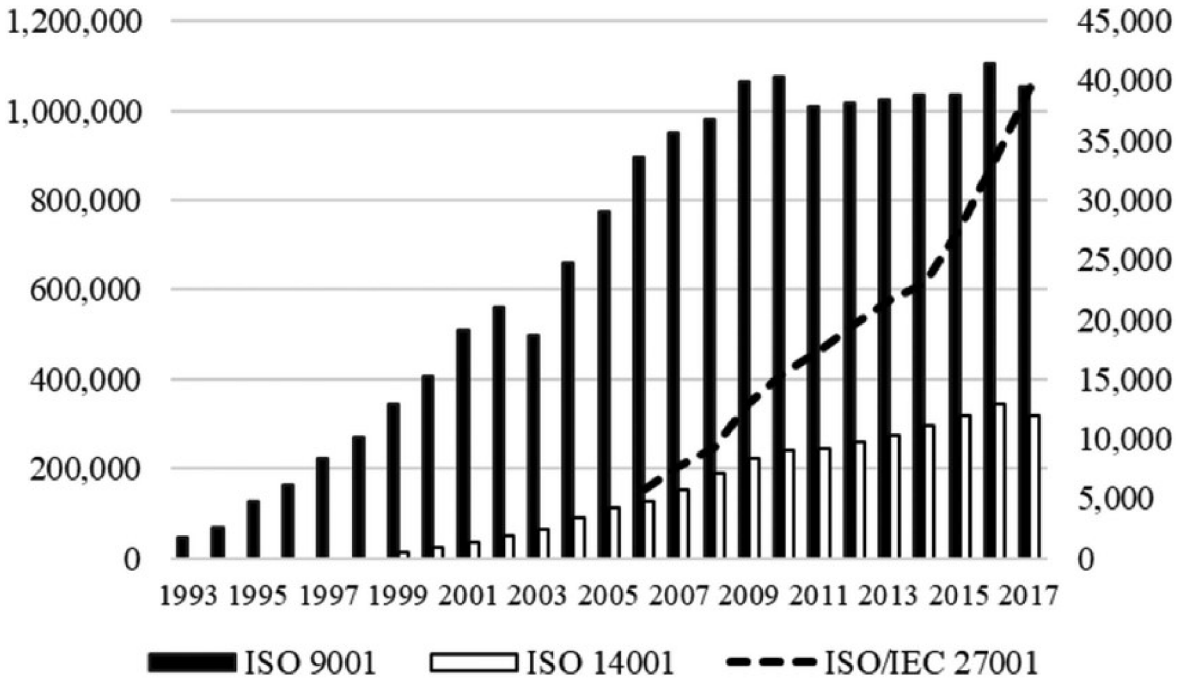
ISO 27001 je mezinárodní norma, která popisuje požadavky pro zavedení, implementaci, udržování a neustálé zlepšování ISMS v organizacích. Tato norma je součástí rodiny norem ISO/IEC 27000, které se zaměřují na různé aspekty bezpečnosti informací. ISO 27001 je

navržena tak, aby byla aplikovatelná na jakýkoliv typ organizace, bez ohledu na její velikost, odvětví nebo obrat.

4.3.1 Historie a vývoj normy ISO 27001

Historie normy ISO 27001 sahá do 90. let 20. století, kdy učiněn první krok ve Spojeném království s vydáním normy BS 7799 v roce 1995. Tento britský standard popsal metodu pro řízení informační bezpečnosti a zahrnoval některé z klíčových prvků, které se později staly součástí ISO 27001, včetně posouzení rizik a bezpečnostních kontrol (20).

Od svého zavedení v roce 2005 se ISO 27001 stalo globálně uznávaným, přičemž zájem o tuto certifikaci se exponenciálně zvyšuje viz Obrázek 8. Tento trend je poháněn narůstajícími hrozbami kybernetické bezpečnosti, regulatorními požadavky a rostoucí potřebou podniků chránit citlivé informace.



Obrázek 8 Evolution of ISO 9001, ISO 14001, and ISO/IEC 27001 (21)

4.3.2 Klíčové principy a cíle normy ISO 27001

Základy normy ISO 27001 spočívají v řadě principů a cílů, které jsou navrženy tak, aby zajistily bezpečné a spolehlivé informační prostředí v rámci organizace. Tato mezinárodně uznávaná norma stanovuje požadavky na systém ISMS, díky němuž mohou

organizace nejen efektivně chránit svá data, ale také flexibilně reagovat na dynamické hrozby a zároveň splňovat související právní a regulační požadavky jako např. GDPR (22).

Mezi základní principy normy ISO 27001 patří systematický přístup k řízení rizik, který podporuje organizace v identifikaci potenciálních hrozeb pro jejich informační systémy a stanovuje procesy pro jejich řízení a minimalizaci. Dále norma klade důraz na prevenci bezpečnostních incidentů a v případě jejich vzniku na minimalizaci jejich dopadů a rychlou obnovu. Klíčovým prvkem je také průběžné zlepšování ISMS, které zahrnuje neustálé monitorování a revize systému, aby bylo možné udržet krok s měnícím se prostředím a hrozbami. Závazek vedení a adaptibilita normy zajišťují, že implementace a udržování ISMS je účinné a přizpůsobené specifickým potřebám organizace bez ohledu na její velikost nebo obor.

Klíčové cíle, ke kterým norma ISO 27001 směřuje, zahrnují ochranu důvěrnosti, integrity a dostupnosti informací. To je realizováno prostřednictvím efektivního řízení rizik a implementace kontinuálních i ad-hoc kontrol. Norma rovněž usnadňuje organizacím dodržování právních a regulačních požadavků týkajících se bezpečnosti informací, čímž zlepšuje jejich bezpečnostní strukturu a zvyšuje schopnost identifikovat, předcházet, detekovat a reagovat na bezpečnostní hrozby a incidenty. Implementací a udržováním efektivního ISMS tak organizace zvyšují důvěru zákazníků, partnerů a dalších zúčastněných stran v jejich schopnost ochránit citlivé informace. Obecně tedy platí, že ISO norma 27001 umožňuje systematicky řídit bezpečnost svých informačních aktiv prostřednictvím logicky strukturovaných procesů. Tímto přístupem se organizace nejen chrání před bezpečnostními hrozbami zvenku i zevnitř, ale také demonstrují své odhodlání ke zvýšení bezpečnosti informací vůči všem zúčastněným stranám (1).

4.3.3 Struktura a hlavní oblasti normy ISO 27001

Struktura a hlavní oblasti normy zahrnují široké spektrum témat od obecných požadavků na ISMS, přes vedení, plánování, podporu, provoz, hodnocení výkonnosti, až po neustálé zlepšování, čímž poskytuje ucelený přístup k bezpečnosti informací (1).

Norma ISO 27001 stanovuje základní rámec pro ISMS, který začíná definicí rozsahu ISMS. Tento krok započíná určením hranic a aplikovatelnosti ISMS v rámci organizace, což je

základem pro efektivní řízení a ochranu informací. Dále je zásadním prvkem závazek vedení organizace k implementaci, udržování a neustálému zlepšování ISMS. To vyžaduje aktivní podporu, uvolnění financování a angažovanost na nejvyšší úrovni vedení, což je nezbytné pro úspěch jakéhokoli bezpečnostního programu. V rámci plánovací fáze ISMS jsou organizace povinny identifikovat rizika spojená s bezpečností informací a plánovat opatření k jejich řízení, což zahrnuje výběr vhodných bezpečnostních kontrol (1).

V oblasti vedení norma klade důraz na význam definování a dokumentace bezpečnostní politiky, která vyjadřuje závazky organizace k bezpečnosti informací a poskytuje rámec pro stanovení cílů bezpečnosti informací. Tato politika by měla být komunikována všem zaměstnancům a všem stranám spolupracující s organizací jejichž povaha se ISMS týká. Dále jsou stanoveny požadavky na definici rolí, odpovědností a pravomocí v rámci ISMS, což zahrnuje zajištění, že každý, kdo má vliv na bezpečnost informací, rozumí svým povinnostem (1).

V plánovací fázi ISO 27001 vyžaduje od organizací, aby provedly posouzení rizik a na jeho základě naplánovaly řízení těchto rizik. Tento proces zahrnuje identifikaci hrozeb a zranitelností, kterým jsou informace vystaveny, a určení opatření potřebných k minimalizaci nebo úplné eliminaci těchto rizik. Cíle bezpečnosti informací jsou stanoveny v souladu s bezpečnostní politikou a jsou základem pro měření úspěšnosti ISMS (1).

Podpora je nezbytná pro implementaci, udržování a zlepšování ISMS. To zahrnuje identifikaci a přidělení potřebných zdrojů, zvyšování povědomí mezi zaměstnanci a zlepšování jejich kompetencí v oblasti bezpečnosti informací. Důležitou součástí je také řízení dokumentovaných informací, které umožňuje organizaci uchovávat důkazy o dodržování bezpečnostních postupů a kontrol (1).

V oblasti provozu norma ISO 27001 zdůrazňuje význam implementace a kontroly plánů a procesů, které jsou v souladu s politikou a cíli bezpečnosti informací. To zahrnuje efektivní hodnocení a řízení bezpečnostních rizik, aby bylo zajištěno, že jsou správně identifikována a řešena (1). Pravidelné monitorování, měření, analýza a hodnocení účinnosti ISMS jsou zásadní pro zajištění jeho efektivity. Interní audity a pravidelné přezkoumávání vedením

poskytují mechanismy pro ověřování, že ISMS je v souladu s normou ISO 27001 a je efektivně implementován a udržován (1).

Identifikace neshod a implementace korektivních opatření jsou nezbytné pro odstranění příčin těchto neshod a prevenci jejich opakování. Norma vyžaduje zavedení opatření pro neustálé zlepšování efektivnosti ISMS, což umožňuje organizaci adaptovat se na měnící se prostředí a hrozby v oblasti bezpečnosti informací (1).

4.3.4 Proces certifikace normy ISO 27001

Proces získání certifikátu ISO 27001, který dokládá soulad organizace s touto mezinárodní normou pro ISMS, je strukturovaný a vyžaduje několik kroků. V počátku průběhu certifikace probíhá příprava, kde je prvním a základním krokem zavedení ISMS v souladu s požadavky ISO 27001. Tento krok obnáší rozsáhlou identifikaci rozsahu systému, posouzení rizik skrze Business Impact Analysis (BIA), implementaci nezbytných kontrolních opatření a zavedení procesů pro průběžné monitorování a zlepšování ISMS (23).

Následuje interní audit, který organizace provádí, aby si ověřila, zda její ISMS splňuje všechny požadavky normy a zda jsou všechny procesy efektivně implementované. Tento krok je klíčový pro odhalení případných nedostatků před podáním žádosti o certifikaci a pomáhá předejít finančním ztrátám spojeným s neúspěšnou certifikací. Poté organizace vybírá certifikační orgán, který je akreditován pro udělování certifikací ISO 27001. Výběr renomovaného a uznávaného certifikačního orgánu je kritický pro zajištění, že certifikace bude mít patřičnou hodnotu (23).

Certifikační audit se dělí na dvě fáze. V první fázi, známé jako "Readiness audit", certifikační orgán provádí předběžnou revizi dokumentace ISMS a posuzuje připravenost organizace na hlavní audit. Tato fáze může odhalit oblasti potřebné pro zlepšení. Po úspěšném absolvování této fáze následuje hloubkový audit, během kterého se ověřuje, že ISMS je efektivně implementován a funguje v praxi v souladu s požadavky normy. Pokud organizace úspěšně projde oběma fázemi auditu a certifikační orgán je přesvědčen o souladu s normou, je organizaci udělen certifikát ISO 27001. Tento certifikát je typicky platný po dobu tří let (23).

Během platnosti certifikátu musí organizace podstoupit pravidelné dohledové audity, které zajišťují pokračující soulad s ISO 27001. Před koncem tříletého cyklu je nutné provést proces recertifikace, aby byla obnovena platnost certifikátu. Tato metodologie zajišťuje, že organizace nejenže získá certifikát ISO 27001, ale také udržuje a neustále zlepšuje svůj systém managementu bezpečnosti informací, což zvyšuje důvěru zákazníků, partnerů a dalších zainteresovaných stran ve schopnost organizace chránit citlivé informace (23).

Proces certifikace ISO 27001 je značně komplexní, vyžaduje pečlivou přípravu a závazek k neustálému zlepšování. Certifikace je cenným uznáním, že organizace má efektivní ISMS, což může významně zvýšit důvěru zákazníků, partnerů a dalších zainteresovaných stran (23).

4.3.5 Přínosy normy ISO 27001

Přínosy normy ISO 27001 pro organizace jsou rozsáhlé a mají zásadní význam pro celkovou strukturu a bezpečnostní postavení podniků v dnešním digitálně orientovaném světě. Tato mezinárodně uznávaná norma přináší komplexní rámec pro zajištění ochrany a bezpečnosti informačních aktiv, který je základem pro budování spolehlivého a bezpečného informačního prostředí. Jedním z klíčových přínosů normy ISO 27001 je posílení ochrany citlivých dat prostřednictvím systematického řízení bezpečnostních rizik. Tento proces umožňuje organizacím efektivně identifikovat, hodnotit a minimalizovat hrozby vůči svým informačním systémům, čímž vede k lepší prevenci bezpečnostních incidentů a minimalizaci potenciálních škod. Tato systematická práce s riziky a kontrolami zvyšuje celkovou bezpečnost informací a zlepšuje schopnost organizace chránit svá data před vnějšími i vnitřními hrozbami (24).

Dalším významným aspektem je, že ISO 27001 napomáhá organizacím v dodržování právních a regulačních požadavků týkajících se ochrany dat. Norma poskytuje jasný rámec pro zavedení postupů a kontrolních opatření, které jsou nezbytné pro splnění právních předpisů, jako je například GDPR. Tím snižuje riziko právních sankcí a pokut, které mohou vyplynout z nedostatečné ochrany dat a zvyšuje právní a regulační soulad organizace.

ISO 27001 rovněž zvyšuje důvěru zákazníků a zlepšuje vztahy s obchodními partnery. Certifikace dle této normy signalizuje závazek organizace k ochraně informací, což je klíčové pro udržení a rozvoj obchodních vztahů. Toto vnímání zodpovědnosti a spolehlivosti může být rozhodujícím faktorem pro zákazníky a partnery při výběru mezi různými dodavateli nebo službami. Norma ISO 27001 přináší konkurenční výhodu v prostředí, kde jsou bezpečnost a ochrana dat stále důležitější. Certifikace může být významným diferenciátorem, který organizaci odlišuje od konkurence a otevírá nové obchodní příležitosti, zvláště v mezinárodním kontextu, kde je kladen důraz na bezpečnost informací stále více (25).

ISO 27001 taktéž podporuje revizi a optimalizaci procesů týkajících se řízení informací, což vede ke zvýšení efektivity a snížení nákladů spojených s informační bezpečností. Kontinuální zlepšování a adaptace na nové hrozby a změny v technologii a regulačním prostředí jsou základem pro udržení účinnosti a relevance bezpečnostních opatření. Celkově norma ISO 27001 poskytuje organizacím rámec pro budování silného ISMS, což je klíčové pro ochranu jejich informačních aktiv a udržení konkurenceschopnosti v dnešním rychle se měnícím a digitalizovaném světě (26).

4.4 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., který byl přijat v České republice roku 2014, představuje důležitý krok k posílení národní kybernetické bezpečnosti a ochrany kritické infrastruktury proti rostoucímu počtu kybernetických hrozbě. Tato část legislativy stanovuje rámec povinností, práv a opatření pro státní instituce, provozovatele základních služeb a poskytovatele digitálních služeb, za cílem zvýšení odolnosti a reakční schopnosti vůči hrozbám, které by mohly narušit bezpečnost informačních a komunikačních technologií.

4.4.1 Přehled a důležité aspekty zákona

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., představuje klíčový legislativní kámen v základech kybernetické bezpečnosti České republiky, zdůrazňující jeho nezbytnost pro ochranu digitálního prostředí v současném digitálně propojeném světě. Tento zákon klade na zmíněné subjekty značné požadavky, aby aktivně přispívaly k celkové kybernetické

odolnosti a efektivně reagovaly na incidenty, které by mohly ohrozit nejen jejich vlastní operace, ale i širší veřejnost. V rámci těchto požadavků zákon detailně specifikuje odpovědnosti a povinnosti těchto subjektů, zahrnující nejen pravidelné hodnocení rizik a implementaci přiměřených bezpečnostních opatření, ale také povinnost hlásit významné kybernetické incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Toto vše tvoří základ pro efektivní ochranu před narůstajícími kybernetickými hrozbami. NÚKIB zaujímá v tomto rámci centrální pozici, neboť se mu dostává odpovědnosti za koordinaci a dohled nad implementací tohoto zákona. Jeho úloha zahrnuje vydávání metodických pokynů, provádění kontrol a reakci na incidenty, což je zásadní pro udržení celostátní kybernetické bezpečnosti a podporu synergické spolupráce mezi veřejným a soukromým sektorem (6).

Důležitým prvkem zákona je také důraz na mezinárodní spolupráci, která umožňuje České republice a jejím subjektům sdílet klíčové informace o hrozbách, koordinovat reakce na incidenty a společně pracovat na podpoře a rozvoji bezpečnostních standardů na mezinárodní úrovni. Tato spolupráce je nezbytná v globálním kontextu kybernetické bezpečnosti, kde hrozby a útoky neznají hranice. Zákon dále stanovuje, že subjekty, které své povinnosti zanedbávají, čelí důsledkům v podobě sankcí, včetně finančních pokut. Tyto sankce podtrhují serióznost a důležitost dodržování stanovených pravidel a povinností, zdůrazňujíce význam zákonu pro udržení robustního a bezpečného kybernetického prostředí. Aspekty společně formují základní kameny, na kterých stojí česká legislativa v oblasti kybernetické bezpečnosti, a jsou klíčové pro její efektivní implementaci a dodržování, čímž chrání jak jednotlivé subjekty, tak celou společnost před kybernetickými hrozbami a útoky (6).

4.4.2 Vztah zákona k procesům ve firmě a jeho požadavky

Vztah zákona o kybernetické bezpečnosti k interním procesům ve firmách tvoří komplexní soubor povinností, jehož cílem je posílit odolnost podniků vůči kybernetickým útokům a zabezpečit ochranu jejich kritických informačních aktiv. Pro splnění požadavků zákona je nezbytné, aby se zapojily všechny úrovně organizace a bylo zajištěno bezpečné a důvěryhodné provozní prostředí, které je klíčové pro udržení kontinuity podnikání a ochranu dat. Jedním z klíčových aspektů je nutnost, aby firmy implementovaly vhodná

technická a organizační opatření, která by chránila jejich sítě, informační systémy a data před kybernetickými hrozbami. Tento požadavek zahrnuje revizi a aktualizaci existujících bezpečnostních politik a kontrol, a to s cílem zajistit, že opatření společnosti jsou v souladu s aktuálními nejlepšími praxemi a standardy v oblasti kybernetické bezpečnosti. Zákon dále klade důraz na systematické posouzení rizik, což firmám umožňuje identifikovat potenciální kybernetické hrozby a zranitelnosti ve svých systémech. Na základě tohoto posouzení jsou organizace povinny plánovat a implementovat opatření na řízení těchto rizik, což může zahrnovat širokou škálu řešení od technických zabezpečení až po organizační změny a vzdělávání zaměstnanců (6).

Dalším zásadním prvkem zákona je požadavek na hlášení kybernetických incidentů příslušným úřadům, především NÚKIB. Tento předpis vyžaduje, aby firmy měly zavedené efektivní procesy pro detekci, hodnocení a hlášení bezpečnostních incidentů, což předpokládá přípravu a školení zaměstnanců pro správnou reakci v případě bezpečnostních incidentů (6).

Zajištění osvěty a školení zaměstnanců je neoddělitelnou součástí plnění požadavků zákona o kybernetické bezpečnosti. Firmy jsou povinny informovat a vzdělávat svůj personál o kybernetických hrozbách a opatřeních, která mají předejít bezpečnostním incidentům nebo na ně adekvátně reagovat. V neposlední řadě, zákon vyžaduje udržování adekvátní dokumentace a záznamů souvisejících s implementací systému řízení bezpečnosti informací, posouzením rizik, přijatými bezpečnostními opatřeními a hlášenými incidenty. Tato dokumentace slouží jako důkaz o dodržování legislativních požadavků a je nezbytná pro účely revizí a auditů. Celkově představuje zákon o kybernetické bezpečnosti zásadní rámec pro podniky, který jim pomáhá chránit se před rostoucími kybernetickými hrozbami a zároveň dodržovat regulační požadavky v této klíčové oblasti (6).

4.4.3 Role vyžadované zákonem o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., spolu s doprovodnými metodickými materiály, stanovuje rozsáhlý rámec rolí a odpovědností, které jsou fundamentální pro zajištění kybernetické bezpečnosti v rámci jakékoli organizace. Tento právní předpis

představuje komplexní přístup k ochraně informačních systémů a dat, který se stává nezbytným v dnešní digitálně propojené době. V rámci tohoto zákona je kladen důraz na důležitost systematického řízení informační bezpečnosti, které zahrnuje identifikaci potenciálních hrozeb, hodnocení rizik a implementaci nezbytných opatření k minimalizaci těchto rizik.

V této souvislosti zaujímá první zásadní pozici role **Chief Information Security Officer (CISO)**, která je zodpovědná za vytváření, implementaci a dohled nad strategií bezpečnosti informací v organizaci. Tato role se vyvinula jako nezbytná odpověď na stále se rozvíjející a sofistikovanější kybernetické hrozby, s cílem zajistit ochranu citlivých informací a systémů (27). CISO hraje klíčovou roli v procesu identifikace rizik, hodnocení jejich dopadu na organizaci a vývoje strategií pro jejich řízení. Kromě toho CISO zajišťuje, že organizace splňuje všechny relevantní právní a regulační požadavky, včetně těch, které jsou stanoveny v zákoně o kybernetické bezpečnosti, a koordinuje reakce na incidenty s cílem minimalizovat jejich dopad na operace organizace a zachovat důvěru zainteresovaných stran (6).

Ačkoli zákon o kybernetické bezpečnosti přímo nevyžaduje jmenování osoby na pozici CISO, je z něj patrný požadavek, aby organizace disponovaly efektivním systémem managementu bezpečnosti informací. Tento systém musí být strukturován tak, aby zahrnoval určení odpovědných osob za kybernetickou bezpečnost, které budou schopné řídit komplexní spektrum hrozeb a rizik souvisejících s kybernetickou bezpečností. Tímto způsobem zákon klade důraz na potřebu systematického přístupu k bezpečnosti informací, který je základním kamenem pro ochranu organizací v kyberprostoru. Implementace těchto povinností a zajištění souladu s požadavky zákona o kybernetické bezpečnosti vyžaduje komplexní a multidisciplinární přístup, který zahrnuje nejen technologická opatření, ale i organizační změny, procesní inovace a kulturu neustálého zlepšování. Role CISO, spolu s podporou a zapojením všech úrovní vedení a zaměstnanců, je proto klíčová pro vytvoření robustního a adaptabilního systému, který je schopen čelit současným i budoucím výzvám v oblasti kybernetické bezpečnosti (6).

Další je role **IT bezpečnostního architekta**, která představuje klíčovou složku v rámci systému managementu bezpečnosti informací organizace, neboť zajišťuje, že všechny informační systémy jsou navrhovány, implementovány a provozovány s maximálním ohledem na bezpečnost. Tato pozice vyžaduje hluboké porozumění technologickým, organizačním a procesním aspektům kybernetické bezpečnosti, jakož i schopnost strategicky plánovat a efektivně komunikovat s ostatními odděleními organizace (6).

Jedním z primárních úkolů IT bezpečnostního architekta je vývoj a implementace bezpečnostní architektury, která pokrývá jak fyzické, tak technologické a organizační aspekty bezpečnosti. V rámci tohoto procesu architekt identifikuje potenciální bezpečnostní rizika a navrhuje architektonická řešení, která tato rizika minimalizují prostřednictvím adekvátních bezpečnostních kontrol a mechanismů. Současně zajišťuje, že všechny navrhované a implementované systémy jsou v souladu s platnými bezpečnostními standardy a legislativními požadavky, což je zásadní pro udržení celkové bezpečnosti a dodržování regulačních a právních rámců (6).

Dalším kritickým aspektem práce IT bezpečnostního architekta je integrace bezpečnostních principů do celého životního cyklu informačních systémů, od fáze návrhu přes vývoj až po nasazení a provoz. Tato integrace vyžaduje úzkou spolupráci s vývojovými týmy, síťovými inženýry a dalšími specialisty v IT sektoru, aby bylo zajištěno, že bezpečnostní aspekty jsou zohledněny na každém kroku. K tomu patří vytváření a implementace bezpečnostních politik, procedur a standardů, které určují, jakým způsobem mají být data a systémy chráněny. Kromě návrhu a implementace bezpečnostní architektury IT bezpečnostní architekt pravidelně hodnotí stávající bezpečnostní opatření a infrastrukturu, aby identifikoval oblasti vyžadující zlepšení. Tato evaluace zahrnuje provádění bezpečnostních auditů, penetračních testů a analýz zranitelností, které odhalují slabá místa v systémech a pomáhají navrhovat řešení pro jejich odstranění. Rovněž je zodpovědný za aktualizaci bezpečnostních strategií a architektur v reakci na nově objevené hrozby a technologické změny v IT odvětví (6).

V konečném důsledku role IT bezpečnostního architekta představuje nezbytný prvek pro zajištění, že organizace může efektivně čelit kybernetickým hrozbám a chránit své

informační aktiva. Tato role vyžaduje nejen technické dovednosti a strategické myšlení, ale také schopnost adaptace na neustále se měnící bezpečnostní prostředí a vývoj technologií.

Poslední rolí je role **interního auditora v oblasti IT** a kybernetické bezpečnosti, která představuje nezastupitelný prvek v rámci systému řízení rizik organizace. Tato pozice je zásadní pro zajištění, že organizace nejenže efektivně spravuje svá rizika, ale také plně dodržuje veškeré relevantní právní a regulační požadavky, jakož i interně stanovené politiky a procedury. Interní auditor provádí nezávislé a objektivní hodnocení IT procesů, systémů a operací s cílem identifikovat potenciální oblasti pro zlepšení a doporučit opatření, která povedou ke zvýšení efektivity a posílení bezpečnostních postupů. Hodnocení kontrol a postupů je klíčovou součástí práce interního auditora, který systematicky prozkoumává efektivitu vnitřních kontrolních mechanismů a postupů v oblasti IT bezpečnosti. Klíčovým aspektem je kontrola, zda jsou bezpečnostní politiky a procedury adekvátně dokumentovány, zda jsou pravidelně revidovány a aktualizovány a zda jsou v praxi účinně implementovány a dodržovány. Interní auditor ověřuje soulad s mezinárodními standardy a normami, jako je ISO 27001, a dalšími relevantními bezpečnostními rámci, čímž zajišťuje, že organizace přijímá a udržuje nejvyšší možné standardy v oblasti kybernetické bezpečnosti (6).

Další zásadní činností interního auditora je identifikace a hodnocení rizik a zranitelností v IT infrastruktuře a systémech organizace. Auditor analyzuje potenciální hrozby pro informační aktiva a hodnotí schopnost organizace tyto hrozby adekvátně řešit. Součástí této práce je také posouzení, zda jsou plány kontinuity provozu a reakce na incidenty dostatečně robustní a zda jsou k dispozici účinné mechanismy pro jejich aktivaci v případě potřeby (6).

Zajištění compliance, tedy dodržování všech aplikovatelných právních a regulačních požadavků, je další klíčovou oblastí, ve které interní auditor působí. Toto zahrnuje revizi souladu s předpisy týkajícími se ochrany osobních údajů, jako je GDPR, a dalšími specifickými regulacemi relevantními pro IT a kybernetickou bezpečnost. Auditor hodnotí, jak efektivně organizace řídí své právní a regulační závazky a zda jsou přijímána adekvátní opatření pro minimalizaci souvisejících rizik. Na základě zjištěných informací interní auditor připravuje zprávy pro vedení organizace, které obsahují podrobný přehled identifikovaných

nedostatků, potenciálních rizik a konkrétních doporučení pro zlepšení. Tato doporučení mohou zahrnovat návrhy na zlepšení vnitřních kontrol, zavedení nových bezpečnostních politik a postupů, změny ve stávajících procesech nebo technologická vylepšení, která by posílila obranyschopnost organizace proti kybernetickým hrozbám (6).

Interní auditor musí rovněž udržovat své odborné znalosti aktuální prostřednictvím pravidelného školení a profesního rozvoje. To je nezbytné pro udržení přehledu o nejnovějších trendech v kybernetické bezpečnosti, nově objevených hrozbách a osvědčených metodách ochrany. Tímto způsobem interní auditor přispívá k neustálému zlepšování bezpečnostního postoje organizace a zajišťuje, že její informační systémy a procesy jsou chráněny proti stále se měnícím výzvám kyberprostoru.

5 Vlastní řešení; výsledky a diskuse

V rámci zpracování vlastního řešení autor práce provedl analýzu organizace, analýzu současného stavu bezpečnosti informací uvnitř organizace, nastavil cíle implementace, navrhnul změny vedoucí ke zlepšení tohoto stavu, identifikoval rizika a navrhl řešení minimalizující tyto rizika. Blíže jsou kroky popsány v následujících kapitolách.

5.1 Představení firmy

Z důvodu anonymizace je organizace prezentována pouze jako přední poskytovatel telekomunikačních služeb v České republice, hrající klíčovou roli v sektoru kritické informační infrastruktury (KII). Organizace tak spadá pod zákon o kybernetické bezpečnosti č. 181/2014 Sb., což znamená, že musí splňovat vysoké standardy kybernetické ochrany a bezpečnosti informací tak, aby zajistila nepřetržitou dostupnost, integritu a důvěrnost svých služeb a dat. Organizace zaměstnává zhruba 5000 zaměstnanců z čehož téměř polovina pracuje pro firmu skrze externí subjekty.

5.1.1 Cíle implementace

Implementace ISO 27001 a ISMS v kontextu přijímání externistů v organizaci má za cíl zajistit vyšší úroveň bezpečnosti informací a ochrany dat v průběhu všech interakcí s externími poskytovateli a konzultanty, kteří představují značnou část všech zaměstnanců firmy. Tento proces je tedy pro organizaci zcela klíčový k udržení správného chodu organizace a jejích cílů.

5.1.2 Organizační struktura

Zákon o kybernetické bezpečnosti č. 181/2014 Sb. ve svém znění a doprovodných metodických materiálech definuje různé role a odpovědnosti, které jsou klíčové pro zajištění kybernetické bezpečnosti v rámci organizací viz kapitola 4.4.3. V organizaci jsou taktéž zavedené role, které úsilí vyvíjené zákonem popsaných rolí podporují a řídí implementaci jejich požadavků do organizace a jejích informačních aktiv viz Příloha 2 (6).

Role **byznys kontinuity manažera (BCM)** je v moderních organizacích nezastupitelná, jelikož představuje základní kámen pro zajištění nepřetržitosti a odolnosti podnikových operací vůči nepředvídatelným událostem a krizím. Tato pozice vyžaduje hluboké

porozumění kritickým byznysovým procesům, identifikaci potenciálních rizik a hrozeb pro operace a vývoj efektivních strategií a plánů pro minimalizaci dopadů případných přerušení. Byznys kontinuity manažer hraje klíčovou roli v přípravě a implementaci komplexních plánů kontinuity činnosti, které umožňují organizaci rychle se zotavit a obnovit normální operace po narušení její činnosti způsobeném různými vnějšími i vnitřními faktory.

Úkolem BCM je nejen identifikovat kritické byznysové procesy, které jsou nezbytné pro pokračování v operacích, ale také analyzovat a hodnotit potenciální rizika a hrozby, které by mohly tyto procesy narušit. To zahrnuje široké spektrum potenciálních událostí, od přírodních katastrof a technologických selhání po kybernetické útoky a další krizové situace. Na základě této analýzy BCM vyvíjí plány kontinuity činnosti a strategie pro obnovu, které jsou specificky navrženy tak, aby minimalizovaly dopady jakýchkoli přerušení a zajistily rychlou obnovu kritických funkcí a služeb. Důležitou součástí role BCM je také komunikace a spolupráce s různými odděleními a týmy v rámci organizace. Byznys kontinuity manažer musí zajišťovat, že všechny relevantní strany jsou plně informovány o plánech kontinuity činnosti a že existují jasné postupy pro jejich aktivaci v případě krize. To zahrnuje pravidelné školení zaměstnanců, cvičení a simulace krizových scénářů, které testují připravenost organizace a identifikují oblasti, kde je potřeba dalšího zlepšení. Kromě toho BCM hraje klíčovou roli v nepřetržitém monitorování a revizi plánů kontinuity činnosti, aby zajistil jejich aktuálnost a efektivitu v reakci na měnící se podnikové prostředí a nově identifikované hrozby. To zahrnuje pravidelné hodnocení a aktualizaci plánů, stejně jako adaptaci strategií na základě zpětné vazby z cvičení a reálných incidentů. Ve výsledku role byznys kontinuity manažera představuje zásadní součást strategie organizace pro řízení rizik a zajištění odolnosti. Efektivní plánování a řízení kontinuity činností umožňuje organizaci minimalizovat potenciální dopady nepředvídaných událostí na její operace a zajistit rychlou obnovu, což je klíčové pro zachování důvěry stakeholderů a dlouhodobé udržitelnosti podnikání.

Role **týmu pro reakci na kybernetické incidenty (CSIRT)** je nepostradatelná pro zajištění kybernetické odolnosti jakékoliv organizace. Jako zásadní prvek v rámci strategie kybernetické bezpečnosti poskytuje CSIRT kritickou první linii obrany proti bezpečnostním incidentům, zajišťující, že organizace může rychle a efektivně reagovat na hrozby,

čímž minimalizuje potenciální negativní dopady na její operace a reputaci. Úloha CSIRT zahrnuje široké spektrum činností od předběžného hodnocení incidentů až po koordinaci reakce v reálném čase a analýzu po incidentu.

Jednou z klíčových odpovědností CSIRT je reagovat na oznámení o kybernetických bezpečnostních incidentech. Tento proces zahrnuje okamžité shromáždění týmu po obdržení oznámení a provádění rychlého a důkladného posouzení situace, aby byly identifikovány příčiny, zdroje, povaha a rozsah škody způsobené incidentem. Na základě tohoto předběžného hodnocení tým doporučuje a implementuje nejvhodnější reakční strategie, což může zahrnovat izolaci postižených částí sítě, okamžité zabezpečení systémů nebo koordinaci s externími odborníky a zúčastněnými stranami pro zajištění komplexní ochrany. Po každém incidentu je nezbytné provést důkladnou analýzu události, identifikovat příčiny a vyvodit důležitá ponaučení, která mohou pomoci zlepšit budoucí preventivní strategie a reakce na podobné incidenty. CSIRT zodpovídá za pečlivou dokumentaci každého incidentu, včetně podrobné analýzy a doporučení pro zlepšení. Tato analýza a zpětná vazba jsou zásadní pro kontinuální zlepšování procesů kybernetické bezpečnosti organizace, což umožňuje adaptaci na měnící se kybernetické hrozby a posílení celkové odolnosti proti budoucím incidentům.

Dalším zásadním prvkem role CSIRT je udržení důvěrnosti a zabezpečení citlivých informací během a po reakci na incident. Tým pracuje v úzké spolupráci s různými odděleními a odborníky, rozšiřující své řady o další členy podle potřeby, přičemž klade důraz na princip "potřeby vědět" pro ochranu citlivých dat. Zajištění pravidelné a přesné komunikace s vedením organizace je rovněž klíčové pro efektivní řízení incidentů a udržení důvěry zainteresovaných stran. Význam CSIRT v moderním kyberprostoru je nesporný a jeho role jakožto zásadního prvku v obranné strategii organizace proti kybernetickým hrozbám představuje klíčový prvek pro zajištění kontinuity podnikání a ochrany kritických informačních aktiv. Tím CSIRT přispívá k udržení důvěry zákazníků a obchodních partnerů a chrání organizaci před potenciálními škodami na její reputaci a operacích.

Manažer IT governance hraje nezastupitelnou úlohu ve vytváření propojení mezi technologickými postupy a širšími cíli podniku v oblastech obchodu a bezpečnosti. Jeho

činnost pokrývá širokou paletu úkolů sahající od správy databází po návrh a implementaci bezpečnostních architektur, přičemž klade základ pro to, aby IT operace nejen podporovaly strategické směřování organizace, ale zároveň splňovaly soubor právních, regulačních a interních standardů. Jeho práce spočívá v integraci zákonných požadavků a nejlepších praktik do všech aspektů IT, což zahrnuje úzkou spolupráci s bezpečnostními týmy, zejména s IT bezpečnostním architektem, aby zajistili, že všechny technologické systémy a postupy jsou v souladu s aktuálními právními rámci a normami jako GDPR, ISO 27001, a další. Tato odpovědnost je klíčová pro zajištění, že IT infrastruktura podniku nejen efektivně podporuje jeho obchodní cíle, ale také aktivně chrání citlivé informace a minimalizuje rizika spojená s kybernetickou bezpečností.

Důležitým úkolem manažera IT governance je také správa konfigurační databáze (CMDB), což je centrální zdroj informací o všech významných IT aktivech a jejich konfiguracích v organizaci. Správné řízení CMDB umožňuje organizaci efektivně monitorovat změny v IT prostředí, což je nezbytné pro zajištění operativní stability a zabezpečení. Manažer zajišťuje, že CMDB je průběžně aktualizována a přesně odráží současný stav IT infrastruktury, což usnadňuje plánování změn a umožňuje rychlou reakci na incidenty.

Poslední klíčovou odpovědností je řízení procesů interního řešení incidentů, které mohou mít významný dopad na IT operace a služby organizace. Tato činnost zahrnuje koordinaci napříč IT týmy za účelem zajištění rychlé a koordinované odpovědi na incidenty, minimalizace jejich dopadu na běžnou činnost organizace a podporu rychlé obnovy služeb. Tímto způsobem manažer IT governance přispívá k odolnosti organizace vůči interním výzvám, podporuje kontinuitu podnikání a zajišťuje, že organizace je schopna udržet nepřetržitý provoz i v případě nečekaných událostí.

5.2 Analýza současného stavu

Na schůzce s CISO organizace bylo rozhodnuto, že analýza současného stavu, návrh změn a jejich případná realizace bude provedena autorem práce. Zaměřena byla především na dvě oblasti. Jako primární byla analýza současného procesu přijímání externistů a s tím spojených rizik. Sekundární oblastí zájmu bylo současné vedení ISMS a s tím spojené procesy, administrativa a role.

5.2.1 Analýza současného procesu přijímání externistů

Analýza současného stavu procesu přijímání externistů v organizaci provedena autorem práce odhalila několik klíčových nedostatků, které vyžadují pozornost a následná zlepšení. Tyto nedostatky mají potenciál negativně ovlivnit jak celkovou efektivitu procesu, tak i bezpečnost informačních systémů organizace.

Velká obsáhlost procesu přijímání externistů představuje značnou výzvu, jelikož tato komplexnost může vést k administrativním chybám v důsledku jeho složitosti a náročnosti na správu. Detailní procesní mapa zřízení externisty viz Příloha 1, ukazuje množství kroků a požadavků nutných pro úspěšnému zavedení externích pracovníků do systému. Tento rozsáhlý proces zvyšuje riziko, že zodpovědné osoby mohou ztratit přehled, což má za následek opomenutí klíčových aspektů procesu a zvýšenou pravděpodobnost lidských chyb, které mohou vést k zpoždění nebo nesprávné integraci externistů do pracovních procesů.

Dále byla identifikována **nedostatečná účast oddělení bezpečnosti** na procesu přijímání externistů, což představuje významnou bezpečnostní mezeru. Tato částečná absence klíčového hráče znamená, že není zajištěna důkladná kontrola nad správným nastavením systémových rolí pro externí pracovníky. To vede k situaci, kdy mohou být externím pracovníkům přidělena širší oprávnění, než je nezbytné pro jejich specifické úkoly, což představuje významné bezpečnostní riziko. Tento efekt sněhové koule, kdy dochází k akumulaci nepotřebných oprávnění, podkopává základní zásady nezbytné pro udržení pevného bezpečnostního řetězce.

Kritickým bodem je také **slabá pravidelná a nepravidelná kontrola aktivity externích pracovníků** v rámci informačních systémů. Existující mechanismy nezajišťují dostatečné monitorování těchto pracovníků po jejich zavedení do systému, což umožňuje, aby jakékoli neautorizované nebo podezřelé chování zůstalo nepovšimnuto a neřešeno. Tato nedostatečná kontrola zvyšuje riziko zneužití přístupových práv a potenciální vznik bezpečnostních incidentů.

Posledním problematickým bodem je **absence předdefinovaných balíčků rolí pro standardní pozice**, jako jsou např. účetní, administrátoři a vývojáři. To vytváří prostor pro nekonzistentní a nesystematické přidělování oprávnění. Nově příchozí zaměstnanci jsou často nuceni přebírat role po jiných zaměstnancích, což vede k akumulaci nadbytečných nebo irelevantních oprávnění. Tento přístup komplikuje správu oprávnění a zvyšuje administrativní náročnost IT systémů, zatímco efektivní auditování a sledování oprávnění se stává téměř nemožným. Tato situace nejenže představuje značnou bezpečnostní hrozbu, ale také ztěžuje dodržování interních i externích pravidel a regulací týkajících se přístupu k informacím a datové bezpečnosti.

5.2.2 Analýza současného ISMS

Analýza současného stavu ISMS v organizaci odhalila klíčové problémy, které vyžadují značnou pozornost a zlepšení, aby se zvýšila efektivita a bezpečnost informačního systému. Tyto nedostatky mají významný vliv na celkovou strukturu a fungování ISMS a ukazují na potřebu revidovat a posílit interní procesy a politiky.

Jedním z hlavních zjištěných problémů současného ISMS je **nejasné rozdělení rolí a odpovědností mezi klíčovými aktéry** v rámci organizace, jako jsou IT governance a bezpečnostní oddělení. Tato nejednoznačnost vede k překrývání úkolů a může způsobovat komunikační a koordinační problémy, které ohrožují efektivitu a reakci systémů při řešení bezpečnostních incidentů a hrozeb.

Dalším zásadním problémem je **akumulace a nesprávné přidělování rolí** v rámci role managementu, kde nedostatečně definovaný proces správy rolí umožňuje kopírování a přidělování rolí bez adekvátního přezkumu a ověření. Tento nedostatek systematického řízení a kontroly rolí může vést k nesprávnému nastavení přístupových práv a zvyšuje riziko bezpečnostních incidentů. V rámci vlastního šetření autor práce realizoval přehled jednotlivých rolí a jejich oprávnění viz Tabulka 2. K tomu se přidává **nedostatek pravidelných a nepravidelných** kontrol oprávnění v rámci organizace, což znamená, že chyby v přidělování rolí mohou zůstat dlouhodobě neodhaleny a neopraveny. Tato situace znásobuje riziko vnitřních a vnějších hrozeb pro bezpečnost informací.

Významným nedostatkem je také **nedokončení BIA**, které způsobuje nejistotu v prioritizaci aplikací a systémů pro plány kontinuity činnosti (BCP) a plány obnovy po havárii (DRP). Bez jasného určení, které systémy jsou kritické pro fungování organizace, je těžké efektivně alokovat zdroje a reagovat na incidenty.

Poslední identifikovaný problém, **absence BIA analýzy pro citlivost dat**, znemožňuje efektivní ochranu citlivých informací, protože není možné přesně určit, kde se citlivá data nacházejí. Tento nedostatek přesné lokalizace citlivých dat komplikuje vytváření adekvátních bezpečnostních opatření a strategií pro jejich ochranu. Tyto zjištěné problémy poukazují na potřebu komplexní revize a zlepšení v oblasti systému managementu bezpečnosti informací v organizaci, což vyžaduje značné úsilí ve formě revize interních politik, procesů a struktur pro zajištění lepší ochrany informačních aktiv a zvýšení celkové bezpečnosti.

Pozice	Emailový systém	Správa databází	Interní komunikační platforma	Serverová místnost	Úložiště	Cloud služby	Finanční systémy	Systém pro správu zakázek	Řízení projektů	Dostupnost aplikací
Síťový Administrátor	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Ne	Ano
Vývojář	Ano	Ano	Ano	Ne	Ano	Ano	Ne	Ano	Ano	Ano
Analytik	Ano	Ne	Ano	Ne	Ne	Ne	Ano	Ne	Ano	Ne
Manažer Projektů	Ano	Ne	Ano	Ne	Ne	Ne	Ano	Ano	Ano	Ne
IT Podpora	Ano	Ano	Ano	Ano	Ano	Ne	Ne	Ne	Ne	Ano
Bezpečnostní Analytik	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ne	Ano
IT Manažer	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Administrátor Databází	Ano	Ano	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne
Vývojář Aplikací	Ano	Ano	Ano	Ne	Ano	Ano	Ne	Ano	Ano	Ano
Uživatelská Podpora	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ne

Tabulka 2 Stav rozdělení rolí před revizí (vlastní zpracování)

5.2.3 Rizika spojená s nedostatečným managementem lifecyclu externistů

V rámci procesu přijímání externistů se objevuje několik rizik, která mají potenciál negativně ovlivnit bezpečnost informací a operace organizace. Jedním z hlavních rizik jsou **administrativní chyby vyplývající ze složitosti** a obsáhlosti tohoto procesu. Tato složitost může vést k přehlížení klíčových aspektů procesu, způsobovat zpoždění ve včlenění externistů do pracovního prostředí a vytvářet prostor pro bezpečnostní hrozby. Dále, nedostatečná účast bezpečnostního oddělení na tomto procesu může vést k nevhodnému nastavení systémových rolí pro externí pracovníky, čímž jim mohou být neúmyslně přidělena širší oprávnění, než je pro jejich úkoly nezbytné. Toto představuje značné bezpečnostní riziko.

Dalším problémem **je slabá pravidelná a nepravidelná kontrola aktivity externích pracovníků** v rámci informačních systémů, což umožňuje, aby potenciálně neautorizované nebo podezřelé aktivity zůstaly nedetekované. Nedostatek adekvátní monitorace a kontrol může vést k zneužití přístupových práv a ohrožení citlivých informací a celkové integrity informačního systému.

Kumulace rolí a přidělování nadbytečných oprávnění zaměstnancům, kteří je pro svou práci nepotřebují, přináší další vrstvu bezpečnostního rizika. Vlastním šetřením bylo zjištěno, že práva jednotlivých uživatelů často neodpovídají jejich potřebám viz Tabulka 2. Tato situace nejen zvyšuje potenciální počet vektorů útoku na organizaci, ale z administrativního hlediska také komplikuje správu oprávnění. Absence standardizovaných balíčků rolí a potřeba individuálního posouzení každého případu přidává na časové náročnosti a zvyšuje šanci na chyby v procesu správy oprávnění. Tento nedostatek systematického přístupu k přidělování a auditování rolí ztěžuje sledování oprávnění a identifikaci toho, kdo má přístup, k jakým datům a proč. V důsledku toho může docházet k nesrovnalostem a problémům s dodržováním interních a externích pravidel a regulací týkajících se přístupu k informacím a datové bezpečnosti, což značně ohrožuje celkovou bezpečnostní strukturu organizace.

5.2.4 Rizika spojená s nedostatky v ISMS

V rámci ISMS organizace se objevují klíčová rizika, která vyžadují důkladnou pozornost pro zajištění celkové efektivity a zabezpečení. Jedním z problémů je **nejasné rozdělení rolí a odpovědností** mezi IT governance, oddělením bezpečnosti a informačním managementem, což může vést k překrývání úkolů a nedostatkům v komunikaci. Tato situace snižuje efektivitu řízení bezpečnosti informací a oslabuje schopnost organizace chránit se proti kybernetickým hrozbám.

Dalším rizikem je **nedostatek pravidelných a nepravidelných kontrol**, které by umožňovaly odhalení a opravu chyb v přidělování rolí a oprávnění. Tato absence kontrol může vést k bezpečnostním slabinám a zneužití systémových oprávnění. **Nedokončené BIA** dále ztěžují určení kritičnosti aplikací a systémů, což má za následek neefektivní prioritizaci v BCP a DRP. Bez jasného určení, které systémy a aplikace jsou pro organizaci nejvíce kritické, nemůže dojít k adekvátní ochraně klíčových aktiv.

Konečně, absenci **BIA analýzy pro určení citlivosti dat** je možné považovat za značné riziko, které brání identifikaci a adekvátní ochraně míst, kde jsou citlivá data uložena. To vede k zvýšenému riziku neoprávněného přístupu, úniku nebo zneužití těchto informací, čímž je ohrožena důvěrnost a integrita dat. Tyto problémy společně poukazují na potřebu komplexní revize a zlepšení stávajícího systému řízení bezpečnosti informací, aby bylo možné efektivně řešit identifikovaná rizika a zlepšit celkovou bezpečnostní situaci organizace.

5.3 Navrhované změny

Pro každé z identifikovaných rizik existují specifické řešení, které by měly být zavedeny k jejich mitigaci. Navrhované změny byly navrženy tak, že se jejich případná realizace bude týkat prakticky celé organizace, tedy počtu uživatelů s přesahem do tisíců.

5.3.1 Procesní změny

Pro řešení rizika administrativních chyb z důvodu složitosti procesu přijímání externistů je esenciální, aby organizace přistoupila k revizi a zjednodušení tohoto procesu.

Klíčem je snížení počtu kroků a požadavků, potenciálně i změna celkového toku práce, což povede ke snížení možnosti vzniku lidských chyb a zvýšení efektivity a přesnosti celého procesu. Implementace standardizovaných šablon a kontrolních seznamů pro běžné úkoly a rozhodovací procesy dále podpoří toto úsilí a usnadní správu a přehlednost. V oblasti nesprávného přístupu k informačním systémům je zásadní zapojení oddělení IT bezpečnosti již od počátku procesu přijímání externistů. Toto oddělení by mělo mít pravomoc přidělovat přístupová práva a systémové role, zajišťující soulad s bezpečnostními požadavky. Tímto způsobem lze zamezit přidělování nepřiměřeně širokých oprávnění externistům, což redukuje bezpečnostní rizika. Přesný přehled návrhů na změnu procesů a systémů nelze do práce z důvodu anonymizace a udržení bezpečnosti začlenit.

Pro řešení rizika zneužití oprávnění je klíčové zavést pravidelné revize a audity oprávnění, které umožní identifikaci a opravu chyb v přidělení oprávnění dále pak systémy pro automatické sledování aktivit a systémy pro včasné varování, které jsou nezbytné pro detekci a rychlou reakci na jakékoli neobvyklé chování, což pomáhá předcházet bezpečnostním incidentům. **Řešení rizika kumulace rolí** spočívá ve vytvoření a implementaci standardizovaných balíčků rolí pro standardní pozice v rámci organizace, navržených na základě autorem provedené důkladné analýzy pracovních potřeb a bezpečnostních požadavků. Implementace robustního systému pro auditování a sledování oprávnění zajišťuje pravidelné přezkoumávání a aktualizaci oprávnění, což zefektivňuje správu oprávnění a minimalizuje riziko zneužití.

Školení a osvěta zaměstnanců o bezpečnostních rizicích a správných postupech pro zacházení s citlivými daty a systémy jsou doplňujícími kroky, které posilují ochranu informací a zvyšují bezpečnostní povědomí v celé organizaci. Tyto kroky v kombinaci s pečlivým plánováním a implementací tvoří robustní základ pro zvýšení bezpečnosti a efektivity ISMS organizace.

5.3.2 Systémové změny

Efektivní řešení problematiky překrývání úkolů a nedostatků v komunikaci a koordinaci v organizaci vyžaduje zavedení jasně definovaného organizačního schématu. Toto schéma musí přesně rozdělit role a odpovědnosti mezi IT governance, oddělení

bezpečnosti a informační management, což zajišťuje, že každá skupina přesně rozumí svým úkolům a odpovědnostem. Důležitým doplňkem jsou pravidelná školení a efektivní komunikační protokoly, které podporují spolupráci mezi týmy a zajistí, že všichni členové mají jasné pochopení procesů a vědí, jak efektivně spolupracovat.

K řešení rizika nedetekovaných, neoprávněných a nesprávně přidělených rolí je nezbytné zavést systém pro pravidelné revize a auditování oprávnění a rolí. Tento systém by měl kombinovat automatické nástroje pro sledování a reportování s manuálními kontrolami prováděnými odborníky na IT bezpečnost, což umožní rychlou identifikaci a nápravu problémů.

Problém neefektivní prioritizace v BCP a DRP vyžaduje dokončení a pravidelnou aktualizaci BIA. Tyto analýzy musí jasně určit kritičnost aplikací a systémů, což umožní organizaci efektivně alokovat zdroje a řídit úsilí v případě vzniku incidentu, zajišťující, že kritické systémy a procesy jsou chráněny a mohou být rychle obnoveny.

Řešení rizika neadekvátní ochrany citlivých dat spočívá ve vytvoření komplexního mapování, které jednoznačně určí, kde jsou citlivá data uložena. Tento krok by měl být podpořen implementací pevných bezpečnostních opatření, včetně šifrování, přístupových kontrol a monitorovacích systémů, což zajistí vysokou úroveň ochrany těchto kritických informací. Tímto způsobem lze adresovat a minimalizovat rizika spojená s ochranou a zabezpečením citlivých dat, což je zásadní pro udržení důvěryhodnosti a integrity organizace ve vztahu k jejím zákazníkům a obchodním partnerům.

5.4 Implementace změn

K implementaci těchto změn je nutné zdůraznit význam komplexního přístupu, který zahrnuje jasné stanovení cílů, rozdělení odpovědností, definování časového rámce pro realizaci a vytvoření mechanismů pro průběžné monitorování a hodnocení efektivity zavedených opatření. Důležité je také zabezpečit angažovanost a podporu vedení organizace, jelikož jejich zapojení je zásadní pro úspěch celého procesu implementace.

5.4.1 Implementace procesních změn

Implementace změn v procesu přijímání externistů s cílem řešit identifikované riziko administrativních chyb z důvodu složitosti procesu představuje významný krok k optimalizaci a zefektivnění tohoto kritického procesu. Klíčovou součástí této implementace byla revize a zjednodušení workflow, které vedlo k významnému snížení počtu kroků a požadavků nezbytných pro úspěšné přijetí externího pracovníka do organizace. Zavedením nového workflow, které vyžaduje, aby všechny zúčastněné strany za svá odpovídající oddělení v rámci jednoho ticketu schválily udělené role a oprávnění konkrétního externisty, se podstatně zvýšila transparentnost a odpovědnosti v procesu. Tento přístup motivuje jednotlivé strany k pečlivému přezkumu a schvalování oprávnění, čímž se minimalizuje pravděpodobnost lidských chyb a zvyšuje celková spolehlivost procesu. Tato strategie nejen že přispívá k lepší správě a kontrole nad udělováním oprávnění, ale také podporuje kulturu odpovědnosti a pečlivosti mezi zaměstnanci. Standardizované šablony a kontrolní seznamy pro běžné úkoly a rozhodovací procesy, které byly rovněž zavedeny, dále usnadňují tento proces, poskytují jasné směrnice a zvyšují efektivitu rozhodování.

V rámci řešení rizika nesprávného přístupu k informačním systémům bylo rozhodnuto podniknout klíčové kroky směrem k zásadnímu zlepšení procesu přijímání externistů. Klíčovou součástí tohoto zlepšení byla redefinice role oddělení IT bezpečnosti v tomto procesu. Procesním „reengineeringem“ byla zvýšena důležitost tohoto oddělení na nejvyšší prioritu, což zajišťuje, že oddělení IT bezpečnosti hraje klíčovou a rozhodující roli od samého počátku procesu definování a vytváření nových uživatelských účtů pro externisty. Toto rozhodnutí přináší značné výhody v kontextu zabezpečení organizace. Zapojením oddělení IT bezpečnosti do procesu již od jeho počátku je možné zajistit, že všechna přístupová práva a systémové role přidělované externistům jsou přísně vyhodnocovány a schvalovány s ohledem na aktuální bezpečnostní potřeby a politiky organizace. Tímto přístupem se výrazně snižuje riziko udělení nevhodných nebo nadměrných oprávnění, která by mohla vést k neautorizovanému přístupu k citlivým informacím a systémům. Navíc, díky tomuto změněnému postupu, je každé udělení oprávnění pečlivě zváženo a dokumentováno, což zlepšuje sledovatelnost a auditovatelnost procesů souvisejících s přístupovými právy. Tento transparentní a kontrolní mechanismus

je nezbytný pro efektivní správu bezpečnostních rizik a pro zajištění, že všechny operace jsou v souladu s interními i externími regulačními požadavky na ochranu dat.

V rámci implementace řešení rizika zneužití oprávnění, které vyplývá ze slabé pravidelné a nepravidelné kontroly aktivity externích pracovníků v informačních systémech, byla provedena komplexní revize rolí a přístupových práv. Tento proces zahrnoval detailní analýzu a identifikaci všech nadbytečných rolí a přístupových práv, které byly následně odebrány nebo změněny viz Tabulka 3. Tímto krokem se významně snížilo riziko neautorizovaného nebo podezřelého přístupu a potenciálního zneužití oprávnění, což přispělo k posílení bezpečnosti informačních systémů a ochraně citlivých informací. Dále byla do odpovědností interního auditingu přidána povinnost pravidelné kontroly nadbytečných rolí a oprávnění. Toto opatření zajišťuje, že revize rolí a oprávnění není jednorázová aktivita, ale stává se součástí běžného auditního cyklu s roční periodicitou. Taková pravidelná kontrola umožňuje organizaci rychle reagovat na jakékoli změny v pracovních potřebách a bezpečnostním prostředí, což minimalizuje riziko zastaralých nebo nevhodných oprávnění, která by mohla ohrozit bezpečnost informačního systému.

V rámci implementace řešení pro mitigaci rizika kumulace rolí byly v organizaci zavedeny klíčové inovace, které přinášejí signifikantní zlepšení v procesu správy oprávnění a rolí. Prvním krokem bylo vytvoření a zavedení standardizovaných "basketů" neboli balíčků rolí pro všechny standardní pozice, s výjimkou specifických rolí, jako jsou CEO, CIO (Chief information officer) a další. Tyto balíčky byly navrženy autorem práce na základě důkladné analýzy pracovních potřeb a bezpečnostních požadavků spojených s každou pozicí, což umožnilo efektivnější a bezpečnější správu oprávnění a minimalizaci rizika nadbytečných oprávnění. Dalším důležitým krokem bylo zavedení robustního systému pro auditování a sledování oprávnění. Tento systém zajišťuje, že všechna oprávnění jsou pravidelně přezkoumávána a aktualizována v souladu s aktuálními potřebami zaměstnanců a bezpečnostními politikami. Systém spočívá především v zaměření na zaměstnance, kteří obdrželi určité role, nové zaměstnance a také zaměstnance, kteří pozici v průběhu setrvání ve společnosti změnili. Díky tomu je možné rychle identifikovat a řešit jakékoli nesrovnalosti nebo neautorizované změny oprávnění, což přispívá k udržení vysoké úrovně bezpečnosti informačního systému.

Pro podporu těchto technických a procesních změn bylo také zavedeno školení pro zaměstnance, jehož cílem je posílit povědomí o důležitosti správného řízení oprávnění a zvýšit porozumění bezpečnostním rizikům a správným postupům při zacházení s citlivými daty a systémy. Toto školení představuje zásadní prvek celé implementace, neboť vzdělávání a osvěta zaměstnanců hraje klíčovou roli v budování silné bezpečnostní kultury a v podpoře udržitelných změn v organizaci.

Pozice	Emailový systém	Správa databází	Interní komunikační platforma	Serverová místnost	Úložiště	Cloud služby	Finanční systémy	Systém pro správu zakázek	Řízení projektů	Dostupnost aplikací
Síťový Administrátor	Ano	Omezeno	Ano	Omezeno	Ano	Ano	Ne	Ano	Ne	Omezeno
Vývojář	Ano	Omezeno	Ano	Ne	Omezeno	Ano	Ne	Omezeno	Ano	Omezeno
Analytik	Ano	Ne	Ano	Ne	Ne	Ne	Ano	Ne	Ano	Ne
Manažer Projektů	Ano	Ne	Ano	Ne	Ne	Ne	Omezeno	Ano	Ano	Ne
IT Podpora	Ano	Omezeno	Ano	Ne	Omezeno	Ne	Ne	Ne	Ne	Omezeno
Bezpečnostní Analytik	Ano	Ano	Ano	Omezeno	Ano	Ano	Ano	Ne	Ne	Ano
IT Manažer	Ano	Ano	Ano	Omezeno	Ano	Ano	Ano	Ano	Ano	Ano
Administrátor Databází	Ano	Ano	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne
Vývojář Aplikací	Ano	Omezeno	Ano	Ne	Omezeno	Ano	Ne	Omezeno	Ano	Omezeno
Uživatelská Podpora	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Ne	Ne

Tabulka 3 Role uživatelů po revizi a implementaci bezpečnostních opatření

5.4.2 Implementace systémových změn

V rámci adresování **rizika překrývání úkolů a nedostatků v komunikaci a koordinaci** byla přijata opatření směřující k zefektivnění správy a koordinace mezi klíčovými odděleními zodpovědnými za IT bezpečnost v organizaci. Implementace těchto opatření zahrnovala vypracování jasného a detailního organizačního schématu, které rozdělilo role a odpovědnosti mezi IT governance, oddělení bezpečnosti a CIO (ředitele IT). Z tohoto nově stanoveného rozdělení odpovědností, oddělení bezpečnosti bylo pověřeno stanovením bezpečnostních pravidel. Tato pravidla představují základní rámec, jenž určuje, jak by měla být bezpečnost informací v organizaci řízena. Aby byla zajištěna jejich účinná implementace, oddělení bezpečnosti úzce spolupracuje s IT governance, které pomáhá s jejich posunem v IT části společnosti. Tato spolupráce zahrnuje jak vývoj strategií pro zavádění bezpečnostních politik do praxe, tak i monitorování jejich dodržování a účinnosti.

Role CIO v tomto procesu je klíčová, jelikož jakožto vrcholový představitel IT odpovídá za dohled nad celkovou implementací bezpečnostních strategií. CIO je zodpovědný za zajištění potřebných finančních a lidských zdrojů pro realizaci bezpečnostních opatření a za integraci bezpečnostních politik do širšího IT plánování a strategie organizace. Společně s CISO, který je zodpovědný za operativní aspekty bezpečnosti informací, CIO zajistí, že bezpečnostní politiky jsou nejen formulovány, ale také efektivně implementovány a dodržovány.

Pro podporu této struktury byla také zavedena pravidelná školení a komunikační protokoly. Cílem těchto opatření je zajištění, že všechny zúčastněné týmy mají jasné pochopení svých úkolů, rolí a odpovědností a jsou schopny efektivně spolupracovat a komunikovat. Pravidelná školení zajišťují, že všechny týmy jsou neustále informovány o aktuálních bezpečnostních hrozbách, trendech a osvědčených postupech v oblasti IT bezpečnosti

Adresování rizika nedetekovaných a neopravených nesprávně přidělených rolí bylo klíčovým bodem v implementační strategii organizace k posílení bezpečnosti informačních systémů. Toto riziko, identifikované jako kritické pro integritu a bezpečnost IT infrastruktury, bylo řešeno prostřednictvím komplexních opatření, jak je popsáno v kapitolách 5.2.3 týkajících se neoprávněného přístupu a kumulace rolí.

Adresování rizika neefektivní prioritizace BCP a DRP bylo zásadní pro zajištění, že organizace je schopna efektivně reagovat na případné incidenty s minimálním dopadem na své operace. Klíčovým krokem v tomto procesu bylo vytvoření nové matice autorem práce s váhováním, která slouží k adekvátnímu ohodnocení a prioritizaci informačních aktiv společnosti. Tento přístup umožnil organizaci nejen správně identifikovat, které aplikace, systémy a služby jsou pro její chod nejkritičtější, ale také určit, jak by měly být alokovány zdroje v případě výpadku nebo jiného incidentu.

Proces vytvoření matice autorem práce zahrnoval pečlivou analýzu všech informačních aktiv a jejich klasifikaci podle kritičnosti pro byznys operace. Toto hodnocení bylo založeno na různých kritériích, včetně potenciálního dopadu na finanční stabilitu, zákaznické vztahy, reputaci a dodržování regulatorních požadavků. Výsledkem byla detailně strukturovaná matice, která poskytla jasné usměrnění pro prioritizaci úsilí a zdrojů v rámci BCP a DRP. S pomocí této matice mohla organizace efektivně směrovat své úsilí k ochraně a obnově těch systémů a aplikací, které byly identifikovány jako nejkritičtější. To zahrnovalo vytváření specifických plánů obnovy, které detailně popisovaly postupy a kroky nutné pro rychlou reakci a minimalizaci dopadů výpadků na klíčové byznys operace.

Zavedení procesu pro pravidelné aktualizace a revize matice s váhováním zajistilo, že všechny informace zůstávají aktuální a odrážejí nejnovější změny v interním i externím prostředí organizace. Tímto způsobem mohla být matice pružně upravována v reakci na nově identifikované hrozby, technologický vývoj nebo změny v byznys modelu organizace.

Důležitou součástí úspěšné implementace tohoto řešení bylo také zavedení školení a osvětových programů pro zaměstnance. Programy měly za cíl posílit povědomí o důležitosti BCP a DRP plánů a zvýšit porozumění procesu váhového hodnocení.

Zaměstnanci byli seznámeni s principy a postupy, které jsou základem pro efektivní prioritizaci a řízení rizik, čímž se zvýšila celková připravenost organizace na potenciální krize.

Adresování rizika neadekvátní ochrany citlivých dat bylo klíčovým krokem k zajištění bezpečnosti a integrity informačních aktiv organizace. V rámci implementace tohoto řešení bylo přijato několik zásadních opatření, která byla zaměřena na identifikaci, ochranu a řízení přístupu k citlivým datům uloženým na sdílených úložištích.

Prvním krokem bylo vytvoření komplexního mapování dat, které poskytlo přehled o umístění všech citlivých dat uložených v organizaci. Tento proces zahrnoval důkladnou analýzu provedenou autorem práce a inventarizaci všech sdílených úložišť a databází, aby bylo možné přesně určit, kde jsou citlivá data uložena. Díky tomuto mapování bylo možné identifikovat oblasti s vysokým rizikem a stanovit priority pro zavedení ochranných opatření. V návaznosti na mapování dat proběhlo ohodnocení kritičnosti dat uložených na jednotlivých úložištích. Toto hodnocení bylo založeno na BIA informačních aktiv, které posoudily dopady potenciální ztráty nebo kompromitace dat na operace organizace. Tímto způsobem bylo možné určit, která data jsou pro organizaci nejkritičtější a vyžadují zvýšenou ochranu. Na základě identifikace a hodnocení kritičnosti dat byla zavedena řada silných ochranných opatření. To zahrnovalo implementaci šifrování dat, aby se zajistila jejich bezpečnost při přenosu i ukládání, zavedení přístupových kontrol pro omezení přístupu k datům pouze oprávněným uživatelům a nasazení monitorovacích systémů pro detekci a reakci na neautorizované přístupy nebo podezřelé aktivity. Kroky byly klíčové pro minimalizaci rizik spojených s únikem nebo zneužitím citlivých informací.

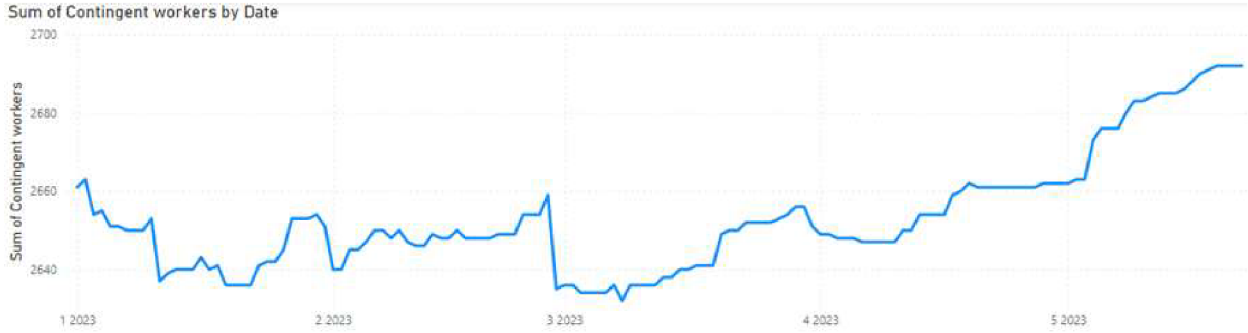
Konečným krokem bylo vytvoření BCP specificky pro sdílená úložiště, který zohledňoval kritičnost uložených dat. Tento plán definoval postupy pro prioritizaci obnovy úložišť v případě výpadku nebo jiného incidentu, aby bylo možné rychle obnovit přístup k nejdůležitějším datům a minimalizovat dopady na operace organizace.

5.5 Výsledky implementace

5.5.1 Výsledky implementace na proces přijímání externistů

V rámci implementace opatření pro lepší správu externistů došlo k významným změnám a zlepšením. Celkově bylo revidováno 2729 externistů, což představuje rozsáhlý přezkum správy přístupů a oprávnění externích pracovníků v organizaci. Tento proces odhalil, že u 327 (12 % z celkového počtu) viz Obrázek 10 externistů byly identifikovány a následně odebrány nadbytečné role. Odebrání těchto rolí bylo zásadní pro minimalizaci bezpečnostních rizik spojených s neoprávněným přístupem k citlivým informacím a systémům.

Celkově ovšem (především kvůli započetí významných projektů v rámci společnosti) k poklesu počtu externistů nedošlo viz Obrázek 9. Lze ovšem vidět postupné snižování jejich počtu během revize oddělení IT governance.



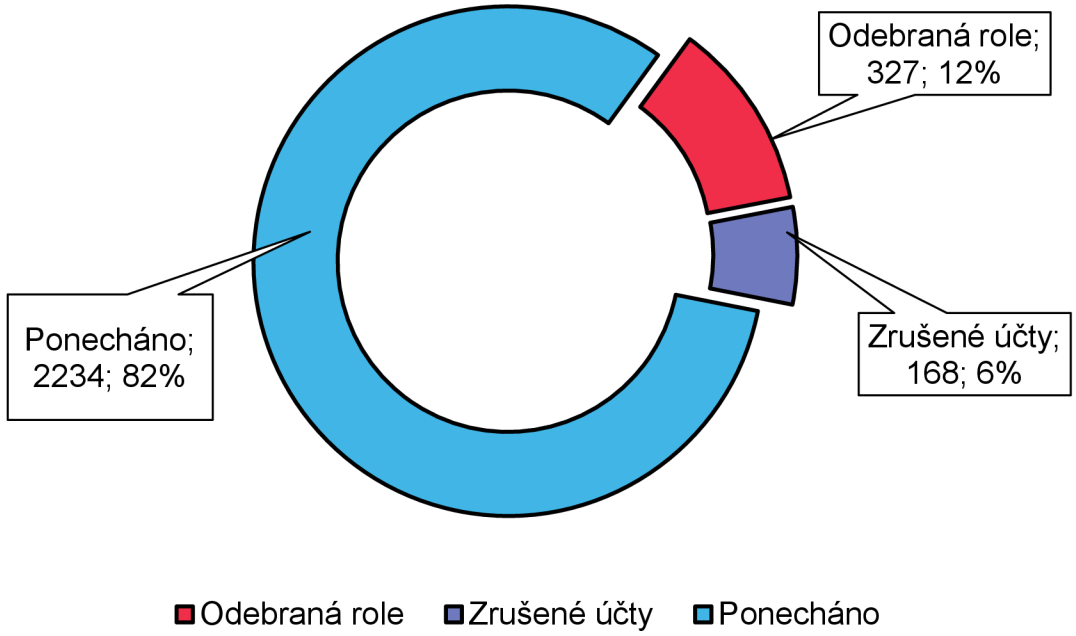
Obrázek 9 Počet externistů v čase revize a nápravných opatření (vlastní zpracování)

Dalším klíčovým krokem bylo zrušení účtů 168 externistů viz Obrázek 10, kteří prokázali neaktivitu delší než půl roku. Tato neaktivita byla důsledkem chybně nastaveného procesu správy externistů, který byl v rámci implementace změněn. Odstranění těchto neaktivních účtů nejenže přispělo k zvýšení bezpečnosti informačních systémů, ale také vedlo k odstranění nevyužívaných licencí Office 365. Celkové úspory na OPEX za licence dosáhly téměř 22 000 €, což představuje významné finanční zlepšení pro organizaci.

Zejména znepokojivým zjištěním bylo, že dvacet z odebraných rolí bylo spojeno s přístupem ke kritickým informačním aktivům organizace. Toto odhalení podtrhlo význam

pečlivé revize a správy rolí externistů, jelikož role představovaly potenciální bezpečnostní riziko. Jejich odebráním se výrazně snížila možnost zneužití přístupu k nejcitlivějším a nejkritičtějším informacím, čímž byla zvýšena celková bezpečnostní odolnost organizace.

Přístup k revizi a optimalizaci správy externistů demonstruje důležitost průběžného monitorování a aktualizace přístupových práv a oprávnění. Systematické přezkoumávání a úpravy nejenže přináší finanční úspory, ale především zajišťuje, že informační systémy a data organizace jsou chráněny před neoprávněným přístupem a potenciálním zneužitím.



Obrázek 10 Revidovaní externisté (vlastní zpracování)

5.5.2 Výsledky implementace na proces přidělování rolí

Implementace bezpečnosti informací v procesu přidělování rolí přinesla výrazné výsledky, které podstatně přispěly k efektivnější a bezpečnější správě uživatelských oprávnění v rámci organizace. Klíčovým krokem bylo vytvoření 25 "basketů" rolí určených pro nejčastější pracovní pozice, což umožnilo standardizaci procesu přidělování oprávnění a zjednodušení celého systému správy rolí.

Celkově bylo v rámci tohoto procesu revidováno 5223 uživatelů, včetně interních zaměstnanců a externistů. U 2998 (57 %) z nich bylo zjištěno, že mají přiděleny nadbytečné role, které byly následně odebrány. Většina těchto rolí (92 %) byla zděděná během nástupu daného pracovníka a většinou neohrožovala chod společnosti ani nemohla vést k neoprávněnému přístupu k citlivým informacím. Tento krok vedl k signifikantnímu snížení počtu udělených rolí novým zaměstnancům – kvartálně došlo k poklesu téměř o polovinu, což dokládá efektivitu zavedených balíčků rolí.

Zbývajících 8 % rolí, které byly zděděné nebo přidělené ad-hoc, byly také odebrány, jelikož mohly představovat potenciální bezpečnostní riziko, včetně možnosti konfliktu zájmů, zneužití pravomocí, nebo neuváženého jednání (shození produkčního serveru). Ačkoli role mohly teoreticky ohrozit bezpečnost informací, díky pečlivému logování aktivit a integrovanému dohledovému centru bylo možné zajistit, že v případě jakéhokoli narušení bezpečnosti by bylo možné rychle identifikovat a lokalizovat potenciálního pachatele.

5.5.3 Výsledky implementace na BIA

V reakci na identifikovanou potřebu komplexního přístupu k BIA byly autorem práce v organizaci podniknuty významné kroky za účelem posílení bezpečnosti informací a zajištění souladu s normou ISO 27001 a zákonem o kybernetické bezpečnosti České republiky. Spolupráce mezi týmem IT governance a informační bezpečnosti vedla k vytvoření nového modelu matice s váhováním, který byl pečlivě navržen tak, aby odrážel specifické požadavky a rizika spojená s informačními aktivy organizace a regulatorními požadavky.

Prvním klíčovým krokem byla komplexní revize všech informačních aktiv organizace. Tento proces umožnil identifikovat 18 aplikací, které byly klasifikovány jako kritická informační aktiva. Toto určení kritičnosti bylo zásadní pro další kroky v procesu řízení a ochrany informačních aktiv, jelikož poskytlo jasný přehled o tom, které systémy a aplikace jsou pro chod organizace nejdůležitější.

Na základě prioritizace získané z revize informačních aktiv byly vytvořeny specifické BCP a DRP. Plány byly navrženy s cílem zajištění rychlé a efektivní reakce na potenciální

incidenty, které by mohly ohrozit dostupnost, integritu nebo důvěrnost kritických informačních aktiv.

K 15. únoru 2024 se organizaci podařilo úspěšně otestovat plány kontinuity činnosti a obnovy po havárii u 15 z identifikovaných kritických aplikací. Testy poskytly cenné informace a zpětnou vazbu, které byly využity pro další finální úpravy a zlepšení BCP a DRP plánů. Úspěšné testování těchto plánů dokládá, že organizace je dobře připravena reagovat na případné narušení chodu kritických systémů a aplikací, což zvyšuje její odolnost vůči potenciálním incidentům.

5.5.4 Výsledky implementace opatření proti ztrátě dat

V rámci iniciativy zaměřené na řešení rizika neadekvátní ochrany citlivých dat došlo k důležitým krokům, které zvýšily bezpečnostní opatření aplikovaná na sdílených úložištích používaných napříč organizací. Kroky byly zásadní pro zajištění ochrany citlivých informací a pro posílení celkové bezpečnosti informačních systémů v organizaci.

Prvním krokem byla pečlivá identifikace sdílených úložišť, na kterých se nacházely citlivé informace. Tento proces umožnil organizaci získat přehled o umístění citlivých dat a vyhodnotit potenciální rizika spojená s jejich uchováváním.

Na základě zjištěných informací autor práce provedl nezbytné úpravy rolí a přístupů k těmto úložištím, aby bylo zajištěno, že přístup mají pouze autorizované osoby s relevantním oprávněním. Tato opatření byla klíčová pro minimalizaci rizika neoprávněného přístupu k citlivým datům.

Dalším důležitým krokem bylo sepsání BCP a DRP specificky pro sdílená úložiště obsahující citlivé informace. Autorem práce zpracované plány zajistily, že organizace má připravené postupy pro rychlou reakci a obnovu v případě incidentů, které by mohly ohrozit dostupnost, integritu nebo důvěrnost uložených dat. K 15. únoru 2024 bylo možné otestovat všechny BCP a DRP plány, což umožnilo organizaci získat cennou zpětnou vazbu od byznysu a identifikovat oblasti pro další zlepšení.

Taktéž byla provedena důkladná kontrola správnosti šifrování dat na sdílených úložištích, což je zásadní pro ochranu dat před potenciálními útoky a úniky informací. Ta byla specialisty zhodnocena jako dostatečná.

5.6 Metodologie vyhodnocení

Metodologie vyhodnocení v kontextu implementace bezpečnosti informací a příslušných plánů v organizaci je klíčová pro měření účinnosti zavedených opatření a pro identifikaci oblastí, které vyžadují další zlepšení. Tato metodologie se opírá o kombinaci kvantitativních a kvalitativních přístupů, aby poskytla komplexní přehled o dopadech implementovaných změn na bezpečnostní postavení organizace a její schopnost reagovat na potenciální incidenty.

Kvantitativní vyhodnocení zahrnuje měření a sledování klíčových ukazatelů úspěchu, které poskytují objektivní přehled o dopadech implementovaných změn na systém správy rolí a oprávnění. Jedná se o zaznamenávání počtu identifikovaných a revidovaných externistů a interních uživatelů, což umožňuje organizaci přesně určit rozsah a hloubku provedených úprav. Důležitým indikátorem je také počet odebraných nadbytečných rolí a licencí, který odráží efektivitu procesu revize a optimalizace přístupových práv. Kvantifikovatelný finanční přínos se měří úsporami nákladů dosaženými odstraněním nevyužívaných licencí a racionalizací správy oprávnění. Další klíčový aspekt kvantitativního hodnocení představuje počet úspěšně otestovaných plánů kontinuity činnosti a obnovy po havárii společně s hodnocením zpětné vazby získané během těchto testů, což odhaluje míru připravenosti organizace na potenciální incidenty.

Kvalitativní vyhodnocení se zaměřuje na analýzu zpětné vazby od zaměstnanců a managementu s cílem získat ucelený obraz o vnímání implementovaných změn. Zkoumá se, jak byly přijaty nové procesy a systémy a jak se změnilo bezpečnostní povědomí mezi zaměstnanci v důsledku školení a osvětových aktivit. Hodnotí se rovněž zlepšení v transparentnosti a efektivitě nově zavedených procesů správy rolí a oprávnění a reakcí na bezpečnostní incidenty. Kvalitativní posouzení nabízí cenné vhledy do toho, jak změny ovlivňují organizaci na úrovni jednotlivců i celkové firemní kultury, což umožňuje identifikovat oblasti pro další zlepšení a rozvoj.

5.7 Doporučení dalšího postupu

Na základě hloubkových analýz, realizovaných změn a identifikovaných rizik autorem práce v rámci diplomové práce vyplynulo několik klíčových doporučení, která by měla být vzata v úvahu pro další rozvoj a zlepšování bezpečnostního prostředí a řízení kontinuity činnosti. Jedná se především o nutnost průběžné revize a aktualizace analýz dopadu na byznys, což je základním pilířem pro udržení aktuálního a přesného přehledu o kritičnosti informačních aktiv. Dále je důležité pokračovat v rozšiřování a aktualizaci komplexního mapování dat společně s posilováním ochranných opatření, jako jsou šifrování a přístupové kontroly, aby se zvýšila odolnost proti potenciálním hrozbám.

Zásadní roli hrají také školení a osvětové programy, které by měly být dále rozvíjeny a přizpůsobeny aktuálním kybernetickým výzvám, s cílem posílit povědomí a připravenost zaměstnanců na různé druhy bezpečnostních incidentů. Implementace pravidelných bezpečnostních auditů a kontrol je nezbytná pro zajištění, že všechny bezpečnostní procesy a opatření jsou nejen efektivně implementovány, ale také správně dodržovány a funkční. Dalším klíčovým krokem je posílení procesů reakce na incidenty a obnovy po havárii, včetně pravidelných cvičení a testování plánů, které zajistí, že organizace je připravena rychle a účinně reagovat na případné bezpečnostní incidenty. Posledním doporučením je vnímání důležitosti a podpory inovací a technologického rozvoje v oblasti bezpečnosti informací, aby bylo možné využít nové nástroje a technologie pro lepší detekci hrozeb, ochranu dat a monitorování bezpečnostního prostředí.

Doporučení představují komplexní rámec pro zvyšování bezpečnosti a odolnosti organizace vůči kybernetickým hrozbám a zajišťují, že informační aktiva jsou chráněna v souladu s nejnovějšími standardy a praxemi v oblasti bezpečnosti informací.

6 Závěr

Cílem této diplomové práce bylo definovat klíčové aspekty a výsledky projektu zaměřeného na návrh a implementaci procesů ve vybrané firmě s ohledem na požadavky normy ISO 27001 a zákona o kybernetické bezpečnosti.

V první části diplomové práce byl popsán teoretický rozbor problematiky bezpečnosti informací, její důležitost pro organizace a způsoby kterýmiž může její absence organizaci ohrozit. V druhé části se diplomová práce zabývá praktickou implementací principů ISO 27001 do skutečné organizace. Ze získaných hodnot vyplývá, že implementace těchto principů může organizaci přinést zvýšení bezpečnosti, a tedy zamezení ztrátě dat a s tím spojených problémů, ale i výhody na straně financování celého IT oddělení. Všechny návrhy k implementaci byly realizovány a management včetně CISO hodnotil jejich provedení jako značně přínosné.

Tato diplomová práce je jako celek přínosný příklad pro implementaci ISMS v jiných organizacích ne nutně stejné velikosti. Informace z práce mohou být využity téměř všude, kde se používá IT infrastruktura jako „srdce“ organizace.

7 Seznam použitých zdrojů

(1) ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN ISO/IEC 27001, Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky. 2023

(2) EVROPSKÝ PARLAMENT A RADA EU. Nařízení Evropského parlamentu a Rady (EU) 2016/679, GDPR. 2016/679/EU. 2016

(3) IRWIN, Luke. IT GOVERNANCE. Insider Threats Unveiled: Definition, Types, and Real-Life Examples [online]. 2023 [cit. 2024-02-20]. Dostupné z: https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

(4) WHITMORE, Charles. Unauthorized access. Online. Dostupné z: https://nordvpn.com/blog/unauthorized-access/. [cit. 2024-02-20]

(5) IBM. Cost of a Data Breach Report 2023. Online. IBM.com. 2023. Dostupné z: https://www.ibm.com/reports/data-breach. [cit. 2024-02-16]

(6) ČESKÁ REPUBLIKA. Zákon o kybernetické bezpečnosti. In: . 2014, číslo 181.

(7) SELAMAT, Ali; ABUAGOUB, Ali M. A. a SAEED, Imtithal A. A survey on malware and malware detection systems. Online. Roč. 2013, s. 7. Dostupné z: https://www.researchgate.net/profile/Imtithal-Saeed/publication/272238656_A_Survey_on_Malwares_and_Malware_Detection_Systems/links/566284c608ae192bbf8cf1a5/A-Survey-on-Malwares-and-Malware-Detection-Systems.pdf. [cit. 2024-03-20]

(8) PETROSYAN, Ani. Ransonware attempts per year. Online. In: . 2020. Dostupné z: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/. [cit. 2024-02-19]

(9) PETROSYAN, Ani. Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2022. Online. 2023. Dostupné z: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/. [cit. 2024-02-17]

(10) KASPERSKY. What is Social Engineering? Online. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering. [cit. 2024-02-20]

(11) SALAHDINE, Fatima. Social Engineering Attacks. Online. School of Electrical Engineering and Computer Science, University of North Dakota, 2019. Dostupné z: https://www.mdpi.com/1999-5903/11/4/89. [cit. 2024-03-20]

(12) PETROSYAN, Ani. Annual number of cyber attacks resulting in data compromises in the United States from 2020 to 2023, by type. Online. 2023. Dostupné z: https://www.statista.com/statistics/1367217/us-annual-number-of-cyber-attacks-leading-data-compromises-by-type/. [cit. 2024-02-17]

(13) Consequences of successful phishing attacks on organizations worldwide in 2021 and 2022. Online. PETROSYAN, Ani. Statista. 2022. Dostupné z: https://www.statista.com/statistics/1350723/consequences-phishing-attacks/. [cit. 2024-02-20]

(14) Google, Largest known DDoS attacks. Online. In: . 2020. Dostupné z: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks. [cit. 2024-02-19].

(15) KASPERSKY. Distributed Denial of Service: Anatomy and Impact of DDoS Attacks. Online. Kaspersky. Dostupné z: https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work. [cit. 2024-02-20]

(16) PETROSYAN, Ani. Most common types of insider threats in the United States in 2020 [online]. In: . 2023 [cit. 2024-02-19]. Dostupné z: https://www.statista.com/statistics/1155585/most-common-insider-threat-types-united-states/

(17) PETROSYAN, Ani. Most commonly exploited applications worldwide from November 2021 to October 2022. Online. In: . 2022. Dostupné z: https://www.statista.com/statistics/434880/cyber-crime-common-exploits-global/. [cit. 2024-02-19]

(18) INTEL. Impact of vulnerability. Online. Dostupné z: https://www.intel.com/content/www/us/en/security-center/impact-of-vulnerability.html. [cit. 2024-02-20]

(19) VERIZON. Data breaches 2023 investigations report. Online. Verizon.com. 2023. Dostupné z: https://www.verizon.com/business/resources/reports/dbir/#industry-reports. [cit. 2024-02-19]

(20) BSI. BS 7799 The Code of Practice for information security management. Online. 1995, 1995. Dostupné z: https://standardsdevelopment.bsigroup.com/projects/9023-09086#/section. [cit. 2024-02-19]

(21) KINNE, Jan; MIRTSCH, Mona a BLIND, Knut. Evolution of ISO 9001, ISO 14001, and ISO/IEC 27001 over time in terms of valid certificates worldwide. Online. Č. 2020. Dostupné z: https://www.researchgate.net/figure/Evolution-of-ISO-9001-ISO-14001-and-ISO-IEC-27001-over-time-in-terms-of-valid_fig1_341058937. [cit. 2024-03-20]

(22) LOPEZ, Isabel Maria; GUARDA, Teresa a OLIVIERA, Pedro. How ISO 27001 Can Help Achieve GDPR Compliance. Online. Roč. 2019. Dostupné z: https://ieeexplore.ieee.org/document/8760937. [cit. 2024-03-20]

(23) ISO 27001 Certification Guide: What You Need to Know. Online. Itgovernance. 2022. Dostupné z: https://www.itgovernance.co.uk/iso27001-certification. [cit. 2024-02-20]

(24) HSU, Carol; WANG, Tawei a LU, Ang. The Impact of ISO 27001 Certification on Firm Performance. Online. IEEE. 2016. ISSN 1530-1605. Dostupné z: https://ieeexplore.ieee.org/document/7427787. [cit. 2024-03-20].

(25) IRWIN, Luke. 5 Benefits of ISO 27001 Certification. Online. Itgovernance. 2023. Dostupné z: https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification. [cit. 2024-02-20]

(26) HARPER, Rebecca. Unpacking the Cost vs ROI of Achieving ISO 27001 Certification. Isms. [online]. [cit. 2024-02-20]. Dostupné z: https://www.isms.online/iso-27001/unpacking-the-cost-vs-roi-of-achieving-iso-27001-certification/

(27) Evolution of the Chief Information Security Officer. Cyber intelligence [online]. [cit. 2024-02-20]. Dostupné z: https://cyberintelligence.world/evolution-of-the-chief-information-security-officer/

8 Přílohy

Příloha 1 – Procesní mapa zřízení externisty (vlastní zpracování)
Příloha 2 – Organizační struktura organizace (vlastní zpracování)