

Administrativní bezpečnost z pohledu doxingu

Štěpán Zbořil

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Štěpán Zbořil
Osobní číslo: A22131
Studijní program: B0688A140008 Informační technologie v administrativě
Forma studia: Prezenční
Téma práce: Administrativní bezpečnost z pohledu doxingu
Téma práce anglicky: Administrative Security from the Perspective of Doxing

Zásady pro vypracování

- Vysvětlíte koncept doxingu z pohledu informační bezpečnosti, včetně technických metod používaných při získávání a šíření osobních údajů.
- Analýzujete dostupnost a šíření osobních údajů na platformě Doxbin s důrazem na technologické aspekty šíření dat a využití nástrojů k jejich ochraně.
- Popíšete dopady doxingu na firemní infrastrukturu a IT procesy správy citlivých údajů v administrativních systémech.
- Analýzujete konkrétní případy z praxe, které demonstrují technické způsoby získání a šíření citlivých údajů, a popis technologických zranitelností, které byly zneužity.
- Navrhněte podnikové procesy z hlediska informatické bezpečnosti zaměřených na ochranu dat před doxingem.
- Vizualizujte navrhované procesy pomocí diagramů. Zvolte pro to vhodný modelovací jazyk.

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

Seznam doporučené literatury:

1. BAILEY, Jane; FLYNN, Asher a HENRY, Nicola. *The Emerald international handbook of technology-facilitated violence and abuse. Emerald studies in digital crime, technology and social harms*. Bingley, U.K.: Emerald Publishing Limited, [2021]. ISBN 9781839828508. Dostupné také z: <https://proxy.k.utb.cz/login?url=https://doi.org/10.1108/9781839828485>
2. MERALI, Alameen Karim. *Malware Analysis of Doxbin*. Online. In: . Dostupné z: https://www.researchgate.net/publication/376205490_Malware_Analysis_of_Doxbin. [cit. 2024-10-23]
3. UNG, Siev Thean. *The Cyber Social Phenomenon of Doxing: An Examination of Hong Kong's Anti-doxing Law*. Online. In: . Dostupné z: <https://dspace.cuni.cz/bitstream/handle/20.500.11956/186883/120436570.pdf?sequence=1&isAllowed=y>. [cit. 2024-10-23]
4. MACALLISTER, Julia M. *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*. Online. In: . 2017. Dostupné z: <https://ir.lawnet.fordham.edu/flr/vol85/iss5/21>. [cit. 2024-10-23]
5. MCINTYRE, Victoria. *"Do(x) You Really Want to Hurt Me?": Adapting IIED as a Solution to Doxing by Reshaping Intent*. Online. In: . ISSN 2169-4567. Dostupné z: <https://journals.tulane.edu/TIP/article/view/2667>. [cit. 2024-10-23]
6. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, CISA. *Mitigating the Impacts of Doxing on Critical Infrastructure*. Online. In: . Dostupné z: https://www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxing_508.pdf. [cit. 2024-10-23]

Vedoucí bakalářské práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **4. prosince 2024**

Termín odevzdání bakalářské práce: **9. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Miroslav Matýsek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 4. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Hlavním cílem této bakalářské práce je vytvoření návrhu a vizualizace podnikových procesů zaměřených na zajištění administrativní bezpečnosti v souvislosti s hrozbou doxingu a dalších pojmů, které s ním úzce souvisí. Práce se zabývá návrhem interních procesů a vhodných bezpečnostních opatření, které mají snížit dané hrozby.

Teoretická část práce zahrnuje pojem doxing, jeho příklady a dopady na infrastrukturu. Svě důležité místo zde má i platforma Doxbin. Praktická část obsahuje návrhy konkrétních procesů, jako je například správa přístupových práv, školení zaměstnanců, reakce na bezpečnostní incidenty nebo bezpečné odstranění dat. Tyto procesy byly modelovány pomocí nástroje ARIS Express s využitím notací EPC a BPMN, a to s ohledem na jejich srozumitelnost i technickou zpracovanost.

Výstupem práce je soubor vizuálně zpracovaných diagramů, které mohou být využity v organizacích ke snížení rizika doxingu. Přínosem práce je vytvoření těchto diagramů pro podporu ochrany osobních údajů a zvýšení bezpečnosti v rámci administrativního prostředí.

Klíčová slova: administrativní bezpečnost, doxing, Doxbin, vizualizace procesů, ARIS Express, BPMN, EPC

ABSTRACT

The main objective of this bachelor's thesis is to create a design and visualization of business processes focused on ensuring administrative security in connection with the threat of doxing and other concepts that are closely related to it. The work deals with the design of internal processes and appropriate security measures that are intended to reduce these threats.

The theoretical part of the work includes the concept of doxing, its examples and impacts on the infrastructure. The Doxbin platform also has an important place here. The practical part contains designs for specific processes, such as access rights management, employee training, response to security incidents or secure data deletion. These processes were modeled using the ARIS Express tool using EPC and BPMN notations, with regard to their clarity and technical sophistication.

The output of the work is a set of visually processed diagrams that can be used in organizations to reduce the risk of doxing. The contribution of the work is the creation of these diagrams to support the protection of personal data and increase security within the administrative environment.

Keywords: administrative security, doxing, Doxbins, process visualization, ARIS Express, BPMN, EPC

Rád bych poděkoval vedoucímu této bakalářské práce, Ing. Lukáši Králíkovi, Ph.D., za jeho vedení, ochotu, čas, rady a konzultace, které mi pomohly při tvorbě této práce.

OBSAH

ÚVOD.....	15
I TEORETICKÁ ČÁST	16
1 DEFINICE POJMU DOXING.....	17
1.1 PŘEHLED HISTORICKÉHO KONTEXTU	17
1.2 TECHNICKÉ METODY POUŽÍVANÉ PŘI ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ	19
1.2.1 Veřejně dostupné zdroje.....	19
1.2.2 Sociální inženýrství	19
1.2.3 Podvodné žádosti o nouzová data	20
1.2.4 Hackerské techniky	20
1.2.5 Soukromé databáze a černý trh	20
1.2.6 Kombinace metod	21
1.3 TECHNICKÉ METODY POUŽÍVANÉ PŘI ŠÍŘENÍ OSOBNÍCH ÚDAJŮ	21
1.3.1 Hosting na anonymních a offshore serverech	21
1.3.2 Sdílení na specializovaných platformách	21
1.3.3 Šíření přes anonymní síť	22
1.3.4 Používání sociálních médií a komunikačních aplikací	22
1.3.5 Využití souborových úložišť a pastebinových služeb	22
1.3.6 Automatizace šíření informací	22
1.3.7 Udržování dostupnosti dat.....	22
1.4 ÚČEL DOXINGU	23
1.4.1 Zastrasování a vydírání	23
1.4.2 Pomsta a osobní konflikty	23
1.4.3 Politické a ideologické důvody	23
1.4.4 Diskreditace a profesní poškození.....	24
1.4.5 Finanční podvody a krádeže identity	24
1.4.6 Cílené útoky na organizace a instituce.....	24
1.4.7 Ochrana veřejného zájmu nebo whistleblowing	24
2 VZNIK DOXBINU A JEHO ROZŠÍŘENÍ V KYBERPROSTORU	26
2.1 DOSTUPNOST OSOBNÍCH ÚDAJŮ NA PLATFORMĚ DOXBIN	26
2.1.1 Způsoby zveřejňování a organizace dat	27
2.1.2 Anonymita uživatelů a bezpečnostní opatření	27
2.1.3 Šíření a sdílení informací mimo Doxbin	27
2.1.4 Následky zveřejnění osobních údajů.....	27
2.2 ŠÍŘENÍ OSOBNÍCH ÚDAJŮ NA PLATFORMĚ DOXBIN	28
2.2.1 Formy nahrávání údajů	28
2.2.2 Role anonymity a redistribuce informací	28
2.2.3 Automatizace šíření a dlouhodobá dostupnost.....	28
3 DOPADY DOXINGU NA INFRASTRUKTURU	29
3.1 OHROŽENÍ FYZICKÉ BEZPEČNOSTI	29
3.2 SOCIÁLNÍ INŽENÝRSTVÍ A MANIPULACE ZAMĚSTNANCŮ.....	29

3.3	FINANČNÍ ZTRÁTY A PRÁVNÍ DŮSLEDKY	29
3.4	POŠKOZENÍ REPUTACE A ZTRÁTA DŮVĚRY	29
3.5	PREVENTIVNÍ OPATŘENÍ A OCHRANA INFRASTRUKTURY	30
3.6	DOPADY DOXINGU NA FIREMNÍ INFRASTRUKTURU	30
3.7	DOPADY NA PROCESY SPRÁVY CITLIVÝCH ÚDAJŮ V ADMINISTRATIVNÍCH SYSTÉMECH	31
4	SPECIFICKÉ PŘÍKLADY Z PRAXE	32
4.1	DOXING POMOCÍ RANSOMWAROVÝCH ÚTOKŮ	32
4.1.1	Demonstrace způsobu získání a šíření citlivých údajů u doxingu pomocí ransomwarových útoků	32
4.1.2	Popis zneužitých technologických zranitelností u doxingu pomocí ransomwarových útoků	32
4.2	DOXING POLITICKÝCH AKTIVISTŮ NA UNIVERZITÁCH.....	33
4.2.1	Demonstrace způsobu získání a šíření citlivých údajů u doxingu politických aktivistů na univerzitách.....	33
4.2.2	Popis zneužitých technologických zranitelností u doxingu politických aktivistů na univerzitách.....	33
II	PRAKTICKÁ ČÁST	34
5	NÁVRH PODNIKOVÝCH PROCESŮ Z HLEDISKA INFORMAČNÍ BEZPEČNOSTI ZAMĚŘENÝ NA OCHRANU DAT PŘED DOXINGEM.....	35
5.1	ÚVOD DO PROBLEMATIKY	35
5.1.1	Vysvětlení potřeby ochrany proti doxingu ve firemním prostředí	39
5.1.2	Význam podnikových procesů v rámci bezpečnostní politiky organizace.....	39
5.2	DEFINICE CÍLE NÁVRHU PROCESŮ	39
5.2.1	Hlavní bezpečnostní cíle procesu	40
5.2.2	Ochrana osobních údajů zaměstnanců a klientů.....	40
5.2.3	Reakce na potenciální hrozby doxingu	40
5.3	DOPORUČENÍ PRO OCHRANU PROTI DOXINGU	40
5.4	BALÍČEK NÁSTROJŮ PRO MINIMALIZACI DIGITÁLNÍ STOPY	42
5.5	OSINT NÁSTROJE PRO MINIMALIZACI DIGITÁLNÍ STOPY	43
5.6	PŘEHLED BEZPLATNÝCH NÁSTROJŮ PRO MODELOVÁNÍ BPMN A EPC DIAGRAMŮ.....	44
5.7	VÝBĚR VHODNÉHO MODELOVACÍHO NÁSTROJE.....	45
5.7.1	Představení nástroje ARIS Express	45
5.7.2	Důvody využití ARIS Express	46
5.8	MODELOVACÍ JAZYKY POUŽITÉ PRO NÁVRHY	46
5.8.1	Business Process Model and Notation	46
5.8.2	Event-driven Process Chain	47
5.9	POPIS MODELOVÉHO PŘÍKLADU ORGANIZACE.....	47

5.9.1	Popis aktuálního stavu.....	47
5.9.2	Identifikace slabin v procesech	48
5.10	NÁVRH BEZPEČNOSTNÍCH PODNIKOVÝCH PROCESŮ	48
5.10.1	Proces klasifikace a označování dat	48
5.10.2	Proces řízení přístupových práv	49
5.10.3	Proces školení zaměstnanců v oblasti bezpečnosti	50
5.10.4	Proces reakce na incidenty typu doxing.....	51
5.10.5	Proces šifrování a archivace citlivých dat	52
5.10.6	Zpracování žádosti o přístup k datům	53
5.10.7	Kontrola přístupových práv.....	54
5.11	PŘÍNOSY NAVRŽENÝCH PROCESŮ	55
5.11.1	Zamezení neoprávněnému přístupu	55
5.11.2	Sledovatelnost činností se zabezpečenými daty.....	56
5.11.3	Zvýšení důvěryhodnosti a reputace organizace	56
6	VIZUALIZACE NAVRŽENÝCH PROCESŮ POMOCÍ DIAGRAMŮ	57
6.1	SROVNÁNÍ BUSINESS PROCESS MODEL AND NOTATION A EVENT-DRIVEN PROCESS CHAIN	57
6.2	VÝBĚR PREFEROVANÉHO MODELOVACÍHO JAZYKA PRO DALŠÍ PRÁCI.....	57
6.3	VIZUALIZACE MODELOVÝCH PROCESŮ POMOCÍ EVENT-DRIVEN PROCESS CHAIN	58
6.3.1	Reakce na incident typu doxing	58
6.3.2	Školení zaměstnanců o rizicích doxingu	59
6.3.3	Audit přístupových práv.....	60
6.3.4	Bezpečné mazání dat.....	61
6.3.5	Periodická revize oprávnění po změně pozice	61
ZÁVĚR		63
SEZNAM POUŽITÉ LITERATURY.....		65
SEZNAM OBRÁZKŮ		68
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....		69
SEZNAM PŘÍLOH.....		70

ÚVOD

Do administrativy a vnitřní bezpečnosti organizace zasahuje velké množství hrozeb. Jednou z těchto hrozeb je doxing, který obnáší cílené získávání a následné zveřejňování osobních údajů bez vědomí či svolení dané osoby či organizace. Tento typ útoku může mít za následek narušení soukromí, ztrátu důvěry, odcizení citlivých informací, psychologické dopady nebo právní důsledky. Hlavním cílem této bakalářské práce je proto přiblížit problematiku doxingu z pohledu administrativní bezpečnosti a navrhnout podnikové procesy, které tak pomohou k systematické ochraně citlivých dat a prevenci proti tomuto druhu útoku.

Téma bylo zvoleno s ohledem na jeho aktuálnost a dopad na každodenní chod organizací. I když se stále zvyšuje informovanost o kybernetických rizicích, na doxing se v rámci firemních procesů stále zapomíná, a to hlavně při řízení přístupu a administrativních operacích.

Teoretická část práce se zabývá popisem doxingu, jeho příklady a dopady na infrastrukturu. V teoretické části má své místo i stránka Doxbin, která je s doxingem úzce spojená. Praktická část se věnuje návrhu konkrétních podnikových procesů zaměřených na ochranu dat před doxingem a snižování digitální stopy v prostředí internetu. Tyto procesy byly vizualizovány prostřednictvím softwarového nástroje ARIS Express a modelovány pomocí notací BPMN a EPC.

V závěru práce jsou shrnuty dosažené výsledky a přínos navržených přístupů. Celkovým výstupem je návrh souboru opatření, která mohou organizacím pomoci při zajištění vyšší úrovně informační bezpečnosti v administrativním prostředí.

I TEORETICKÁ ČÁST

1 DEFINICE POJMU DOXING

Doxing, který je označován také jako „doxxing“, je velkým problémem v oblasti digitální bezpečnosti. Tento termín popisuje proces, při kterém jsou bez souhlasu jednotlivce získávány a zveřejňovány jeho citlivé či soukromé údaje do prostředí internetu. Tento postup chce obvykle způsobit oběti újmu, ohrožit její osobní bezpečnost, narušit soukromí nebo poškodit její dobré jméno. Slovo doxing vychází z anglického termínu documents (dokumenty) a vztahuje se k činnosti, při které jsou veřejně odhalovány identity a soukromé informace různých jedinců. [1], [2]

Doxing lze rozdělit do tří hlavních kategorií, a to na základě jeho dopadů na oběť. První kategorií je deanonymizační doxing, který zahrnuje odhalení identity, například zveřejněním osobních údajů osoby, která vystupuje pod nějakým pseudonymem v prostředí sociálních sítí či na internetu jako takovém. Druhou kategorií je cílený doxing, který se zaměřuje na narušení soukromí, například prostřednictvím zveřejnění adresy bydliště nebo telefonního kontaktu dané osoby. Třetí kategorií je delegitimizační doxing, který zahrnuje šíření informací, jež mají oběť zdiskreditovat, například zveřejněním údajného nevhodného chování. Tato praktika se často používá v politickém prostředí. [2]

Z hlediska informační bezpečnosti představuje doxing zásadní hrozbu, která vyžaduje komplexní preventivní strategie, které by měli zahrnovat právní opatření, technické inovace a průběžné vzdělávání veřejnosti. Tato opatření jsou klíčová pro ochranu jednotlivců, veřejnosti a organizací před možnými dopady, jako jsou například psychická újma, ekonomické ztráty nebo dokonce fyzické nebezpečí. [2], [4]

1.1 Přehled historického kontextu

Doxing byl poprvé zaznamenán v rámci hackerských komunit 90. let, kdy se technika s názvem „drop dox“ (zveřejnění dokumentů) začala používat jako nástroj k odhalení identity anonymních uživatelů na internetu. Tato metoda byla původně využívána mezi jednotlivými členy hackerských skupin, často jako prostředek pomsty nebo jako forma určitého nátlaku. [1], [5]

Postupem času byla tato strategie rozšířena a začala nacházet uplatnění v širším kontextu. Na přelomu 21. století se s nástupem internetu a větší dostupností osobních informací stal doxing vážnou hrozbou. Tato hrozba nezasáhla pouze jednotlivce, ale ovlivnila i celou společnost. Bylo doloženo, že první rozsáhlé případy doxingu byly spojeny

s platformami jako 4chan a později s weby typu Pastebin, které umožňovaly anonymní sdílení textových dokumentů s osobními údaji obětí. [5], [6]

V první dekádě 21. století byl doxing stále častěji spojován s politickými a sociálními konflikty. Například skupina Anonymous využívala doxing, pomocí kterého docházelo k veřejnému odhalování osob obviňovaných z neetického či nezákonného chování. Tento přístup však vyvolával etické otázky, protože zveřejňování citlivých informací mělo často za následek značné důsledky pro oběti, včetně obtěžování, vyhrožování násilím nebo také ztrátu zaměstnání. [2], [3]

Od poloviny první dekády 21. století byl doxing centralizován na specializovaných platformách, jako je Doxbin. Tato platforma vznikla jako místo, kde bylo možné zveřejňovat osobní údaje obětí s minimální pravděpodobností toho, že by došlo k jejich odstranění. Web Doxbin se stal centrem aktivit doxerů a tím tak získal rozsáhlou uživatelskou základnu. Bylo prokázáno, že tato platforma podporovala zveřejňování soukromých informací a napomáhala k zastrašování obětí, například prostřednictvím hrozeb zveřejnění údajů širší veřejnosti. [5], [6]

V posledních letech byla činnost některých významných skupin doxerů, jako je například ViLE, detailněji zkoumána a stíhána. Skupina ViLE se proslavila získáváním citlivých dat prostřednictvím nelegálních technik, včetně zneužití federálních databází a podvodného podávání žádostí o nouzová data (Emergency Data Requests). Tyto metody byly často používány k sestavení podrobných doxů, které obsahovaly jména, adresy, telefonní čísla a další citlivé osobní údaje. [5]

S rostoucím povědomím o rizicích spojených s doxingem začaly státní instituce a mezinárodní organizace zavádět opatření k jeho regulaci. Byly zavedeny legislativní rámce, které trestají neoprávněné šíření osobních údajů, avšak kvůli globální povaze internetu a doxerských komunit je vynucování těchto pravidel velmi často komplikované. Přesto zůstává doxing v mnoha zemích legální kvůli právním mezerám, například kvůli ochraně poskytovatelů obsahu prostřednictvím zákona o ochraně komunikace (Communications Decency Act, sekce 230) v USA. [5]

1.2 Technické metody používané při získávání osobních údajů

Získávání informací v oblasti doxingu je proces, který kombinuje různé metody a nástroje pro shromažďování citlivých údajů o konkrétních osobách nebo organizacích, kterým se bude potenciální dox zabývat. Tyto postupy jsou navrženy tak, aby využívaly zranitelností jak v digitální bezpečnosti, tak v sociálním prostředí. Následuje detailní přehled klíčových metod, které jsou při těchto aktivitách využívány.

1.2.1 Veřejně dostupné zdroje

Veřejně dostupné zdroje, které jsou známy jako Open-Source Intelligence (OSINT) představují jednu z nejjednodušších, ale překvapivě velmi efektivních metod získávání informací. Často jsou detailně analyzovány sociální sítě, kde oběti bez jejich vědomí zveřejňují jejich osobní informace, jako jsou jména, pracovní pozice, fotografie, data narození nebo dokonce aktuální poloha prostřednictvím příspěvků, které obsahují geotagy.

Tyto údaje bývají doplňovány informacemi z veřejných registrů, například obchodního rejstříku, katastru nemovitostí nebo soudních databází, které jsou snadno přístupné online. Různé blogy, webové stránky nebo diskusní fóra mohou rovněž obsahovat informace a tím pádem i důležité zdroje pro vytvoření podrobného profilu oběti. [1], [2], [5]

Sociální platformy jako jsou Facebook, Instagram, X, Discord, TikTok, Snapchat nebo LinkedIn umožňují doxerům vytvářet mapy sociálních a profesních souvislostí dané oběti. Například fotografie označené přáteli mohou odhalit osobní vztahy oběti, zatímco profesní profily mohou poskytnout údaje o pracovní historii a někdy dokonce i kontaktní informace. Tato data jsou následně využívána k manipulaci nebo jako základ pro aplikaci dalších technik. [5]

1.2.2 Sociální inženýrství

Sociální inženýrství je považováno za jednu z nejmanipulativnějších a zároveň také nejúčinnějších metod získávání citlivých informací. Tato technika spočívá v tom, že jsou cílené osoby nebo třetí strany manipulovány k dobrovolnému poskytnutí citlivých údajů, aniž by si byly vědomy skutečného záměru útočníka. Často se útočníci vydávají za pracovníky technické podpory, zaměstnance banky nebo jiné důvěryhodné osoby, aby přesvědčili oběť o nutnosti sdílení hesel, přístupových údajů nebo dalších citlivých dat. [5]

Tato metoda je často zaměřena i na organizace, například poskytovatele telekomunikačních služeb. V těchto případech jsou zaměstnanci manipulováni k tomu, aby

poskytnou citlivé informace o klientech, jako jsou adresy nebo telefonní čísla. Tato data jsou poté využívána k vytvoření detailního profilu oběti nebo k dalším formám zneužití. [5]

1.2.3 Podvodné žádosti o nouzová data

Podvodné žádosti o nouzová data neboli Emergency Data Requests (EDR) představují poměrně vyspělou metodu, při níž jsou zneužívány procesy navržené pro ochranu široké veřejnosti. Tyto žádosti bývají standardně využívány orgány činnými v trestním řízení k rychlému získání přístupu k důležitým informacím v naléhavých situacích. Útočníci však tento proces manipulují tím, že si zajistí přístup k vládním e-mailovým adresám nebo nepravdivě ověří svou identitu skrz autentizační portály.

Tímto způsobem mohou od poskytovatelů služeb získat data, jako jsou IP adresy, e-mailové adresy, telefonní čísla a fyzické adresy. Tyto informace se následně používají v dalších fázích útoku, například k zastrašování obětí nebo k vytvoření podrobného doxu, který je později zveřejněn například na platformě Doxbin. [5]

1.2.4 Hackerské techniky

Když veřejně dostupné a manipulativní metody nezajistí dostatečné a podrobné množství informací, dochází k využití hackerských technik. Mezi tyto techniky patří například přímé útoky na systémy, zneužívání zranitelností webových aplikací nebo distribuce škodlivého softwaru. Malware je často maskován jako legitimní nástroj, například „autodox“ aplikace, které se tváří, že nabízejí užitečné funkce, ale ve skutečnosti obsahují skrytý škodlivý kód. Tento malware může napadnout zařízení obětí a shromažďovat citlivá data, jako jsou hesla, přihlašovací údaje nebo finanční informace. [5], [6]

Také bylo zjištěno, že některé hackerské techniky jsou zaměřeny na zneužívání zranitelností v síťové infrastruktuře nebo na napadení cloudových úložišť, kde mohou být uloženy velké objemy dat uživatelů. Tato data jsou poté získávána a využita k dalším účelům, například ke zveřejnění nebo k dalšímu prodeji. [5]

1.2.5 Soukromé databáze a černý trh

Doxing také často bere informace ze soukromých databází, které mohou být zakoupeny na černém trhu nebo získány od osob pracujících uvnitř různých organizací. Tyto databáze obsahují informace, jako jsou čísla sociálního zabezpečení, záznamy o zaměstnání, historie transakcí nebo zdravotní dokumentace.

Na černém trhu jsou tyto databáze často nabízeny za relativně nízké ceny, což jejich získání značně usnadňuje. Také bylo doloženo, že doxeři tyto zdroje používají pro zlepšení a zpřesnění doxů, aby tím tak zajistili vyšší kvalitu zveřejněných informací. [5]

1.2.6 Kombinace metod

Pro zvýšení účinnosti jsou často dohromady kombinovány výše popsané techniky. Data získaná z metody OSINT bývají propojena s informacemi získanými hackerskými útoky nebo prostřednictvím podvodných žádostí o nouzová data. Tento přístup umožňuje vytvoření detailního a přesného profilu oběti. Například zde dojde k propojení informací z veřejných registrů s daty získanými malwarovými útoky. To všechno zajišťuje, že doxeři mají přístup nejen k základním údajům, ale i k velmi vysoce citlivým osobním nebo finančním datům. [2], [3], [5]

1.3 Technické metody používané při šíření osobních údajů

Při šíření osobních údajů v rámci doxingu je využívána široká škála technických metod, které zajišťují anonymitu útočníků, rozšiřují dosah zveřejněných informací a podporují jejich přístupnost na různých platformách. Tyto techniky jsou často přizpůsobovány konkrétním cílům a podmínkám při kterých jsou data šířena.

Všechny technické metody používané při šíření dat v rámci doxingu se postupně vyvíjejí. Útočníci upravují své přístupy podle změn technologického prostředí a zlepšují svou efektivitu pomocí různých moderních postupů. Tyto postupy představují zásadní problém pro vytvoření vhodných opatření na ochranu dat.

1.3.1 Hosting na anonymních a offshore serverech

Osobní údaje bývají šířeny prostřednictvím serverů, kde nejsou zákony na ochranu osobních údajů dostatečně přísné. Tyto servery, které jsou označovány jako offshore hosting, poskytují vyšší míru anonymity a chrání útočníky před právními důsledky. Například platforma Doxbin byla provozována na „bulletproof hostinzích“, které minimalizují zásahy třetích stran a umožňují dlouhodobé uchovávání zveřejněných dat. [5], [7]

1.3.2 Sdílení na specializovaných platformách

Mezi známé platformy sloužící k šíření citlivých údajů patří Doxbin. Tato platforma uživatelům umožňuje zveřejňovat informace o obětech formou veřejných či soukromých doxů. Přístup k soukromým doxům je omezen na uživatele s prémiovými účty, které generují

příjmy pro provozovatele této platformy. Tento model umožňuje, aby osobní údaje byly sdíleny cíleně a efektivně v rámci uzavřených skupin. [7]

1.3.3 Šíření přes anonymní síť

K šíření dat se často využívají anonymní sítě, které poskytují možnost skrytí identity útočníků, uživatelů i lokalizace serverů. Jednou z nich je například Tor. Tyto sítě tak dělají proces šíření dat velmi obtížně sledovatelným a právně se tak špatně postihuje. Data jsou často publikována na dark webu, který zajišťuje jejich dostupnost širšímu okruhu útočníků. [5], [7]

1.3.4 Používání sociálních médií a komunikačních aplikací

Sociální média a různé komunikační aplikace jsou dalšími nástroji, které se používají k šíření citlivých údajů. Skupiny na těchto platformách, jako například na Telegramu nebo uzavřené komunity na Discordu, slouží ke sdílení informací v reálném čase. Tyto zmíněné platformy umožňují rychlý proces výměny dat mezi jejich členy a tím tak snižují pravděpodobnost odhalení. [5]

1.3.5 Využití souborových úložišť a pastebinových služeb

Osobní údaje jsou také ukládány a šířeny prostřednictvím veřejných či šifrovaných úložišť, patří sem například Google Drive, Mega nebo pastebinové služby. Pastebinová platforma, jako je Pastebin.com, umožňuje zveřejňování textových souborů, které obsahují citlivé informace bez složitého ověřování identity. Tyto služby jsou oblíbené pro svou jednoduchost a anonymitu. Zveřejněné informace se zobrazují ve velmi jednoduchém formátu pro jejich čtení. [1], [7]

1.3.6 Automatizace šíření informací

Pro účinné šíření dat jsou využívány i automatizované nástroje. Existují různé skripty, které umožňují hromadné nahrávání doxů na platformy nebo jejich distribuci pomocí botnetů. Tato automatizace totiž zajišťuje rychlé a lehké šíření údajů. [5], [6]

1.3.7 Udržování dostupnosti dat

K zajištění dlouhodobé dostupnosti citlivých informací, dochází k nahrávání dat na redundantní servery nebo k jejich šifrování, které chrání jejich obsah před zásahem třetích stran. Transparentní reporty, jako například ty, které spravuje platforma Doxbin, mají

vytvářet dojem důvěryhodnosti a zároveň chránit provozovatele před právní odpovědností. Tyto postupy dokazují, jak důkladně jsou tyto mechanismy šíření dat promyšlené a využívány. [7]

1.4 Účel doxingu

Doxing je prováděn z různých důvodů v závislosti na úmyslech útočníků a také na zaměřené skupině obětí. Tento postup, při kterém jsou osobní informace neoprávněně získávány, publikovány a dále šířeny, může být využit s cílem způsobit psychickou, společenskou, finanční či dokonce fyzickou újmu. Následky těchto útoků mohou být rozsáhlé a zasáhnout nejen jednotlivce, ale také organizace a klíčovou infrastrukturu podniků či státu. Níže je uveden podrobný přehled hlavních motivací doxingu a jeho účelů.

1.4.1 Zastrasování a vydírání

Jedním z nejčastějších cílů doxingu je zastrašení obětí. Zveřejněním sesbíraných citlivých informací, jako jsou adresy bydliště, telefonní čísla, osobní údaje nebo údaje o rodině, je na oběť vyvíjen velký psychologický tlak, který ji může přimět ke změně chování. Tato taktika je často namířena proti novinářům, aktivistům či politickým odpůrcům s cílem potlačit jejich veřejné aktivity, umlčet je či zastrašit. [1], [2]

Doxing bývá rovněž používán k vydírání, kdy dané oběti hrozí zveřejnění jejich citlivých údajů, pokud nesplní určité podmínky. Tento typ doxingu může zahrnovat finanční požadavky, nátlak k určitému jednání nebo manipulaci obětí, aby vykonala kroky v zájmu útočníka. [3]

1.4.2 Pomsta a osobní konflikty

Často je doxing prováděn také jako forma pomsty. Tento motiv se obvykle vyskytuje v osobních konfliktech, například mezi bývalými partnery, kolegy nebo členy internetových či herních komunit. Osobní údaje jsou zveřejňovány s cílem poškodit oběť, vystavit ji obtěžování nebo narušit její osobní či profesní život. [5], [6]

1.4.3 Politické a ideologické důvody

V politických a ideologických konfliktech je doxing často využíván jako prostředek nátlaku. Během protestů, volebních kampaní nebo geopolitických krizí jsou osobní údaje odpůrců zveřejňovány s cílem je veřejně zdiskreditovat, zastrašit nebo vystavit fyzickému ohrožení.

Tento postup byl zaznamenán například v rámci aktivit hnutí Anonymous či u jiných aktivistických skupin. [2], [6]

1.4.4 Diskreditace a profesní poškození

Doxing je také používán k poškození profesní pověsti jednotlivců. Zaměstnanci, akademičtí pracovníci, novináři či veřejně činné osoby se mohou stát terčem doxingu, při kterém jsou jejich osobní údaje zveřejňovány s cílem vyvolat negativní reakce veřejnosti na ně samotné nebo na jejich zaměstnavatele. Tento přístup bývá často doprovázen šířením dezinformací či úmyslnou manipulací s obsahem, aby byla oběť prezentována v negativním světle. [5]

1.4.5 Finanční podvody a krádeže identity

Doxing se též využívá k finančním podvodům. Získané informace, jako jsou údaje o kreditních kartách, přihlašovací údaje k bankovním účtům nebo přístupové kódy, mohou být využity k nelegálním transakcím, odcizení finančních prostředků či k získání a následnému zneužití celé bankovní identity. Osobní data obětí mohou být dále prodávána na černém trhu nebo použita k dalším kybernetickým útokům, jako je phishing nebo sociální inženýrství. [6]

1.4.6 Cílené útoky na organizace a instituce

Kromě jednotlivců může být doxing namířen také proti organizacím, institucím či státům. Kritická infrastruktura, veřejné instituce nebo soukromé společnosti se mohou stát cílem útoků prostřednictvím zveřejnění citlivých údajů zaměstnanců či interních dokumentů. Takové incidenty mohou vést k narušení provozu, poškození reputace nebo dokonce ke zvýšeným bezpečnostním rizikům. V těchto případech útočníci velmi často požadují výkupné za zaručení toho, že získané údaje a dokumenty nebudou zveřejněny. [4], [5]

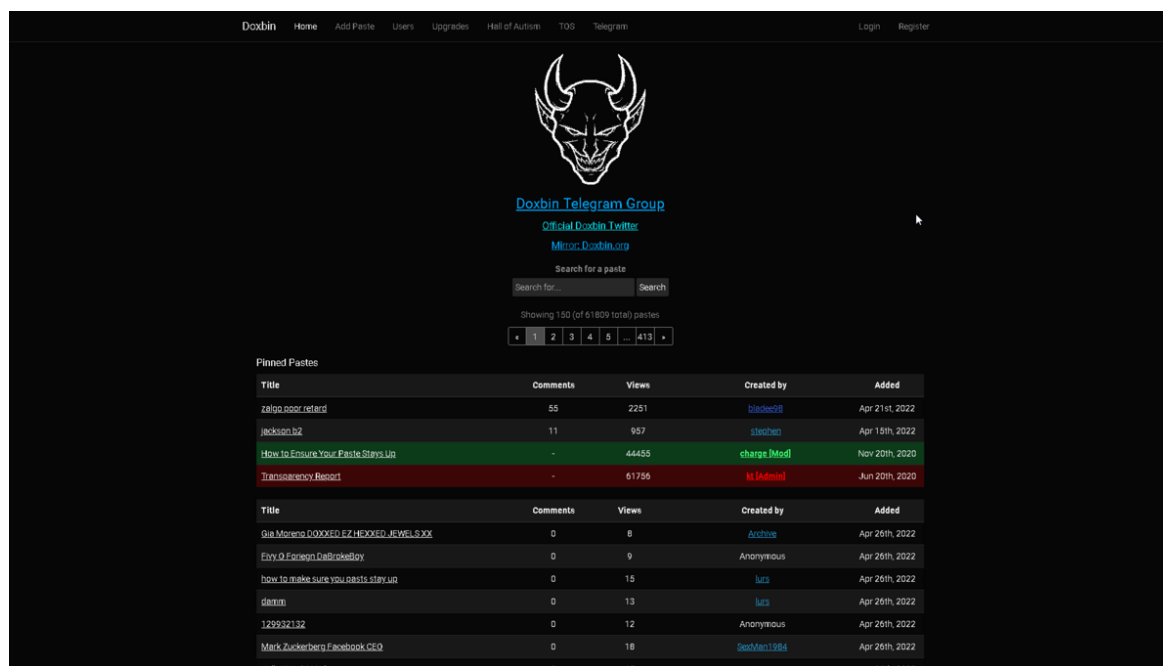
1.4.7 Ochrana veřejného zájmu nebo whistleblowing

Přestože je doxing obecně považován za neetickou a v mnoha případech i nezákonnou praxi, někdy bývá využíván k odhalení nelegálních nebo neetických aktivit. Investigativní novináři a různí oznamovatelé mohou zveřejňovat citlivé informace o veřejných činitelích, korporacích nebo státních institucích s cílem upozornit na závažná pochybení, úplatkářství či nekalou soutěž. Tento typ doxingu však zůstává eticky kontroverzní, jelikož i v těchto případech může vést k ohrožení soukromí a bezpečnosti osob, kterých se tento případ týká. [2]

Účel doxingu se odvíjí od záměrů jednotlivých útočníků. S tím přitom souvisí způsobené následky, které mohou být velmi vážné. Přestože určité formy doxingu bývají někdy obhajovány jako nástroj v boji proti neetickému jednání či korupci, většina případů představuje obrovský zásah do soukromí a ohrožení bezpečnosti. Z tohoto důvodu je doxing vnímán jako vážná hrozba, která vyžaduje odpovídající právní a bezpečnostní opatření.

2 VZNIK DOXBINU A JEHO ROZŠÍŘENÍ V KYBERPROSTORU

Doxbin vznikl v roce 2011 jako specializovaná platforma zaměřená na sdílení osobních informací jednotlivců bez jejich vědomí či svolení. Jeho hlavním záměrem bylo vytvoření centralizovaného úložiště určeného pro zveřejňování citlivých údajů, které by bylo snadno dostupné široké komunitě uživatelů zabývajících se doxingem. Platforma umožňovala anonymní nahrávání i vyhledávání dat a tím se tak rychle stala nástrojem pro identifikaci osob a jejich veřejnou diskreditaci. [5], [6]



Obrázek 1 - Úvodní stránka Doxbinu

(zdroj: [16])

Na uvedeném obrázku (Obrázek 1) je zachycena úvodní stránka, která se zobrazí při návštěvě webu Doxbin. Tento web se v průběhu let stal nejen místem pro zveřejňování citlivých údajů, ale také komunitním centrem, kde si uživatelé vyměňovali informace a strategie související s doxingem. Aktivita této komunity přispěla k udržení platformy v provozu a podporovala šíření zveřejněných dat na další internetová úložiště a diskusní fóra. Díky této činnosti se Doxbin zařadil mezi nejznámější a nejkontroverznější nástroje v oblasti kybernetických hrozeb spojených s doxingem. [5]

2.1 Dostupnost osobních údajů na platformě Doxbin

Platforma Doxbin byla navržena jako anonymní úložiště, kde mohly být osobní údaje jednotlivců publikovány a šířeny bez jejich vědomí či svolení. Její struktura a způsob

fungování zajišťovaly snadný přístup k citlivým informacím široké komunitě uživatelů. Díky tomu se Doxbin stal jednou z nejznámějších platform spojených s doxingem a vážným narušením soukromí jednotlivců. [5], [6]

2.1.1 Způsoby zveřejňování a organizace dat

Na této platformě jsou osobní údaje zveřejňovány ve formě doxů, což jsou textové soubory obsahující podrobné informace, jako jsou jména, adresy, telefonní kontakty, e-mailové adresy, rodinné kontakty, profily na sociálních sítích a v některých případech i finanční či zdravotní data obětí. Tyto soubory bývají systematicky organizovány podle specifických kritérií, aby bylo jejich vyhledávání a sdílení co nejjednodušší. Přístup k veřejným doxům je umožněn všem návštěvníkům platformy, zatímco soukromé doxy byly dostupné pouze uživatelům s vyšším statusem nebo placeným členstvím. [6]

2.1.2 Anonymita uživatelů a bezpečnostní opatření

Doxbin byl provozován na anonymních serverech, což útočníkům poskytovalo vysokou úroveň ochrany před odhalením. K přístupu na platformu bylo často využíváno připojení prostřednictvím sítě Tor, která maskovala skutečné IP adresy uživatelů a znemožňovala jejich snadnou identifikaci. Kromě toho byla data ukládána na šifrovaná úložiště, což znemožňovalo jejich snadné odstranění právními zásahy. Tato bezpečnostní opatření výrazně přispěla k dlouhodobé dostupnosti zveřejněných údajů. [5]

2.1.3 Šíření a sdílení informací mimo Doxbin

Osobní údaje zveřejněné na Doxbinu se často dostávaly i mimo platformu. Po jejich zveřejnění byly doxy přebírány a šířeny prostřednictvím dalších internetových fór, pastebinových služeb či šifrovaných komunikačních aplikací, jako je Telegram. Tento způsob distribuce znemožňoval efektivní odstranění citlivých informací a zajišťoval jejich dlouhodobou přístupnost v online prostředí. [6]

2.1.4 Následky zveřejnění osobních údajů

Dostupnost citlivých údajů na Doxbinu vedla k závažným důsledkům pro oběti, které se stávaly terčem obtěžování, vydírání či dokonce fyzického nebezpečí. V některých případech byly tyto informace zneužity ke krádežím identity, finančním podvodům nebo jiným kybernetickým útokům. Právě kvůli těmto negativním dopadům se Doxbin stal jedním z

hlavních cílů organizací zabývajících se kybernetickou bezpečností a ochranou soukromí. [5]

2.2 Šíření osobních údajů na platformě Doxbin

Na platformě Doxbin jsou osobní údaje šířeny pomocí mechanismů, které byly vytvořeny tak, aby umožňovaly volné a rozsáhlé sdílení informací bez možnosti jejich účinného odstranění. Data zveřejněná na této platformě jsou následně rozšiřována nejen v rámci samotného Doxbinu, ale i napříč kyberprostorem, což značně komplikuje ochranu soukromí dotčených jednotlivců. [5], [6]

2.2.1 Formy nahrávání údajů

Útočníci na Doxbin nahrávají své vytvořené doxy se všemi získanými informacemi, které se jim podařilo o jejich obětech najít a sesbírat. Systém Doxbinu je dále nastaven tak, aby byla tato data snadno dostupná a jejich odstranění značně ztíženo. To zaručuje, že jednou zveřejněné informace zůstávají v archivu a mohou být opakovaně šířeny mezi jednotlivými uživateli. [6]

2.2.2 Role anonymity a redistribuce informací

Anonymita je zajišťována speciálními hostingovými technologiemi a anonymními sítěmi, které výrazně podporují distribuci těchto údajů. Uživatelům je umožněno publikovat informace bez nutnosti odhalení vlastní identity, což vede k masovému zveřejňování doxů a jejich rychlému šíření. Tato anonymita také usnadňuje šíření informací prostřednictvím odkazů, které jsou následně sdíleny na sociálních sítích, internetových fórech nebo pastebinových platformách. [5]

2.2.3 Automatizace šíření a dlouhodobá dostupnost

Mechanismus kopírování a opětovného zveřejňování dat hraje důležitou roli při zajištění trvalé dostupnosti osobních údajů. Když jsou informace zveřejněny, bývají často stahovány, archivovány a následně sdíleny na dalších platformách. Tímto způsobem se tak výrazně prodlužuje jejich životnost. Automatizované nástroje, včetně různých programů, jsou využívány k hromadnému nahrávání doxů. Tyto nástroje tak umožňují jejich rychlou distribuci s minimálními nároky na úsilí ze strany útočníků. [5]

3 DOPADY DOXINGU NA INFRASTRUKTURU

Doxing ovlivňuje nejen jednotlivce, ale i celkovou bezpečnost a stabilitu organizací. Během těchto útoků jsou citlivé informace získávány a následně zveřejňovány s úmyslem poškodit infrastrukturu dané organizace. Zveřejnění těchto údajů může mít vážné dopady, se kterými se bude muset napadená organizace určitým způsobem vypořádat. [8]

3.1 Ohrožení fyzické bezpečnosti

Zveřejnění adres a stavebních plánů může vést k neoprávněnému vniknutí do chráněných prostor organizace, čímž se výrazně zvyšuje riziko narušení fyzické bezpečnosti. Kritická infrastruktura, jako jsou serverová centra nebo síťové uzly, se tak může stát terčem neoprávněných osob. To dále může vést k sabotáži nebo odcizení důležitých datových nosičů. [8]

3.2 Sociální inženýrství a manipulace zaměstnanců

Informace získané o zaměstnancích mohou být útočníky zneužity k provádění pokročilých forem sociálního inženýrství. Osobní údaje mohou být využity k vydávání se za důvěryhodné osoby s cílem získat přístup k firemním systémům nebo k citlivým údajům organizace. Tento typ útoku představuje vážnou hrozbu pro bezpečnost IT infrastruktury, jelikož standardní bezpečnostní opatření, jako jsou firewally nebo antivirové programy, nejsou proti těmto metodám dostatečně efektivní. [8]

3.3 Finanční ztráty a právní důsledky

Úspěšné útoky spojené s doxingem mohou organizacím způsobit značné finanční ztráty. Tyto škody mohou vzniknout v důsledku přímé krádeže dat, poškození hardware nebo nákladů na obnovu narušených systémů. Organizace může zároveň čelit právním následkům, pokud dojde k úniku chráněných firemních informací či údajů o zaměstnancích. To všechno může vyústit v soudní spory s poškozenými účastníky. Může také dojít k udělení vysokých pokut regulačními orgány. [8]

3.4 Poškození reputace a ztráta důvěry

Incidenty, při kterých došlo k doxingu mohou vážně narušit důvěryhodnost organizace. Zveřejnění citlivých informací o zaměstnancích, klientech nebo obchodních partnerech může vést k oslabení důvěry a negativně ovlivnit obchodní vztahy. Společnosti, které se

stanou terčem doxingu, mohou čelit dlouhodobým problémům při obnově svého dobrého jména a reputace na trhu. [8]

3.5 Preventivní opatření a ochrana infrastruktury

Aby se snížily negativní dopady doxingu na infrastrukturu, organizace by měly přijmout bezpečnostní opatření, která se zaměřují jak na prevenci, tak na rychlou reakci v případě incidentu. Jedním z klíčových prvků ochrany je pravidelné školení zaměstnanců, které jim umožní lépe identifikovat pokusy o sociální inženýrství a osvojit si zásady bezpečného chování. Díky tomu lze významně omezit pravděpodobnost úspěšného útoku. [8]

Další důležitou oblastí je ochrana osobních údajů, která zahrnuje zavedení přísných pravidel pro manipulaci s citlivými informacemi. Mezi základní opatření patří například omezení sdílení těchto údajů na veřejných platformách, využívání pokročilých metod šifrování a důsledná kontrola přístupových oprávnění, která přispívá k minimalizaci rizika neoprávněného úniku dat. [8]

Neodmyslitelnou součástí obrany proti doxingu jsou také technická opatření, mezi které patří implementace pokročilých systémů pro detekci neoprávněných průniků, nasazení firewallů a zavedení vícefaktorové autentizace. Tyto prvky výrazně zvyšují úroveň ochrany IT infrastruktury a zároveň snižují riziko zneužití přístupových údajů neoprávněnými osobami. [8]

Mimo tyto preventivní kroky hraje zásadní roli i průběžné monitorování a rychlá reakce na bezpečnostní hrozby. Pravidelná analýza síťového provozu pomáhá včas odhalit podezřelé aktivity a umožňuje organizacím efektivně zasáhnout. Tím tak lze minimalizovat případné škody způsobené doxingem. Důslednou implementací těchto opatření lze významně snížit riziko kybernetických útoků a posílit bezpečnost organizace. To zajistí ochranu nejen její infrastruktury, ale také citlivých údajů zaměstnanců a klientů. [8]

3.6 Dopady doxingu na firemní infrastrukturu

Doxing představuje pro firemní infrastrukturu závažné riziko. Útočníci získávají citlivé údaje, například adresy zaměstnanců, telefonní kontakty či firemní e-mailové adresy, které mohou být následně zneužity k útokům na interní systémy nebo k narušení fyzické bezpečnosti organizace. [8]

Zveřejnění informací o infrastruktuře, včetně plánů budov či umístění serverů, může vést k neoprávněnému přístupu do zabezpečených prostor. Tím se zvyšuje pravděpodobnost sabotáže nebo fyzických útoků na klíčové prvky, jako jsou datová centra nebo síťová zařízení. Tyto aktivity tak mohou zásadně narušit provoz celé organizace. [8]

Údaje o zaměstnancích mohou být zneužity v rámci útoků sociálního inženýrství. Útočníci se mohou vydávat za interní pracovníky nebo externí dodavatele s cílem získat přístup k firemním systémům. Takovým způsobem mohou obejít standardní bezpečnostní opatření a získat přístup ke kritickým datům nebo do interních databází. [8]

Doxing může mít také významné finanční důsledky. Organizace mohou čelit ztrátám v důsledku úniku citlivých informací, poškození hardwaru nebo vysokých nákladů na obnovu narušených systémů. Navíc může dojít k právním důsledkům v případě porušení ochrany osobních údajů, což může vést k vysokým pokutám a soudním sporům. Kromě přímých finančních škod ohrožuje doxing i pověst organizací. Zveřejnění citlivých informací může oslabit důvěru klientů a obchodních partnerů. Tímto způsobem tak útočníci na dlouhou dobu negativně ovlivní stabilitu firmy i její obchodní aktivity. [8]

3.7 Dopady na procesy správy citlivých údajů v administrativních systémech

Administrativní systémy jsou v důsledku doxingu vystaveny riziku neoprávněného přístupu. Útočníci mohou využít zveřejněné citlivé informace k obejití bezpečnostních opatření. Dále to může vést až k narušení provozu systémů a ohrožení jejich bezpečnosti. To všechno může mít negativní dopad na důvěru uživatelů a poškodit celkovou stabilitu organizace. [4]

K tomu, aby se minimalizovaly dopady doxingu na správu citlivých údajů, je nutné zavést odpovídající bezpečnostní opatření. Mezi tyto klíčové strategie patří šifrování citlivých dat, pravidelná aktualizace bezpečnostních protokolů a školení zaměstnanců v oblasti kybernetické bezpečnosti. Tato opatření mohou pomoci chránit administrativní systémy před hrozbami souvisejícími s doxingem a zajistit bezpečné nakládání s citlivými informacemi. [4]

4 SPECIFICKÉ PŘÍKLADY Z PRAXE

V praxi stále dochází k případům, kdy jsou důvěrné informace zveřejňovány v souvislosti s politickou angažovaností, pracovním postavením či osobními spory. Mezi nejčastější oběti doxingu patří novináři, aktivisté, státní úředníci a soukromé osoby. [8]

S narůstající digitalizací a snadnou dostupností osobních údajů na internetu představuje doxing stále větší hrozbu pro bezpečnost. Organizace i jednotlivci proto musí čelit překážce, jak efektivně chránit své citlivé údaje a snížit riziko jejich neoprávněného zveřejnění. [9]

4.1 Doxing pomocí ransomwarových útoků

Jako první příklad zde lze okomentovat incident, který se odehrál v roce 2021, kde se průmyslové společnosti staly jedním z hlavních cílů ransomwarových útoků, při kterých útočníci zašifrovali firemní data, ale také získané informace zveřejňovali jako prostředek nátlaku. Firmy, které odmítly výkupné zaplatit poté dále čelily doxingu, při kterém byly zveřejněny citlivé interní dokumenty, personální informace, obchodní strategie i smlouvy. Získané materiály byly šířeny na specializovaných darknetových platformách. Tyto události vedly nejen k finančním ztrátám, ale také k vážnému narušení reputace a právním komplikacím. [10], [11]

4.1.1 Demonstrace způsobu získání a šíření citlivých údajů u doxingu pomocí ransomwarových útoků

Útočníci pronikli do firemních sítí prostřednictvím ransomwaru a zaměřili se na organizace s nedostatečně chráněnými IT systémy a slabou správou uživatelských oprávnění. Ke zveřejnění získaných informací využili nejen darknetová fóra, ale i sociální sítě. Tímto způsobem tak zvýšili dosah úniku a zvětšili tlak na oběti, aby požadovanou částku zaplatily. [10], [11]

4.1.2 Popis zneužitých technologických zranitelností u doxingu pomocí ransomwarových útoků

Mezi zranitelnosti, které byly v tomto případě zneužity, patřilo používání zastaralých softwarů, nedostatečné zabezpečení vzdáleného přístupu a chybějící vícefaktorová autentizace. Tyto slabiny útočníkům umožnily získat neoprávněný přístup do systémů a následně odcizit citlivé údaje. To následně vedlo k rozsáhlému doxingu průmyslových firem. [10], [11]

4.2 Doxing politických aktivistů na univerzitách

Jako druhý příklad lze uvést událost z roku 2023, kdy se terčem doxingu stali studenti a aktivisté z několika amerických univerzit, kteří se veřejně angažovali v politických a sociálních otázkách. Jejich osobní údaje jako jména, fotografie, adresy a univerzitní e-maily byly zveřejněny na extremistických diskusních fórech s cílem vyvolat strach a ohrozit jejich budoucnost. Tento incident ukázal, jak snadno mohou být veřejně dostupné informace zneužity k cílenému obtěžování a kybernetickým útokům. [8], [9]

4.2.1 Demonstrace způsobu získání a šíření citlivých údajů u doxingu politických aktivistů na univerzitách

Útočníci získali údaje o aktivistech z veřejných univerzitních databází, sociálních sítí a online petic. Tyto informace byly následně zveřejněny na anonymních internetových platformách, kde se diskutovalo o dalších způsobech jejich zneužití, například prostřednictvím šíření dezinformací nebo podvržené e-mailové komunikace. V tomto případě byl doxing využit k vytvoření atmosféry strachu a tlaku. Tyto události vedly k omezení veřejné činnosti dotčených osob. [8], [9]

4.2.2 Popis zneužitých technologických zranitelností u doxingu politických aktivistů na univerzitách

Mezi hlavní bezpečnostní nedostatky zde patřila slabá ochrana osobních údajů na univerzitních serverech, špatné nastavení soukromí na sociálních sítích a žádná opatření proti automatizovanému sběru dat. Tyto zranitelnosti daly útočníkům příležitost hromadně shromažďovat informace, které potom byly využity k cílenému doxingu jednotlivců. [8], [9]

II PRAKTICKÁ ČÁST

5 NÁVRH PODNIKOVÝCH PROCESŮ Z HLEDISKA INFORMAČNÍ BEZPEČNOSTI ZAMĚŘENÝ NA OCHRANU DAT PŘED DOXINGEM

Se zrychlující digitalizací a narůstajícím množstvím osobních údajů dostupných na internetu se hrozba doxingu stává vážným problémem i pro podniky. Aby bylo možné těmto rizikům čelit, je nutné zaměřit se na zabezpečení citlivých dat prostřednictvím dobře navržených podnikových procesů.

Tato část práce si klade za cíl navrhnout podnikové procesy, které přispějí ke zvýšení úrovně informační bezpečnosti v rámci celé organizace. Tyto procesy budou vyvíjeny s důrazem na prevenci neoprávněného sběru, zveřejnění a šíření dat.

Zároveň bude zajištěno, aby navržená řešení dodržovala klíčové principy informační bezpečnosti, konkrétně důvěrnost, integritu a dostupnost dat. Také by měla být začleněna do bezpečnostní strategie firmy.

5.1 Úvod do problematiky

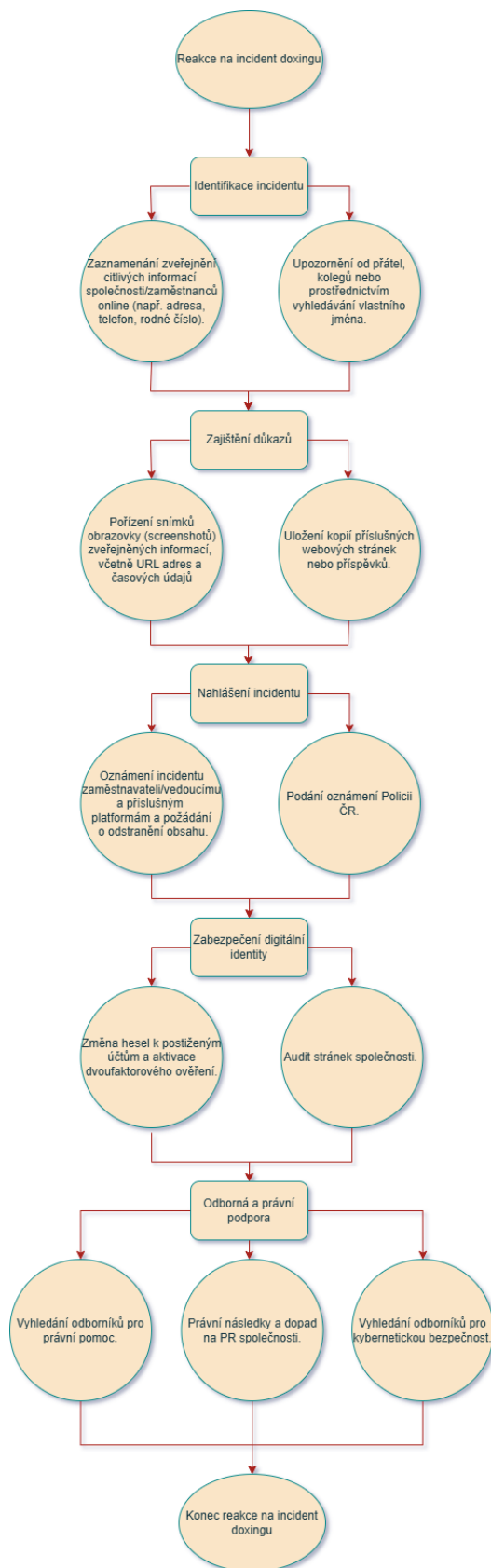
V oblasti podnikání je ochrana citlivých údajů jedním z hlavních pilířů bezpečnostní strategie každé firmy. Vzhledem k rozšířenému používání internetových nástrojů a cloudových systémů roste riziko útoků, které se zaměřují na neoprávněné získávání a publikování osobních informací. Doxing může v tomto kontextu sloužit jako prostředek cíleného útoku na zaměstnance, ke ztrátě důvěry zákazníků nebo dokonce k narušení stability celé firmy. [12]

Z těchto důvodů je nezbytné využívat firemní procesy, které zajistí systematickou ochranu citlivých informací v rámci každodenního provozu. Opatření zaměřená na ochranu dat musí být pevně zakotvena nejen v technickém zabezpečení, ale i v interních postupech a kultuře organizace. [12]

V situaci, kdy nastane incident spojený s doxingem, je důležité, aby organizace měla připravený reaktivní workflow, který zajistí rychlou odpověď na danou hrozbu. V diagramu (Obrázek 2) workflow je jako první provedeno rozpoznání incidentu a následně je ověřena přesnost a rozsah zveřejněných dat. Po potvrzení případu následuje odpojení všech zasažených systémů a zapojení interního bezpečnostního týmu. Součástí postupu je také informování dotčených osob, případně kontaktování úřadů, právního zástupce či Policie ČR. Po zvládnutí těchto událostí je provedena zpětná revize a analýza příčin s cílem navrhnout

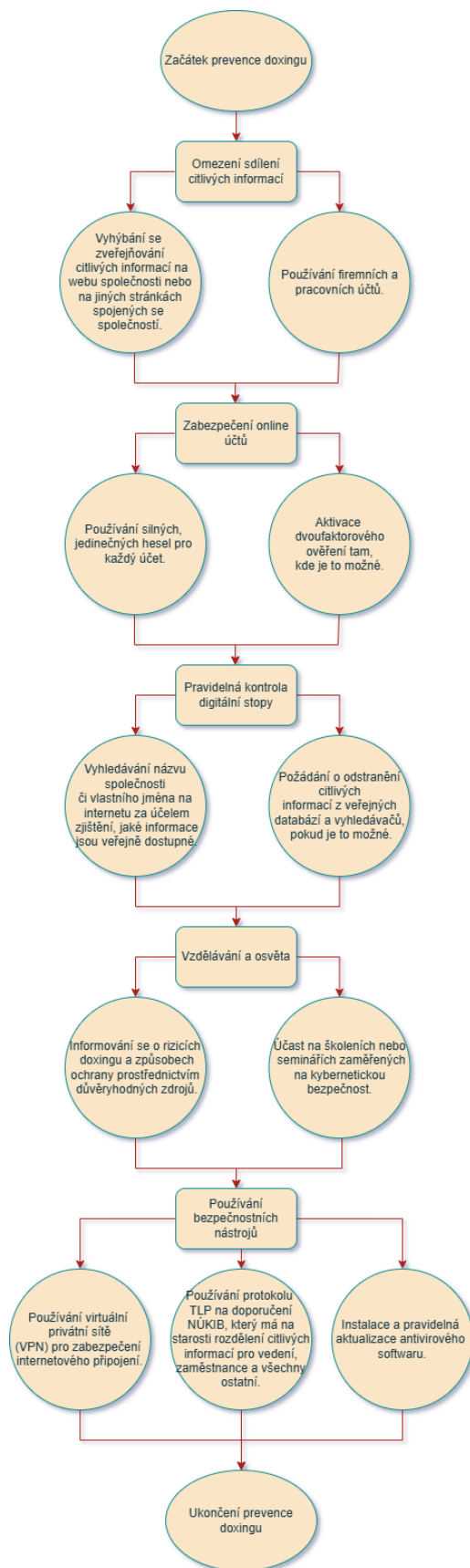
preventivní kroky. Takto je zajištěno nejen omezení následků incidentu, ale i prevence jeho opakování v budoucnu.

Na dalším schématu (Obrázek 3) je znázorněn workflow zaměřený na prevenci útoků typu doxing. Tento model je navržen tak, aby pomáhal snižovat pravděpodobnost úniku nebo zneužití citlivých údajů. V rámci procesu byla implementována opatření jako pravidelná školení zaměstnanců v oblasti kybernetické bezpečnosti, řízení přístupových práv a zavedení pravidel pro sdílení dat. Důležitou součástí je také kontrola digitální stopy pomocí nástrojů OSINT a úprava nastavení soukromí na platformách, které jsou spojené s danou společností. Součástí procesu jsou i bezpečnostní audity a úpravy ochranných prvků dle aktuálních hrozeb. Cílem workflow je zvýšit odolnost firmy vůči útokům typu doxing.



Obrázek 2 - Workflow: Reakce na incident doxingu

(zdroj: vlastní)



Obrázek 3 - Workflow: Prevence doxingu

(zdroj: vlastní)

5.1.1 Vysvětlení potřeby ochrany proti doxingu ve firemním prostředí

V dnešním digitálním světě se ochrana osobních a citlivých informací stává klíčovou prioritou pro všechny typy organizací. Doxing, jako forma neoprávněného získávání a šíření osobních údajů, představuje závažnou bezpečnostní hrozbu, která může negativně ovlivnit nejen zaměstnance a partnery, ale i celou firmu. Ve firemním prostředí je dopad doxingu velmi citelný. Zásah do soukromí jednotlivců může vést ke kompromitaci interních systémů, úniku strategických dat, právním problémům nebo poškození dobrého jména společnosti. [8]

Zveřejněním detailů o pracovnících, jako jsou jejich pozice, kontakty nebo informace o IT infrastruktuře, se organizace může stát terčem cílených kybernetických útoků. Útočníci tyto informace následně využívají k narušení bezpečnosti a fungování firmy. S ohledem na tato rizika je nutné zavádět preventivní bezpečnostní opatření již v rámci administrativních procesů a řízení přístupu k datům. [8]

5.1.2 Význam podnikových procesů v rámci bezpečnostní politiky organizace

Podnikové procesy tvoří základ každé moderní organizace a určují, jak se s informacemi v organizaci pracuje, jak jsou chráněny a jakým způsobem dochází k jejich sdílení. Z pohledu informační bezpečnosti hrají tyto procesy zásadní roli při zavádění ochranných mechanismů, které slouží k zabezpečení citlivých informací. Dobře definované a řízené procesy pomáhají minimalizovat rizika vyplývající z případné lidské chyby, brání přístupu nepovolaným osobám a umožňují včasné odhalení potenciálních hrozeb. [8]

5.2 Definice cíle návrhu procesů

Účelem návrhu podnikových procesů z hlediska informační bezpečnosti je vytvořit systém, který efektivně ochrání data před jejich zneužitím, únikem nebo neautorizovaným zveřejněním. Tyto procesy musí pokrývat celý životní cyklus dat. Začíná to u jejich sběru a zpracování až po archivaci a bezpečné odstranění. Klíčovým předpokladem je naplnění principů CIA triády, tedy důvěrnosti, integrity a dostupnosti. Tímto způsobem lze výrazně snížit riziko úspěšného útoku typu doxing, který často vzniká v důsledku nedostatečných kontrolních mechanismů nebo chybějící ochrany. [8], [15]

Procesy zaměřené na bezpečnost také umožňují přesně sledovat, kdo a za jakých okolností má přístup k citlivým údajům. Tento přístup je zásadní nejen kvůli ochraně proti doxingu, ale i pro zajištění souladu s právními předpisy, jako je například GDPR. [14]

5.2.1 Hlavní bezpečnostní cíle procesu

Každý proces, který se zabývá ochranou informací, by měl být navržen v souladu s třemi hlavními body bezpečnosti a to důvěrností, integritou a dostupností. Jsou také známé pod už zmíněným označením CIA triáda. Důvěrnost zaručuje, že citlivé informace jsou dostupné jen oprávněným osobám, a tak se předchází jejich možnému zneužití. Princip integrity zase zajišťuje, že údaje zůstávají neměnné a nejsou během přenosu nebo zpracování pozměněny někým jiným. Dostupnost znamená, že autorizovaní uživatelé mají přístup k potřebným údajům vždy, když je to nezbytné. Tyto tři principy je nutné respektovat zejména při návrhu procesů, které mají chránit organizaci před riziky, jako je doxing. [8], [15]

5.2.2 Ochrana osobních údajů zaměstnanců a klientů

V každé organizaci je důležité dbát na důslednou ochranu osobních údajů všech subjektů, se kterými přichází do styku. Jde o zaměstnance, zákazníky, partnery nebo dodavatele. Veškeré zpracování těchto dat by mělo probíhat v souladu s legislativou, zejména s nařízením GDPR, a také zároveň v souladu s interními bezpečnostními standardy. Mezi základní opatření patří omezený přístup, šifrování, pravidelné bezpečnostní audity a důsledné mazání dat po ukončení jejich využití. V opačném případě hrozí, že budou tyto informace zneužity při útocích spojených s doxingem. Mohou být zneužity například k nátlaku, poškození pověsti nebo digitálnímu obtěžování. [8], [14]

5.2.3 Reakce na potenciální hrozby doxingu

Modelování podnikových procesů by nemělo zahrnovat pouze preventivní mechanismy, ale i reakční strategie pro případ výskytu hrozby spojené s doxingem. Každá organizace by měla mít připravený postup pro zvládání možných incidentů. V případě incidentu se může jednat o okamžité izolace napadených systémů, upozornění odpovědných pracovníků a důkladné dokumentace situace. Pokud se skutečně potvrdí, že došlo k doxingu, je nutné provést právní kroky, informovat zasažené osoby a analyzovat příčinu problému. Zároveň je třeba přizpůsobit procesy tak, aby se podobný incident neopakoval. Schopnost rychle a efektivně reagovat na hrozby představuje klíčový faktor pro udržení odolnosti organizace a omezení negativních dopadů na její činnost. [8], [14]

5.3 Doporučení pro ochranu proti doxingu

Pořád je důležité se zabývat ochranou osobních informací. Neoprávněné získávání a následné šíření citlivých dat s cílem uškodit jednotlivcům nebo organizacím představují

velké hrozby. Ke zmírnění rizik, které z toho plynou, je nutné přijmout preventivní pravidla a ochranné kroky. Tato opatření mohou být uplatněna jak na individuální úrovni, tak v rámci organizací jako součást celkové bezpečnostní strategie.

Za jeden z klíčových kroků při ochraně před doxingem je považováno snižování objemu osobních dat sdílených na internetu. Údaje jako datum narození, telefonní číslo, adresa, osobní snímky nebo informace o rodině by neměly být veřejně přístupné. Čím méně těchto informací je dostupných, tím nižší je riziko jejich zneužití. Doporučeno je používat oddělené e-mailové adresy pro pracovní a soukromou komunikaci a neuvádět skutečné jméno na všech online platformách. Viditelnost profilových údajů na sociálních sítích by měla být upravena pomocí nastavení soukromí. [17]

Důležitou součástí prevence je také pravidelná kontrola digitální stopy. Jedná se o přehled informací, které jsou o uživateli volně dostupné a dohledatelné. Mělo by být pravidelně prováděno procházení osobních účtů, příspěvků, komentářů a diskusních platform s cílem zjistit, zda se někde nenachází obsah, který by mohl být pro tento účel zneužit. Pokud jsou nalezeny citlivé nebo nevhodné údaje, je vhodné je upravit nebo smazat, pokud je to možné. Pro vyhledání osobních dat je možné použít běžné vyhledávače či specializované služby monitorující úniky údajů. [17]

Velkou roli při ochraně proti doxingu má správné zabezpečení účtů a přístupových údajů. Hesla by měla být dostatečně silná, unikátní a pravidelně obnovována. Doporučeno je také zapnout vícefaktorové ověřování, které poskytuje vyšší úroveň ochrany i v případě úniku hesla. Pro bezpečné ukládání přihlašovacích údajů by měl být využíván správce hesel a při připojení na veřejných sítích by mělo být používáno zabezpečené VPN připojení. [17]

Opatrnost je nezbytná i při každodenní online komunikaci. Uživatelům je doporučeno nevěřit nevyžádaným e-mailům, zprávám nebo přílohám a postupovat při jejich otevírání obezřetně. Pozornost by měla být věnována zejména phishingovým útokům, které slouží jako prostředek pro sběr osobních dat k pozdějšímu zneužití. Podezřelá komunikace by měla být ověřena a případně oznámena poskytovateli nebo odpovědnému správci systému. [17]

Důležité místo má také vzdělávání v oblasti kybernetické bezpečnosti. Je třeba, aby uživatelé byli pravidelně informováni o aktuálních hrozbách, metodách ochrany dat a správných bezpečnostních návycích. Ve firemním prostředí je doporučeno zavádět školení zaměřená na prevenci sociálního inženýrství, bezpečné nakládání s informacemi a

rozpoznávání pokusů o doxing. Zvyšováním povědomí se posiluje celková bezpečnostní kultura v organizaci. [17]

Nasazením uvedených doporučení může být významně sníženo riziko úspěšného doxingového útoku. Ochrana citlivých dat by tak neměla být vnímána jen jako jednorázová aktivita, ale jako nepřetržitý proces, který by měli využívat jednotlivci i společnosti.

5.4 Balíček nástrojů pro minimalizaci digitální stopy

U preventivních opatření proti útokům typu doxing je důležité znát hlavní proces. Tímto klíčovým procesem je snižování digitální stopy, která by mohla být zneužita k identifikaci nebo ohrožení konkrétní osoby. Tento postup zahrnuje sadu kroků a nástrojů. Jejich úkolem je omezit objem osobních údajů zveřejněných na internetu a zabránit jejich neoprávněnému využití, rozšíření nebo manipulaci. Doporučeno je pravidelné sledování vlastního online prezentování, odstranění nadbytečných informací a správné zabezpečení účtů, a to hlavně na sociálních sítích. [17]

K omezení zobrazování citlivých údajů ve výsledcích internetových vyhledávačů se doporučuje využití dostupných nástrojů poskytovaných samotnými vyhledávači, jako je například Google. Prostřednictvím jednoduchého online formuláře je možné zažádat o odstranění konkrétních výsledků vyhledávání, které obsahují například adresy, telefonní čísla nebo jiná osobní data. Tento postup vychází z práva na výmaz, které je známé také jako „právo být zapomenut“. [18]

Také se doporučuje pravidelně kontrolovat, jestli nedošlo k úniku některého z osobních údajů, například e-mailových adres, telefonních čísel nebo přihlašovacích údajů. Za tímto účelem mohou být využívány nástroje jako Have I Been Pwned nebo Firefox Monitor, které umožňují pomocí e-mailové adresy ověřit, zda byl uživatel zahrnut do známých úniků dat. V případě zjištění kompromitace je možné okamžitě podniknout kroky, jako je změna hesel nebo zrušení účtů [19], [20]. Použití těchto nástrojů může být sporné, protože pro ověření zmíněné e-mailové adresy je třeba vybranou adresu ručně zadat a ověřit.

Další součástí ochrany představuje použití anonymizačních nástrojů a alternativních vyhledávačů, které neshromažďují ani neukládají uživatelská data. Příkladem může být vyhledávač DuckDuckGo, který zajišťuje soukromí tím, že nevede záznamy o vyhledávání, IP adresách ani identitě uživatelů. Tím je minimalizováno množství údajů, které mohou být později zneužity. [21]

Patří zde také webový prohlížeč Brave, který je využíván díky svému zaměření na ochranu uživatelského soukromí. Tento prohlížeč byl navržen s cílem automaticky blokovat sledovací prvky, reklamy a externí skripty, které běžně slouží k monitorování velkého množství online aktivit uživatelů. Kromě standardní ochrany je v prohlížeči Brave integrována také funkce anonymního režimu s využitím sítě Tor. Tímto způsobem je tak zvýšena úroveň anonymizace při procházení webu. Také je umožněno pravidelné automatické odstraňování cookies, cache a historie prohlížení. S pomocí těchto aktivit se tak výrazně snižuje množství údajů, které by mohly být zneužity v rámci útoku typu doxing. Díky těmto bezpečnostním prvkům je Brave doporučován uživatelům, kteří mají zájem o kontrolu nad svými osobními daty a snaží se minimalizovat svou digitální stopu. [29]

Účinnou obranou je také zabezpečení všech účtů silnými a unikátními hesly a aktivace vícefaktorového ověřování. Doporučeno je rovněž důsledné nastavení soukromí na sociálních sítích, kde lze určit, kdo má přístup k jednotlivým údajům, fotografiím či příspěvkům. Citlivé informace by měly být sdíleny pouze s ověřenými kontakty a v co nejmenším nutném rozsahu. [22]

Postupné snižování digitální stopy tvoří nedílnou součást širší bezpečnostní politiky a její význam je zásadní pro jednotlivce i pro různé společnosti. Správným využíváním uvedených nástrojů může být výrazně sníženo riziko úspěšného doxingu a současně zvýšena administrativní bezpečnost. [17]

5.5 OSINT nástroje pro minimalizaci digitální stopy

Pro ochranu před doxingem se stále častěji uplatňují nástroje a metody spadající do kategorie OSINT (Open Source Intelligence), které jsou běžně využívány k získávání a analýze veřejně dostupných dat z otevřených zdrojů. V oblasti informační bezpečnosti však mohou být tyto nástroje efektivně využity také při monitorování vlastní digitální stopy a identifikaci údajů, které mohou být potenciálně zneužity útočníky k doxingu. [17]

Velmi užitečným prostředkem je platforma Intelligence X, pomocí které lze vyhledávat informace v různých typech úložišť. Mezi tyto úložiště patří veřejné databáze, pastebiny, darknet a WHOIS záznamy. Tento nástroj může být využit ke zjištění, jaké informace jsou aktuálně online dohledatelné o určité osobě nebo organizaci. [20], [23]

Pro vizualizaci vztahů mezi různými přezdívkami, pod kterými se skrývá určitá osoba, je často nasazován nástroj Maltego. Tento nástroj je určen pro pokročilou analýzu souvislostí

mezi doménami, e-mailovými adresami, účty na sociálních sítích a dalšími objekty. Pomocí tohoto nástroje může být vytvořen přehledný graf vztahů, které mohou být útočníky zneužity k vytvoření komplexního profilu cílové osoby nebo instituce. [24]

Dalším příkladem OSINT nástroje vhodného pro obranné účely je Recon-ng, který nabízí prostředí pro strukturovaný sběr dat. Tento nástroj umožňuje analýzu informací získaných z různých veřejných zdrojů, jako jsou WHOIS záznamy, úložiště fotografií, sociální sítě nebo veřejně dostupné e-mailové databáze. Identifikované informace pak mohou být zpracovány a následně je doporučeno jejich odstranění, anonymizace či omezení k jejich přístupu. [25]

Při použití všech výše uvedených nástrojů je doporučeno pravidelně prověřovat, jaké informace o konkrétní osobě nebo společnosti jsou veřejně dostupné, a tyto údaje dle potřeby aktualizovat nebo se je snažit odstranit, i když je nelze z prostředí internetu úplně vymazat. Práce s OSINT nástroji tak představuje důležitý bod ochrany proti doxingu v rámci bezpečnosti konkrétní osoby nebo společnosti. [17]

5.6 Přehled bezplatných nástrojů pro modelování BPMN a EPC diagramů

K modelování podnikových procesů existuje celá řada dostupných nástrojů, které umožňují bezplatné vytváření a úpravu diagramů v notacích BPMN a EPC. Mezi nejznámější desktopové aplikace patří ARIS Express. [12]

Vedle programu ARIS Express lze využít také jiné nástroje s otevřeným kódem či online platformy. Příkladem může být Camunda Modeler, který plně podporuje BPMN 2.0, nebo Bizagi Modeler, který je zase vhodný pro grafické znázornění složitějších procesů v jednoduchém prostředí. Pro uživatele, kteří preferují práci bez instalace je k dispozici webová aplikace bpmn.io, umožňující rychlé sestavení BPMN modelů přímo v prohlížeči. Co se týče EPC notace, vedle ARIS Express lze využít i Yaoqiang BPMN Editor, který poskytuje základní modelovací funkce a je vhodný například pro výuku nebo jednodušší projekty. Výhodou těchto nástrojů je jejich snadná dostupnost, bezplatnost a kompatibilita se zavedenými standardy. [26], [27]

Pro základní diagramy byl v rámci práce použit také webový editor Diagrams.net, který byl dříve znám také jako Draw.io. Tento editor je volně přístupný a umožňuje tvorbu různých typů schémat, včetně diagramů typu BPMN i EPC. Tento nástroj se hodí jak pro

modelování podnikových procesů, tak pro kreslení technických návrhů, organizačních schémat nebo přehledných workflow diagramů. V praktické části práce byly s využitím tohoto nástroje vytvořeny dva modely znázorňující reakci na doxingové útoky, které ukazují jednotlivé kroky vedoucí ke zmírnění dopadů a ochraně online identity. Díky jednoduchému ovládání, podpoře cloudového uložení a možnosti exportu ve formátech jako PNG, SVG či PDF. Diagrams.net tak představuje vhodné řešení pro rychlou vizualizaci různých procesů do diagramů, a to bez potřeby složité instalace. [28]

5.7 Výběr vhodného modelovacího nástroje

Pro modelování podnikových procesů zaměřených na zvýšení ochrany údajů před doxingem byl zvolen software ARIS Express. Tato volba byla učiněna na základě několika parametrů, mezi které patřila dostupnost podpory různých notací, uživatelská přívětivost prostředí a možnosti exportu hotových diagramů pro další zpracování.

Modelovací nástroj musel umožnit práci s notací BPMN pro technicky podrobný popis procesů, ale také EPC, která je vhodnější pro manažerskou úroveň vizualizace. Také bylo nutné, aby vybraný nástroj podporoval systematickou práci s procesními prvky a jejich vzájemné logické propojení.

Na základě těchto požadavků byl pro zpracování vybrán ARIS Express, který nabízí komplexní prostředí pro tvorbu modelů procesů včetně podpory dalších struktur, jako jsou organizační schémata, datové struktury nebo informační toky. Tento nástroj se osvědčil nejen pro technické specialisty, ale také pro studenty a analytiky zaměřené na procesní řízení.

5.7.1 Představení nástroje ARIS Express

Z aplikace ARIS Express lze vyzdvihnout, že se jedná o bezplatný nástroj vyvinutý společností Software AG, který je založen na renomované metodice ARIS. Nabízí intuitivní rozhraní pro návrh podnikových procesů a umožňuje modelování pomocí různých notací, jako jsou BPMN a EPC. Díky své přehlednosti a snadnému ovládání je vhodný pro vizualizaci procesů jak na technické, tak i manažerské úrovni. Modely lze exportovat do běžně využívaných formátů, jako je PDF nebo obrázek, což usnadňuje jejich další použití v dokumentaci a prezentacích. [12]

5.7.2 Důvody využití ARIS Express

Volba nástroje ARIS Express byla provedena s ohledem na specifické požadavky, mezi které patří efektivní, bezplatné a přístupné prostředí pro modelování. Výhodou je jeho nulová pořizovací cena, což z něj činí ideální volbu především pro vysokoškolské studenty, malé podniky a různé další instituce. Nástroj podporuje modelování pomocí BPMN, ale také EPC diagramy, které jsou vhodné hlavně pro popis procesů z pohledu manažerského řízení. [12]

Uživatelské rozhraní je navrženo tak, aby ho mohli bez problémů ovládat i ti, kdo nemají zkušenosti s procesním modelováním. Mezi hlavní přednosti patří možnost snadného exportu a dokumentace výsledků modelování. Grafické zpracování je přehledné a jednoznačně vymezuje jednotlivé toky a odpovědnosti. [12]

Současně je zajištěna plná kompatibilita s ARIS metodikou, která umožňuje navazující rozvoj modelování v profesionálním prostředí. Na základě těchto charakteristik byl ARIS Express využit jako hlavní nástroj pro návrh modelů, které jsou součástí praktické části této bakalářské práce. [12]

5.8 Modelovací jazyky použité pro návrhy

Při návrhu ochranných procesů zaměřených na zabezpečení dat proti doxingu byly využity dva modelovací jazyky s názvem BPMN a EPC. Obě tyto notace umožňují strukturovaně a vizuálně znázornit procesy. Každý z nich se hodí pro jinou úroveň popisu. BPMN se osvědčuje při modelování technických nebo operativních činností díky velmi detailní symbolice. Naopak EPC lépe vyhovuje při popisu procesů z hlediska událostí a funkcí, které jsou snadno pochopitelné i bez širší znalosti technické oblasti. V této práci byly oba přístupy kombinovány tak, aby pokrývaly různé úrovně řízení i administrativní aspekty ochrany dat. [12], [13]

5.8.1 Business Process Model and Notation

Modelovací jazyk BPMN (Business Process Model and Notation), který byl vytvořený organizací OMG, představuje mezinárodně uznávaný standard pro grafický zápis podnikových procesů. Je navržen tak, aby byl srozumitelný nejen pro IT odborníky, ale také pro manažerské pracovníky bez technického zaměření. Díky své strukturovanosti umožňuje BPMN detailní vizualizaci složitých technických procesů včetně rozhodovacích uzlů, datových objektů nebo rolí uživatelů. V této bakalářské práci byl využit k modelování klíčových bezpečnostních procesů, jako je správa přístupových práv, šifrování citlivých

informací či reakce na incidenty. BPMN tak přispěl k přehlednému a systematickému zachycení jednotlivých kroků, odpovědných aktérů a výstupů procesů. To dále usnadňuje jejich další využití v rámci celé organizace. [12]

5.8.2 Event-driven Process Chain

Modelovací jazyk EPC (Event-driven Process Chain) je často využíván pro znázornění podnikových procesů z pohledu sledování událostí a s nimi souvisejících činností. Tento přístup, který vznikl v rámci metodiky ARIS, se řadí mezi nejrozšířenější nástroje v oblasti procesního řízení. Díky své jednoduché struktuře a přehlednosti je vhodný pro modelování procesů na úrovni řízení a strategického rozhodování. Základem EPC notace je střídání událostí a funkcí. Umožňuje to tak zachytit logiku jednotlivých kroků procesu bez toho, aby bylo nutné zabíhat do složitých technických detailů. V této práci byly EPC diagramy použity k modelování situací, jako je reakce na žádosti o přístup k datům, realizace školení zaměstnanců nebo řešení bezpečnostních incidentů. Další výhodou EPC je také možnost doplnit model o prvky jako jsou organizační role, dokumenty, IT systémy nebo datová úložiště. Pomocí těchto prvků lze vytvořit ucelené a dobře srozumitelné procesní schéma. Vzhledem ke své srozumitelnosti se EPC ukázal jako ideální prostředek pro vizualizaci procesů zaměřených na administrativní bezpečnost a ochranu citlivých údajů. [13]

5.9 Popis modelového příkladu organizace

Modelovým příkladem je společnost SecureData s.r.o., která se zaměřuje na správu dat, hostingové služby a provoz cloudových úložišť pro malé a střední podniky. Firma provozuje vlastní serverové zázemí v datovém centru a současně poskytuje přístupová rozhraní, která klientům umožňují bezpečně ukládat, spravovat dokumenty, databáze i personální informace. Zaměstnanci mají přiřazené rozdílné úrovně přístupu podle své pracovní pozice a při plnění úkolů běžně zpracovávají osobní data zákazníků i citlivé informace o partnerech a vnitropodnikových procesech.

5.9.1 Popis aktuálního stavu

Aktuálně probíhá manipulace s důvěrnými údaji prostřednictvím interního informačního systému. Problémem zde může být to, že přístupová oprávnění nejsou vždy jednoznačně nastavena. Některé činnosti, jako například žádost o přístup k údajům nebo archivace smluv, probíhají bez jasně stanoveného schvalovacího řízení a chybí jim odpovídající dokumentace. Bezpečnostní školení se konají jen při nástupu nových zaměstnanců a v organizaci chybí

průběžné vzdělávací aktivity. Záznamy o přístupech nejsou systematicky kontrolovány a firma nedisponuje oficiálním plánem reakce na bezpečnostní incidenty.

5.9.2 Identifikace slabin v procesech

Kontrola současného stavu odhalila několik závažných nedostatků, které mohou vést k útokům s využitím doxingu. Kritické slabiny zahrnují neexistující šifrování některých vnitřních databází, především těch s osobními informacemi zaměstnanců. Zároveň bylo zjištěno, že přístupová oprávnění nejsou pravidelně přehodnocována, což umožňuje přístup i těm pracovníkům, kteří s daty již nepracují. Významným nedostatkem je také chybějící vícefaktorové ověření při přihlašování. Tento nedostatek zvyšuje pravděpodobnost zneužití přihlašovacích údajů. Byla také zaznamenána nízká úroveň povědomí pracovníků o rizicích doxingu a nedostatečná frekvence školení v oblasti ochrany proti sociálnímu inženýrství. Navíc chybí definovaný postup pro řešení bezpečnostních incidentů. Ten tak omezuje schopnost firmy reagovat včas a efektivně. Archivace neprobíhá podle bezpečnostních zásad a momentálně není definována klasifikace dat dle stupně citlivosti. Dále bude zavedeno plošné šifrování v rámci životního cyklu dat. Chybí také celkový proces pravidelné kontroly přístupových oprávnění. V následujících částech práce budou představeny nové návrhy podnikových procesů. Jejich cílem je tyto slabiny odstranit a posílit celkovou administrativní bezpečnost.

5.10 Návrh bezpečnostních podnikových procesů

Na základě zjištěných slabin byly navrženy nové podnikové procesy, jejichž implementace povede k výraznému snížení rizika doxingu. Každý z procesů cílí na konkrétní oblast bezpečnosti a společně vytvářejí komplexní systém ochrany důvěrných dat.

5.10.1 Proces klasifikace a označování dat

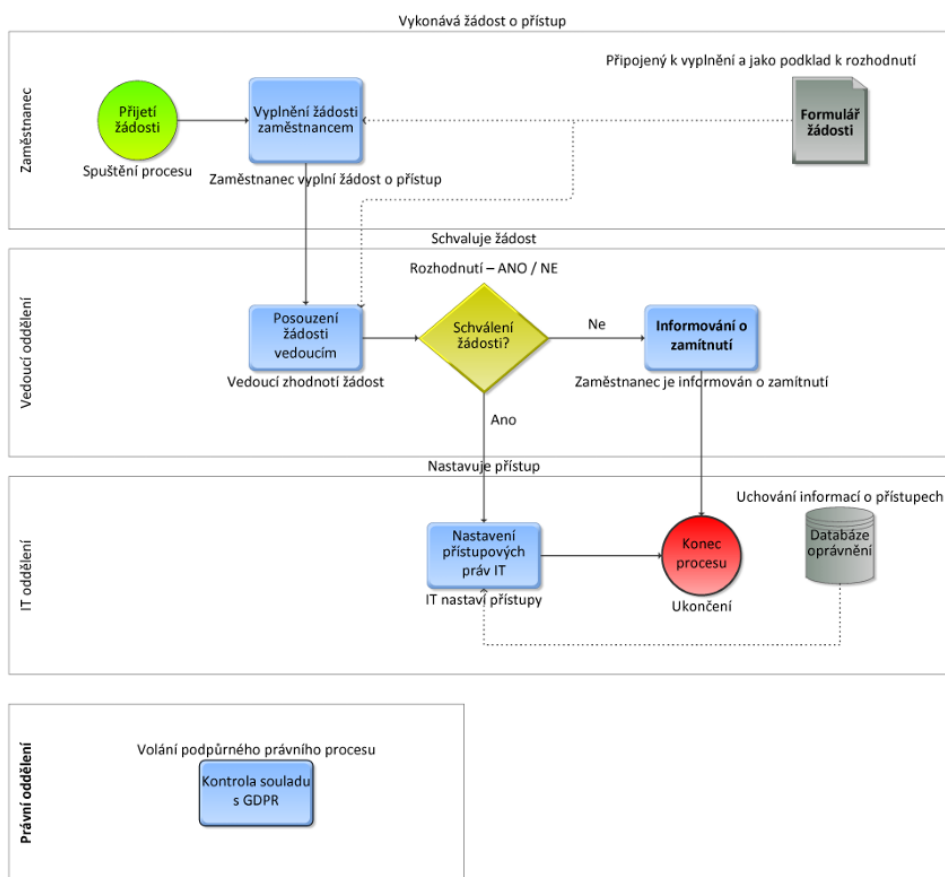
Základem pro zajištění bezpečnosti je přesná klasifikace dat. Každá datová položka je zařazena do příslušné kategorie, a to například veřejná, interní, důvěrná nebo přísně důvěrná. Těmto datům je přiřazen bezpečnostní štítek, který určuje pravidla pro jejich přístup, přenos, uchování a likvidaci.

Klasifikace se provádí při vytváření dokumentu nebo při jeho vložení do systému. Za správnost klasifikace odpovídá IT bezpečnostní pracovník a správnost je dále kontrolována v rámci pravidelných auditů. Tento proces omezuje riziko neautorizovaného šíření údajů.

5.10.2 Proces řízení přístupových práv

Správa přístupových oprávnění probíhá v souladu s principem minimálních práv. Zaměstnanci mají povolení jen k informacím, které přímo souvisejí s jejich pracovními úkoly. Požadavky na rozšíření přístupu jsou nejprve schvalovány nadřízeným a následně potvrzeny IT oddělením. Revize přístupů probíhá pravidelně každé tři měsíce. Při každé personální změně jako například při nástupu, odchodu nebo změně pozice dojde k automatickému přehodnocení přístupových práv. [8], [14]

Na obrázku (Obrázek 4) je představen strukturovaný postup řízení přístupových oprávnění k citlivým datům v rámci společnosti. Diagram zobrazuje sled kroků od vyplnění žádosti pracovníkem až po její schválení a technické zajištění přístupu ze strany IT oddělení. Pomocí BPMN notace je detailně zachycena odpovědnost zapojených rolí i rozhodovací fáze. Díky tomuto modelu může být dosaženo větší kontroly a zpětné dohledatelnosti při přidělování přístupů.



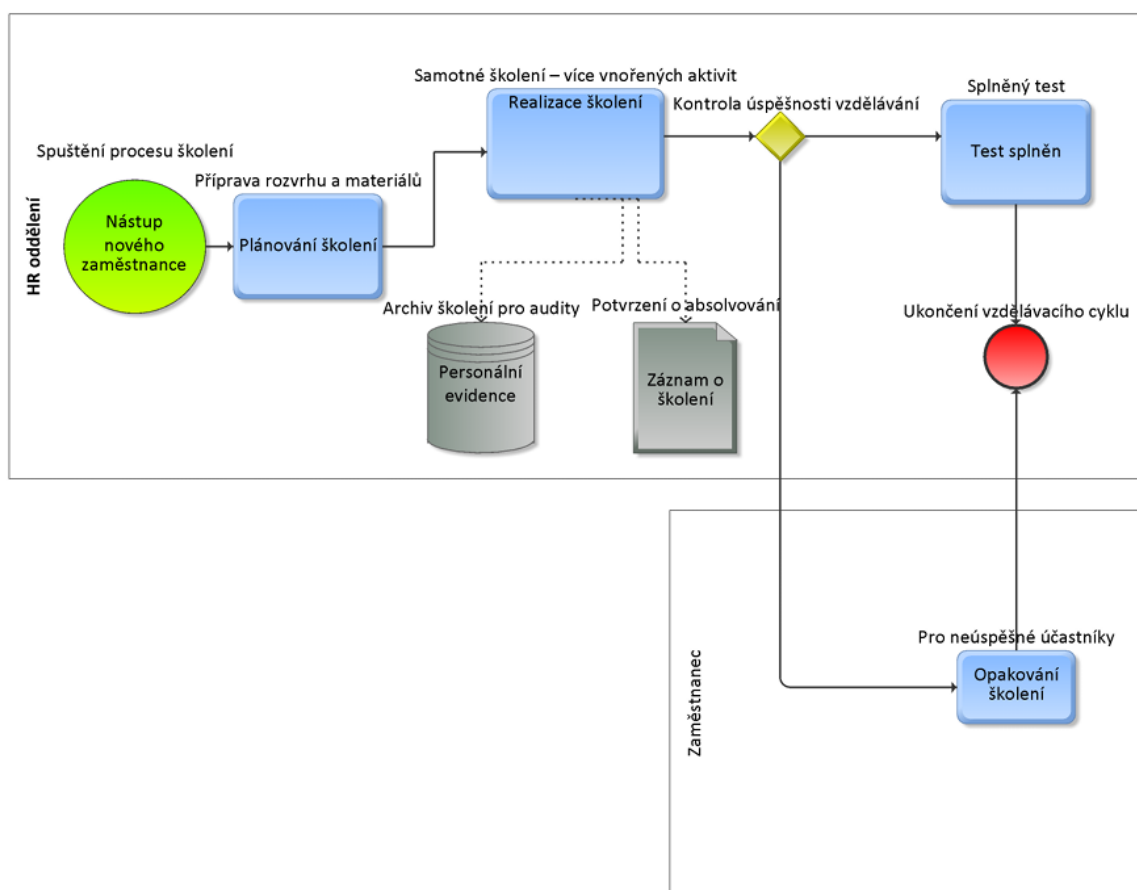
Obrázek 4 - BPMN diagram: Řízení přístupových práv

(zdroj: vlastní)

5.10.3 Proces školení zaměstnanců v oblasti bezpečnosti

Zaměstnanci absolvují pravidelná školení v oblasti kybernetické bezpečnosti, včetně hrozeb souvisejících s doxingem. První školení probíhá během adaptačního období a následně je opakováno každoročně formou prezenčních kurzů. Obsah školení se zaměřuje na identifikaci phishingových útoků, bezpečné nakládání s daty, používání silných hesel, dvoufázové ověřování a prevenci manipulativních technik. [14]

Model procesu na obrázku (Obrázek 5) slouží k zachycení školení pracovníků v oblasti informační a administrativní bezpečnosti. Diagram obsahuje činnosti jako je vstupní zaškolení nových zaměstnanců a vyhodnocení jeho absolvování. Využití BPMN notace umožňuje zachytit tok činností včetně odpovědných oddělení i generovaných výstupů. Tento proces tak pomáhá zvýšit bezpečnost a snížit rizika, která jsou spojená s doxingem.



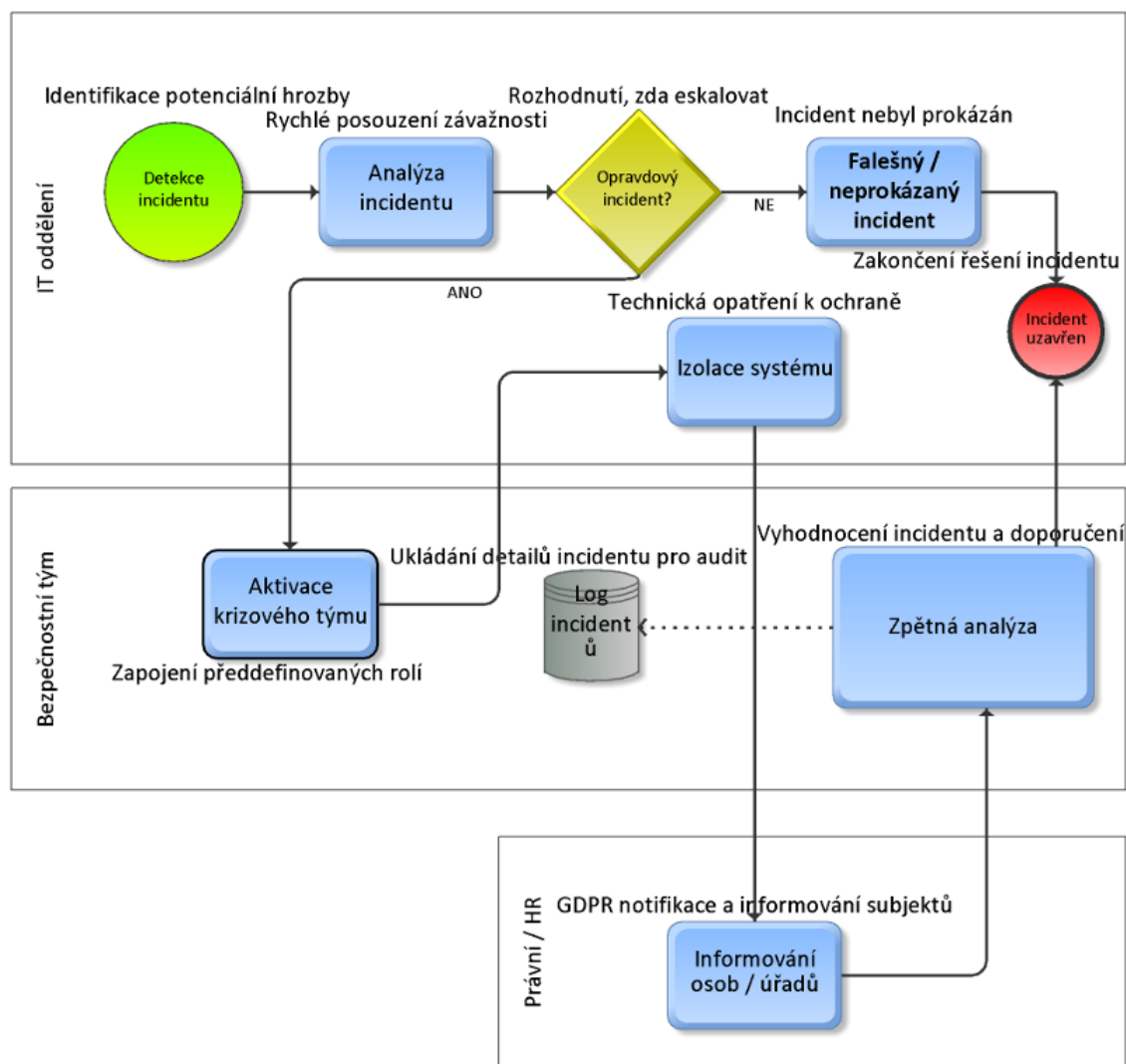
Obrázek 5 - BPMN diagram: Školení zaměstnanců v oblasti bezpečnosti

(zdroj: vlastní)

5.10.4 Proces reakce na incidenty typu doxing

Při podezření na únik nebo zveřejnění citlivých informací se spouští proces reakce na incident. Tento proces zahrnuje identifikaci problému, izolaci dotčených systémů, informování krizového týmu, kontaktování postižených osob i příslušných úřadů a následnou analýzu incidentu včetně přijetí nápravných kroků. Reakce na incidenty se řídí předem připravenými scénáři s jasně definovanými odpovědnostmi. Tyto scénáře tak umožňují rychlý a koordinovaný zásah v případě vážné bezpečnostní události. [8]

Na obrázku (Obrázek 6) je zachycen model postupu aktivovaného při podezření na únik dat a následný incident typu doxing. Proces zahrnuje fáze jako identifikace problému, odpojení zasažených systémů, informování odpovědných osob a zavedení opatření. BPMN notace zde umožňuje detailní znázornění jednotlivých kroků, odpovědných pracovníků i způsobu komunikace. Tento model je důležitý pro rychlou reakci na incident a dodržení interních bezpečnostních pravidel.



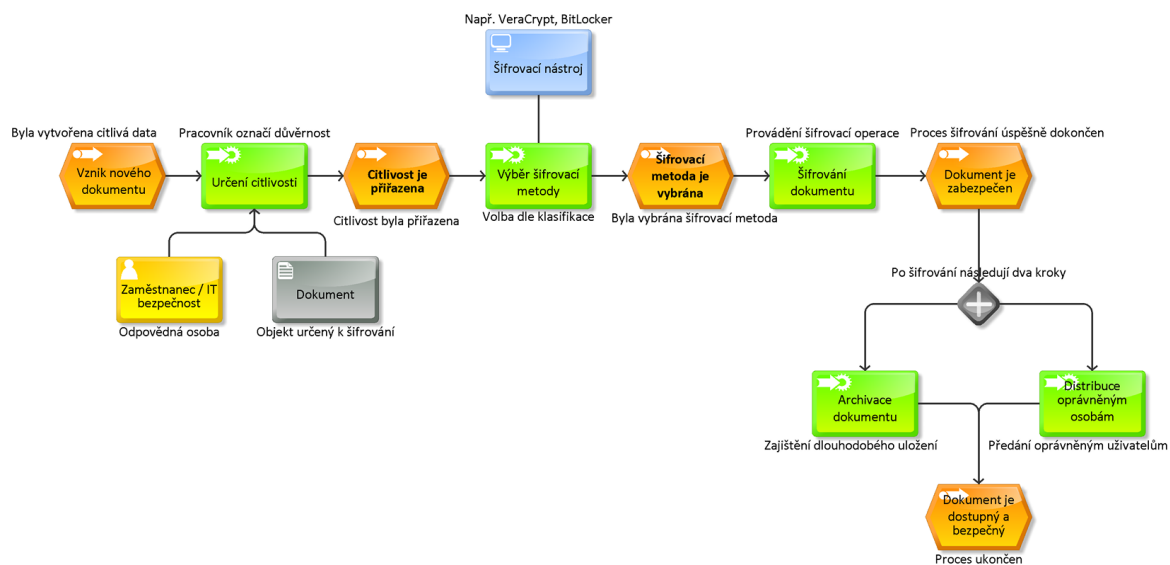
Obrázek 6 - BPMN diagram: Reakce na incident

(zdroj: vlastní)

5.10.5 Proces šifrování a archivace citlivých dat

Důvěrná data jsou po celou dobu svého životního cyklu chráněna šifrováním. Konkrétně při ukládání i při přenosu. Všechny přenosy probíhají výhradně přes zabezpečené komunikační kanály, jako jsou HTTPS, SFTP nebo VPN. Klíče jsou spravovány samostatně a přístupy k nim podléhají auditu.

Diagram na obrázku (Obrázek 7) znázorňuje nový proces šifrování citlivých dat v průběhu jejich uložení i přenosu. V EPC modelu jsou zaznamenány kroky jako výběr dat k zabezpečení, použití šifrovací metody a uložení do chráněného archivu. V procesu jsou zohledněny IT systémy a příslušné role, které vykonávají jednotlivé činnosti. Tento model zajišťuje šifrování v organizaci a snižuje riziko neautorizovaného přístupu k informacím.



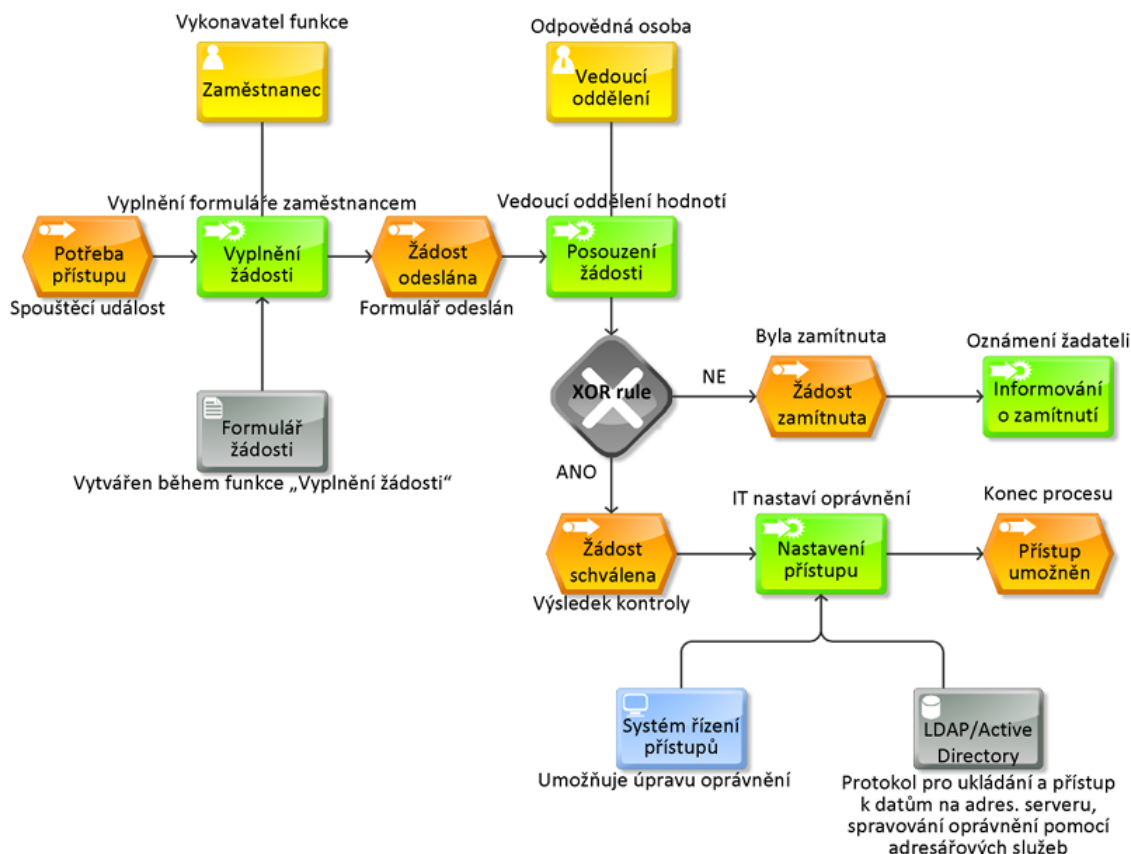
Obrázek 7 - EPC diagram: Proces šifrování dat

(zdroj: vlastní)

Archivace se provádí podle vnitropodnikových směrnic s ohledem na zákonem stanovené lhůty pro uchování a bezpečné odstranění. Před uložením do archivu se data kontrolují z hlediska integrity a po vypršení lhůty jsou bezpečně odstraněna pomocí nástrojů s příslušnou certifikací. [14]

5.10.6 Zpracování žádosti o přístup k datům

Tento diagram na obrázku (Obrázek 8) popisuje průběh žádosti zaměstnance o přístup k důvěrným informacím. Proces je zobrazen s důrazem na logiku událostí a funkcí. Začíná od vyplnění formuláře, přes schvalování až po technické nastavení přístupu. V EPC notaci je znázorněno nejen provázání jednotlivých kroků, ale i zapojení uživatelských rolí a nutných dokumentů. Tento model tak vede k větší transparentnosti a souladu s pravidly bezpečnostní politiky dané firmy.

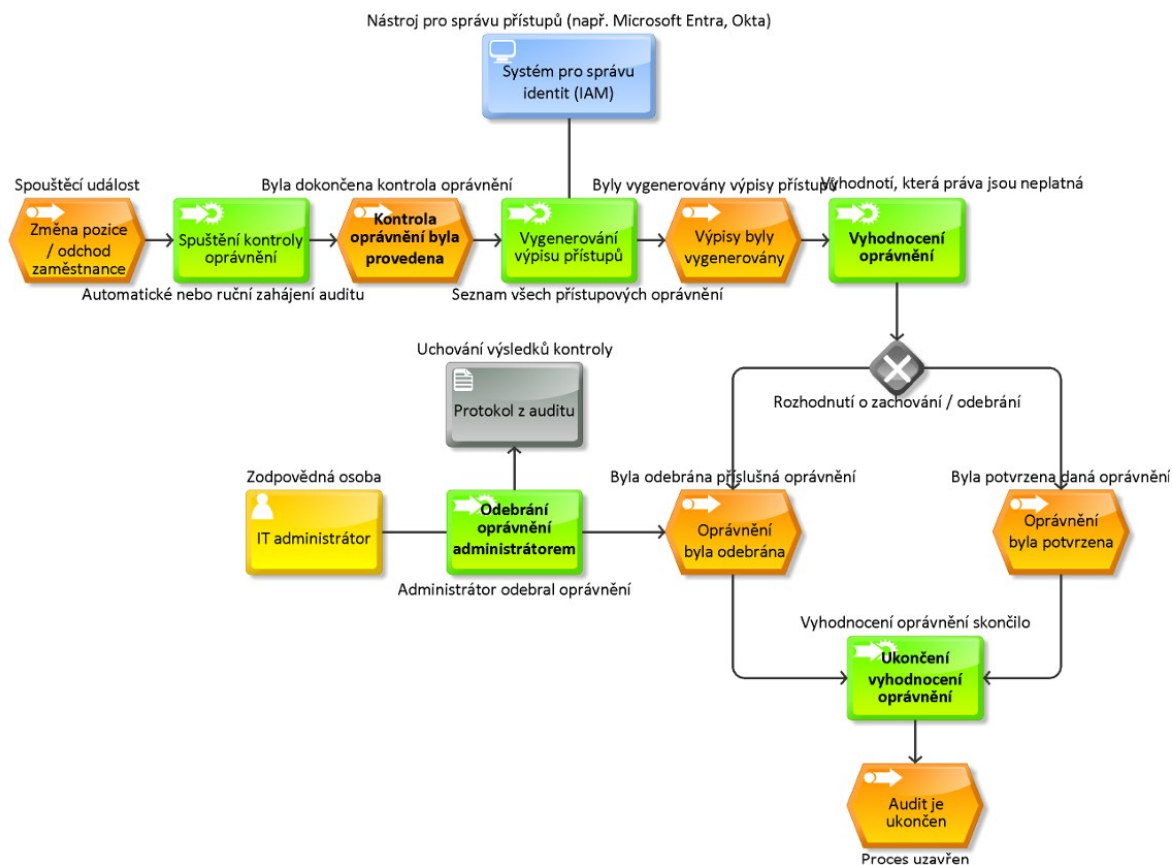


Obrázek 8 - EPC diagram: Zpracování žádosti o přístup k datům

(zdroj: vlastní)

5.10.7 Kontrola přístupových práv

V tomto obrázku (Obrázek 9) je zobrazen proces pravidelné revize oprávnění, který slouží k ověření jejich aktuálnosti. EPC notace zde umožňuje vyjádřit funkce, události i rozhodovací uzly jako je analýza, potvrzení či návrh na odebrání oprávnění. V rámci modelu je aplikováno logické pravidlo XOR a také je zapojena role IT administrátora. Tento postup tak snižuje riziko neoprávněného přístupu.



Obrázek 9 - EPC diagram: Kontrola přístupových práv

(zdroj: vlastní)

5.11 Přínosy navržených procesů

Zavedením nových podnikových procesů zaměřených na zvýšení ochrany dat před doxingem dochází ke zvýšení úrovně informatické a administrativní bezpečnosti v rámci organizace. Přijatá opatření nejen snižují pravděpodobnost neoprávněného přístupu k citlivým údajům, ale rovněž podporují vyšší transparentnost v práci s daty a přispívají k upevnění důvěry veřejnosti ve stabilitu a odpovědnost dané instituce. Následující části se věnují podrobnému popisu klíčových přínosů navržených řešení procesů.

5.11.1 Zamezení neoprávněnému přístupu

Jednou z hlavních výhod těchto nově implementovaných bezpečnostních procesů je výrazné snížení rizika neautorizovaného přístupu k důvěrným informacím. Zavedení dvoufázového ověřování, efektivní správa přístupových oprávnění a pravidelné přezkoumávání přístupových práv zajišťují, že důvěrné informace jsou přístupné výhradně uživatelům s odpovídající autorizací. Pečlivé řízení oprávnění rovněž minimalizuje možnost zneužití dat ze strany bývalých pracovníků nebo neidentifikovaných osob. [12]

5.11.2 Sledovatelnost činností se zabezpečenými daty

Neméně důležitým přínosem je posílení sledovatelnosti všech operací spojených s důvěrnými údaji. Zavedením systémových logů, sledováním přístupových aktivit a pravidelným vyhodnocováním operací lze přesně určit, který uživatel, v jakém čase a jakým způsobem s danými daty pracoval. Tím je zvýšena odpovědnost jednotlivých uživatelů a zároveň umožněno efektivní rozpoznání možných bezpečnostních hrozeb. [12]

5.11.3 Zvýšení důvěryhodnosti a reputace organizace

Díky zabezpečenému zacházení s osobními a důvěrnými daty se zároveň posiluje důvěra veřejnosti, klientů i obchodních partnerů vůči organizaci. V dnešním konkurenčním prostředí je bezpečné zpracování údajů často rozhodujícím faktorem při výběru partnera pro spolupráci. Firma, která aktivně chrání své citlivé informace si tak zvyšuje svou reputaci a také získává konkurenční výhodu. Tímto způsobem snižuje pravděpodobnost vzniku právních postihů nebo finančních ztrát spojených s únikem dat. [15]

6 VIZUALIZACE NAVRŽENÝCH PROCESŮ POMOCÍ DIAGRAMŮ

Navržené podnikové procesy určené k ochraně citlivých dat před útoky typu doxing byly znázorněny pomocí vizuálních modelů. K vytvoření vizualizací procesů byly využity dvě odlišné modelovací notace, a to BPMN (Business Process Model and Notation) a EPC (Event-driven Process Chain). Výběr těchto notací byl proveden s ohledem na jejich specifické vlastnosti, přednosti i vhodnost pro odlišné úrovně modelování.

6.1 Srovnání Business Process Model and Notation a Event-driven Process Chain

V rámci této bakalářské práce byly pro vizualizaci procesů v oblasti administrativní bezpečnosti využity dva standardizované modelovací jazyky BPMN a EPC. Každý z těchto přístupů nabízí své specifické výhody v závislosti na povaze modelovaného procesu a cílové skupině uživatelů. BPMN je určen především pro detailní technické modelování procesů a využívá se zejména v IT a vývoji. EPC představuje variantu vhodnou pro manažerské a strategické účely, kde je kladen důraz na srozumitelnost a organizační přehlednost. [12], [13]

Notace BPMN díky své široké sadě symbolů a přesně stanovené syntaxi umožňuje modelovat komplexní procesní logiku včetně větvení, zpracování událostí, výměny zpráv či práce s datovými objekty. Naproti tomu EPC se zakládá na střídání funkcí a událostí, což umožňuje přehledně zachytit logiku rozhodovacích toků bez nutnosti hluboké technické znalosti. Ve společnosti SecureData s.r.o. byly proto využity oba přístupy. EPC bylo využito pro znázornění obecného procesního rámce a BPMN pro podrobný návrh technických bezpečnostních opatření. [12], [13]

6.2 Výběr preferovaného modelovacího jazyka pro další práci

Pro potřeby této bakalářské práce byl jako hlavní modelovací jazyk pro další části zvolen EPC (Event-driven Process Chain). Rozhodnutí vychází z porovnání mezi notacemi BPMN a EPC s důrazem na vhodnost pro modelování administrativních bezpečnostních procesů zaměřených na ochranu dat před doxingem. EPC lépe odpovídá organizační a procesní úrovni řízení, která je běžná v podnicích při nastavování bezpečnostních opatření.

Modely vytvářené pomocí EPC umožňují zobrazit jak jednotlivé činnosti, tak i události, které tyto činnosti spouštějí. Tento přístup přináší přehledné zobrazení událostí, a to například při řešení bezpečnostních incidentů, žádostech o přístup nebo při zavádění opatření

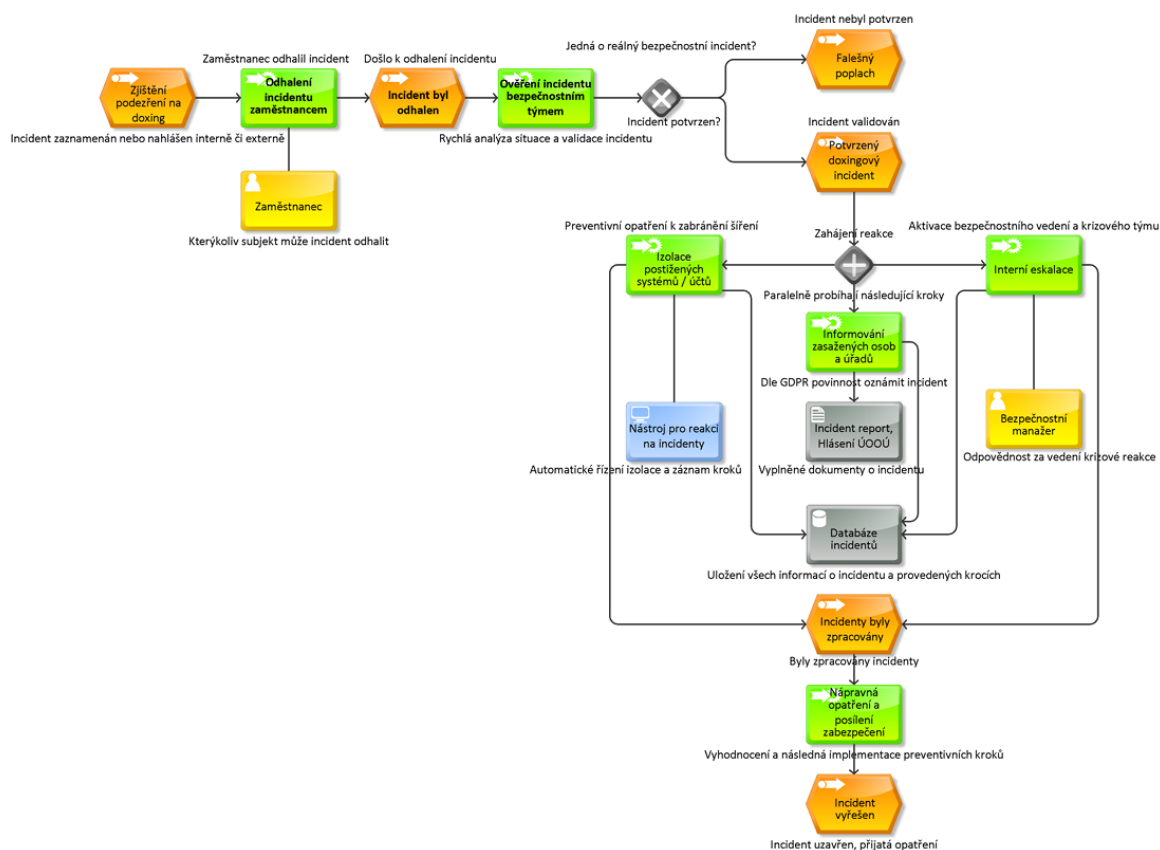
na ochranu osobních údajů. Výhodou EPC je také plná kompatibilita s nástrojem ARIS Express, který je určen právě pro tuto notaci a podporuje její standardizované prvky v souladu s metodikou ARIS. [13]

Z pohledu souladu s normami informační bezpečnosti je notace EPC přínosná tím, že podporuje modelování v rámci principů CIA triády a odpovídá požadavkům rámců jako GDPR. Díky tomu lze prostřednictvím EPC přesně definovat odpovědnosti, navázat bezpečnostní opatření na konkrétní procesní kroky a dokumentovat je způsobem, který je využitelný při auditech nebo při nastavování bezpečnostní politiky organizace. [13], [15]

6.3 Vizualizace modelových procesů pomocí Event-driven Process Chain

6.3.1 Reakce na incident typu doxing

Tento diagram na obrázku (Obrázek 10) zachycuje procesní model, pomocí kterého se v organizaci reaguje na podezření z doxingu, tedy neoprávněného zveřejnění důvěrných údajů společnosti. V EPC diagramu je zobrazena posloupnost činností. Jako první je identifikace incidentu a dále následuje jeho eskalace až po aktivaci krizového týmu a přijetí příslušných opatření. Pomocí notace EPC jsou zachyceny nejen klíčové funkce a události, ale i odpovědné role. Cílem tohoto postupu je minimalizace dopadů incidentu a ochrana citlivých informací společnosti a zaměstnanců, kterých se incident týká.

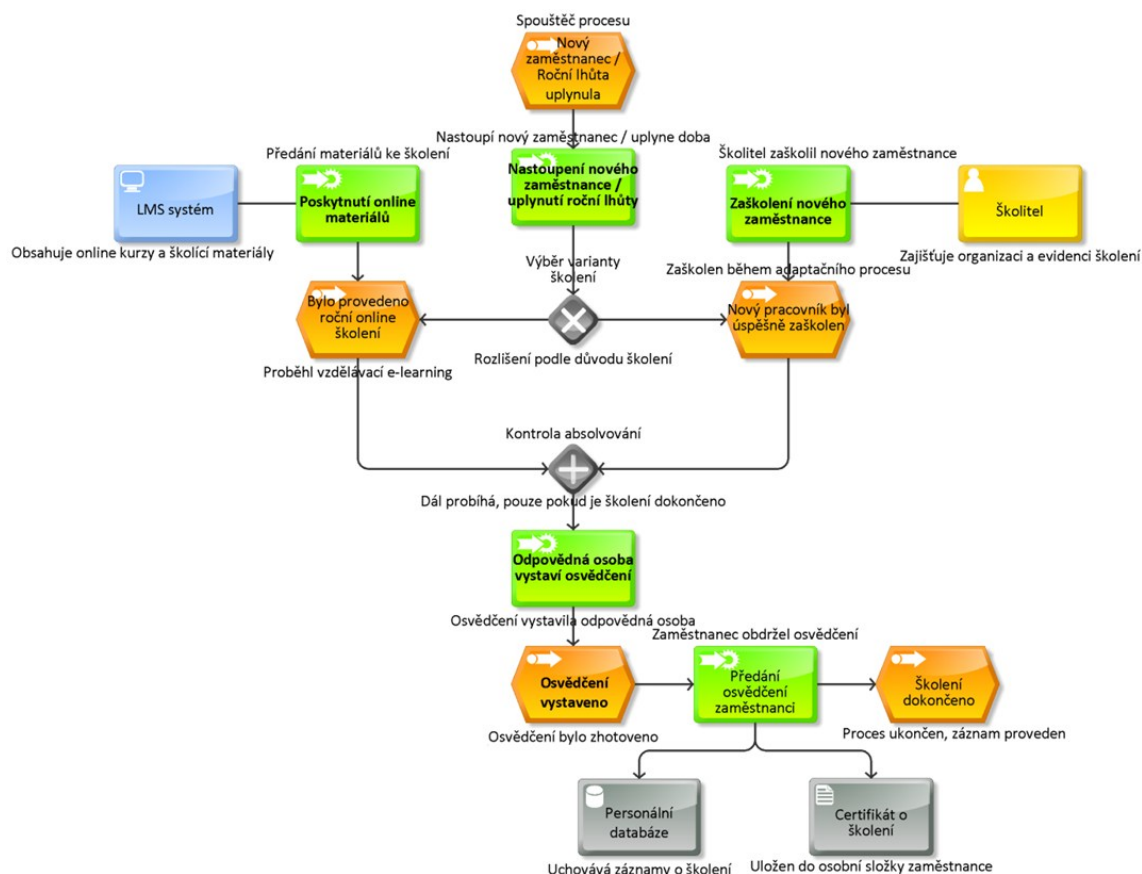


Obrázek 10 - EPC diagram: Reakce na incident typu doxing

(zdroj: vlastní)

6.3.2 Školení zaměstnanců o rizicích doxingu

Diagram, který je zobrazený na obrázku (Obrázek 11) představuje proces pravidelného školení zaměstnanců. Proces je zaměřený na oblast kybernetické bezpečnosti a větší pozornost je věnována také problematice doxingu. EPC notace zde zobrazuje události, jako je nástup nového pracovníka nebo opakované roční školení. Také obsahuje následné funkce, které zahrnují organizaci školení, testování znalostí a archivaci výsledků. Model rovněž zahrnuje přiřazené role, příslušné dokumenty a podpůrné IT nástroje, které celý proces doplňují. Tímto způsobem tak dochází ke snížení rizika lidského selhání při práci s důvěrnými informacemi.

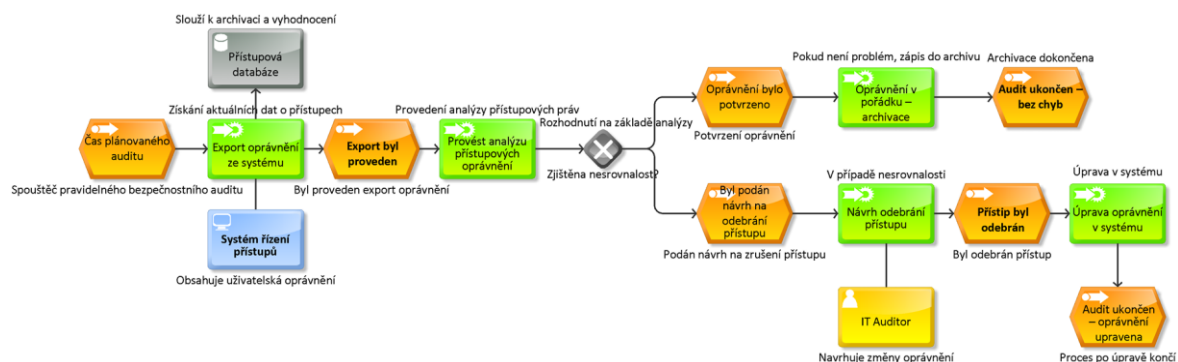


Obrázek 11 - EPC diagram: Školení zaměstnanců o rizicích doxingu

(zdroj: vlastní)

6.3.3 Audit přístupových práv

Tento procesní model na obrázku (Obrázek 12) se zaměřuje na kontrolu oprávnění uživatelů k vnitřním systémům a datům organizace. V EPC modelu je zachycen průběh auditu, který začíná zahájením kontroly, pokračuje analýzou existujících oprávnění a končí jejich potvrzením či návrhem na odebrání. Diagram obsahuje také spouštěcí události a rozhodovací body vyjádřené pomocí logického pravidla XOR. Hlavním cílem tohoto modelu je zajistit, že zaměstnanci mají přístup výhradně k datům, která nezbytně souvisí s jejich pracovním zařazením a pozicí.

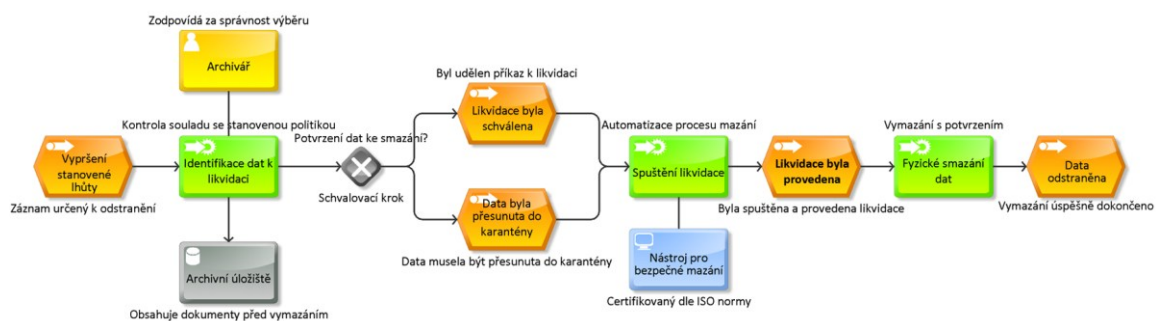


Obrázek 12 - EPC diagram: Audit přístupových práv

(zdroj: vlastní)

6.3.4 Bezpečné mazání dat

Diagram, který je na obrázku (Obrázek 13) popisuje postup, kterým je zajištěno bezpečné odstranění citlivých dat po uplynutí dané lhůty nebo na základě žádosti fyzické osoby. EPC notace znázorňuje jednotlivé kroky včetně určení dat ke skartaci, volby vhodné metody likvidace, závěrečné archivace a potvrzení o provedení. Součástí modelu je také zodpovědná osoba, využívaný IT systém a rozhodovací okamžiky, jako je výběr typu dat a způsob jejich odstranění. Tento proces vede k dodržování právních předpisů a k ochraně organizace před únikem starších citlivých informací.



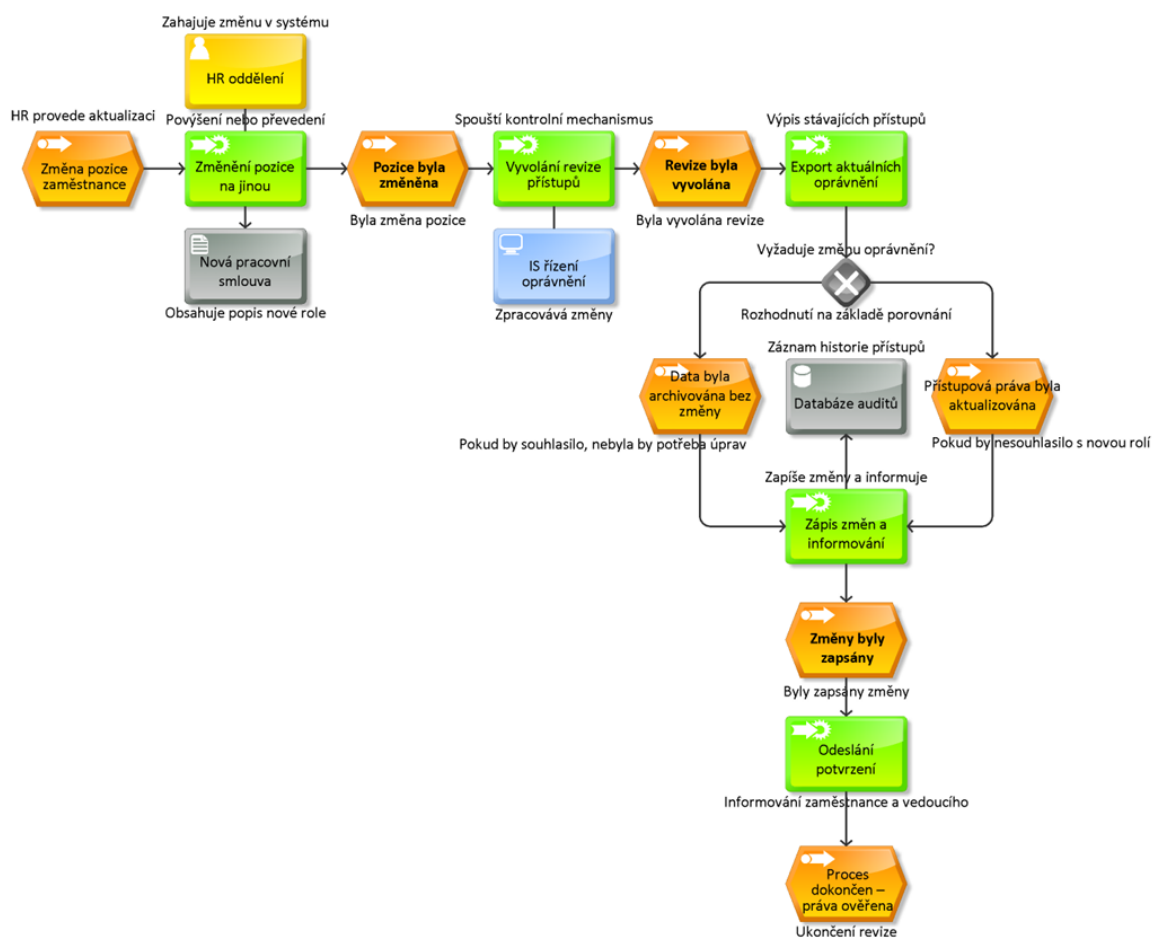
Obrázek 13 - EPC diagram: Bezpečné mazání dat

(zdroj: vlastní)

6.3.5 Periodická revize oprávnění po změně pozice

Na obrázku (Obrázek 14) je interní proces revize přístupových oprávnění, který se provádí v důsledku personálních změn. Jedná se například o změnu pracovní pozice nebo o odchod zaměstnance. EPC model zobrazuje události a funkce, které začínají oznámením změny, pokračují kontrolou přístupů a vedou až k jejich aktualizaci, potvrzení nebo odebrání. Do procesu je také zapojeno personální oddělení, které má danou úlohu na starosti. Díky tomuto

opatření je zajištěno, že přístup k citlivým informacím odpovídá aktuálnímu pracovnímu zařazení a nehrozí tak neoprávněné využívání dat.



Obrázek 14 - EPC diagram: Periodická revize oprávnění po změně pozice

(zdroj: vlastní)

ZÁVĚR

Cílem této bakalářské práce bylo zhodnotit problematiku doxingu z pohledu administrativní bezpečnosti a navrhnout konkrétní podnikové procesy, které by mohly vést k jeho účinné prevenci. V úvodní části bylo objasněno, co všechno doxing obnáší, jaké další pojmy jsou s ním spojené, jaké hrozby z něj plynou a jaké následky může mít pro jednotlivce i organizace.

V navazující praktické části byly navrženy podnikové procesy zaměřené na ochranu dat před riziky doxingu. Tyto návrhy zahrnovaly preventivní i reaktivní přístupy. Například se jedná o školení zaměstnanců, kontrolu oprávnění nebo reakční plán při bezpečnostním incidentu. Vizualizace jednotlivých procesů byla zpracována prostřednictvím nástroje ARIS Express a využity byly dvě modelovací notace, a to konkrétně BPMN a EPC. Na základě jejich porovnání byla zvolena notace EPC jako vhodnější pro znázornění administrativních procesů.

Z výsledků práce vyplývá, že doxing je reálnou a velkou hrozbou i pro firmy a instituce. Ochrana před tímto typem útoku by měla být kombinací technických opatření a organizačních procesů. Procesní modelování se ukázalo jako efektivní nástroj pro zapojení těchto opatření do běžného provozu. Navržené modely zajišťují přehlednost při rozdělování odpovědností. Také zlepšují kontrolu nad jednotlivými kroky bezpečnostního řízení.

Práce zároveň přináší praktický rámec, který může organizacím sloužit jako výchozí bod pro analýzu vlastní připravenosti na útoky typu doxing. Díky své flexibilitě lze navržené procesy snadno přizpůsobit specifickému prostředí a využít je při školeních, interních kontrolách či úpravách bezpečnostní politiky dané firmy.

SEZNAM POUŽITÉ LITERATURY

- [1] TUNG, Siev Thean. The Cyber Social Phenomenon of Doxing: An Examination of Hong Kong's Anti-doxing Law. Online. Dostupné z: <https://dspace.cuni.cz/bitstream/handle/20.500.11956/186883/120436570.pdf?sequence=1&isAllowed=y>. [cit. 2025-01-03].
- [2] BAILEY, Jane; FLYNN, Asher a HENRY, Nicola. *The Emerald international handbook of technology-facilitated violence and abuse. Emerald studies in digital crime, technology and social harms*. Bingley, U.K.: Emerald Publishing Limited, [2021]. ISBN 9781839828508. Dostupné také z: <https://proxy.k.utb.cz/login?url=https://doi.org/10.1108/9781839828485>. [cit. 2025-01-03].
- [3] MACALLISTER, Julia M. The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information. Online. 2017. Dostupné z: <https://ir.lawnet.fordham.edu/flr/vol85/iss5/21>. [cit. 2025-01-03].
- [4] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, CISA. Mitigating the Impacts of Doxing on Critical Infrastructure. Online. Dostupné z: https://www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxing_508.pdf. [cit. 2025-01-03].
- [5] LARSEN, Jacob. From Doxing to Doorstep: Exposing Privacy Intrusion Techniques used by Hackers for Extortion. *Black Hat USA Conference Presentation*, August 2024. Dostupné z: <https://larsencyber.com/blog/2024-08-07-blackhat-interviews-extorters/>. [cit. 2025-01-03].
- [6] MERALI, Alameen Karim. Malware Analysis of Doxbin. *Medium*, December 2023. Dostupné z: <https://medium.com/@brotheralameen/malware-analysis-of-doxbin-4a822cb8aa30>. [cit. 2025-01-03].
- [7] DOXBIN. From Doxing to Doorstep: Exposing Privacy Intrusion Techniques used by Hackers for Extortion. *Black Hat USA Conference Presentation*. [cit. 2025-01-03].
- [8] UNIVERSITY OF CALIFORNIA, BERKELEY. *Protect Yourself from Doxxing*. Office of Ethics, Risk and Compliance Services, 2025. Dostupné z: <https://oercs.berkeley.edu/privacy/privacy-resources/protect-yourself-doxxing>. [cit. 2025-02-22].

- [9] SOSAFE. *What Is Doxxing? | Examples & Prevention Tips*. 2023. Dostupné z: <https://sosafe-awareness.com/glossary/doxxing/>. [cit. 2025-03-19].
- [10] COVEWARE. *Doxxing Trends: Industrial Sector as Ransom “Non-Payor” in Q4*. 2021. Dostupné z: <https://www.coveware.com/blog/2021/2/18/q4-doxxing-victim-trends-industrial-sector-emerges-as-primary-ransom-non-payor>. [cit. 2025-03-19].
- [11] VERIZON. *2023 Data Breach Investigations Report*. 2023. Dostupné z: <https://www.verizon.com/business/resources/reports/dbir/>. [cit. 2025-03-19].
- [12] IDS SCHEER. *ARIS Express Manual*. Software AG, 2010. Dostupné z: <https://www.ariscommunity.com/aris-express>. [cit. 2025-04-23].
- [13] ONDRA, Pavel. *Procesní řetězec tažený událostmi (EPC)*. ARIS Architect, 2022. [cit. 2025-04-23].
- [14] EUROPEAN PARLIAMENT AND COUNCIL. *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*. Official Journal of the European Union, 2016. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. [cit. 2025-04-23].
- [15] APTIEN. *Co je CIA triáda informační bezpečnosti*. Aptien, 2025. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-cia-triad>. [cit. 2025-04-27].
- [16] VASTCAST [Doxbin Homepage]. In: *Wikimedia.org* [online]. 26. dubna 2022 [cit. 2025-05-04]. Dostupné z: https://upload.wikimedia.org/wikipedia/en/7/71/Doxbin_Homepage.png
- [17] ESET. *Co je to doxing a jak se mu bránit*. Digital Security Guide, 2023. Dostupné z: <https://digitalsecurityguide.eset.com/cz/co-je-to-doxing-a-jak-se-mu-branit>. [cit. 2025-05-18].
- [18] GOOGLE. Odstranění osobních údajů z vyhledávání. *Google Support*, 2024. Dostupné z: <https://support.google.com/websearch/answer/9673730>. [cit. 2025-05-18].
- [19] MOZILLA FOUNDATION. Firefox Monitor – Check for Data Breaches. *Mozilla*, 2024. Dostupné z: <https://monitor.firefox.com/>. [cit. 2025-05-18].
- [20] HAVE I BEEN PWNED. Check if your email or phone is in a data breach. *HaveIBeenPwned.com*, 2024. Dostupné z: <https://haveibeenpwned.com/>. [cit. 2025-05-18].

- [21] DUCKDUCKGO. Protecting Your Privacy Online. *DuckDuckGo Help Pages*, 2024. Dostupné z: <https://help.duckduckgo.com/privacy/>. [cit. 2025-05-18].
- [22] NATIONAL CYBERSECURITY ALLIANCE. Online Safety Basics: Protect Your Personal Information. *StaySafeOnline.org*, 2024. Dostupné z: <https://staysafeonline.org/stay-safe-online/online-safety-basics/>. [cit. 2025-05-18].
- [23] INTELLIGENCE X. Intelligence X – Search Engine for Investigators. *IntelligenceX.com*, 2024. Dostupné z: <https://intelx.io/>. [cit. 2025-05-18].
- [24] MALTEGO. Maltego CE: Community Edition. *Maltego Technologies*, 2024. Dostupné z: <https://www.maltego.com/>. [cit. 2025-05-18].
- [25] RECON-NG. Recon-ng Framework Documentation. *Github.com*, 2023. Dostupné z: <https://github.com/lanmaster53/recon-ng>. [cit. 2025-05-18].
- [26] CAMUNDA. *Camunda Modeler*. Camunda Services GmbH. Dostupné z: <https://camunda.com/products/modeler/>. [cit. 2025-05-23].
- [27] BIZAGI. *Bizagi Modeler*. Bizagi Limited. Dostupné z: <https://www.bizagi.com/en/products/bpm-suite/modeler>. [cit. 2025-05-23].
- [28] DIAGRAMS.NET. *Draw.io – Diagramming on the Web*. *diagrams.net*, 2025. Dostupné z: <https://www.diagrams.net/>. [cit. 2025-05-23].
- [29] BRAVE SOFTWARE. *Brave Browser: Secure, Fast & Private Web Browser with Adblocker*. Brave Software, 2025. Dostupné z: <https://brave.com/>. [cit. 2025-05-23].

SEZNAM OBRÁZKŮ

Obrázek 1 - Úvodní stránka Doxbinu	26
Obrázek 2 - Workflow: Reakce na incident doxingu.....	37
Obrázek 3 - Workflow: Prevence doxingu	38
Obrázek 4 - BPMN diagram: Řízení přístupových práv	49
Obrázek 5 - BPMN diagram: Školení zaměstnanců v oblasti bezpečnosti.....	50
Obrázek 6 - BPMN diagram: Reakce na incident.....	52
Obrázek 7 - EPC diagram: Proces šifrování dat	53
Obrázek 8 - EPC diagram: Zpracování žádosti o přístup k datům.....	54
Obrázek 9 - EPC diagram: Kontrola přístupových práv	55
Obrázek 10 - EPC diagram: Reakce na incident typu doxing.....	59
Obrázek 11 - EPC diagram: Školení zaměstnanců o rizicích doxingu	60
Obrázek 12 - EPC diagram: Audit přístupových práv	61
Obrázek 13 - EPC diagram: Bezpečné mazání dat	61
Obrázek 14 - EPC diagram: Periodická revize oprávnění po změně pozice	62

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EPC	Event-driven Process Chain
BPMN	Business Process Model and Notation
ARIS	Architecture of Integrated Information Systems
OSINT	Open Source Intelligence
EDR	Emergency Data Requests
IP	Internet Protocol
TOR	The Onion Router
CIA	Confidentiality, integrity and availability
GDPR	General Data Protection Regulation
VPN	Virtual Private Network
IT	Information Technology
HTTPS	Hypertext Transfer Protocol Secure
SFTP	Secure File Transfer Protocol
XOR	eXclusive OR
HR	Human Resources
IS	Information Systém
LDAP	Lightweight Directory Access Protocol
IAM	Identity and Access Management
OMG	Object Management Group
ÚOOÚ	Úřad pro ochranu osobních údajů
LMS	Learning Management Systém

SEZNAM PŘÍLOH

Příloha P I: ZIP soubor s diagramy v IS STAG

PŘÍLOHA P I: ZIP SOUBOR S DIAGRAMY V IS STAG

Příloha s jednotlivými diagramy ve formátech .pdf a .png.

Diagramy podle složek v ZIP souboru:

Složka s názvem „BPMN diagramy“ obsahuje tyto konkrétní diagramy:

BPMN - Reakce na únik dat.pdf

BPMN - Řízení přístupových práv.pdf

BPMN - Školení zaměstnanců v oblasti bezpečnosti.pdf

Složka s názvem „EPC diagramy“ obsahuje tyto konkrétní diagramy:

EPC - Audit přístupových práv.pdf

EPC - Bezpečné mazání dat.pdf

EPC - Kontrola přístupových práv.pdf

EPC - Periodická revize oprávnění po změně pozice.pdf

EPC - Proces šifrování dat.pdf

EPC - Reakce na incident typu doxing.pdf

EPC - Školení zaměstnanců o rizicích doxingu.pdf

EPC - Zpracování žádosti o přístup k datům.pdf

Složka s názvem „Workflow“ obsahuje tyto konkrétní diagramy:

Prevence doxingu (proaktivní workflow).png

Reakce na incident doxingu (reaktivní workflow).png