UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

# BAKALÁŘSKÁ PRÁCE

2024 Posselyonnaya Viktoriya

Univerzita Pardubice

Fakulta Ekonomicko-správní

# Vliv zabezpečení dat na podnikovou reputaci a vztah se zákazníky

Bakalářská práce

2024 Posselyonnaya Viktoriya

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

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Viktoriya Posselyonnaya** |
| Osobní číslo: | **E21592** |
| Studijní program: | **B0688A140004 Informatika a systémové inženýrství** |
| Specializace: | **Informační a bezpečnostní systémy** |
| Téma práce: | **Vliv zabezpečení dat na podnikovou reputaci a vztah se zákazníky** |
| Zadávající katedra: | **Ústav matematiky a kvantitativních metod** |

## Zásady pro vypracování

Cílem práce je popsat metody ochrany firemních dat a možností využití jejich cloudového uložení. Dále budou uvedeny příkladové studie vlivu zabezpečení dat na podnikovou reputaci a na vztah se zákazníky. V praktické části bude popsána praxe zabezpečení dat vybrané firmy a včetně pozitiv, negativ a návrhů do budoucna.

Osnova:
- Formulace specifik zabezpečení dat.
- Reputace firmy a její aspekty vlivu.
- Hrozby a způsoby zabezpečení.
- Příkladové studie vlivu zabezpečení dat na podnikovou reputaci.
- Navržení zabezpečení dat vybrané firmy.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

ACKERMAN, Pascal. Modern Cybersecurity Practises. BPB Publications, 2020. ISBN 978-9389328257.
DOSEDĚL, Tomáš.Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251--0106-1.
MORGUNOV, A.V. Informační bezpečnost. NGTU, 2023. 978-5-7782-3918-0.
PRESTON,W.Curtis. Modern Data Protection. O'Reilly Media, Inc.,2021. ISBN: 9781492094050.
RODRYČOVÁ, Danuše a Pavel STAŠA.Bezpečnost informací jako podmínka prosperity firmy. Praha: Grada, 2000. Manažer. ISBN 80-7169-144-5.

Vedoucí bakalářské práce: **Mgr. Jana Heckenbergerová, Ph.D.**
Ústav matematiky a kvantitativních metod

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

L.S.

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

**Ing. et Ing. Martin Lněnička, PhD.** v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

**Prohlašuji:**

Práci s názvem Vliv zabezpečení dat na podnikovou reputaci a vztah se zákazníky jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně nebo doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 06. 2024

Posselyonnaya Viktoriya v.r.

## Poděkování

Ráda bych poděkovala paní Janě Heckenbergerové za vedení a podporu během psaní mé bakalářské práce. Její snaha pomoct, odborné znalosti a schopnost předávat je srozumitelným způsobem mi umožnily lépe porozumět problematice mého tématu. Také bych chtěla poděkovat řediteli EPAM Kazachstán Artyomu Vetluginovi za poskytnutou pomoc a možnost spolupráce. Díky této spolupráce jsem získala cenné dovednosti, které mi budou nepochybně prospěšné v mé budoucí kariéře.

## ANOTACE

Tato bakalářská práce se zabývá analýzou vlivu zabezpečení dat na podnikovou reputaci a na vztah se zákazníky. Dnes, kde jsou podniky často terčem kybernetických útoků a porušení datového bezpečí, je důležité zkoumat, jaký dopad má takové porušení na pověst společnosti. Práce se zaměřuje na průzkum literatury a analýzu případových studií, pro porozumění dopadu bezpečnostních incidentů na podnikovou reputaci a důvěru zákazníků. Dále zkoumá opatření, která podniky mohou přijmout k ochraně dat a prevenci kybernetických útoků, a analyzuje jejich efektivitu pro zachování dobré reputace. Výsledky této práce poskytnou podnikům užitečné poznatky o důležitosti zabezpečení dat a jeho vlivu. To pomůže podnikům lépe porozumět rizikům spojeným s kybernetickou bezpečností a přijmout vhodná opatření k ochraně svých dat a udržení důvěry zákazníků.



## KLÍČOVÁ SLOVA

Zabezpečení dat, reputace, kybernetické hrozby


## TITLE

The influence of data security on corporate reputation and customer relationships


## ANNOTATION

This bachelor thesis examines the influence of data security on corporate reputation and customer relationships. Today, where businesses are often targets of cyber-attacks and data breaches, it is important to investigate the impact of such breaches on a company's reputation and its relationships with customers. The thesis focuses on literature review and analysis of case studies to understand the impact of security incidents on corporate reputation and customer trust. It further explores measures that businesses can take to protect data and prevent cyber-attacks, analyzing their effectiveness in maintaining a good reputation and customer relationships. The findings of this thesis will provide businesses with valuable insights into the importance of data security and its impact on corporate reputation and customer relationships. This will help businesses better understand the risks associated with cybersecurity and take appropriate measures to protect their data and maintain customer trust.



## KEYWORDS

Data security, reputation, cyber threats

# OBSAH

# SEZNAM OBRÁZKŮ

# SEZNAM ZKRATEK

ISO – International Organization for Standardization

ISMS – Information Security Management System

NDA – Nondisclosure Agreement

VPN – Virtual Private Network

IB – Informační bezpečnost

DDoS – Disitributed Denial-of – Service

IPS – Intrusion Prevention System

IDS – Intrusion Detection Systém

AI – Artificial Intelligence

IoT – Internet of Things

GDPR – General Data Protection Regulation

MFA – Multifaktorová autentizace

GRC – Governance Risk Management and Compliance

MGR – Managed Detection and Response

BAS – Breach and Attack Simulation

SIEM – Security Information and Event Management

# ÚVOD

Vzhledem k tomu, že digitalizace proniká do všech oblastí podnikání, stává se zabezpečení dat jedním z klíčových faktorů úspěchu pro společnosti všech velikostí a odvětví. Zabezpečení dat nejen chrání důvěrné informace a obchodní tajemství, ale má také významný dopad na reputace společnosti a vztahy se zákazníky. Tato bakalářská práce zkoumá, jaké konkrétní faktory ovlivňují pověst společnosti z hlediska zabezpečení dat a jaké důsledky má špatné zabezpečení dat na vztahy se zákazníky.

Cílem této práce je poskytnout komplexní pohled na bezpečnost dat, reputaci firmy a vztahy se zákazníky prostřednictvím analýzy teoretických poznatků a příkladů z praxe. Konkrétně se zaměří na identifikaci klíčových aspektů zabezpečení dat, které ovlivňují vnímání společnosti zákazníky a celkovou reputaci společnosti na trhu.

Studium této problematiky má důležitý praktický význam pro podnikání. Pomůže identifikovat klíčové faktory ovlivňující formování a udržování důvěry klientů. Také určí účinné strategie zajištění bezpečnosti dat na příkladu vybrané firmy. Tyto strategie přispívají ke zpevnění korporátní reputace a zlepšení vztahů s klienty. Nakonec může studium této problematiky přispět k rozvoji odolnějších a úspěšnějších organizací v podmínkách moderního digitálního byznysu.

# 1. DŮLEŽITOST ZABEZPEČENÍ DAT V PODNIKU

## 1.1. Definice a klasifikace dat

Data jsou nezbytnou součástí digitálního světa, mohou to být čísla, texty, obrázky, videa, zvukové nahrávky a další typy informací. Také jsou data pro podniky neocenitelným aktivem a klíčovým faktorem pro úspěch. Od malých podniků až po velké korporace jsou data hnací silou rozhodovacího procesu, strategického plánování a inovace. Správné využití a analýza dat umožňují podnikům pochopit své zákazníky, trhy a operace na nové úrovni, což vede k lepším strategickým rozhodnutím a konkurenční výhodě.

**Data** lze definovat jako soubor hodnot, které popisují vlastnosti objektu, události nebo jevu. Tyto hodnoty se mohou skládat z různých typů dat, jako jsou čísla, text nebo obrázky. Data se dají interpretovat a analyzovat za účelem získání informací [1]

**Správa dat** – je proces používaný k organizaci, uchování, aktualizaci, zabezpečení a zpracování dat v organizaci nebo informačním systému. Účelem správy dat je zajistit dostupnost, konzistenci, přesnost a aktuálnost data zároveň je chránit před neoprávněným přístupem nebo ztrátou. Správa dat je klíčovým prvkem pro zajištění efektivního využívání dat a podpory obchodních procesů v moderních organizacích.

**Klasifikace dat**

Data se dají klasifikovat podle různých kritérií, která usnadňují jejich pochopení a práci s nimi [2]:

**A. Podle typu:**

- **Numerická data:** Kvantitativní data, která se vyjadřují čísly (např. 12,5, 5). Mohou být dále rozdělena na diskrétní (celá čísla) a kontinuální (desetinná čísla).
- **Textová data:** Kvalitativní data, která se skládají z písmen, slov a vět (např. "Dobrý den"). Mohou zahrnovat různé formáty, jako je běžný text, HTML, XML a JSON.
- **Kategorická data:** Skupiny s pevně danými možnostmi, které se obvykle nazývají kategorie (např. "muž" nebo "žena").
- **Temporální data:** Informace o čase, která se obvykle ukládají v konkrétním formátu (např. datum a čas).
- **Prostorová data:** Informace o poloze, která se obvykle ukládají v souřadnicích (např. GPS souřadnice).

**B. Podle struktury:**

- **Strukturovaná data**

Tato data jsou uspořádána do tabulek s řádky a sloupci, které mají pevně definovanou strukturou a vztahy mezi nimi (např. databáze). Umožňují efektivní analýzu a dotazování. Strukturovaná data se nejčastěji řadí do kategorie kvantitativních dat a je to typ dat, se kterým je většina z nás zvyklá pracovat. Jedná se o informace, které se úhledně vejdou do pevně daných polí a sloupců v relačních databázích a tabulkových procesorech. Příkladem strukturovaných dat jsou jména, data, adresy, čísla kreditních karet, informace o zásobách, zeměpisná poloha a další. Strukturovaná data jsou dobře organizovaná a snadno srozumitelná pro strojový jazyk. Uživatelé relačních databází s nimi můžou relativně rychle pracovat – zadávat je, vyhledávat a upravovat. To je největší předností strukturovaných dat. Pro práci s nimi se používá programovací jazyk známý také jako SQL.

- **Nestrukturovaná data**

Nestrukturovaná data se nejčastěji řadí do kategorie kvalitativních dat a nelze je zpracovávat a analyzovat pomocí běžných nástrojů a metod. Mezi příklady nestrukturovaných dat patří text, video, audio, mobilní aktivita, aktivita na sociálních sítích, satelitní snímky, kamerové záznamy atd. Nestrukturovaná data se obtížně dekonstruují, protože nemají předem definovaný model, tzn. nelze je uspořádat v relačních databázích. Pro správu nestrukturovaných dat jsou proto nejvhodnější nereferenční databáze neboli databáze NoSQL. Zpracování a analýza těchto dat je náročnější [3].

**C. Podle zdroje:**

- **Interní data**

Informace a údaje, které organizace vytvářejí, udržují a uchovávají v rámci svých vlastních systémů a procesů. Tato data jsou často generována interními operacemi organizace, jako jsou transakce, záznamy o zákaznících, inventář, účetnictví, zaměstnanecké informace a další interní dokumentace. Interní data jsou obvykle specifická pro danou organizaci a zahrnují informace, které jsou citlivé a strategické pro fungování podniku. Organizace často využívají interní data pro analýzu výkonnosti, plánování zásob, posouzení efektivity procesů a řízení rizik. Kvalitní interní data jsou klíčovou součástí úspěšného řízení a rozvoje podniku.

- **Externí data**

Informace získané z externích zdrojů mimo organizaci. Tyto data jsou často dostupná veřejně nebo prostřednictvím placených služeb a zahrnují širokou škálu informací, jako jsou tržní trendy, demografické údaje, konkurenční analýzy a zpravodajství. Externí data mohou pocházet

z různých zdrojů, včetně průzkumů trhu, webových stránek, sociálních médií, vládních databází nebo specializovaných datových poskytovatelů. Jejich využití může pomoci organizacím lépe porozumět svému trhu, konkurenci a potenciálním rizikům a příležitostem.

## 1.2. Vlastnosti zabezpečení dat

Vlastnosti zabezpečení dat označují charakteristiky, rysy nebo atributy opatření a strategií používaných k ochraně dat před neoprávněným přístupem, zneužitím, poškozením nebo ztrátou. Ve světě tak existují základní regulační normy, které určují požadavky na zajištění bezpečnosti dat, jednou z nich je norma ISO 27001 [4].

ISO 27001 je mezinárodní norma pro řízení informační bezpečnosti, která poskytuje rámec pro efektivní ochranu informací a dat v organizacích. Tato norma stanovuje požadavky na implementaci a udržování systému řízení informační bezpečnosti (ISMS), který pomáhá organizacím identifikovat, řídit a minimalizovat rizika spojená s informační bezpečností. ISO 27001 poskytuje přístup k zajištění důvěrnosti, integrity a dostupnosti informací, ať už jsou to firemní údaje, osobní informace zákazníků nebo jiné citlivé informace. Tato norma je využívána organizacemi po celém světě jako prostředek k ochraně informací a posílení důvěry zákazníků, partnerů a dalších zainteresovaných stran. Podle normy ISO 27001 se rozdělují na tyto klíčové charakteristiky [5]:

A. **Důvěrnost** (Confidentiality):

- Identifikace citlivých informací: Organizace musí identifikovat data a informace, které mají zvláštní citlivost a vyžadují ochranu.
- Řízení přístupu: Implementace opatření a kontrolních mechanismů pro omezení přístupu k citlivým informacím pouze na oprávněné osoby nebo role.
- Šifrování: Použití šifrování pro ochranu dat při jejich přenosu nebo uložení, aby byla zajištěna jejich důvěrnost.

B. **Integrita** (Integrity):

- Ochrana proti neoprávněným změnám: Implementace opatření pro zajištění integrity dat, například digitální podpisy, kontrolní součty nebo mechanismy záznamu změn.
- Kontrola změn: Pravidelné monitorování a auditování dat a systémů pro detekci neoprávněných změn a manipulace s daty.
- Zálohování: Pravidelné zálohování dat a informací s cílem obnovit jejich integritu v případě jejich poškození nebo ztráty.

C. **Dostupnost** (Availability):

- Ochrana proti výpadkům: Implementace opatření a plánů pro minimalizaci rizika výpadků a zajištění nepřetržité dostupnosti dat a informací.
- Zálohování a obnova: Zajištění pravidelného zálohování dat a vypracování plánů pro obnovu dat v případě havárie nebo výpadku služby.
- Monitorování výkonnosti: Pravidelné monitorování výkonnosti a dostupnosti systémů a služeb pro identifikaci a řešení potenciálních problémů a výpadků.

## 1.3. Role zabezpečení dat

Zabezpečení dat představuje soubor opatření, technologií a procesů, které slouží k ochraně informací a dat proti různým rizikům a hrozbám. Zabezpečení dat není pouze o technologiích, ale i o politikách, postupech a vzdělávání zaměstnanců. Zahrnuje ochranu důvěrnosti dat, zajištění integrity dat a zabezpečení dostupnosti informací [4]. To znamená, že se snažíme zabránit neoprávněnému přístupu k datům, minimalizovat riziko neoprávněných změn nebo manipulací s daty a zajišťovat, aby byla data dostupná pro oprávněné uživatele, kdykoliv je potřebují. Je to neustále se vyvíjející oblast, která reaguje na nové hrozby a technologické inovace.

Zabezpečení dat je pro podniky všech velikostí nezbytné. Pomáhá chránit citlivé informace, dodržovat předpisy, chránit reputaci a zachovat kontinuitu provozu. Je to velmi důležité chránit svá data před neoprávněným přístupem, zneužitím, ztrátou a zničením. Zabezpečení dat je komplexní proces, který zahrnuje širokou škálu technických a organizačních opatření.

### A. Důvody pro zabezpečení dat

Existuje mnoho důvodů, proč je zabezpečení dat pro podniky tak důležité:

- Ochrana citlivých informací: Podniky shromažďují a zpracovávají velké množství citlivých informací, jako jsou osobní údaje zákazníků, obchodní tajemství a finanční data. Zabezpečení dat pomáhá organizacím zajistit, že tyto citlivé informace zůstanou v bezpečí před různými hrozbami, jako je krádež dat, zneužití informací a ztráta dat [6].Implementace vhodných opatření zabezpečení dat může pomoci minimalizovat riziko úniku dat a potenciálních škod, které by mohly organizaci způsobit jak z hlediska pověsti, tak i z hlediska právních a regulačních důsledků.
- Dodržování předpisů: Mnoho firem podléhá regulačním požadavkům, které jim ukládají povinnost chránit data. Zabezpečení dat pomáhá firmám splnit tyto požadavky a vyhnout se pokutám a sankcím.

- Ochrana reputace: Únik dat nebo kybernetický útok může poškodit reputaci firmy, vést ke negativní publicitě, poklesu ceny akcií, pokutám a sankcím a také ke ztrátě zákazníků a partnerů. Zabezpečení dat pomáhá firmám předcházet těmto událostem a chránit svou reputaci. Zákazníci, partneři a investoři jsou ochotnější spolupracovat s těmi, kteří berou ochranu dat vážně. Silná ochrana dat buduje důvěru a ukazuje, že firma je zodpovědná a spolehlivá.
- Zachování kontinuity provozu: Zachování kontinuity provozu je klíčovým cílem každé firmy, a to zejména v dnešní době, kdy jsou organizace stále závislejší na digitálních systémech a technologiích. Kybernetické útoky, jako jsou malware, ransomware nebo DDoS útoky, mohou mít devastující dopady na provoz firmy a vést k dočasnému nebo dokonce trvalému přerušení činnosti. Důležité je také mít vytvořené plány kontinuity provozu a obnovy po havárii (BCP/DRP), které stanoví postupy a záložní mechanismy pro rychlé obnovení operací v případě krize. To zahrnuje pravidelné zálohy dat, vytváření záložních kopií klíčových systémů a aplikací, a trénink zaměstnanců na případné reakce na krizové situace [7].

### B. Klíčové oblasti zabezpečení dat

Zabezpečení dat zahrnuje širokou škálu oblastí, z nichž nejdůležitější jsou:

- Fyzická bezpečnost: Ochrana datových center a zařízení před neoprávněným přístupem.
- Kybernetická bezpečnost: Ochrana počítačových systémů a sítí před kybernetickými útoky.
- Správa přístupu: Kontrola toho, kdo má přístup k datům a jak je může používat.
- Zálohování a obnova dat: Ochrana dat před ztrátou a zničením.
- Povědomí o kybernetické bezpečnosti: Vzdělávání zaměstnanců o rizicích kybernetické bezpečnosti a o tom, jak chránit data.

# 2. REPUTACE

## 2.1. Vliv reputace na podnik

Reputace je jedním z nejdůležitějších faktorů ovlivňujících dlouhodobý a udržitelný rozvoj firem. Pozitivní reputace podniku určuje rozhodnutí protistrany o otázkách spolupráce s ním, pomáhá přilákat vysoce kvalifikované pracovníky, zajišťuje přístup k investičním zdrojům a kvalitním odborným službám, působí jako určitý kredit důvěry pro své spotřebitele. Pozitivní obchodní pověst, její "dobré jméno" se tak stává zdrojem dalších výhod jak pro samotnou společnost, tak pro všechny strany, které mají zájem na úspěšné interakci s ní. Jako důležitá součást nehmotného majetku slouží jako významná ekonomická síla při strategickém rozvoji podniku. V podmínkách ekonomické nestability a zvýšené konkurence na trzích je navíc pozitivní reputace udržitelnou konkurenční výhodou podniku, kterou konkurence nemůže napodobit [8].

V éře globalizace a zvýšené konkurence o zdroje je nejdůležitější reputační charakteristikou společenská odpovědnost podniku, která zahrnuje zohlednění a minimalizaci negativních dopadů podniku nejen na ekonomiku, ale i na společnost a životní prostředí. Proto je třeba uvažovat o vytváření a posilování pověsti podniku v závislosti na tom, jak jeho činnost vnímají všechny zainteresované skupiny vlivu [9]. Ve státní praxi je zvyšování konkurenceschopnosti zboží a služeb přímo závislé na image podniků. Stabilní reputace vede ke zvýšení hodnoty akcií společností a přitahuje významný počet investorů, včetně zahraničních. Také společensky odpovědný podnik získává velké výhody na trhu práce jako zaměstnavatel, který přitahuje vysoce profesionální odborníky. Rozvoj podnikové kultury, budování pozitivní pověsti a dobré image podniků přispívají k posílení celkového postavení podniku na trhu.

Faktor reputace podniků se v poslední době stává vysoce aktuálním. V podmínkách, kdy se trhy nasytily podobně kvalitním zbožím a službami, se dopředu dostaly tzv. nezjevné faktory, jinými slovy nehmotná aktiva hodnoty podniku: reputace firmy, značky, reputace vedoucích pracovníků a vrcholových manažerů, strategie kvality a systém efektivní komunikace s cílovými skupinami. Celosvětovým trendem je neustálé zvyšování podílu nehmotných aktiv na hodnotě podniků. Reputace postupně nahrazuje tradiční reklamu jako hlavní "motor obchodu". Hodnota zboží je postupně nahrazována materiálními složkami, jinými slovy, nastal čas obchodování s obrazy a dojmy. Nyní již nestačí mít dokonalé výrobky a poskytovat kvalitní služby. Rozhodující se stává postavení firmy na trhu a nejvyšší postavení pro firmu je takové, v jakém zákazníci vnímají její image a dobrou reputaci. V tomto případě se pověst stává pro kupujícího nutností, něčím jako vírou ve svou firmu. Nekupují jen zboží a služby, ale i samotný postoj k firmě. A ten je zase

nejdůležitější nehmotnou složkou její hodnoty. Takto se stává úspěšná činnost firem možnou nejen na základě zvyšování objemu prodeje a růstu zisku. Na první místo se dostává reputace společnosti.

## 2.2. Sociálně-ekonomické aspekty vlivu reputace

V současné době se nevěnuje dostatečná pozornost analýze rizika poškození reputace společností v důsledku narušení zabezpečení dat. Tato nedostatečnost je způsobena také i chybějícími směrnicemi pro řízení vztahů podniků v oblasti zajištění dat. Při analýze incidentů v oblasti bezpečnosti, které vedou ke ztrátě reputace, můžeme rozlišit následující hlavní typy vztahů: vztahy se zaměstnanci (HR), s veřejností (PR), s vládními agenturami (GR) a s investory (IR) [9].

**Vztahy se zaměstnanci (HR)** jsou hlavním typem vztahů, které se vyskytují v každém podniku. Nebezpečí výskytu interního narušitele (insidera) je mimořádně vysoké, protože v současné době neexistuje plnohodnotná obrana proti jeho aktivitám. Chápání významu zabezpečení dat ze strany zaměstnanců je ve většině případů nedostatečné, což vede k neúmyslnému jednání zaměstnance, které umožňuje únik důležitých informací pro organizaci. Nelze také zakázat zaměstnanci, aby jednal "nestandardně", šířil rozporuplné, nepravdivé informace o své činnosti nebo o činnosti organizace, ale i skutečné informace o problémech v organizaci mezi známými, na internetu apod.

**Vztahy s veřejností (PR)** je samostatný typ vztahu, který je přímo zodpovědný za reputační složku aktivit společnosti. Porušení bezpečnosti informací v rámci public relations může být iniciováno buď útočníkem (v rámci "černého PR"), nebo osobou jednající v rámci svých úředních pravomocí, případně zaměstnancem, který dostatečně nerozumí kultuře zabezpečení dat (zveřejnění důležitých informací v otevřených mediálních zdrojích). Tyto incidenty mají za následek poškození dobré reputaci, což způsobuje společnostem různé typy ztrát.

**Vztahy se státní správou (GR)** znamenají budování a navazování vztahů s orgány veřejné správy, včetně státních, regionálních a místních orgánů. Pro udržení dobrého jména podniku ve veřejném sektoru je obvykle nutné budovat jeho podnikání v souladu s mnoha požadavky federálních zákonů, které upravují jeho činnost. V souvislosti s bezpečností informací existuje, jak seznam legislativních aktů, jejichž ustanovení musí brát v úvahu každá společnost bez ohledu na druh své činnosti, tak jednotlivé články odvětvových zákonů upravující různé aspekty zabezpečení dat. Za nesplnění požadavků zpravidla hrozí sankce ze strany státních struktur. Při problémech ve vztazích se státními orgány v rámci zajištění bezpečnosti informací tak podnik získává status

nevyhovující požadavkům úřadů, což způsobuje nedůvěru a ztrátu zákazníků, obchodních partnerů, akcionářů a následně vede ke ztrátám.

**Vztahy s investory** (IR) jsou pro velké společnosti, jejichž provoz je přímo závislý na investicích, velmi důležité. Pro řadu společností jsou investoři v podstatě jediným zdrojem financování, jehož ztráta by fakticky znamenala ukončení činnosti. Proto je velmi důležité vybudovat účinnou komunikační politiku ve vztazích mezi společností a investiční komunitou. Hlavním nástrojem pro budování úspěšných vztahů s investory ze strany podniku je včasné a úplné poskytování informací o jeho činnosti. Tyto informace jsou zpravidla poskytovány v rámci výroční zprávy, která je speciálně připravena pro investory a představuje potvrzení o účelném vynakládání finančních prostředků investorů. Je důležité si uvědomit, že jedním ze základních faktorů pro investora jsou informace o ziskovosti podnikání společnosti. Šíření informací o problémech v podniku, ať už nepravdivých nebo pravdivých, bude mít negativní dopad na názory investorů.

# 3. HROZBY ZABEZPEČENÍ DAT

## 3.1. Typy a původy hrozeb

Existence informační bezpečnosti je podmíněna faktorem negativního působení přírodních či umělých hrozeb. Hrozby zabezpečení dat jsou souborem faktorů, které narušují mechanismus ochrany informací. Například útok na software, krádež duševního vlastnictví, krádež identity, krádež zařízení nebo informací, sabotáž a vydírání informací. Hrozbou může být cokoli, co může využít zranitelnosti systému k narušení bezpečnosti, nepříznivé změně, vymazání, poškození objektu nebo objektů zájmu [10].

Existuje více než sto typů hrozeb pro informační systém. Je nezbytné analyzovat všechna rizika s využitím různých diagnostických metod. Na základě těchto podrobných analýz lze následně vytvořit účinný systém ochrany před hrozbami v informačním prostoru.

Mezi zdroje přírodních hrozeb patří například:

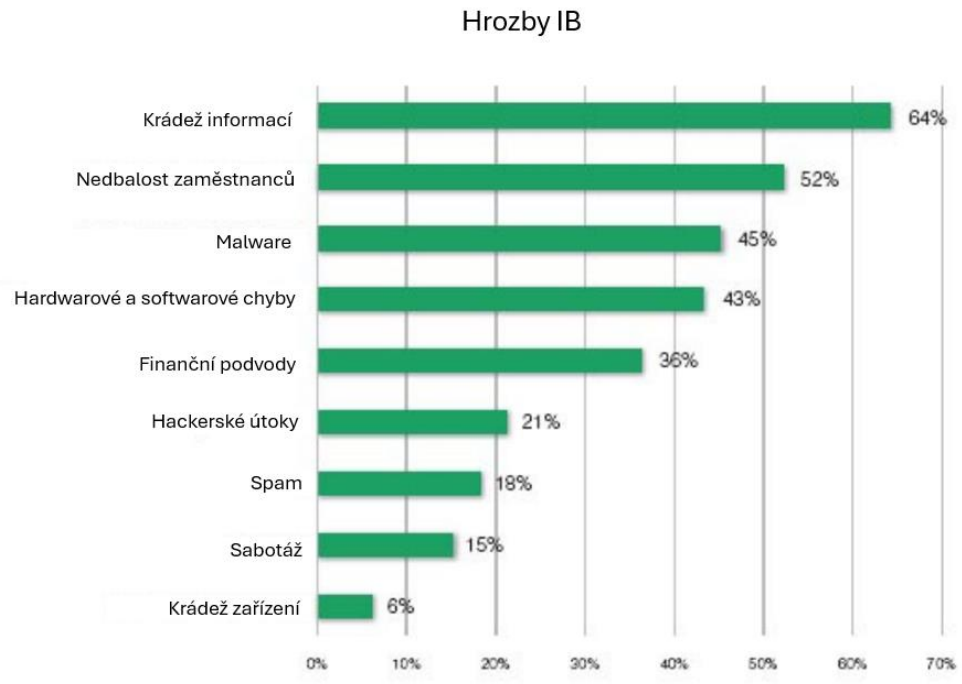
- Přírodní katastrofy a přírodní jevy, které člověk nemůže ovlivnit.

Příklady takových hrozeb zahrnují zemětřesení, které může způsobit fyzické poškození budov a infrastruktury, včetně serverových místností a datových center. Povodně mohou způsobit zaplavení zařízení a ztrátu dat, zatímco bouře a blesky mohou poškodit elektrickou infrastrukturu, což vede k přerušení dodávek elektrické energie a možným poruchám počítačových systémů. Dále, požáry mohou způsobit vážné škody na fyzickém vybavení a zasažení datových skladů. Tyto přírodní katastrofy nejenže ohrožují fyzickou infrastrukturu, ale mohou také ovlivnit dostupnost informačních systémů a jejich schopnost poskytovat služby.

- Poruchy počítačových systémů.

Pokud jde o poruchy počítačových systémů, ty mohou nastat z různých důvodů včetně technických závad, selhání hardwaru nebo softwaru a nedostatečné údržby. Tyto problémy mohou vést k neplánovaným výpadkům systémů a snížení jejich dostupnosti pro uživatele. Z tohoto důvodu je klíčové, aby organizace prováděly pravidelnou údržbu a monitorování svých IT systémů a měly připravené plány pro obnovu a kontinuitu provozu v případě, že dojde k poruše.

Umělé hrozby naproti tomu způsobují větší škody na následném fungování celého informačního systému, a naopak se dělí na umělé úmyslné a umělé neúmyslné hrozby.




**Obrázek 1:** Hrozby Informační Bezpečnosti

Zdroj: převzato z [11]

Obrázek znázorňuje graf s procenty, která ukazují, jak často se vyskytují různé hrozby informační bezpečnosti. Z toho lze usoudit, že největší nebezpečí představují krádeže informací a nedbalost zaměstnanců a nejmenší hrozbou je krádež zařízení.

Dle [6] lze hrozby dále dělit na:

Umělé úmyslné hrozby:

- Kopírování a krádeže dokumentů;
- Ničení informací;
- Sabotáž;
- Hackerský útok;
- Prozrazení informací;
- Porušení integrity informací;
- Neoprávněný přístup.

Umělé neúmyslné hrozby:

- Nedbalost;
- Zvědavost;

- Chyby softwaru;
- Chyba uživatele a podobně.

Hlavní rozdíl mezi přirozenými a umělými hrozbami spočívá v tom, že umělé hrozby jsou záměrně vytvořeny s cílem poškodit informační systém nebo jeho uživatele a získat tak osobní prospěch.

## 3.2. Základní metody hrozeb

Útočníci aktivně používají několik běžných metod útoků dat. Dle [3] mezi ně patří:

**Nelicencovaný software**. Velmi často vede snaha manažerů ušetřit finance nákupem nelicencovaného softwaru k selhání systému zabezpečení informací. Je důležité si uvědomit, že pirátský software nechrání před podvodníky, jejichž hlavním cílem je krádež informací. Majitel pirátského softwaru nemá mnoho výhod, jako je technická podpora a nezbytné aktualizace, které nabízejí vývojáři. Naopak, nelegální software může být plný virů, které ohrožují ochranu dat. Je známo, že 10 % pirátského softwaru má nainstalované viry, které kradou přihlašovací údaje a hesla uživatelů.

**Virový software** je v dnešní době jedním z největších nebezpečí. Je těžké si představit výši ztrát, které jsou každoročně způsobeny virovými hrozbami IT systémům podniků po celém světě. Podle odborníků je nárůst počtu virových útoků způsoben tím, že existuje stále více kanálů pro průnik škodlivého softwaru, především e-mail a messengery. Zvýšil se také počet cílů virových útoků. Dříve byly virům vystaveny pouze servery běžných webových provozovatelů, nyní však mohou viry napadat firewally, směrovače a další komponenty a části operačních systémů a podpůrné infrastruktury.

**Útoky DDoS** představují obrovské množství hackerských průniků do operačního systému s cílem vyřadit jej z provozu, tj. vytvořit nemožné podmínky pro práci zaměstnanců organizace. Útoky DDoS jsou vedeny na komunikační kanál, který může být blokován tokem nepotřebných informací, nebo na hlavní server IT systému. Výsledkem je jeho vyřazení z provozu na dlouhou dobu, od několika hodin až po několik dní. Takové útoky zpravidla používají konkurenti jako formu průmyslového vydírání nebo k uspání sysadminů při krádeži peněz z firemních účtů. Právě krádež finančních prostředků je často cílem útoků DDoS [4].

Kromě informačních hrozeb existují i další zásahy do činnosti služby informační bezpečnosti. Při kontrolách podniků mohou státní orgány zabavovat zařízení a všechna zařízení pro ukládání dat (HDD, paměťové karty, flash-USB atd.). Vzhledem k tomu, že většina důležitých podnikových

dat je uložena v digitální podobě na serverech, v případě jejich zabavení přestane společnost na určitou dobu fungovat. Současně propadlá data nikdo nenahradí, a pokud bude kontrola trvat déle než obvykle, může ztráta vést až k uzavření podniku [12].

# 4. ZPŮSOBY ZABEZPEČENÍ DAT

**Technické prostředky** zahrnují různé typy zařízení a metodiky navržené k ochraně informací na fyzické úrovni, což omezuje neoprávněný přístup k nim. Tyto prostředky mohou zahrnovat speciální zařízení, která blokují internetové signály v prostorách jako jsou konferenční místnosti, zámky a alarmy, které zabraňují přístupu do serverovny nebo archivu papírových dokumentů. Dalším příkladem je použití hesla na telefonu, které chrání data obsažená v něm v případě krádeže zařízení. Tyto technické opatření představují fyzickou bariéru, která brání neoprávněnému uživateli v přístupu k důvěrným informacím. Jejich cílem je minimalizovat rizika spojená s fyzickým přístupem ke zranitelným datům a zajištění, že pouze oprávnění jedinci mají možnost získat přístup k nim.

**Softwarové prostředky** jsou programy, které mohou detekovat a zabránit hrozbám bezpečnosti digitálních dat. Mezi nejběžnější patří antivirové programy, které monitorují a ochraňují systém před škodlivým softwarem, jako jsou viry, červi či trojské koně. Dalšími užitečnými nástroji jsou programy pro detekci a prevenci vniknutí, které sledují síťový provoz a identifikují podezřelou činnost, jako jsou neoprávněné pokusy o přihlášení nebo přenosy dat do neznámých lokalit.

K softwarovým prostředkům ochrany informací patří také technologie pro šifrování. Tyto technologie převádějí data do sady znaků, které nelze dešifrovat bez správných klíčů. Tím se chrání informace před odhalením v případě úniku. Softwarové nástroje jsou důležitou součástí strategie zabezpečení informací v organizacích, protože pomáhají detekovat a odpovědět na různé hrozby a chrání citlivé údaje před zneužitím nebo únikem.

**Organizační prostředky** představují klíčový prvek v rámci ochrany informací v organizaci a zahrnují široké spektrum kroků, které podniká vedení firmy. Jedním z těchto opatření je vytvoření a implementace přísných politik korporátní bezpečnosti, které stanovují pravidla a postupy pro zacházení s citlivými informacemi a systémy. Důležitou součástí organizačních opatření je také dohled a kontrola dodržování těchto bezpečnostních politik, které zajišťují, že zaměstnanci dodržují stanovené postupy a omezení. Kromě toho organizace provádí školení zaměstnanců ohledně bezpečnostních pravidel a postupů, aby byli informováni o nejnovějších hrozbách a způsobech ochrany. Dalším důležitým krokem je podpis NDA (Non-Disclosure Agreement) při nástupu nových zaměstnanců, což zajišťuje, že zaměstnanci jsou vázáni k zachování důvěrnosti a ochraně citlivých informací firmy. Organizační opatření jsou klíčovým prvkem celkové strategie zabezpečení informací a pomáhají minimalizovat riziko úniku dat a zneužití informací v organizaci [1].

Pokud mluvíme o ochraně osobních údajů, k organizačním opatřením můžeme zařadit pravidla internetové hygieny a života. Například nedůvěřovat podezřelým odkazům, nenechávat elektronická zařízení bez dozoru na veřejných místech, nebo používat VPN při připojování k veřejné Wi-Fi síti v kavárnách. Organizační opatření mají klíčový význam pro prevenci rizik spojených s nedostatečnou ochranou dat a zajištění, že zaměstnanci jsou informováni a schopni dodržovat bezpečnostní politiky a postupy stanovené společností.

## 4.1. Metody zabezpečení dat

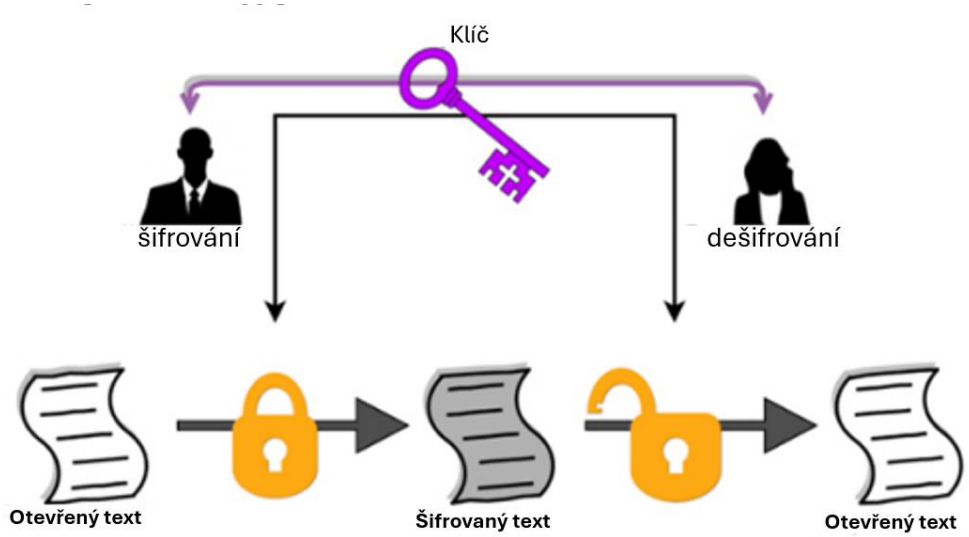
Metody zabezpečení dat jsou souborem postupů, technik a nástrojů navržených k ochraně citlivých informací před neoprávněným přístupem, zneužitím nebo únikem. Tato kapitola se zabývá různými přístupy k zabezpečení dat, které organizace mohou použít k ochraně svých aktiv a zachování integrity a důvěrnosti informací.

K ochraně digitálních materiálů lze použít několik metod zabezpečení informací [2]:

**A. Šifrování.**

Šifrování je kryptografická metoda, která chrání digitální materiál tím, že jej převede do zašifrované podoby (viz Obr 2). Šifrování lze použít na mnoha úrovních, od jednoho souboru až po celý disk. Existuje mnoho šifrovacích algoritmů, z nichž každý šifruje informace jiným způsobem a vyžaduje použití klíče k dešifrování dat a jejich převedení do původní podoby. Síla šifrovací metody závisí na velikosti klíče. Například 256bitové šifrování bude bezpečnější než 128bitové.

Je třeba poznamenat, že šifrování informací je účinné, pokud třetí strana nemá přístup k používanému klíči. Uživatel, který zadá heslo k šifrovanému disku a nechá svůj počítač bez dozoru, poskytne třetí straně možnost přístupu k datům uloženým v šifrované oblasti, což může vést ke krádeži, kopírování a dalším úmyslným hrozbám. K zašifrovanému digitálnímu materiálu lze přistupovat pouze pomocí klíčů. Ztráta nebo zničení těchto klíčů proto povede ke znepřístupnění dat.




**Obrázek 2:** Šifrování dokumentů

Zdroj: upraveno dle [3]

### B. Blockchain

Blockchain je technologie decentralizovaného ukládání dat. Data jsou rozdělena do bloků, každý blok je propojen s předchozím, což vytváří řetězec. Změny dat v předchozích blocích jsou náročným procesem a ve většině případů jsou nemožné. Proto vše, co je zaznamenáno do blockchain sítě, zůstává nezměněno navždy. Tato technologie se využívá například v zdravotnictví, kde organizace ukládají zdravotní záznamy pacientů do blockchainu.

Blockchain umožňuje vytvoření decentralizovaného registru transakcí nebo datového úložiště, které není pod kontrolou jediné entity. To znamená, že žádná centrální autorita nemá úplnou kontrolu nad blockchain sítí, což může zlepšit transparentnost a důvěru ve výměnu dat a transakcí. V zdravotnictví může toto využití blockchainu znamenat zvýšení bezpečnosti a integrity záznamů pacientů a usnadnění sdílení informací mezi různými poskytovateli péče o zdraví [13].

### C. IDS-systémy

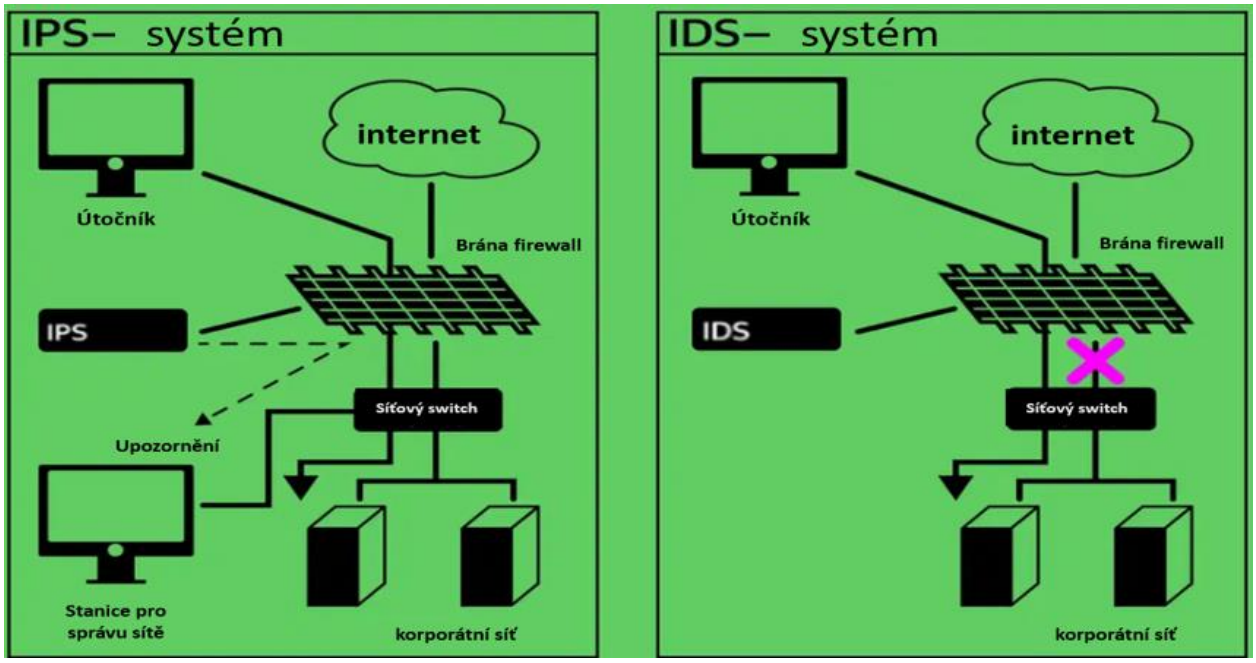
IDS je technologie určená k detekci neoprávněných vniknutí. IDS sleduje síťový provoz nebo provoz v rámci korporátního systému a identifikuje neobvyklou aktivitu, která naznačuje možné bezpečnostní porušení. Například se jedná o pokusy o proniknutí do sítě nebo útoky na servery. IDS systém lze nainstalovat na úrovni sítě nebo na úrovni jednotlivých zařízení. V prvním případě systém analyzuje veškerý provoz, zatímco v druhém pouze ten, který prochází daným zařízením. IDS systémy jsou klíčové pro prevenci a detekci kybernetických hrozeb a útoků. Pomáhají organizacím identifikovat potenciální bezpečnostní incidenty a reagovat na ně včas, což může

minimalizovat riziko ztráty dat nebo narušení provozu. Integrace IDS do bezpečnostní infrastruktury organizace je důležitým krokem k ochraně citlivých informací a udržení integrity a bezpečnosti sítě a systémů.

### D. IPS-systémy

IPS je technologie určená k prevenci neoprávněných vniknutí. Na rozdíl od IDS nejenom zaznamenává potenciální bezpečnostní hrozby, ale také přijímá aktivní opatření k ochraně informací. Například automaticky blokuje IP adresy, ze kterých se pokouší prolomit systém. IPS také identifikuje nejen externí útoky, ale i interní – když útok probíhá z počítače některého z pracovníků.

IPS systém může také skenovat stahované soubory a zabránit nainstalování virů na počítače uživatelů. Tímto způsobem IPS aktivně chrání síť a systémy před škodlivým softwarem a útoky, a to jak zvenčí, tak i zevnitř organizace. Integrace IPS do bezpečnostní infrastruktury organizace je klíčová pro posílení ochrany dat a zachování integrity a bezpečnosti sítě. Pomáhá organizacím předcházet kybernetickým hrozbám a útokům a minimalizovat riziko ztráty dat nebo narušení provozu.




**Obrázek 3:** IPS a IDS systémy

zdroj: upraveno dle [14]

### E. Firewall

Firewall je technologie, která poskytuje ochranný štít mezi zařízením a externími sítěmi. Pomocí firewallu lze například distribuovat provoz mezi zařízeními a omezit přístup k určitým zdrojům. Firewally jsou instalovány například ve školách, aby chránily děti před nevhodným nebo nebezpečným obsahem. Nebo v organizacích, aby blokovaly spam, který posílají potenciální zločinci na e-maily zaměstnanců. Firewally mají různé funkce a mohou být nastaveny podle potřeb konkrétního prostředí. Mohou filtrovat síťový provoz na základě určitých pravidel, monitorovat přenos dat a blokovat nebezpečné nebo podezřelé aktivity. Díky firewallům mohou organizace lépe chránit své sítě a data před různými hrozbami a útoky z internetu [5].

## 4.2. Trendy zabezpečení dat

**Umělá inteligence** se stává nedílnou součástí moderního zabezpečení dat. Pomáhá organizacím předcházet, identifikovat a reagovat na různé hrozby v reálném čase. Jednou z klíčových oblastí, kde AI přináší revoluci, je detekce hrozeb. Díky pokročilým algoritmům a strojovému učení je AI schopna analyzovat obrovské množství dat a identifikovat vzory, které naznačují potenciální hrozby, jako jsou malware, phishingové útoky nebo anomální aktivity v síti.

Dalším významným aspektem AI v zabezpečení dat je automatizace. AI může automatizovat mnoho úloh spojených s bezpečností, jako je detekce a odpověď na hrozby, správa incidentů a aktualizace bezpečnostních opatření. To nejenže zvyšuje efektivitu a rychlost reakce na incidenty, ale také uvolňuje lidské zdroje pro strategické úkoly. Umělá inteligence také posiluje schopnost predikce a prevence hrozeb. Na základě analýzy historických dat a trendů může AI předpovědět možné budoucí hrozby a navrhnout proaktivní opatření k ochraně organizace [15]. Tímto způsobem může předcházet vzniku incidentů a minimalizovat jejich dopady.

**Biometrické technologie pro kontrolu přístupu**. Systémy pro kontrolu přístupu prochází ještě přechodným obdobím, avšak stále jasněji se projevuje trend přechodu na biometrické technologie. V současné době trh nabízí širokou škálu biometrických řešení pro identifikaci: rozpoznání obličeje, snímání otisků prstů, dlaní, žilní struktury, sítnice oka. Hlavní výhodou biometrie je vysoká úroveň spolehlivosti a přesnosti rozpoznávání. Systémy rozpoznávání obličeje se v tomto seznamu stávají více rozšířenými jako nejpohodlnější a nejrychlejší způsob bezkontaktní identifikace uživatele. Vzhledem k přechodnému období si zákazníci také všímají možnosti multifaktorového ověření nebo nastavení různých metod ověřování pro různé skupiny uživatelů.

**Model Zero Trust**. Po řadě velkých hackerských útoků na infrastrukturu po celém světě v posledních letech se posílení architektury zabezpečení sítě, stejně jako vzdělávání koncových uživatelů a zvyšování jejich znalostí v této oblasti, stalo nejvyšší prioritou. Koncept Zero Trust, nebo také "Nulové důvěry", byl vyvinut již v roce 2010, ale širokou popularitu a rozšíření získal až nedávno. Strategická iniciativa Zero Trust vychází z postulátu "nikdy nedůvěřuj a vždy ověřuj" a zaměřuje se na prevenci úniku dat a zvýšení bezpečnosti moderních informačních systémů. Původně byl tento koncept přijat v IT průmyslu, ale nyní se jeho přístupy používají také v oblasti fyzické bezpečnosti, jakmile se ochranná zařízení stávají důležitou součástí směřování IoT (Internet of Things) [16].

# 5. PŘÍPADOVÉ STUDIE VLIVU ZABEZPEČENÍ DAT

V této kapitole se podíváme na příklady úniků dat, které měly významný dopad na podnikovou reputaci. Pro názornější příklad jsou uvedeny velké mezinárodní společnosti, na které měly tyto incidenty největší dopad z hlediska pověsti a tržní hodnoty.

Prvním příkladem je únik dat ze společnosti META(Facebook) v roce 2018, kdy se dostal ven soubor s osobními údaji více než 50 milionů uživatelů. Druhým příkladem je únik dat ze americké společnosti Equifax, kdy unikly osobní údaje téměř poloviny populace Spojených států. Posledním příkladem je podobná situace ve společnosti Uber v roce 2016, která zasáhla 56 milionů lidí včetně zaměstnanců firmy.

## 5.1. Equifax

V této kapitole se podíváme na dva příklady úniků dat, které měly významný dopad na podnikovou reputaci. Prvním příkladem je únik dat ze společnosti META(Facebook) v roce 2018, kdy se dostal ven soubor s osobními údaji více než 50 milionů uživatelů. Druhým příkladem je únik dat ze americké společnosti Equifax, kdy unikly osobní údaje téměř poloviny populace Spojených států.

Equifax je globální společnost specializující se na poskytování úvěrových informací o spotřebitelích a firmách. Únik dat ve společnosti byl způsoben narušením bezpečnosti, ke kterému došlo v období od května do července 2017. Hackeři zneužili zranitelnost v open-source softwaru Apache Struts, který společnost používala ve svých webových aplikacích [17]. Tato zranitelnost byla veřejně známá a byla vydána oprava, ale Equifax ji neaplikoval včas, což umožnilo útočníkům proniknout do systému. Během útoku získali hackeři přístup k citlivým osobním informacím, včetně jmen, adres, dat narození a čísel řidičských průkazů. Celkově bylo kompromitovány osobní údaje přibližně 147 milionů lidí. Tento rozsah úniku způsobil značné obavy o ochranu osobních údajů a kybernetickou bezpečnost.

Ihned po oznámení úniku dat, které proběhlo v září 2017, došlo k prudkému poklesu hodnoty akcií Equifaxu:


**Obrázek 4** Equifax akcie

Zdroj: převzato z [18]

Akcie společnosti se během několika dní propadly o více než 13 %, což znamenalo ztrátu miliard dolarů v tržní hodnotě. Tento pokles byl způsoben několika faktory [17]:

a. Ztráta investorů:

Investoři reagovali na zprávy o úniku dat negativně, protože ztráta důvěry veřejnosti v bezpečnost a integritu společnosti může mít dlouhodobé negativní dopady na její finanční výsledky. Ztráta důvěry investorů vedla k hromadnému prodeji akcií.

b. Očekávané právní a regulační sankce:

Únik dat vyvolal vyšetřování ze strany vládních orgánů, což znamenalo, že Equifax čelil možnosti vysokých pokut a dalších sankcí. Investoři brali v úvahu potenciální finanční zátěž spojenou s těmito sankcemi, což přispělo k poklesu hodnoty akcií.

c. Náklady na nápravu a posílení bezpečnosti:

Společnost musela investovat značné prostředky do zlepšení svých bezpečnostních opatření a poskytnout postiženým zákazníkům ochranu před zneužitím jejich dat, například prostřednictvím bezplatného monitorování úvěrů. Tyto náklady měly také negativní dopad na finanční výkonnost společnosti.

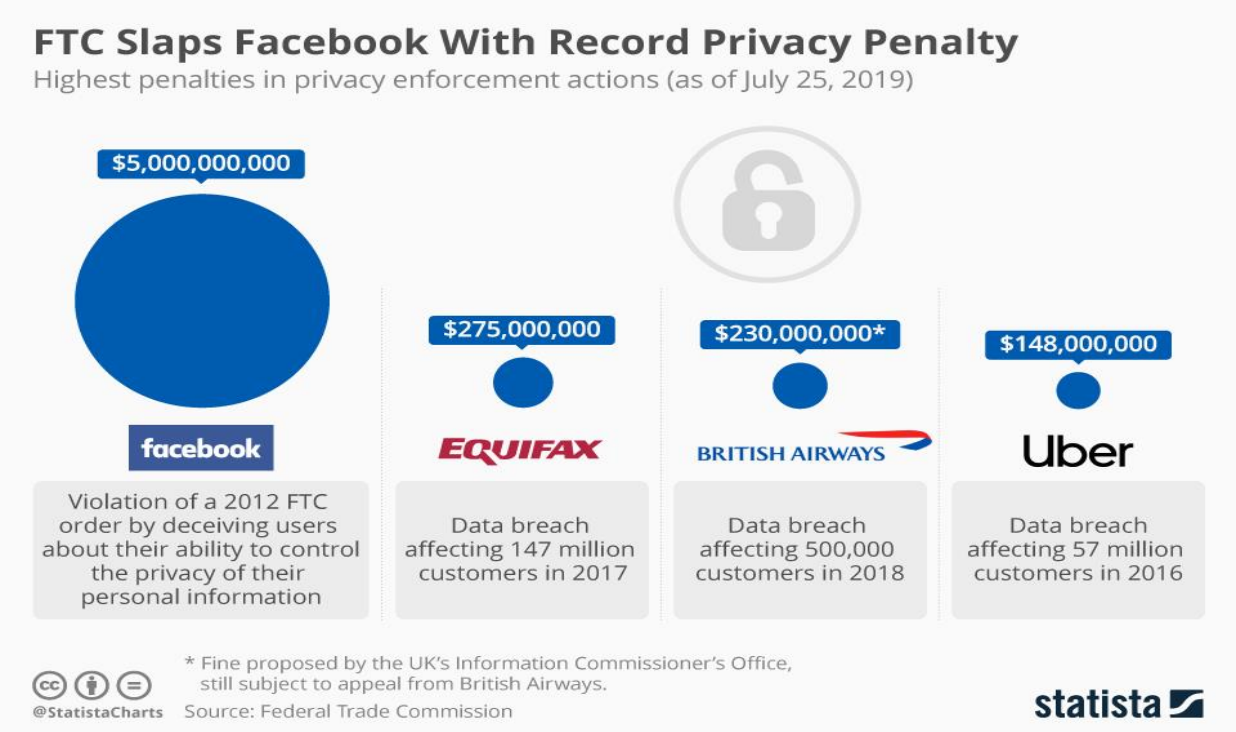
## Opatření

V případě Equifaxu, společnost byla nucena přijmout několik klíčových technických opatření, včetně posílení šifrování citlivých údajů, zavedení vícefaktorové autentizace (MFA) a pravidelných penetračních testů a bezpečnostních auditů. Interně Equifax přepracoval své procesy týkající se ochrany dat, zavedl přísnější kontrolu přístupu a investoval do školení zaměstnanců v oblasti kybernetické bezpečnosti, aby zvýšil povědomí o hrozbách a zlepšil reakci na bezpečnostní incidenty.

Incident zdůraznil zranitelnost velkých organizací a potřebu dalšího zlepšování bezpečnostních opatření. Zatímco Equifax čelil významným finančním a reputačním škodám, incident také přinesl pozitivní změny v oblasti zabezpečení dar a kybernetické bezpečnosti po celém světě.

## 5.2. Facebook

Důsledkem úniku dat však nemusí být jen pokles akcií, například společnost **Facebook** dostala v roce 2019 rekordní pokutu 5 miliard dolarů za masivní únik osobních údajů svých uživatelů. Pro srovnání, čistý příjem sociální sítě v roce 2019 činil 18,5 miliardy dolarů. Tato platba byla první velkou sankcí pro Facebook v USA za předání dat společnosti Cambridge Analytica [19].




**Obrázek 5** Rekordní pokuta za únik dat Facebook

Zdroj: převzato z [20]

Celý incident začal, když společnost Cambridge Analytica, politická konzultační firma, získala přístup k osobním údajům milionů uživatelů Facebooku bez jejich výslovného souhlasu. Tento přístup byl umožněn prostřednictvím aplikace „thisisyourdigitallife“. Aplikace byla původně navržena jako nástroj pro psychologický výzkum a nabízela uživatelům možnost účastnit se kvízů výměnou za přístup k jejich osobním údajům. Facebook o úniku věděl, ale nic s tím neudělal [19].

Problém nastal, když aplikace nejenže shromažďovala data od uživatelů, kteří ji používali, ale také získávala data od jejich přátel na Facebooku, a to bez jejich vědomí či souhlasu. Tímto způsobem byly shromážděny osobní informace přibližně 87 milionů uživatelů. Cambridge Analytica poté využila tato data k vytváření profilů voličů a k cíleným politickým kampaním, což zahrnovalo i kampaň pro prezidentské volby v USA v roce 2016.

Skandál byl odhalen v 2018, kdy novináři z The New York Times a The Guardian zveřejnili podrobné informace o tom, jak byla data zneužita. Zveřejnění těchto informací mělo okamžité a vážné důsledky pro Facebook.

Únik dat ve firmě Facebook měl několik významných dopadů:

1. Ztráta důvěry:

Mnoho uživatelů ztratilo důvěru ve schopnost Facebooku chránit jejich soukromí. To vedlo k odlivu uživatelů a opatrnějšímu přístupu inzerentů, což negativně ovlivnilo obchodní model společnosti založený na reklamách.

2. Negativní publicita:

Média po celém světě věnovala velkou pozornost tomuto incidentu, což trvale poškodilo image společnosti v očích veřejnosti a přivedlo k menší aktivitě na platformě.

3. Hromadné žaloby:

Facebook čelil mnoha hromadným žalobám ze strany uživatelů, kteří byli postiženi únikem dat. Hromadné žaloby umožnily tisícům uživatelů, kteří by jinak neměli prostředky na individuální soudní řízení, se připojit k jedné společné žalobě proti Facebooku. Tyto případy se táhly po několik let a vyžadovaly značné právní zdroje a náklady na obou stranách.

4. Změny v politice ochrany dat:

Společnost musela přehodnotit a aktualizovat své zásady ochrany osobních údajů, aby lépe chránila data uživatelů a byla v souladu s novými regulacemi.

## Opatření

Facebook po skandálu rovněž musel zavést rozsáhlá opatření ke zlepšení své bezpečnosti. Společnost omezila přístup třetích stran k uživatelským datům prostřednictvím API, zavedla přísnější pravidla pro přístup a automatizované nástroje pro detekci a blokování problematických aplikací. Transparentnost byla posílena zavedením nových nástrojů, které uživatelům umožňují snadno zjistit a spravovat sdílené informace. Facebook také posílil své bezpečnostní týmy a investoval do technologií pro prevenci kybernetických útoků.

### 5.3. Uber

Únik dat ve společnosti Uber se odehrál v říjnu 2016, ale veřejnost o něm byla informována až o více než rok později, v listopadu 2017. Hackeři využili zranitelnosti v kódu na serverech Uberu, což jim umožnilo přístup k citlivým informacím. Během tohoto útoku se hackerům podařilo získat osobní údaje zhruba 57 milionů uživatelů Uberu, včetně jejich jmen, e-mailových adres, telefonních čísel a údajů o řidičích, včetně čísla řidičských průkazů. Místo toho, aby společnost únik okamžitě zveřejnila a informovala postižené osoby, rozhodla se zaplatit hackerům 100 000 dolarů za zničení získaných dat a zamlčela incident [21]

Uber zažíval podobné důsledky jako Facebook a Equifax:

1. Finanční ztráty:

Společnost Uber zaplatila útočníkům 100 000 dolarů za to, aby incident utajila, což bylo později kritizováno jako pokus o zatajení narušení bezpečnosti. Kromě toho byla Uberu udělena pokuta ve výši 148 milionů dolarů v rámci urovnání s americkými státními zástupci.

2. Poškození reputace:

Incident značně poškodil důvěru zákazníků a partnerů Uberu. Společnost byla kritizována za svůj přístup k bezpečnosti dat a za snahu utajit narušení před veřejností a regulačními orgány.

3.Změny ve vedení společnosti:

Incident přispěl ke změnám ve vrcholovém vedení společnosti. Generální ředitel odstoupil a Uber přijal nové vedení, které mělo za úkol zlepšit bezpečnostní politiku a obnovit důvěru veřejnosti.

## Opatření

Po odhalení úniku dat a následné veřejné kritice přijala společnost Uber řadu opatření k nápravě situace a obnovení důvěry svých uživatelů a zaměstnanců. Jedním z prvních kroků bylo zřízení

speciálního týmu pro kybernetickou bezpečnost, který měl za úkol posílit ochranu dat a zabránit dalším útokům. Dále byla zahájena spolupráce s externími bezpečnostními firmami, které prováděly pravidelné audity a hodnocení bezpečnostních opatření Uberu. Zaměstnanci byli školeni v oblasti kybernetické bezpečnosti a ochrany osobních údajů, aby se zamezilo opakování podobných incidentů.

Celkově lze konstatovat, že všechny společnosti musely pracovat na obnově své reputace. To zahrnovalo nejen technická vylepšení, ale také aktivní komunikaci s veřejností a regulačními orgány. Veřejnost a zákazníci začali více dbát na ochranu svých osobních údajů a očekávali od firem vyšší standardy bezpečnosti [17]. Transparentnost a odpovědnost se staly klíčovými faktory v jejich snaze obnovit důvěru. Přijetí přísnějších bezpečnostních opatření a větší otevřenost vůči uživatelům byly nezbytné kroky, aby ukázaly, že berou ochranu osobních údajů vážně. Tyto kroky byly důležité nejen pro obnovu důvěry, ale i pro udržení konkurenceschopnosti na trhu, kde je bezpečnost dat stále důležitější. Tyto události také přispěly k většímu tlaku na regulátory, aby zpřísnili pravidla týkající se ochrany osobních údajů, což vedlo k zavedení přísnějších legislativních opatření, jako je například evropské nařízení GDPR (General Data Protection Regulation).

# 6. NAVRŽENÍ ZABEZPEČENÍ DAT VYBRANÉ FIRMY

## 6.1. Popis vybrané společnosti

EPAM Kazachstán je součástí společnosti EPAM Systems, globální společnosti zabývající se vývojem softwaru a IT poradenstvím. Společnost EPAM Systems byla založena v roce 1993 a rychle se stala jedním z vedoucích světových poskytovatelů služeb v oblasti vývoje softwaru a IT poradenství. Společnost je známá svými odbornými znalostmi v oblasti vývoje softwarových produktů, který zahrnuje celý vývojový cyklus od koncepce a návrhu až po implementaci a podporu. Mezi projekty, na kterých EPAM Kazachstán pracuje, patří vývoj komplexních informačních systémů pro bankovní sektor, tvorba mobilních aplikací pro velké obchodní řetězce a implementace řešení umělé inteligence a strojového učení pro zdravotnická zařízení. Každé z těchto řešení je zaměřeno na zvýšení efektivity a použitelnosti pro koncové uživatele.

Jedním z klíčových aspektů činnosti společnosti EPAM Kazachstán je informační bezpečnost. V dnešním světě kybernetických hrozeb se zabezpečení dat stalo kritickým prvkem pro každou IT společnost a EPAM Kazachstán není výjimkou. Společnost zavádí nejmodernější bezpečnostní opatření na ochranu dat klientů a zajišťuje jejich důvěrnost a integritu. Patří sem používání moderních nástrojů a technologií, které zabraňují úniku dat, obrana proti kybernetickým útokům a pravidelné bezpečnostní kontroly a aktualizace.

Na základě výše uvedených skutečností závisí reputace společnosti do značné míry na jejím přístupu k tomu zabezpečení. Vzhledem ke stále častějším únikům dat a kybernetickým útokům hledají klienti společnosti, kterým mohou svěřit svá data. Vysoké bezpečnostní standardy společnosti EPAM Kazachstán pomáhají budovat důvěru zákazníků a zajišťují stálý přísun objednávek. Spolehlivé zabezpečení informací je pro společnost také důležitou konkurenční výhodou, která jí umožňuje vyniknout na trhu a přilákat nové zákazníky. Také se společnosti daří udržovat vysokou úroveň spokojenosti zákazníků díky jasnému a transparentnímu procesu vývoje. Zákazníci jsou zapojeni do všech fází projektu, což umožňuje zohlednit jejich přání a upravit průběh prací v souladu s jejich očekáváními. Tento přístup zajišťuje nejen kvalitní výsledky, ale také posiluje dlouhodobé vztahy s klienty.

## 6.2. Popis stávajících technologií a metod

Společnost EPAM, jakožto globální lídr v oblasti softwarového inženýrství a IT služeb, přikládá mimořádný význam ochraně dat a neustále investuje do moderních technologií a metod pro zajištění nejvyšší úrovně zabezpečení. Tato kapitola se zaměřuje na detailní popis jednotlivých

technologií a metod, které společnost EPAM implementuje k ochraně dat svých zákazníků a interních informací, a ukazuje, jak tyto postupy přispívají k robustnímu zabezpečení a ochraně proti stále sofistikovanějším kybernetickým hrozbám.

### A. Šifrování dat

Šifrování je jedním z klíčových prvků zabezpečení dat, které EPAM využívá k ochraně citlivých informací. Podle slov manažera infrastruktury – všechna data, ať už při přenosu nebo v klidu, jsou šifrována pomocí pokročilých šifrovacích algoritmů jako AES-256. Tento přístup zajišťuje, že i v případě neoprávněného přístupu k datům jsou tyto informace nečitelné bez odpovídajícího dešifrovacího klíče.

### B. SIEM

SIEM (Security Information and Event Management) je třída softwarových produktů určených ke sběru a analýze informací o bezpečnostních událostech. SIEM kombinuje správu informací o bezpečnosti (SIM) a správu událostí v oblasti bezpečnosti (SEM).

Princip fungování:

SIEM sbírá a analyzuje data o bezpečnostních událostech z různých zdrojů, jako jsou síťová zařízení, servery a aplikace. SIEM systémy korelují a analyzují data pomocí pravidel, behaviorální analýzy a strojového učení, aby identifikovaly potenciální hrozby a anomálie. Při detekci bezpečnostního incidentu generuje SIEM výstrahy pro bezpečnostní týmy. Tyto týmy pak vyšetřují výstrahy, určují zdroj a rozsah hrozby a podnikají kroky k její vyřešení. SIEM také uchovává data pro splnění regulačních požadavků a umožňuje dlouhodobé sledování a analýzu bezpečnostních trendů, poskytuje reporty a dashboardy pro přehled o bezpečnostním stavu organizace [21].

SIEM systémy shromažďují data z různých zdrojů v rámci IT infrastruktury organizace. Tyto zdroje mohou zahrnovat:

- Síťová zařízení (např. routery, switche, firewally);
- Servery a pracovní stanice;
- Aplikační logy;
- Antivirové programy;
- Systémy pro detekci a prevenci průniků (IDS/IPS);
- Systémy pro správu přístupu a autentizaci.

### C. MDR

Managed Detection and Response je přístup kybernetické bezpečnosti, který spojuje monitorování, detekci a reakci na hrozby do jediné služby. MDR je služba poskytovaná externím poskytovatelem, která zahrnuje detekci, monitoring a reakci na kybernetické hrozby. MDR poskytuje firmám odbornou podporu v oblasti bezpečnosti pomocí pokročilých technologií, jako je SIEM, ale navíc zahrnují expertní analýzu a aktivní reakci na incidenty.

Princip fungování:

Hlavním principem MDR je, že odborníci na kybernetickou bezpečnost neustále monitorují a analyzují aktivity na sítích, serverech a dalších zdrojích organizace. To umožňuje včasné odhalení anomálního chování a potenciálních hrozeb. Po odhalení incidentu přijmou MDR poskytovatelé opatření k jeho řešení. MDR také poskytuje firmám cenné informace a zprávy o aktuálním stavu bezpečnosti, zjištěných hrozbách a doporučeních pro zlepšení celkové úrovně ochrany. Hlavními výhodami MDR jsou rychlá reakce na hrozby, proaktivní detekce nových typů kybernetických útoků, schopnost odhalit falešné poplachy a odstranění slabých míst v bezpečnostních systémech. To vše pomáhá předcházet potenciálním kybernetickým útokům a minimalizovat možné ztráty pro organizaci [22].

Nástroje MDR:

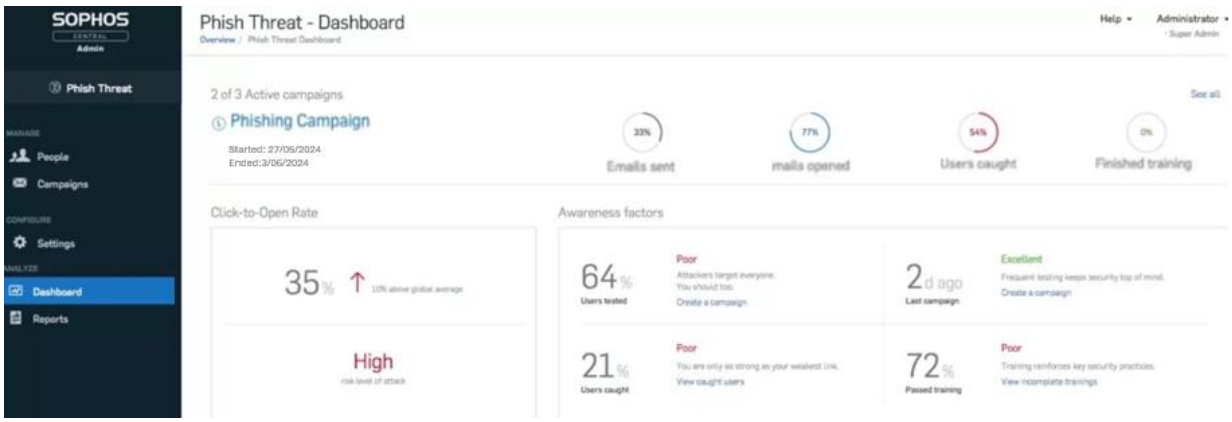
Dle [23] do služby MDR mohou být zahrnuty následující technologie:

- **Endpoint Detection and Response (EDR)**, **Network Detection and Response (NDR)** nebo **Extended Detection and Response (XDR)** — řešení pro detekci a reakci na kybernetické hrozby. EDR pracuje s hrozbami na koncových bodech (serverech, počítačích zaměstnanců atd.), NDR na úrovni sítě a XDR na různých úrovních.
- **Endpoint Protection Platform (EPP)** — komplexní ochranná řešení pro koncové body, která zahrnují antivirový software, technologie šifrování dat, technologie pro sledování a odstraňování zranitelností, kontrolu aplikací a zařízení atd.
- **Security Information and Event Management (SIEM)** — řešení pro sběr a automatickou analýzu informací o bezpečnostních událostech.
- **Intrusion Detection System (IDS)** — řešení pro detekci podezřelé aktivity uvnitř firemní infrastruktury.

## 6.3. Identifikace slabých míst

I přestože společnost bere ochranu svých dat vážně a používá nejmodernější technologie k jejích zabezpečení, stále existují i slabá místa jako je například lidský faktor, který je často považován za jeden z nejslabších článků v oblasti zabezpečení dat společnosti (viz Obr 1., str 19). I když technologická opatření jako firewally, šifrování, antivirové programy atp. mohou výrazně zvýšit ochranu dat, chyby a nepozornost zaměstnanců mohou tyto obranné mechanismy snadno narušit. Lidské chyby, jako je nedodržování bezpečnostních protokolů, používání slabých hesel nebo klikání na škodlivé odkazy v e-mailech, mohou vést k závažným bezpečnostním incidentům. Navíc sociální inženýrství, kde útočníci manipulují s lidmi za účelem získání citlivých informací, představuje další významnou hrozbu. Z tohoto důvodu bylo rozhodnuto provést phishing jako způsob ověření této teze.

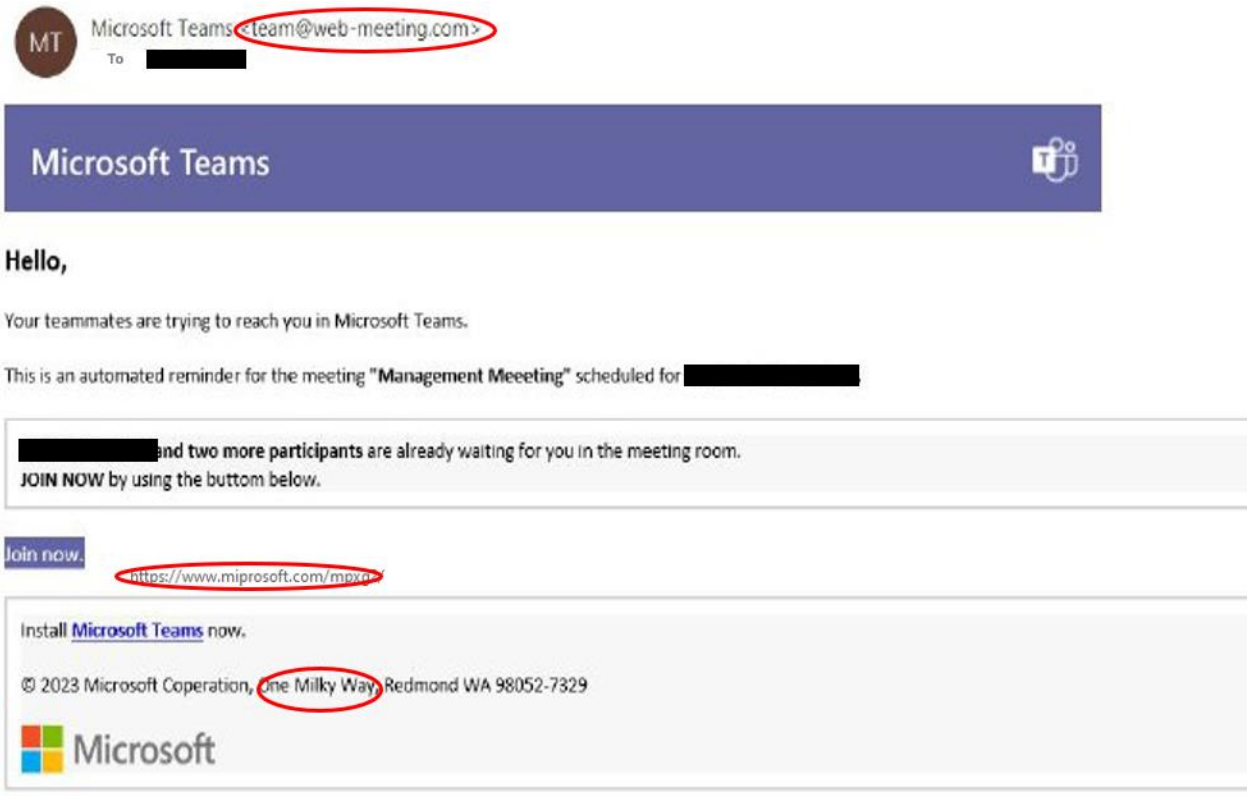
Pro realizaci phishingové kampaně bylo nezbytné provést několik kroků. Nejprve bylo potřebné vytvořit Excelový list obsahující detailní informace o zaměstnancích. Tento soubor zahrnoval jméno a příjmení každého zaměstnance, jméno a příjmení jeho přímého manažera a název oddělení, do kterého zaměstnanec patří. Tyto údaje poskytly základní informace potřebné pro personalizaci phishingové kampaně.




**Obrázek 6** Sophos dashboard

Zdroj: vlastní z [24]

Dalším krokem bylo použití specializovaného phishingového softwaru Sophos. Do tohoto softwaru byl importován vytvořený Excelový soubor s údaji o zaměstnancích. Poté byla vybrána vhodná phishingová šablona, která byla přizpůsobena pro testovací phishing. Nakonec byli nastaveni přesný čas a datum, kdy měla být phishingová kampaň spuštěna.




**Obrázek 7** Vzhled testovací phishingové zprávy

Zdroj: vlastní z MS Teams

Jak zaměstnance mohli rozpoznat, že tato zpráva je phishingová? Podle obrázku jsou tři hlavní indikátory: 1) e-mailová adresa odesílatele, 2) "One Milky Way" a 3) odkaz, který při otevření zobrazuje chybnou URL adresu a vede na externí webovou stránku.

**1. Neplatná e-mailová adresa:**

E-mailová adresa odesílatele je **team@web-meeting.com** má:

- **Nesoulad formátu:**

  Platné e-mailové adresy Microsoft Teams obvykle mají jiný formát (například arsen.bulatov@epam.com; noreply.account@mcdonalds.cz)

- **Nesprávná doménová adresa:**

  Doménová adresa "team@web-meeting.com" není doménou Microsoft Teams.

**2. Pochybný obsah:**

E-mail obsahuje gramatické chyby a překlepy jako je „One Milky Way“ v názvu společnosti.

- **Nízká kvalita textu:**

Chyby v pravopise a formátování mohou být známkou toho, že e-mail byl vytvořen automaticky nebo podvodníkem.

- Záměna písmen: Například „teh“ místo „the“.
- Špatně napsaná slova: Například jak je na obrázku „Meeeting“ místo „Meeting“.
- Nesprávné nebo náhodné použití různých typů písma: Například kombinace různých stylů a velikostí písma v jednom e-mailu.

**3. Odkaz na podezřelý zdroj:**

E-mail obsahuje odkaz "Microsoft Teams", který vede na adresu URL **https://www.miprosoft.com/mpx**.

- **Pravopisná chyba:**
  V URL adrese je pravopisná chyba: místo "microsoft" je uvedeno "miprosoft".
- **Nespolehlivá doména:**
  Doména "miprosoft.com" není doménou Microsoft Teams.
- **Zkrácená URL adresa:**
  Zkrácené URL adresy mohou skrývat škodlivé webové stránky.

Při otevření phishingového odkazu tlačítkem „Join now“ se v prohlížeči otevřel článek, který informoval, že se jedná o phishingovou kampaň, a že je třeba být příště opatrnější. Faktor kliknutí byl také zaznamenán do systému Sophos pro statistické účely. Z důvodu ochrany osobních údajů nebylo možné zjistit jméno a příjmení účastníka, ale pouze jeho oddělení. Pokud zaměstnanec rozpoznal phishing, měl několik možností: 1) ignorovat odkaz, 2) odstranit ho, nebo 3) nahlásit phishing a poslat ho k ověření do IT podpory. Nejlepší volbou byla třetí možnost, protože bylo možně ověřit, zda se skutečně jedná o phishing nebo spam, a také zablokovat odesílatele.

Podle slov manažera informační bezpečnosti: “ Celkově lze výsledky považovat za uspokojivé, avšak procentuální podíl byl 10.6 %. Je to vyšší, než bylo stanoveno v bezpečnostních zásadách společnosti. Výsledky phishingové kampaně budou zohledněny při plánování kampaně na příští rok.“

Při analýze phishingové kampaně byly identifikovány oblasti, na které je třeba se zaměřit a zlepšit:

1. Zvýšení povědomí a lepší školení zaměstnanců: Zajistit pravidelná školení zaměřená na rozpoznávání phishingových útoků nebo jiných informačních hrozeb. To lze provést pomocí přednášek, tematických screensaverů ohledně zabezpečení dat, praktických cvičení a simulací. Zaměstnanci by měli být důkladně informováni o nebezpečích a způsobech, jak jej rozpoznat.

2. Zpětná vazba a motivace zaměstnanců: Poskytovat zaměstnancům zpětnou vazbu o jejich účasti v phishingových kampaních a motivovat je k lepšímu výkonu prostřednictvím interních soutěží nebo odměn za správné rozpoznání a hlášení phishingu.

## 6.4. Hodnocení souladu s relevantními normami a předpisy

Hodnocení souladu s relevantními normami a předpisy pro zabezpečení dat je klíčovým aspektem moderního řízení zabezpečení dat. Dnes, kdy je množství citlivých dat neustále na vzestupu, je důležité zajistit, aby organizace dodržovaly zákony a standardy zaměřené na ochranu těchto dat. Soulad s předpisy, jako je například GDPR v Evropské unii zajišťuje, že osobní údaje jsou zpracovávány a chráněny v souladu s nejvyššími standardy ochrany soukromí.

1. **„Zákon o osobních údajích a jejich ochraně“ v Kazachstánu**

Jedním z nejdůležitějších předpisů pro zabezpečení dat, který používá EPAM Kazachstán je „Zákon o osobních údajích a jejich ochraně“. Tento zákon stanovuje pravidla pro sběr, zpracování a ochranu osobních údajů, aby byla zajištěna práva a svobody jednotlivců [25].

Klíčové prvky zákona:

a. **Definice osobních údajů**:

- Osobní údaje jsou jakékoliv informace týkající se fyzické osoby, které umožňují její identifikaci, jako je jméno, adresa, rodné číslo, kontaktní údaje atd.

b. **Podmínky pro sběr a zpracování osobních údajů**:

- Osobní údaje mohou být zpracovávány pouze se souhlasem subjektu údajů nebo na základě jiných právních důvodů uvedených v zákoně.
- Subjekt údajů musí být informován o účelu, rozsahu a způsobu zpracování jeho osobních údajů.

c. **Práva subjektů údajů**:

- Subjekty údajů mají právo na přístup ke svým osobním údajům, právo na jejich opravu nebo výmaz, pokud jsou nepřesné nebo byly zpracovány neoprávněně.
- Mají také právo na omezení zpracování a právo vznést námitku proti zpracování jejich osobních údajů.

**d. Ochrana osobních údajů**:

- Organizace musí přijmout nezbytná opatření k ochraně osobních údajů před neoprávněným přístupem, ztrátou, změnou nebo zničením.
- Bezpečnostní opatření musí odpovídat povaze a objemu zpracovávaných osobních údajů.

**e. Přenos osobních údajů do zahraničí**:

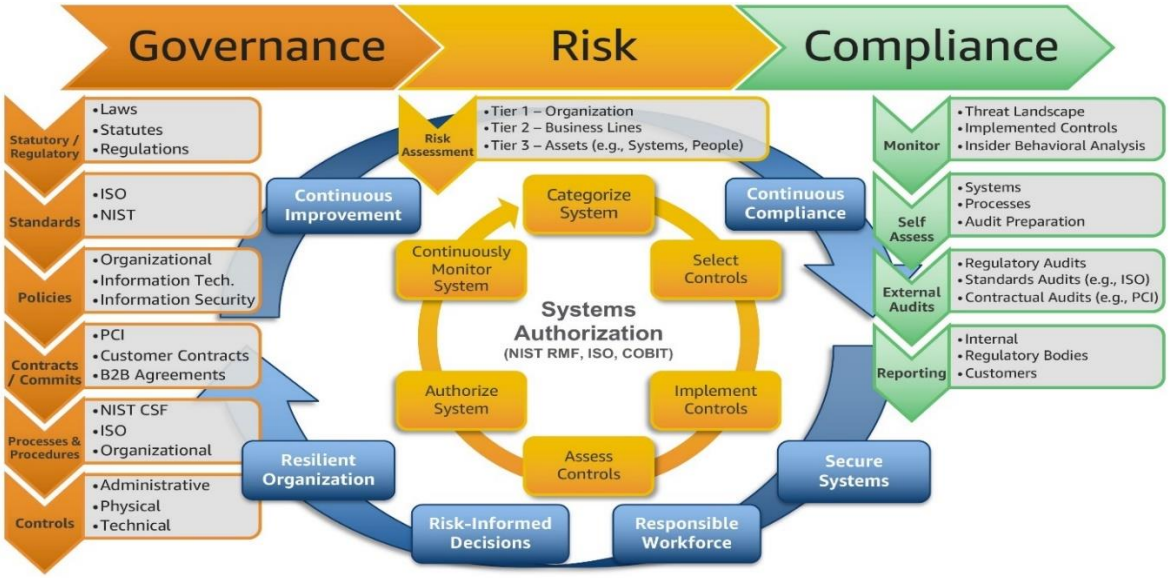
- Přenos osobních údajů do zahraničí je možný pouze za podmínek stanovených zákonem, včetně zajištění odpovídající úrovně ochrany v zemi příjemce.

**f. Sankce za porušení zákona**:

- Organizace, které nedodrží ustanovení zákona, mohou čelit sankcím, které zahrnují pokuty a jiné právní postihy.

## 2. GRC

GRC (Governance, Risk Management, and Compliance) je integrovaný přístup, který spojuje efektivní správu, řízení rizik a dodržování předpisů do jednotného koordinovaného modelu. Pro společnost EPAM Kazachstán je GRC klíčovým nástrojem pro udržení vysoké úrovně bezpečnosti dat a zajištění souladu s místními a mezinárodními normami a požadavky. Tento přístup pomáhá organizaci lépe řídit rizika, snížit ztráty, minimalizovat možné dopady bezpečnostních incidentů a zlepšovat celkovou správu a řízení zabezpečení dat.




**Obrázek 8** GRC

Zdroj: převzato z [26]

Dle [26] GRC se skládá ze 3 prvků:

**Řízení**

Řízení je soubor politik, pravidel nebo rámců, které společnost používá k dosažení svých obchodních cílů. Určuje odpovědnosti klíčových zainteresovaných stran, jako jsou představenstvo a vrcholové vedení. Například dobré firemní řízení pomáhá vašemu týmu začlenit politiku sociální odpovědnosti společnosti do svých plánů.

Náležité řízení zahrnuje následující:

- Etika a odpovědnost;
- Transparentní sdílení informací;
- Politika řešení konfliktů;
- Správa zdrojů.

**Řízení rizik**

Podniky čelí různým druhům rizik, včetně finančních, právních, strategických a bezpečnostních rizik. Správné řízení rizik pomáhá podnikům tato rizika identifikovat a najít způsoby, jak je eliminovat. Společnosti používají program řízení rizik k předvídání potenciálních problémů a minimalizaci ztrát. Například můžete použít hodnocení rizik k nalezení slabých míst v bezpečnostním systému vašeho počítačového systému a jejich odstranění.

**Dodržování předpisů**

Dodržování předpisů znamená shoda se stanovenými pravidly, zákony a normy. Vztahuje se na právní a regulační požadavky stanovené průmyslovými orgány i na vnitřní firemní politiku. V rámci GRC dodržování předpisů znamená zavedení postupů, které zajistí, že obchodní činnost bude v souladu s příslušnými právními předpisy. Například zdravotnické organizace musí dodržovat zákony, jako je HIPAA, které chrání důvěrnost pacientů [27].

## 3. Normy ISO

ISO/IEC 27001 jsou mezinárodně uznávané standardy pro řízení bezpečnosti informací, které poskytuje rámec pro správu citlivých dat a jejich ochranu před hrozbami, což zajišťuje integritu, důvěrnost a dostupnost informací [4].

V rámci těchto norem společnost zavádí a udržuje zásady a postupy pro bezpečné zpracování dat, identifikuje, hodnotí a řídí rizika spojená s bezpečností informací a pravidelně provádí interní audity k ověření souladu s normami a identifikaci oblastí pro zlepšení. Klíčovou součástí je také

školení zaměstnanců, aby všichni byli informováni o zásadách a postupech bezpečnosti informací. Důsledné dodržování těchto předpisů pomáhá organizacím minimalizovat rizika spojená s únikem dat, zvyšovat důvěru zákazníků a zajišťovat právní a etickou odpovědnost.

Abychom to shrnuly, implementace GRC rámce, dodržování norem ISO a „Zákona o osobních údajích a jejich ochraně“ zajišťuje ochranu osobních údajů, minimalizaci rizik a udržení důvěry klientů a partnerů. Důsledné dodržování těchto zásad pomáhá EPAM Kazachstán dosáhnout vysoké úrovně bezpečnosti dat a splnit všechny právní a regulatorní požadavky.

Přestože kazašský zákon o ochraně osobních údajů má podobné základní cíle jako například GDPR v Evropské unii. Třeba se uvědomit **nedokonalost používaného zákonu**. Kazašský zákon o ochraně osobních údajů je méně detailní a méně přísný v porovnání s GDPR. Například, požadavky na souhlas subjektů údajů nejsou tak striktně definovány a vynucování pravidel není tak silně monitorováno a penalizováno. Z tohoto důvodu by EPAM Kazachstán mohl těžit z implementace některých specifických ustanovení GDPR. Přijetím přísnějších a podrobnějších pravidel pro zpracování osobních údajů se společnost může vyhnout potenciálním právním problémům a sankcím, které mohou vzniknout v důsledku nedostatečné ochrany dat. Tím by se nejen zlepšila ochrana dat ve firmě, ale také by se posílila důvěra ve zpracování osobních údajů na mezinárodní úrovni.

## 6.5. Návrh na vylepšení zabezpečení.

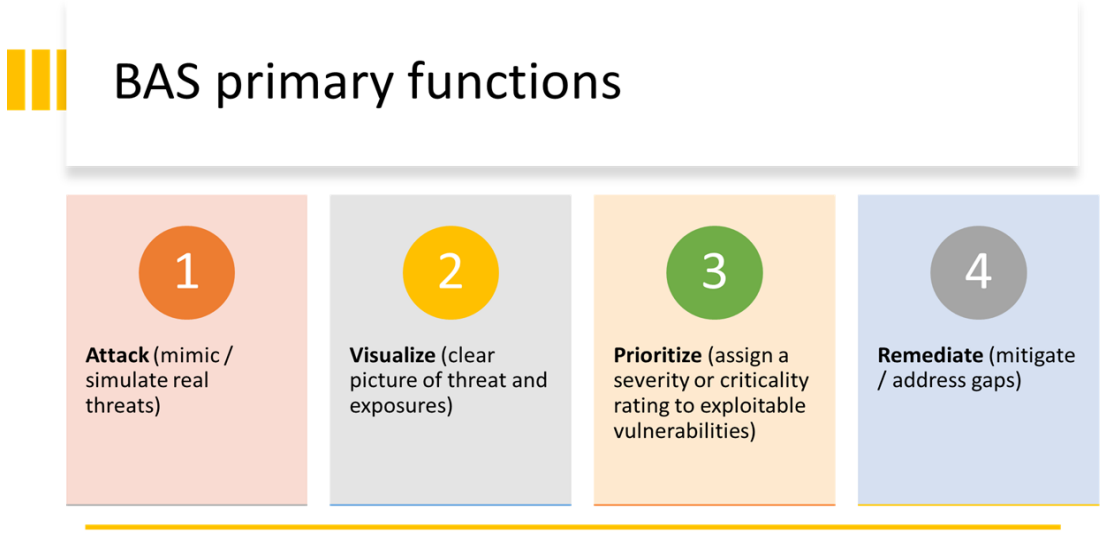
Po důkladné analýze firmy, jako jsou její zákony a předpisy, slabá místa, technologií a metody zabezpečení, byly identifikovány 3 hlavní body pro zlepšení zabezpečení dat – implementace moderní metody zabezpečení BAS; doplňování přísnějších pravidel používaného zákona v souladu s GDPR a lepší školení zaměstnanců. Tyto návrhy pomůžou společnosti EPAM dosáhnout vyšší úrovně zabezpečení, udržovat a posilovat svou dobrou reputaci a vztahy se zákazníky

### 6.5.1. Metoda BAS

Metoda BAS byla zvolena pro posílení zabezpečení, protože je dneska trendem v oblasti informační bezpečností a řízení rizik, a je určená pro velké společnosti s vysokými požadavky na zabezpečení dat.

**Breach and Attack Simulation** (BAS) je nový způsob ověření IT bezpečnosti, který napodobuje činnosti skutečných útoků, aby zjistil, zda různá bezpečnostní opatření společnosti skutečně plní svůj účel.

Tyto platformy umožňují organizacím provádět nepřetržitou simulaci kybernetické bezpečnosti na vyžádání kdykoli, aniž by to ovlivnilo produkční systémy. Napodobují různé útoky, interní nebo externí, které útočí nejnovějšími způsoby odhalování zranitelností [28]. Tyto simulované útoky odhalují mezery v bezpečnosti, což umožňuje organizaci určit, zda architektura zabezpečení poskytuje dostatečnou ochranu a zda jsou správně implementovány konfigurace. Celkově se platformy pro simulaci narušení a útoků staly mocnými spojenci týmů pro kybernetickou bezpečnost organizace.




**Obrázek 9** Hlavní funkce BAS

Zdroj: převzato z [29]

Hlavní funkce BAS**:**

a. **Simulace útoku:** Systém dokáže simulovat různé typy útoků, jako je phishing, vložení malwaru a síťové průniky.

b. **Vizualizace:** Systém dokáže vizualizovat výsledky simulovaných útoků a poskytnout organizacím jasnou představu o tom, jak by únik dat ovlivnil jejich systémy. Tyto informace lze použít k prioritizaci nápravných opatření.

c. **Prioritizace:** Systém může prioritizovat zranitelnosti podle jejich závažnosti a pravděpodobnosti zneužití.

d. **Náprava:** Systém může poskytnout doporučení pro nápravu zranitelností. Tyto informace lze využít k vývoji a implementaci bezpečnostních opatření.

Implementace metody BAS pro společnost EPAM Kazachstán by mohla mít významné důsledky a přínosy v několika klíčových oblastech. Níže je uvedeno několik možných aspektů, jak by tato implementace mohla ovlivnit fungování a strategii EPAM.

- Zvýšení efektivity a kvality projektů

Implementace metody BAS může vést ke zvýšení efektivity a kvality projektů díky systematickému přístupu k analýze a návrhu systémů. To zahrnuje přesné definování požadavků, identifikaci potenciálních rizik a vytvoření robustních řešení. EPAM Kazachstán by mohl dosáhnout lepších výsledků v dodávání projektů včas a v rámci rozpočtu.

- Lepší komunikace se zákazníky

Metoda BAS zahrnuje důkladnou analýzu potřeb a požadavků zákazníků. To může vést k lepší komunikaci a porozumění mezi týmem EPAM a jeho klienty. Zákazníci budou moci lépe formulovat své potřeby a EPAM bude schopen nabídnout přesněji cílená řešení, což zvyšuje spokojenost zákazníků.

- Zlepšení interních procesů

Implementace BAS může také přinést zlepšení interních procesů. Systematický přístup k analýze a řízení projektů může vést k identifikaci a odstranění neefektivit, což umožní hladší a efektivnější fungování společnosti. To může zahrnovat optimalizaci pracovních postupů, lepší řízení zdrojů a zlepšení celkové organizace práce.

- Posílení konkurenční pozice

Díky zlepšení kvality služeb a efektivity může EPAM Kazachstán získat konkurenční výhodu na trhu. Schopnost poskytovat vysokou úroveň služeb a přinášet inovativní řešení může přilákat nové zákazníky a posílit vztahy s existujícími klienty.

### 6.5.2. Zákon o osobních údajích a jejich ochraně

Jak bylo uvedeno výše, mezi používaným zákonem a GDPR skutečně existují výrazné rozdíly, které nelze ignorovat. Je však také nutné zdůraznit, že existují mezi nimi určité společné rysy

jako: sběr a zpracování osobních údajů; ochrana osobních údajů; práva subjektu údajů; přenos osobních údajů.

Nicméně při podrobném srovnání lze identifikovat několik zásadních rozdílů:

**Co chybí v kazašském zákoně ve srovnání s GDPR:**

- Rozšířená práva subjektů údajů: Právo na přenositelnost údajů a právo být zapomenut nejsou v kazašském zákoně zahrnuty.
- Pověřenec pro ochranu osobních údajů (DPO): Neexistuje povinnost jmenovat DPO.
- Hlášení o narušení bezpečnosti: Chybí specifická lhůta pro hlášení narušení bezpečnosti osobních údajů.
- Přísné pokuty: Sankce nejsou tak přísné a podrobně specifikované jako v GDPR.
- Podrobné principy zpracování údajů: Kazašský zákon neuvádí principy zpracování osobních údajů tak podrobně jako GDPR.
- Ochrana údajů dětí: Chybí specifická ustanovení týkající se zpracování osobních údajů dětí.

Po upřesnění stálých a doplnění chybějících ustanovení se může zvýšit úroveň ochrany osobních údajů. Pro společnost to bude znamenat zvýšené náklady na zajištění dodržování právních předpisů, implementaci dalších kontrolních procesů a ochranu osobních údajů podle GDPR. Také to bude vyžadovat přehodnocení a případné změny rolí oddělení ISO (Information Security Office) a DPO včetně jejich pracovního týmu a rozpočtu. Ale taková implementace poskytne konkurenční výhodu na trhu kvůli vysokým standardům na ochranu dat.

### 6.5.3. Školení zaměstnanců

Jak bylo zjištěno z phishingové kampaní – školení zaměstnanců v oblasti zabezpečení dat je klíčové pro každou organizaci, protože lidský faktor představuje jednu z největších hrozeb. Školení může zaměstnance naučit rozpoznávat techniky, jakými jsou phishingové e-maily nebo falešné telefonáty. Často lidé nejsou dostatečně informováni o nejnovějších hrozbách a bezpečnostních postupech. Školení může poskytnout aktualizované informace a učit zaměstnance, jaké praktiky a politiky dodržovat pro ochranu dat.

Pro dosažení lepšího školení zaměstnanců v oblasti zabezpečení dat můžeme podniknout několik kroků: Prvně, je klíčové aktualizovat školení pravidelně, aby reflektovalo nejnovější hrozby a bezpečnostní postupy. Dále je důležité školení personalizovat podle rolí zaměstnanců, aby bylo

relevantní pro jejich pracovní prostředí. Interaktivní přístup je také klíčový, například prostřednictvím cvičení a scénářů, které umožní zaměstnancům procvičit si praktické dovednosti při reakci na bezpečnostní incidenty. Měli bychom využívat různé vzdělávací metody, jako jsou online kurzy, webináře a workshopy, aby bylo školení přístupné a efektivní. Zapojení vedení firmy je také klíčové pro podporu školení v oblasti zabezpečení dat jako součásti firemní kultury. Průběžné monitorování účinnosti školení a získávání zpětné vazby od zaměstnanců jsou důležité pro neustálé zdokonalování školení a přizpůsobení aktuálním potřebám organizace. Tímto způsobem můžeme efektivně posílit školení zaměstnanců v oblasti zabezpečení dat a zvýšit celkovou bezpečnost organizace.

**Význam školení pro společnost**

Školení zaměstnanců pro firmu EPAM má zásadní význam z několika důvodů. Především přispívá k zvýšení odbornosti a dovedností zaměstnanců. Když zaměstnanci získají nové znalosti a dovednosti, které jsou přímo relevantní pro jejich pracovní pozice, mohou pracovat efektivněji a produktivněji. To se následně projevuje ve vyšší kvalitě jejich práce a celkové výkonnosti týmu.

Investice do školení má také pozitivní dopad na motivaci a spokojenost zaměstnanců. Když firma ukazuje ochotu investovat do jejich rozvoje, zaměstnanci cítí, že jsou ceněni a že jejich kariérní růst je pro firmu důležitý. To může zvýšit jejich loajalitu, což je pro firmu dlouhodobě výhodné.

Kromě toho, dobře vyškolení zaměstnanci mají menší pravděpodobnost chybovat, což vede ke snížení nákladů spojených s opravami chyb a ztrátami. Menší chybovost přispívá k plynulejšímu provozu a vyšší efektivitě celého týmu.

## 6.6. Reakce společnosti

Velmi důležitou součástí bakalářské práce bylo nejen teoretické zkoumání možných návrhů pro zlepšení zabezpečení dat ve společnosti EPAM Kazachstán, ale také praktická implementace těchto metod do firemní struktury. Za tímto účelem byla uspořádána schůzka s vedením, kde byly prezentovány výše zmíněné body s podrobnou argumentací. Na základě této schůzky lze říci, že vedení projevilo zájem o toto téma a slíbilo všestrannou podporu při implementaci těchto projektů. Je však také důležité poznamenat, že ne všechny navržené body se podařilo realizovat z různých vnějších a vnitřních důvodů.

**Implementace moderní metody zabezpečení BAS**

Diskuse ohledně zavedení moderní metody BAS probíhají. Zvažuje se, jak by mohla být tato technologie integrována do stávajících systémů, a jaké by byly náklady a přínosy této implementace. Závěrečné rozhodnutí bude učiněno po pečlivém zvážení všech faktorů.

**Doplnění přísnějších pravidel v souladu s GDPR**

Návrh na doplnění přísnějších pravidel používaného zákona v souladu s GDPR byl zamítnut. Po pečlivé úvaze a zhodnocení nákladů a přínosů tohoto kroku se společnost EPAM rozhodla, že implementace těchto změn by nebyla optimální. Zamítnutí tohoto návrhu bylo založeno na závěru, že dodatečné úpravy by mohly vést ke zbytečným komplikacím a nákladům bez výrazného zlepšení bezpečnosti.

**Lepší školení zaměstnanců**

Návrh na zlepšení školení zaměstnanců byl přijat s nadšením. Společnost EPAM si uvědomuje, že dobře vyškolení zaměstnanci jsou klíčem k efektivnímu zabezpečení dat. Školení bude zaměřeno na zvyšování povědomí o bezpečnostních hrozbách, správných postupech pro ochranu dat a na nové technologické nástroje a metodiky. Tímto krokem EPAM nejen zvýší úroveň zabezpečení, ale také posílí kompetence svých zaměstnanců, což přispěje k celkové efektivitě a spokojenosti týmu.

## 6.7. Hodnocení nákladů

Na základě jednání s vedením firmy bylo rozhodnuto, že v současné době bude plně implementován pouze projekt školení zaměstnanců. Tato kapitola podrobně prozkoumá možné výdaje, zhodnotí investice a potenciální návratnost investic (ROI) z implementace programu. Všechny výdaje vychází ze zkoumání průměrných platů a cen za služby v Kazachstánu, ale budou uvedeny v českých korunách (CZK).

**Struktura programu**

Pro zvýšení povědomí zaměstnanců se navrhuje vytvoření série screensaverů a článků na firemním portálu, které budou obsahovat základní pravidla informační bezpečnosti a podrobnější instrukce. Vývoj těchto materiálů zahrnuje několik fází: vytvoření koncepce, designu, psaní a editaci textů. Dále budou vytvořeny školící kurzy, které budou testovány na skupině zaměstnanců.

### 6.7.1. Hodnocení TCO

Celkové náklady (TCO) na projekt se rozdělují na přímé a nepřímé náklady:

Přímé náklady zahrnují mzdy zaměstnanců zapojených do vývoje materiálů a provádění kampaní. Tento segment zahrnuje designéry, copywritery a školitele. Průměrná měsíční mzda a doba práce umožňují odhadnout celkové náklady na jejich odměňování. Designéři, kteří pracují 2 měsíce, mají průměrnou mzdu 25,000 CZK/měsíc, a vzhledem k účasti 2 designérů činí jejich celkové náklady 100,000 CZK. Jeden školitel s průměrnou mzdou 30,000CZK/měsíc, má celkové náklady 60,000CZK. Dva copywriteři, pracující stejnou dobu, s průměrnou mzdou 20,000 CZK/měsíc, mají celkové náklady 80,000 CZK. Celkové náklady na mzdy zaměstnanců činí 240,000 CZK.

Náklady na software a nástroje zahrnují licence na software pro animaci a ozvučení ve výši 90,000 CZK, což činí celkové náklady 90,000 CZK.

Externí služby mohou zahrnovat konzultace a audity prováděné externími odborníky. Náklady na konzultační služby činí 70,000 CZK.

Nepřímé náklady zahrnují odhady na snížení produktivity během školení ve výši 50,000 CZK a náklady na další vybavení a podporu IT infrastruktury ve výši 100,000 CZK, což činí celkové nepřímé náklady 150,000 CZK.

Celkové náklady (TCO) projektu se spočítají jako součet všech výše uvedených částek:

- Celkové přímé náklady: 240,000 CZK + 90,000 CZK + 70,000 CZK = 400,000 CZK
- Celkové nepřímé náklady: 150,000 CZK

Celkové náklady (TCO) projektu činí 550,000 CZK.

### 6.7.2. Hodnocení ROI

Na základě poskytnutých dat o projektu odborného školení zaměstnanců v oblasti kybernetické bezpečnosti provedeme hlubší analýzu jeho ekonomické efektivnosti s využitím ukazatele návratnosti investic (ROI). Celkové náklady na projekt (TCO) jsou odhadnuty na 550,000 Kč. Předpokládejme, že realizace projektu povede k výraznému snížení úspěšných kybernetických útoků na firmu, což potenciálně může ušetřit náklady na reakci a obnovu po těchto incidentech. Předpokládané ekonomické výhody jsou odhadovány přibližně na 1,000,000 Kč, s ohledem na snížení nákladů na odstranění důsledků útoků a zvýšení operační efektivity.

Kromě toho je nutné zohlednit také možné reputační ztráty spojené s úspěšnými útoky, které mohou poškodit pověst společnosti a vést k ztrátě důvěry zákazníků a partnerů. Tento aspekt může být obtížně kvantifikovatelný, ale je důležitým faktorem při komplexní analýze návratnosti investic.

S použitím uvedených dat vypočteme upravený ROI:

ROI = (Očekávané úspory – celkové náklady/ celkové náklady) * 100%

ROI= (1,000,000-550,000/550,000) *100 %= 81%

V tomto případě hodnota ROI naznačuje, že očekávané ekonomické výhody projektu převyšují současné náklady na projekt. Tento výsledek ukazuje na silné ekonomické argumenty pro realizaci projektu školení zaměstnanců. Navíc je důležité brát v úvahu i možné reputační výhody, které by mohly významně přispět k celkové hodnotě ROI, pokud se podaří minimalizovat rizika úspěšných kybernetických útoků a jejich potenciální negativní dopad na pověst společnosti.

Vzhledem k výše uvedenému je doporučeno, aby organizace vážně zvážila implementaci tohoto projektu, neboť přináší nejen ekonomické výhody, ale také posiluje bezpečnostní postupy společnosti. Dlouhodobé výhody zlepšení zabezpečení dat mohou dále podpořit tržní pozici a konkurenceschopnost organizace.

# ZÁVĚR

Bakalářská práce se zaměřuje na důležitost zabezpečení dat podniku a vliv jeho kvality na podnikovou reputaci. Zabezpečení dat je klíčovým aspektem, který ovlivňuje nejen technickou infrastrukturu podniku, ale i jeho celkovou stabilitu a důvěryhodnost na trhu.

Úniky dat mohou značně poškodit pověst společnosti a vést k finančním ztrátám a ztrátě klientů. Na příkladech společností jako Equifax, Facebook a Uber je patrné, jaké následky může mít nedostatečné zabezpečení dat a jak důležité je mít efektivní strategie pro řízení rizik a rychlou reakci na incidenty.

V teoretické části jsou zkoumány hrozby zabezpečení dat a metody jejich ochrany. Hrozby pro zabezpečení dat zahrnují kybernetické útoky, jako je phishing, malware, hardwarové chyby, a také interní hrozby způsobené chybami zaměstnanců. Pro ochranu dat před těmito hrozbami jsou používány různé metody a technologie ochrany jako je šifrování, firewally, blockchainy, IDS/IPS systémy atd.

V praktické části, na základě analýzy konkrétní společnosti, byly identifikovány současné metody zabezpečení a zjištěna slabá místa. Bylo navrženo zlepšení zahrnující implementaci metody BAS, dodržování zákona o ochraně osobních údajů a pravidelná školení zaměstnanců.

Na základě provedené práce lze dospět k závěru, že je to nezbytné, aby podniky investovaly do zabezpečení dat jako do klíčového aspektu svého podnikání. To zahrnuje nejen investice do technologických nástrojů a bezpečnostní infrastruktury, ale také vytváření bezpečnostní kultury a pravidelné školení zaměstnanců. Bezpečnost dat by měla být začleněna do každodenních pracovních procesů a stanovena jako prioritní cíl v rámci strategie podniku. Kromě toho je důležité sledovat nejnovější trendy a vývoj v oblasti kybernetických hrozeb a přizpůsobit bezpečnostní opatření podle potřeby.

# SEZNAM POUŽITÝCH ZDROJŮ

## POUŽITÁ LITERATURA

[1] BIRYUKOV, A. *Informařní bezpečnost. Obrana a útok.* místo neznámé : DMK-Press, 2017. ISBN 978-5-97060-435-9.

{2] MOLDOVYAN, A.A. *Informatika: úvod do informační bezpečnosti.* Moskva : Právní centrum, 2004. ISBN 5-94201-399-3.

[3] MORGUNOV, A.V. *Informační bezpečnost.* místo neznámé : NGTU, 2023. ISBN 978-5-7782-3918-0.

[4] DOSEDĚL, TOMÁŠ. *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, Doseděl Tomáš. ISBN 80-251-0106-1.

[5] PRESTON, W.CURTIS. *Modern Data Protection.* místo neznámé : O"Reilly Media , 2021. ISBN 9781492094050.

[6] PASCAL, ACKERMAN. *Modern Cybersecurity Practises.* místo neznámé : BPB Publications, 2020. ISBN 978-9389328257.

[7] RODRYČOVÁ, DANUŠE A PAVEL STAŠA. *Bezpečnost informací jako podmínka prosperity firmy.* Praha : Grada, 2000. ISBN 80-7169-144-5.

[8] DOWLING, GRAHAME. *Reputace firmy. Vytváření, řízení a hodnocení efektivity.* místo neznámé : Infra-M, 2004. ISBN 5-16-000950-7.

## ELEKTRONICKÉ ZDROJE

[9] POVĚST SPOLEČNOSTI: co ovlivnuje, jak ji řidit. *sales-generator.ru.* [Online] 3. srpen 2022. Dostupné z: https://sales-generator.ru/blog/reputatsiya-kompanii/.[cit.2024-10-07]

[10] KRISHTALYUK, A. Management bezpečnosti podnikání. [Online] 2014. Dostupné z: https://mybook.ru/author/aleksandr-krishtalyuk/upravlenie-bezopasnostyu-biznesa/read/ . [cit.2024-10-15]

[11] HROZBY INFORMAČNÍ BEZPEČNOSTI. *anti-malware.ru.* [Online]. Dostupné z: https://www.anti-malware.ru/threats/information-security-threats. [cit.2024-04-02]

[12] CYBERSECURITY THREATS. *imperva.com.* [Online]. Dostupné z:https://www.imperva.com/learn/application-security/cyber-security-threats/.[cit.2024-04-02]

[13] BLOCKCHAIN FACTS: What Is It, How It Works, and How It Can Be Used. *investopedia.com.* [Online]. Dostupné z: https://www.investopedia.com/terms/b/blockchain.asp. [cit.2024-05-04]

[14] INFORMAČNÍ BEZPEČNOST: co jí hrozí a jak s tím bojovat. *practicum.yandex.ru.* [Online]. Dostupné z: https://practicum.yandex.ru/blog/tehnologii-zaschity-informatsii/.[cit.2024-05-05]

[15] Using Artificial Intelligence in Cybersecurity. *balbix.com.* [Online]. Dostupné z: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.[cit.2024-05-19]

[16] ZERO TRUST: nový přístup k informační bezpečnosti. *securitymedia.org.* [Online]. Dostupné z: https://securitymedia.org/info/zero-trust-novyy-podkhod-k-informatsionnoy-bezopasnosti.html. [cit.2024-05-22]

[17] epic.org. *Equifax Data Breach.* [Online]. Dostupné z: https://archive.epic.org/privacy/data-breach/equifax/.[cit.2024-05-30]

[18] AKCIE EQIUFAX. *kurzyakcie.cz.* [Online]. Dostupné z:] https://www.kurzyakcie.cz/akcie/equifax-efx-cena-graf-informace?odday=1&odmonth=7&odyear=2017&doday=1&domonth=1&doyear=2018&czk=1&submit=Vybrat. [cit.2024-05-30]

[19] www.infowatch.ru. *analytics.* [Online]. Dostupné z: https://www.infowatch.ru/analytics/utechki-informatsii/facebook-khronika-skandalnoy-utechki. [cit.2024-05-30]

[20] .STATISTA.COM. *Highest penalties in privacy enforcement actions worldwide.* [Online]. Dostupné z: https://www.statista.com/chart/18805/highest-penalties-in-privacy-enforcement-actions-worldwide/.[cit.2024-06-03]

[21] What is SIEM? *www.ibm.com.* [Online]. Dostupné z:. https://www.ibm.com/topics/siem. [cit.2024-06-04]

[22] What is MDR. *www.sophos.com.* [Online]. Dostupné z:. https://www.sophos.com/en-us/cybersecurity-explained/what-is-mdr. [cit.2024-06-06]

[23] MDR SECURITY. *www.bluevoyant.com.* [Online]. Dostupné z: https://www.bluevoyant.com/knowledge-center/understanding-mdr-security-benefits-and-core-technologies. [cit.2024-06-06]

[24] PHISH THREAT. *sophos.com.* [Online]. Dostupné z: https://www.sophos.com/en-us. [cit.2024-06-14]

[25] *adilet.zan.kz.* [Online]. Dostupné z: https://adilet.zan.kz/rus/docs/Z1300000094. [cit.2024-06-13]

[26] GRC. Scaling a governance, risk, and compliance program for the cloud. *amazon.com.* [Online]. Dostupné z: https://aws.amazon.com/ru/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/.[cit.2024-06-13]

[27] Security, compliance a GDPR. *kpcs.cz* . [Online]. Dostupné z: https://www.kpcs.cz/cs/co-delame/reseni/security-compliance-gdpr.html. [cit.2024-06-13]

[28] WHAT ARE BREACH AND ATTACK SIMULATIONS. *xmcyber.com.* [Online]. Dostupné z: https://xmcyber.com/glossary/what-are-breach-and-attack-simulations/. [cit.2024-06-14]

[29] BREACH ATTACK SIMULATION. . *linkedin.com.* [Online]. Dostupné z: https://www.linkedin.com/pulse/breach-attack-simulation-technology-short-version-gaurav-agarwaal/. [cit.2024-06-14]