Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

KIT – Katedra informačních technologií

Bakalářská práce

Zálohování, archivace dat a datová úložiště

Tomáš Horejsek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Tomáš Horejsek

Informatika

Název práce

Zálohování, archivace dat a datová úložiště

Název anglicky

Backup, archiving and data storages

Cíle práce

Hlavní cíl:
Navrhnout řešení, které pomůže uživatelům zabezpečit data na svých počítačích před úmyslným i neúmyslným smazáním a případným útokem hackerů.

Dílčí cíle:
Analýza již existujících nástrojů použitelných k zabezpečení uživatelských dat.
Navrhnout způsoby zabezpečení proti zneužití dat.
Návrh a implementace řešení pro zvolenou firmu/malý až střední podnik.

Metodika

V teoretické části bude na základě rešerší odborné literatury a dostupných elektronických zdrojů zpracován souhrn základních informací k vybranému tématu. V praktické části se bakalářská práce bude věnovat analýze současného stavu zabezpečení a zálohování dat ve vybraném podniku a po zpracování výsledků analýzy budou sepsány návrhy pro zlepšení současné situace firmy v oblasti bezpečnosti a archivace dat i s ohledem na ekonomickou situaci společnosti. Pro zvolený podnik implementován jeden z návrhů řešení.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Bezpečnost, archivace, záloha dat, datová úložiště

Doporučené zdroje informací

Best Alternatives to OwnCloud in 2020. In: FileCloud Blog [online]. CodeLathe Technologies Inc, 2020. Dostupné z: https: //www.getfilecloud.com/blog/2020/01/best-alternatives-toowncloud-2020/.

FELDMAN, David. Battle of the Clouds. In: Nextcloud vs ownCloud – The Whole Story [online]. CiviHosting, 2020. Dostupné z: https://civihosting.com/blog/nextcloud-vs-owncloud/.

HOLVE, Michael. Pokročilé zálohování s Rsync. In: ROOT.CZ [online]. Internet Info, 2007. Dostupné z: https://www.root. cz/clanky/pokrocile-zalohovani-s-rsync/.

JANÍK, David. Proč a jak nainstalovat Nextcloud? In: Váš Hosting [online]. Váš Hosting, 2018. Dostupné z: https://www. vas – hosting . cz / blog – proc – a – jak – nainstalovat – nextcloud # koliknextcloudstoji.

PRESTON, W.Curtis. Backup & Recovery: Inexpensive Backup Solutions for Open Systems. O'Reilly Media, January 3, 2007. ISBN B0043GXMUM.

ZÍTKO, Jan. GOOGLE APPS A BEZPEČNOST. In: blog GAPPs [online]. Sievert Consulting, 2014. Dostupné z: https:// google-apps.cz/google_apps_bezpecnost/.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 30. 11. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zálohování, archivace dat a datová úložiště" jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2023 _____

Poděkování

Rád bych touto cestou poděkoval(a) Ing.Mgr.Vladimíru Očenáškovi Ph.D. za vedení, rady a pomoc při tvorbě této práce. Dále bych rád poděkoval vybrané, byť nejmenované společnosti a své rodině za podporu během studia.

Zálohování, archivace dat a datová úložiště

Abstrakt

Bakalářská práce se zaměřuje na problematiku zálohování, archivace a datových úložišť, s důrazem na aspekty kybernetické bezpečnosti. Analyzuje zabezpečení dat vybraného nejmenovaného podniku a nabízí mu řešení ztráty dat.

Práce sumarizuje základní přehled vybrané problematiky a identifikuje klíčové výzvy spojené s uchováváním a zabezpečením dat. Zaměřuje se na implementaci interní firemní směrnice, tedy šifrování, pravidelné aktualizace, správu přístupu k datům apod. Výsledky práce nabízejí doporučení pro efektivní správu záloh, archivace a datových úložišť s ohledem na kybernetickou bezpečnost.

Klíčová slova: Bezpečnost, archivace, záloha dat, datová úložiště, kybernetická bezpečnost, ztráta dat, krizový plán, obnova dat

Backup, data archiving and data storage

Abstract

The bachelor thesis focuses on the issues of backup, archiving and data storage, with an emphasis on cybersecurity aspects. It analyses the data security of a selected unnamed enterprise and offers a solution to data loss.

The paper summarizes a basic overview of the selected issue and identifies the key challenges associated with data storage and security. It focuses on the implementation of internal company guidelines, i.e. encryption, regular updates, data access management, etc. The results of the paper offer recommendations for effective management of backups, archiving and data storage with respect to cybersecurity.

Keywords: Security, archiving, data backup, data storage, cybersecurity, data loss, crisis plan, data recovery

Obsah

Úvod

Tato práce se zabývá problematikou zálohování, archivace dat a datových úložišť. Aktuální rozvoj informačních a komunikačních technologií vede k tomu, že stále větší počet osob, podniků, států a dalších aktérů uchovává velké množství dat v online prostoru či na svých informačních a komunikačních zařízeních. To však zároveň znamená, že se takové subjekty musí zabývat otázkou, jak zajistit jejich bezpečnost. Data mají v dnešním globalizovaném světě velký význam a mohou přímo rozhodovat o úspěchu či neúspěchu podnikatelských subjektů. Ztráta či zneužití dat tedy představuje velmi významné riziko, na které musí být aktivně reagováno. Právě tato práce se zabývá tématem, které přímo souvisí s ochranou dat před jejich ztrátou či zneužitím. Opomenutí či podcenění zálohování a archivace dat může výrazně negativně ovlivňovat zranitelnost organizace.

Dalším významným rizikem je stabilita dat, protože dnešní informační a komunikační technologie mohou vykazovat různé chyby, které povedou k jejich selhání. Takové selhání pak může vést právě ke ztrátě dat, a proto je velmi vhodné realizovat kroky na posílení bezpečnosti dat a případné rychlé obnovy dat, což právě souvisí s problematikou zálohování a archivace dat. Z těchto závěrů lze konstatovat, že je řešené téma velmi aktuální a potřebné. Dotýká se prakticky každého podnikatelského subjektu, který působí v současném tržním prostředí.

Hlavním cílem je navrhnout řešení, které pomůže uživatelům zabezpečit data na svých počítačích před úmyslným i neúmyslným smazáním a případným útokem hackerů. Jedná se o uživatele, kteří pracují ve vybrané organizaci XY. To znamená, že návrh řešení směřuje k této organizaci a jejím zaměstnancům a dotýká se dat, která využívají v rámci práce.

Dílčím cílem je analýza již existujících nástrojů použitelných k zabezpečení uživatelských dat. Dále navrhnout způsoby zabezpečení proti zneužití dat či sestavení návrhu a implementace řešení pro zvolenou firmu (malý až střední podnik).

Za účelem splnění cílů práce je její struktura rozdělena na teoretickou a praktickou část. Teoretická část práce využívá rešerši odborné literatury a dostupných elektronických zdrojů za účelem zpracování souhrnu základních informací o zálohování, archivaci dat a datových úložištích. Čerpáno je nejen z tuzemských, ale také zahraničních zdrojů jako jsou odborné publikace, odborné články, sekundární empirické výzkumy, názory odborníků apod.

Praktická část práce se zabývá analýzou současného stavu zabezpečení a zálohování dat ve vybraném podniku. Na základě výsledků analýzy jsou definované návrhy pro zlepšení

současné situace firmy v oblasti bezpečnosti a archivace dat s ohledem na ekonomickou situaci organizace.

Z tohoto vyplývá, že je pro zpracování práce využito metod rešerše odborné literatury a dostupných elektronických zdrojů, analýzy a syntézy, ale také komparace různých možností zabezpečení, zálohování či archivace dat.

Výstupy z práce budou předložené managementu organizace XY, aby zvážil implementaci návrhu v praxi. Závěry však mohou využít i další malé a střední organizace, které řeší podobné problémy v oblasti zálohování a archivace dat.

1. Teoretická část

Teoretická část práce popisuje pojme kybernetická bezpečnost, dále se věnuje rozboru pojmů zálohování, archivace a datové úložiště.

1.1. Kybernetická bezpečnost

V současné době patří obor informačních a komunikačních technologií mezi nejdynamičtěji se rozvíjející. To je dáno obrovským rozmachem těchto technologií a výhodami, které lidské společnosti přinášejí. Masivní rozmach však zároveň generuje i bezpečnostní rizika, a proto je nutné klást důraz i na relevantní zabezpečení informačních a komunikačních systémů (Bašta et al., 2019).

Oblast informačních a komunikačních technologií je však natolik specifická, že v podstatě neexistují žádná univerzálně platná bezpečnostní opatření, která by komplexně ochránila informační a komunikační systémy. Jednotně fungující řešení neexistuje. Z tohoto důvodu je nutné vždy přistupovat k jejich zabezpečení individuálně, akceptovat individuální podmínky a charakteristiky těchto systémů, aby mohlo dojít k minimalizaci bezpečnostních rizik (Gála, Šedivá, Pour, 2015, s. 221).

Hledáním těchto řešení se zabývá obor kybernetické bezpečnosti, který reaguje na to, že je v současné době většina dat v digitální podobě, a proto je nutné klást důraz na jejich zabezpečení (Nezmar, 2017, s. 195).

Z obecného hlediska lze kybernetickou bezpečnost vymezit jako komplexní ochranu sítí před kybernetickými útoky a hrozbami, a to za účelem zajištění a zachování bezpečnosti informací (Vláda České republiky, 2021).

Kybernetická bezpečnost je *„definicí pro prevenci a ochranu počítačových a informačních systémů, sítí, programů a technologií před digitálními kybernetickými útoky, které jejich pachatelé (hackeři) obvykle zaměřují na prolomení přístupových údajů k citlivým informacím, jejich změnu nebo cílené zničení, ale také k vydírání uživatelů v podobě vymáhání peněz (CRDR spol. s r. o., 2022).“*

Kybernetická bezpečnost je základním prvkem v oblasti ochrany před kybernetickou kriminalitou. Tuto formu kriminality lze charakterizovat jako jednání, které je namířeno proti počítačům, případně počítačové síti či jedná, při kterém je počítač využíván jako nástroj k páchání trestné činnosti. Klíčovou charakteristikou kybernetické kriminality je to, že se odehrává v kyberprostoru (tj. prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět) (Kolouch, 2016).

Kybernetická bezpečnost je prevencí negativních důsledků kybernetických útoků. V krajním případě mohou kybernetické útoky vést ke kaskádovitému zničení řady prvků kritické infrastruktury, tedy mohou zastavit ropovody, přerušit výrobu v továrnách, znemožnit využití bankomatů apod. Zajištění kybernetické bezpečnosti se tímto stává otázkou bytí či nebytí moderní civilizace (Balabán, 2015, s. 64).

„Cílem kybernetické bezpečnosti je zajištění bezpečnosti informací vzniklých či zpracovávaných v kybernetickém prostoru. Dále všude tam, kde je to relevantní, musí být zahrnut i fyzický svět. Kybernetická bezpečnost tak zahrnuje v mnoha případech i fyzickou bezpečnost. Například datacentrum, ve kterém jsou ukládány informace, musí být pečlivě fyzicky chráněno, aby se do něj nedostala nepovolaná osoba, musí být zajištěna jeho odolnost vůči různým klimatickým vlivům, důvěrnost vytištěných dokumentů musí být chráněna na stejné úrovni jako jejich elektronické originály (Národní úřad pro kybernetickou a informační bezpečnost, 2022b, s. 16).“

Význam kybernetické bezpečnosti roste i v důsledku rozvoje práce na dálku. Řada i menších podniků využívá tzv. cloudové technologie a nástroje, které však musí být také chráněné (Kaspersky, 2023).

V současnosti je kybernetická bezpečnost stále poměrně nový obor, a proto se neustále objevují nové výzvy, kterým musí čelit. V budoucnosti lze očekávat nástup dalších technologií, které ještě více zdůrazní potřebu zajištění kybernetické bezpečnosti. Jde například o nové a přelomové technologie typu kvantových počítačů a umělé inteligence apod. (Vláda České republiky, 2021).

Zajištění kyberbezpečnosti představuje klíčovou výzvu v dnešní době, protože jakákoliv ztráta citlivých aktiv může výrazně ohrožovat subjekt, který byl napaden kybernetickým útokem. K těmto citlivým aktivům se řadí velmi rozmanité množství různých zařízení, což znamená, že se lze setkat s rozmanitou škálou kybernetických útoků. Mohou směřovat na osobní počítače, mobilní telefony, tablety, externí harddisky, cloudová úložiště, bankovní účty, platební karty, emailové účty, tzv. chytrá zařízení jako chytré hodinky, chytré náramky apod. Dále například na kritickou infrastrukturu státu, tj. elektrárny, dopravní systémy, letiště, satelitní systémy, databáze občanů, železniční provoz apod. V případě podnikatelských subjektů jde například o aktiva jako zákaznická databáze, webové stránky, interní informační systémy atd.

(Janeja, 2022, s. 2).

Klíčovou ambicí kybernetické bezpečnosti je optimální nastavení preventivních opatření za účelem ochrany digitálních systémů organizace, ale také samotných uživatelů těchto systémů před neoprávněnými přístupy a kybernetickými útoky (CRDR spol. s r. o., 2022).

K základním prvkům kybernetické bezpečnosti se řadí procesy, technologie a lidé. Porušení kybernetické bezpečnosti znamená, že došlo k porušení některého z těchto prvků, případně některých těchto prvků. Z tohoto pohledu je nutné klást důraz na prevenci, detekci a reakci na útoky na tyto prvky (Kolouch, 2016).

Kybernetické útoky ve stále větší míře cílí i na podnikatelské subjekty, a proto se musí i podniky zabývat problematikou kybernetické bezpečnosti. Kybernetický útok může organizaci způsobit takové škody, které nakonec mohou vést až ke krachu organizace. K nejčastějším dopadům patří zvyšování nákladů, přerušení provozu, poškození dobré pověsti, ušlý zisk, ukončení provozu, ztráta know-how (CRDR spol. s r. o., 2022).

Až 60 % malých podniků ve Spojených státech amerických, které se staly terčem kybernetického útoku ukončilo činnost do šesti měsíců po tomto útoku. Odchod z trhu je však nejdrastičtější následek, což znamená, že se zbylých 40 % podniků potýkalo s dalšími negativními důsledky jako jsou finanční ztráty, vysoké náklady na odstranění důsledku a dalších hrozeb či poškození pověsti (Kaspersky, 2023).

Proč je kybernetická bezpečnost podstatná i pro malé podniky? Kybernetické útoky ohrožují jejich peníze, data, softwarové a hardwarové vybavení. Pokud hacker získá přístup do podnikové sítě, tak může například získat seznamy zákazníků, informace o kreditních kartách zákazníků, informace o bankovních převodech, strategické a jiné plány, návrhy produktů, podobu výrobních procesů, či další typy duševního vlastnictví. Takovéto útoky tedy ohrožují samotnou podstatu organizace. Zároveň však ohrožují i další subjekty, jejichž data jsou v organizaci k dispozici. Může jít o dodavatele, odběratele a další složky dodavatelského řetězce (Kaspersky, 2023).

Podnikatelským subjektům se v oblasti zajištění ochrany před kybernetickými útoky doporučuje investovat do prevence a ochrany, což sebou přináší zejména nutnost následujících kroků (CRDR spol. s r. o., 2022):

- Pochopení problematiky – znalost problematiky kybernetické bezpečnosti je klíčovým předpokladem pro zajištění efektivní ochrany před útočníky.
- Proškolení zaměstnanců – mezi kritické faktory kybernetické bezpečnosti patří lidská chyba, a proto musí každá organizace reagovat na tuto hrozbu. To lze nejlépe zajištěním vzdělávání zaměstnanců v této oblasti.

- Kontrola a aktualizace – informační a komunikační technologie se neustále rozvíjí, a proto je nutné pravidelně kontrolovat funkčnost bezpečnostních systémů a přijatých opatření, dále realizovat aktualizace hardwaru i softwaru a klást důraz na vzdělávání.

V oblasti kyberbezpečnosti lze dále malým organizacím doporučit zejména následující (Kaspersky, 2023):

- Proškolení zaměstnanců – lidský faktor je nejslabším článkem ochrany před kybernetickými útoky, a proto je nutné provést proškolení pracovníků v této oblasti. Je nutné stanovit jasné zásady a pravidla.
- Realizace hodnocení rizik – jde o analýzu a hodnocení potenciálních rizik v oblasti zabezpečení informačních a komunikačních systémů, které organizace využívá.
- Využití antivirového software a jeho aktualizace – je nutné zvolit antivirový program, který dokáže ochránit všechna zařízení před viry, spyware, ransomware či phishingovými podvody. Tento je pak nutné neustále aktualizovat.
- Pravidelné zálohování souborů a omezení přístupu k citlivým informacím – je vhodné pravidelně zálohovat soubory, ale také udělit přístupová práva k různým informacím.
- Šifrování a zabezpečení, firewall – pokud je pravidelně pracována s daty jako čísla platebních karet, bankovní účty apod., tak je vhodné využívat šifrovací programy. Firewall je pak nezbytností ve všech případech, protože chrání hardware i software.
- Zavedení politiky silných hesel – je nutné zaměstnancům přikázat, ať využívají velmi silná přístupová hesla.
- Využití Virtual Private Network (VPN) – využití VPN umožňuje bezpečný přístup k podnikové síti v rámci práce na dálku. Uživatelům poskytuje bezpečné připojení, i když je například využito veřejného internetového připojení.
- Ochrana před fyzickou krádeží – jde zejména o ochranu hardwarového vybavení, které může být fyzicky ukradeno z prostor podniku či je ukradeno zaměstnanci pracujícímu na dálku, nebo jej zaměstnanec ztratí.
- Nepodcenění mobilních zařízení – mobilní zařízení představují významnou bezpečnostní výzvu v dnešní době, a proto jejich ochrana nesmí být přehlížena.
- Průzkum obchodních partnerů v oblasti zabezpečení dat – je nutné zohlednit i to, jestli mají obchodní partneři a dodavatelé přístup k systémům podniku a zde zohlednit případná rizika.

1.2. Zálohování, archivace dat a datová úložiště

Dnešní informační revoluce má přímou souvislost se sběrem, zpracováním, uchováváním a využitím dat. Data jsou optimálním způsobem zachycení zprávy, kdy vypovídají o okolní realitě a jsou srozumitelné pro příjemce. Data jsou nositeli informace a informace vznikají z dat v okamžiku jejich užití. Z dat vznikají informace, protože informace jsou data, kterým uživatel přisuzuje určitý význam a uspokojují jeho informační potřebu (Mašín, 2020, s. 106).

„Data, která člověk záměrně a soustavně vytváří ať již v podobě textů, fotografií nebo třeba výsledků různých měření, patří mezi nejcennější artikly, které se současně typicky velice složitě substituují (Černý, 2019, s. 102).“

Data představují vše, co lze zaregistrovat smysly člověka, jde o výsledky pozorování procesů, projevů, činností a prvků reálného světa. Za tvrdá data se považují údaje, které jsou jasně vymezené a kvantifikované (tj. numericky jako fyzikální či ekonomické jednotky apod.) Měkká data představují názory a postoje lidí (Veber et al., 2016, s. 73-74).

„Data musí někde vzniknout (lidé, stroje, organizace), někde se uložit, zpracovat pro potřeby budoucího využití a musí být přístupná (Štětinová, Bernat, Löffler, 2021, s. 75).“

1.2.1. Zálohování dat

Zálohování dat patří mezi klíčové nástroje ochrany dat. Případná ztráta dat nemusí kriticky ohrožovat existenci organizace, pokud existuje aktuální záloha. Z tohoto důvodu se organizacím doporučuje, ať vytvoří interní směrnici ohledně zálohování dat. Tato by měla zejména definovat, jakým způsobem budou data zálohována, jak často budou zálohována, kdo bude zodpovídat za zálohování, kde a jakým způsobem budou zálohy uložené, včetně přístupových práv k záloze dat (Nguyen, 2018).

Nutnost zálohování dat je dána technickou povahou médií, na která lze data ukládat. Každé médium má pouze omezenou životnost, po jejímž překročení dojde k dynamickému růstu rizika poškození nosiče dat, a to takovým způsobem, že již nebude možné data získat či bude proces obnovení dat velmi nákladný a nejistý (Černý, 2019, s. 102).

„Účelem zálohování je především možnost obnovy dat ve chvíli, kdy dojde k jejich ztrátě. Taková situace může nastat například kvůli selhání hardwaru nebo chybě v softwaru zajišťujícího zápis dat. Důvodem může být i lidský zásah, a to jak nechtěný (přepsání či smazání dat), tak chtěný (hackerský útok) (Můčka, 2022).“

Zálohování je obvyklou součástí práce s daty, protože představuje jedno ze základních bezpečnostních opatření. V rámci zálohování je jako první nutné určit, jestli budou data uložena

v cloudu či na fyzickém úložišti, nad kterým má uživatel přímo fyzickou kontrolu. Fyzická kontrola je však pocitem zkresleným, protože zpravidla platí, že data, která jsou uložena na fyzickém nosiči, jsou zpravidla méně zabezpečena než data, která jsou uložená u velkých cloudových organizaci. V případě požárů, povodní, krádeží dochází u fyzických nosičů ke ztrátě jak primárního, tak i sekundárního média. Z tohoto pohledu se cloudové úložiště jeví jako levnější a bezpečnější, kdy je riziko fyzické ztráty dat poměrně nízké (Černý, 2019, s. 102). Zálohování dat sebou přináší i různá rizika. Zálohování sice na jednu stranu snižuje riziko ztráty či porušení dat, ale zároveň se jeho prostřednictvím zvyšuje riziko ukradení dat, zejména pokud není dodržen archivační proces a nedochází k relevantnímu zabezpečení (Nezmar, 2017, s. 114-116).

Při zálohování dat se v praxi osvědčuje tzv. pravidlo 3-2-1, které doporučuje mít uložené minimálně tři kopie dat. To znamená původní data a jejich dvě zálohy. Dále se doporučuje využívat dva různé typy zálohy, protože pravděpodobnost, že selžou zcela dva odlišné formáty zároveň je velmi malá. Pokud jsou tedy data uložené na interním pevném disku, tak je vhodné využívat i externí pevný disk či datové úložiště. Minimálně jednu zálohu dat je vhodné uchovávat mimo pracoviště, což může být i datové úložiště (Gandhi et al., 2022).

Při rozhodování o intervalu zálohování je také vhodné zodpovědět základní otázky jako: o kolik dat je přijatelné přijít? Za jak dlouho se tato data nasbírají či vytvoří? Při tom je nutné identifikovat optimální poměr mezi potenciálním rizikem a náklady na zálohování (Můčka, 2022).

1.2.2. Archivace dat

Archivací podnikových dat a informací se rozumí rozsáhlá archivace různých typů digitálního obsahu, včetně elektronických zpráv, veřejné a interní sociální sítě, telefonických hovorů, textových a hlasových zpráv. V současnosti lze taková data archivovat prostřednictvím robustních softwarových řešení, které dokáží shromažďovat a uchovávat data z různých zdrojů, dále provádět jejich indexaci, aby v nich bylo možné provádět vyhledávání. Specializovaná softwarová řešení také dokáží zajišťovat dlouhodobé a bezpečné ukládání dat (Dinic, 2022).

Archivace dat je klíčovou oblastí řízení informací, protože organizaci poskytuje lepší kontrolu nad informacemi. Z tohoto důvodu by zejména digitální archivace měla být běžnou součástí každého podnikání. Archivace zjednodušuje nalezení a ochranu dokumentů, a to po celou dobu jejich životního cyklu (Polanský, 2023).

„Archivace je proces ukládání neaktivních informací v jakémkoliv formátu, které již pravidelně nepoužíváme k dlouhodobému uchovávání. Informace, které se archivují, mohou, ale nemusí být, v budoucnu znovu použity. Archivace zajišťuje, že jsou všechna data přístupná, bezpečně uložená a kontrolovaná (Polanský, 2023).“

V oblasti archivace dat je podstatný pojem durabilita dat, tj. trvanlivost. Dále jde o náklady či geografickou vzdálenost (doporučuje se mít data archivována v jiném prostoru než probíhá podnikání) (Můčka, 2022).

Pojmy zálohování a archivace se velmi často zaměňují, ale nemají stejný význam, a proto je nutné mezi těmito rozlišovat. Zálohování je proces, kterým se zajišťuje, že jsou data obnovitelná ve formě kopie aktivních dat, kdy je organizace bude potřebovat v případě ztráty či poškození dat. Primárním cílem zálohy dat je vrátit data do určitého časového okamžiku. Zálohy jsou krátkodobé a pravidelně se přepisují. Archivace dat je sběrem historických dat, které se musí uchovávat za účelem dlouhodobé archivace, například s cílem dodržování legislativních předpisů (Polanský, 2023).

Klíčovým rozdílem mezi zálohováním a archivací dat je důvod, proč mají být data duplikována a skladována na odděleném úložišti. Záměrem archivace je dlouhodobé skladování dat, a proto není prioritní jejich rychlá obnova. Obvykle se archivují data jako účetní doklady apod., kdy taková data nejsou nezbytná pro každodenní provoz, ale je vhodné mít je zabezpečené (Můčka, 2022).

Další rozdíly mezi archivací a zálohováním dat shrnuje následující tabulka. Je zřejmé, že archivace souvisí s přesunem dat, avšak zálohování s kopírováním dat. Archivace se zaměřuje na přístupné informace, ale zálohování klade důraz na obnovitelné informace. Předmětem archivace dat jsou data neaktivní, což u zálohování neplatí, protože je pracováno s aktivními daty. Archivace dat slouží pro dlouhodobé uchování dat. U zálohování dat je jejich uchování krátkodobějšího charakteru.

Tabulka 1 Rozdíly mezi archivací a zálohováním

Archivace	Zálohování
Přesun dat	Kopírování dat
Přístupné informace	Obnovitelné informace
Neaktivní data	Aktivní data
Dlouhodobé uchování	Krátkodobé uchování

Zdroj: Polanský, 2023

Archivace i zálohování dat jsou založené na stejném postupu, kdy dochází ke kopírování dat z jednoho úložiště na druhé, a to za účelem jejich budoucího použití. To je však v podstatě jediný společný znak, protože jde o velmi odlišné pojmy. Rozdíly lze nalézt v účelu uchovávání dat, v intervalu zapisování, ve způsobu skladování, v rychlosti obnovy a s tím souvisejícím typem řešení archivace či zálohování (Můčka, 2022).

Archivovaná data jsou data, která jsou starší, avšak pro organizaci stále důležitá, či je jejich uchování nutné z hlediska legislativního. Archiv je živým záznamem minulosti, ve kterém se vyskytují důkazy a vysvětlení minulých a současných činů (Polanský, 2023).

K základním výhodám elektronické archivace dat pro podniky se řadí zejména následující (Polanský, 2023):

- Eliminace rizika ztráty dat – uložení dokumentů v centralizovaném a zabezpečeném digitálním úložišti eliminuje riziko jejich ztráty.
- Snížení provozních nákladů – archivace dat v písemné formě vyžaduje zpravidla vyčlenění fyzických prostorů (archivu), které přináší náklady na jejich pronájem, správu apod.
- Zlepšení zabezpečení – využití digitálního úložiště umožňuje poskytnout přístupová oprávnění konkrétním zaměstnancům.
- Zjednodušení auditů – audit obsahuje kontrolu záznamů, a proto lze elektronickou evidencí mít k dispozici rychlou a přehlednou kontrolu dokumentů.

1.2.3. Datová úložiště

V současnosti jsou již cloudové služby (služby datových úložišť) nezbytnou součástí byznys modelů moderních organizací. Zároveň se očekává i další růst jejich využití, takže trend cloudových služeb bude i dále růst (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Datové úložiště (cloudové úložiště) je formou ukládání dat, které zprostředkovává třetí strana. Externí subjekt v tomto případě nabízí uložení dat na vzdálených datových serverech, kdy lze k těmto datům přistupovat prostřednictvím webových stránek či internetových aplikací. Data jsou tímto zálohována mimo organizaci a její interní prostředí a interní informační technologie (Gandhi et al., 2022).

Cloud computing lze vymezit jako službu, která zprostředkovává vzdálený samoobslužný přístup k výpočetním zdrojům, které jsou schopné přizpůsobovat se potřebám zákazníků. Mezi takové výpočetní zdroje se řadí sítě, servery či jiná infrastruktura, dále například operační

systémy, software, úložiště, aplikace nebo služby (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Cloudové úložiště je služba, *„díky které může nejen jedna kancelář, ale celá firma ukládat data do virtuálního prostoru (tzv. cloudu)…Místo ukládání na fyzická úložiště uvnitř firmy tak pracovníci veškeré soubory odesílají na vzdálený server (Hájek, 2022).“*

Výhodou datového úložiště je možnost přístupu k datům z různých míst. Navíc někteří zprostředkovatelé nabízí cloudové služby i bez poplatku a k provozovatelům se řadí největší technologické firmy jako Google, Microsoft či Apple (Gandhi et al., 2022).

„Pokud uživatelé chtějí zajistit co možná nejvyšší úroveň bezpečnosti svých dat, musí se na jejich ochraně sami významnou měrou spolupodílet a nespoléhat se jen na kapacity poskytovatele (Národní úřad pro kybernetickou a informační bezpečnost, 2022, s. 4).“

Rozvoj služeb datových úložišť byl podnícen pandemií koronaviru, která nutila organizace rychle se přeorientovat na režim práce z domova, což sebou přineslo nutnost spolehlivého a vzdáleného přístupu k datům pro všechny pracovníka. Právě datové úložiště přineslo vhodnou variantu řešení tohoto problému (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Služby datového úložiště velmi často nabízí i další služby, než pouze ukládání dat. Jde na příklad o server hosting, webhosting, další platformy nebo aplikační hosting, aby bylo možné na cloudu provozovat i podnikové aplikace (Hájek, 2022).

I využití služeb cloudu může vést k problémům. Za prvé, jde o riziko ukončení služby či změny podmínek nebo funkcí takové služby. Uživatel pak nemá v podstatě žádnou možnost, jak ovlivnit, jestli bude služba dále fungovat, jaká bude její cena. Původní výhodné a funkční řešení může být změněno na mimořádně nákladné a vysoce problematické. Za druhé, pak může vzniknout problém s migrací dat mezi cloudovými úložišti. Za třetí, jsou velké cloudové služby častým cílem hackerských útoků, protože shromažďují data milionů uživatelů (Černý, 2019, s. 102).

K nevýhodám datových úložišť patří omezená kapacita v rámci bezplatnosti služby, kdy od určité hranice datové kapacity je nutné platit za jejich využití. Dále se mohou problémy objevovat v situaci, ve které je nutné ukládaná data často načítat. Zohlednit je nutné i přítomnost vysokorychlostního internetu, aby se rychlost internetu a pokrytí nestalo překážkou pro využití těchto služeb (Gandhi et al., 2022).

„Ukládat data a využívat další cloudové služby v infrastruktuře poskytovatele přináší pro uživatele bezpečnostní výzvy. Při využívání cloudových služeb nevyhnutelně dochází

k předávání velké části kontroly nad daty poskytovateli, a je tak klíčová jeho důvěryhodnost (Národní úřad pro kybernetickou a informační bezpečnost, 2022).“

Za největší riziko cloudových služeb lze považovat předávání velké části kontroly nad daty poskytovateli cloudové služby, a dále pak je rizikem to, že zpracování dat probíhá zpravidla na území jiného státu, kde může platit odlišný přístup k zajištění bezpečnosti dat (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Datové úložiště pro podnikové účely by mělo splňovat následující (Hájek, 2022):

- Dispozice robustním zabezpečením, které funguje na 100 %.
- Schopnost operativně se přizpůsobovat změnám.
- Být 24 hodin denně a 7 dní v týdnu pod dohledem expertů.
- Dispozice neomezeným prostorem pro ukládání dat.
- Záloha dat takovým způsobem, aby je bylo možné kdykoliv a kdekoliv obnovovat.
- Funkcionalita takovým způsobem, aby zaměstnance ovládání nezdržovalo od práce.

2. Praktická část

Praktická část práce se zabývá profilem organizace, dále analýzou stavu zabezpečení a zálohování dat ve vybraném podniku. V závěru kapitoly se nachází návrhy a doporučení, které reagují na zjištěné problémy a nedostatky.

2.1. Profil organizace

Pro účely zpracování práce poskytla organizace XY interní informace, a proto si nepřála zveřejnit svoje jméno. Z tohoto důvodu bude označena anonymní zkratkou XY.

Organizace byla založena v březnu roku 2023 se záměrem realizovat developerské projekty v různých částech České republiky. Jediný společník ve společnosti s ručením omezeným XY je zároveň majitelem velkoobchodní a maloobchodní prodejny se stavebním materiálem. Nově vznikající podnik rozšiřuje portfolio produktů této organizace právě o developerské projekty. V jejich rámci dochází výstavbě bytových a řadových domů. V současnosti jsou realizované dva developerské projekty v Jihomoravském kraji a v Moravskoslezském kraji. V roce 2024 se pak plánuje zahájení dalších čtyř projektů.

Organizace sídlí v Praze, ale její kanceláře se nachází i v Brně a v Ostravě, tedy v krajích, kde dochází k realizaci developerských projektů. Finanční prognóza očekává v roce 2023 dosažení úrovně tržeb ve výši 15 mil. Kč, a to při nákladech 25 mil. Kč, což znamená, že by mělo dojít ke ztrátovému hospodaření.

V pražské centrále organizace pracuje celkem 12 pracovníků, tj. ředitel organizace, dvě asistentky, ředitel marketingu, dva marketingový pracovníci, technický a provozní ředitel, finanční ředitel a projektový manažer. Na každé pobočce pak pracuje ředitel pobočky, obchodní zástupci, asistentky.

Nově vznikající organizace XY zároveň řeší otázky zabezpečení a zálohování dat či využití datových úložišť. V další části textu by mělo dojít k řešení tohoto problému.

2.2. Analýza stavu zabezpečení a zálohování dat ve vybraném podniku

Vzhledem k tomu, že organizace vznikla před nedávnou dobou, tak nemá jednoznačně formulovanou strategii v oblasti zabezpečení a zálohování dat. Inspirací by pro organizaci mohl být přístup mateřské společnosti k této problematice, avšak bylo zjištěno, že taková strategie

v podstatě neexistuje ani u mateřské společnosti. Tato mateřská organizace provádí pravidelnou zálohu dat v ročním intervalu, tj. vždy po schválení účetní závěrky. To platí i o archivaci dat. Roční interval zálohy dat však nelze chápat jako zcela dostačující. Každodenně je organizace vystavena různým kybernetickým hrozbám, a proto je vhodné, aby prováděla zálohu častěji, včetně například i archivace dat.

Personální odpovědnosti v souvislosti se zabezpečením a zálohou dat

Personální odpovědnost v souvislosti se zabezpečením a zálohou dat nese ředitel celé organizace. V organizaci není zřízeno oddělení informačních technologií a v této oblasti je využíváno externí spolupráce. V oblasti zabezpečení a zálohy dat však neprobíhá žádná dlouhodobá a specializovaná spolupráce, takže v organizaci není zřízena specializovaná pracovní pozice, která by se problematikou zabezpečení a zálohy dat či archivací dat zabývala.

Informační systémy a data v organizaci (hardware, software)

Z hlediska informačních systémů využívá organizace účetní a mzdový systém, dále CRM systém. Účetní a mzdový systém v organizaci slouží pro správu účetních operací, sledování nákladů a výdajů, poskytování informací pro finanční rozhodování apod. Jeho součástí je i skladová a personální evidence. CRM systém je využíván pro správu informací o zákaznících organizace. Oba systémy jsou poskytované externími dodavateli. Organizace má pořízenou licenci k jejich využití. Data z těchto systémů jsou ukládané na hardwarové zařízení organizace. Není zde využíváno cloudového úložiště.

Dále organizace využívá Microsoft 365, což je skupina různých cloudových služeb, které mají podobu kancelářského softwaru. Jejich prostřednictvím je v organizaci zajišťována realizace projektů a úkolů, vzájemná elektronická komunikace členů pracovních týmů, tvorba a správa různých dokumentů. V tomto případě jsou data ukládaná na datové úložiště.

Pro antivirovou ochranu je využíváno externího řešení od poskytovatele antivirového software. Jedná se o software společnosti ESET ve variantě Protect Complete, který zajišťuje kompletní a vícevrstvou ochranu koncových zařízení, cloudových aplikací a elektronické pošty. Řešení je určeno přímo pro malé a střední podniky.

Z hlediska hardwarového vybavení se lze v organizaci setkat s následujícími:

- Notebooky a příslušenství
- Tiskárny a skenery
- Síťová infrastruktura

- Firewall
- Chytré telefony, tablety

Každý pracovník organizace má k dispozici notebook a příslušenství (tj. myš, klávesnice, externí monitor, sluchátka, webová kamera), dále chytrý služební telefon. Kanceláře organizace jsou také vybavené tiskárnou či skenerem, které lze využívat v rámci potřeby. Tablet si může každý pracovník vypůjčit, pokud jede například na služební jednání mimo kancelář a jeho použití je vhodnější než využití notebooku.

Síťová infrastruktura v organizaci slouží k vzájemnému propojení hardwaru a softwaru v organizaci, aby se usnadnila spolupráce mezi pracovníky organizace, zlepšil se přístup managementu k datům a informacím, na základě kterých pak realizují různá rozhodnutí.

Firewall je určen pro zajištění bezpečnosti síťové infrastruktury tím způsobem, že podporuje kontrolu a řízení toku dat mezi touto interní sítí a internetem. Cílem využití firewallu je zajistit, že nedojde k neautorizovanému přístupu a nebude ohrožena kyberbezpečnost organizace. Firewall je využíván v rámci antivirového řešení od společnosti ESET.

Archivace dat a zálohování dat

Pravidla archivace dat a zálohování dat zatím v organizaci nejsou pevně stanovena. Předpokládá se, že bude využito stejného postupu jako v případě mateřské organizace, ale jak bylo uvedeno, tak takový postup nelze pokládat za dostačující. Z tohoto důvodu je nutné formulovat doporučení ke zlepšení (tj. uvedeno v příslušné části práce).

Datová úložiště

Z hlediska využití datových úložišť využívá organizace cloud společnosti Microsoft, který se vztahuje pouze k využívanému softwarovému řešení. Jiné formy datových úložišť nejsou využívané.

Způsoby zabezpečení dat před úmyslným a neúmyslným smazáním

Otázka zabezpečení dat před úmyslným a neúmyslným smazáním není momentálně v organizaci aktivně řešena, i když jde o jednu z klíčových oblastí v rámci zálohování a archivace dat.

Způsoby zabezpečení dat před případným útokem hackerů

Před případným útokem hackerů se organizace chrání prostřednictvím antivirového software ESET, včetně firewallu. Jiné formy zabezpečení nejsou v organizaci využívané. Nástroje užívané pro zabezpečení uživatelských dat mají tedy pouze charakter využití antivirového systému. Situaci lze zlepšit využitím preciznějšího přístupu k zálohování dat, aby se snížilo riziko ztráty dat, které může organizaci ohrozit.

Hodnocení rizik kybernetické bezpečnosti

Rizika kybernetické bezpečnosti jsou hodnocena prostřednictvím určení pravděpodobnosti jejich vzniku a očekávaného dopadu na organizaci. Kvantitativní hodnocení je provedeno autorem práce. Pravděpodobnost vzniku je hodnocena na škále: 1 = velmi nepravděpodobné, 2 = spíše nepravděpodobné, 3 = neutrální, 4 = spíše pravděpodobné, 5 = velmi pravděpodobné. Dopad vzniku rizika na organizaci je hodnocen na škále: 1 = téměř žádný dopad na podnik, 2 = spíše žádný dopad na organizaci, 3 = neutrální, 4 = spíše vysoký negativní dopad, 5 = velmi negativní dopad.

Jedná se o následující:

- Napadení viry, trojskými koni, ransomware, spyware apod.
- Phishingové útoky
- DDoS útoky
- Ztráta a únik dat
- Selhání lidského faktoru
- Nedodržení legislativních předpisů

Výstupy z hodnocení rizik poskytuje následující tabulka, která zároveň doporučuje i opatření, resp. reakci na dané riziko a výsledek jeho hodnocení (výsledek je součinem pravděpodobnosti vzniku a dopadu rizika). Z celkové hodnoty pak lze odvodit významnost rizika a definovat opatření. K méně závažným rizikům patří napadení viry apod., či DDoS útoky, u kterých se doporučuje monitoring těchto rizik. Phishingové útoky pak patří také do kategorie méně pravděpodobných rizik, kdy se doporučuje jejich monitoring. K závažnějším rizikům pak patří ztráta a únik dat či nedodržení legislativních předpisů v souvislosti s archivací dat. Zde je nutné provádět konkrétní kroky, zejména pak právě v oblasti zlepšení zálohování a edukace pracovníků. To se vztahuje i k riziku selhání lidského faktoru.

Tabulka 2 Hodnocení rizik kybernetické oblasti

Hodnocení rizik kybernetické oblasti	Pravděpodobnost vzniku	Dopad rizika	Celkem	Opatření
Napadení viry, trojskými koni, ransomware, spyware apod.	2	5	10	Monitorovat
Phishingové útoky	3	5	15	Monitorovat
DDoS útoky	2	5	10	Monitorovat
Ztráta a únik dat	4	5	20	Zlepšit zálohování a edukaci
Selhání lidského faktoru	5	5	25	Zlepšit zálohování a edukaci
Nedodržení legislativních předpisů	4	5	20	Zlepšit archivaci dat

Zdroj: vlastní zpracování

Z výsledků hodnocení rizik vyplývá, že je nutné zlepšit aktivity v oblasti zálohování a archivace dat. Ztráta a únik dat představují výrazná rizika, na které není v současnosti dostatečně reagováno, což platí i o selhání lidského faktoru. Rizika v rámci nedodržení legislativních předpisů zase mohou být eliminována při vyšším důrazu na archivaci dat, která mají být v rámci legislativy uchovávána. Řešení v oblasti zálohování a archivace dat je tedy v organizaci velmi žádoucí.

2.3. Návrhy a doporučení

Z výše uvedených výsledků stavu zabezpečení a zálohování dat v organizaci vyplývá, že sice organizace XY některá z rizik jednoznačně nepodceňuje, ale zároveň existují možnosti, jak aktuální situaci zlepšit. Organizace by měla ve větší míře investovat do kybernetické bezpečnosti, aby zajistila bezpečnost informací vzniklých či zpracovávaných v jejím kybernetickém prostoru. Tato problematika úzce souvisí i s archivací a zálohováním dat.

Nedostatečné zabezpečení v oblasti kybernetické bezpečnosti může vést až k bankrotu organizace, a proto jde o velmi podstatnou a důležitou oblast, kterou nesmí organizace XY podceňovat. Kybernetické útoky jsou ohrožením financí a dat, které organizace shromažďuje. Jakýkoliv kybernetický útok může vést ke ztrátě image organizace, ale může poškodit i obchodní partnery nebo zákazníky. Z tohoto důvodu je nutné neustále zlepšovat oblast zajištění kybernetické bezpečnosti. Tento návrh by měl organizaci XY pomoci k dosažení žádoucího stavu.

Základním návrhem je tvorba interní směrnice pro zabezpečení a zálohování dat v podniku XY. Návrh směrnice vychází z konkrétní situace a potřeb organizace, takže respektuje její aktuální situaci.

Interní směrnice zálohování a archivace dat je pro organizaci velmi podstatným dokumentem, který povede ke zlepšení praxe v této oblasti. Dosavadní situace nebyla na zcela optimální úrovni, a proto existuje prostor pro zlepšení, který právě interní směrnice využívá.

Návrh interní směrnice pro zabezpečení a zálohování dat

Účelem interní směrnice pro zabezpečení a zálohování dat je zajištění dostupnosti dat a eliminace rizika ztráty dat takovým způsobem, aby nebyla ohrožena stabilita organizace. Interní směrnice obsahuje základní doporučení ke splnění uvedeného cíle.

Personální odpovědnosti

Klíčovou personální odpovědnost za zabezpečení a zálohování dat nese majitel organizace, resp. generální ředitel. Generální ředitel některé úkony související se zabezpečením a zálohováním dat deleguje na svoje podřízené. Nesplnění povinností a příkazů generálního ředitele (resp. pravidel v navrhované směrnici) povede k sankcím (o sankci rozhoduje generální ředitel).

Z hlediska personální odpovědnosti je také nutné zohlednit fyzické prostory na pracovišti, aby například nepovolaná osoba neměla přístup k počítačům, na kterých jsou uložena důvěrná data apod.

Kategorie dat

Organizace využívá různá data, a proto nelze ke všem datům přistupovat stejným způsobem. Základní ochrana dat je pro všechny kategorie stejná, ale některé kategorie dat vyžadují odlišný přístup vzhledem k jejich citlivosti a důležitosti. Z tohoto důvodu je nutné provést kategorizaci dat, aby bylo možné nastavit efektivní bezpečnostní postupy pro jejich zálohování a archivaci. Organizaci lze doporučit následující kategorizaci dat:

- Účetnictví, mzdy
- Hospodaření podniku (náklady, výnosy, ziskovost)
- Zákazníky
- Personalistika
- Intranetový systém (data v intranetovém systému, včetně komunikace)
- Interní směrnice
- Know-how

U těchto kategorií je nutné data rozčlenit dle jejich citlivosti a důležitosti, dále určit zaměstnance či skupiny zaměstnanců, kteří k těmto kategoriím dat budou mít přístup. Určením přístupu k datům by se měla zvýšit pravděpodobnost, že každý pracovník bude mít přístup pouze k datům, které potřebuje pro výkon svojí práce. To znamená, že se k tajným a důvěrným datům nedostane nepovolaná osoba.

Zálohování dat

Zálohování dat je klíčovým nástrojem pro zajištění ochrany dat, a proto by měla organizace k zálohování přistupovat aktivním způsobem. Každé médium má svoji omezenou životnost, což znamená, že data uložená na médiu jsou ohrožená ztrátou. Z tohoto důvodu nelze spoléhat na to, že budou zálohovaná data vždy dostupná. Organizace XY musí přijmout takové kroky, které zajistí dostupnost dat i v okamžiku, kdy dojde k jejich ztrátě (na jednom z nosičů dat apod.) Lze se tedy zabývat otázkou, jakým způsobem budou data zálohována? Organizaci XY lze v rámci zálohování doporučit, aby dodržovala pravidlo 3-2-1, tj. zajistila uložení minimálně tří kopií dat. To znamená mít k dispozici původní data, ale také jejich dvě kopie. Jako další lze doporučit využití dvou různých typů záloh a z toho mít jednu zálohu uloženou mimo fyzické prostory pracoviště. Konkrétně bude mít organizace uložená data na konkrétním nosiči (v původní verzi), tj. například ve služebním notebooku. Dále tato data bude zálohovat na cloudové úložiště a vytvoří i zálohu na externí harddisk. Externí harddisky budou uložené v uzamykatelném skladu. Zaměstnanci si je vždy vyzvednou za účelem provedení zálohy.

Pro zálohování a archivaci dat se organizaci XY doporučuje i využití cloudu. Cloudová úložiště mají řadu výhod oproti fyzickým nosičům, a proto by organizace neměla tuto variantu ignorovat. Pokud by například došlo v organizaci k požáru či krádeži, tak jsou tímto fyzicky uložená data v ohrožení, což v případě cloudového řešení neplatí.

Využití služeb datového úložiště je v souladu s moderními trendy, protože organizace po celém světě využívají tato řešení k zálohování a archivaci dat, ale také pro ukládání dat, s kterými aktivně zaměstnanci pracují. Prostřednictvím cloudového řešení mají zaměstnanci přístup k relevantním datům prakticky odkudkoliv, pokud mají připojení k internetu.

Na nevýhody a rizika cloudových služeb je nutné reagovat. Na riziko ukončení služby či změny podmínek poskytování služby lze reagovat právě tvorbou zálohy na externích harddiscích, ale také je možné zvolit ověřeného a stabilního poskytovatele cloudového řešení, u kterého toto riziko bude minimální.

Na riziko zvyšujících se nákladů na využití cloudových služeb je možné reagovat přípravou rozpočtů, které zohlední i předpoklad růstu nákladu. V případě výrazného zvýšení poplatků je možné do cloudového úložiště ukládat pouze některé kategorie dat.
Na riziko hackerských útoků je nutné reagovat prostřednictvím výběru spolehlivého poskytovatele, který toto riziko aktivně řeší a klade vysoký důraz na zajištění bezpečnosti.
Lze doporučit, aby vybrané cloudové úložiště plnilo minimálně doporučení, která jsou uvedená v teoretické části práce, tedy disponovalo robustním zabezpečením, bylo schopné se operativně přizpůsobovat změnám, bylo k dispozici 24 hodin denně, disponovalo neomezeným prostorem k ukládání dat, aktivně zálohovalo data, aby je bylo možné kdykoliv a kdekoliv obnovit, či disponovalo uživatelsky příjemnou funkcionalitou.

Frekvence zálohování

Definice frekvence zálohování dat má zajistit, že bude docházet k pravidelnému zálohování dat a k jejich bezpečnému uložení. Pokud by došlo ke ztrátě dat, tak právě záloha má zajistit, že budou data rychle obnovené.
V rámci rozhodování o intervalu zálohování dat je nutné zodpovědět otázky: o kolik dat je přijatelné přijít? Za jak dlouho se tato data nasbírají či vytvoří? V souvislosti s tímto lze doporučit, aby docházelo k zálohování dat na týdenní bázi. Dle názoru generálního ředitele není týdenní ztráta dat natolik významná, aby způsobila nestabilitu organizace. Pravidelnější frekvence zálohování by mohla zatěžovat zaměstnance, takže se v tomto směru jedná o určitý kompromis.

Archivace dat

Dále musí interní směrnice definovat podmínky pro archivaci dat jako archivaci různých typů digitálního obsahu. V organizaci je využíváno digitálního obsahu v podobě elektronických zpráv, příspěvků a komunikace na sociální síti, telefonické hovory, textové a hlasové zprávy. Konkrétní podoba archivace dat by také měla zajistit efektivnější nalezení a ochranu dokumentů po celou dobu jejich životního cyklu. Archivace dat bude realizována v prostorech podniku i mimo prostor podniku.

Bezpečnostní pravidla pro práci s daty

Jako další musí v interní směrnici dojít k sestavení bezpečnostních pravidel pro práci s daty. K těmto patří například následující:

1) Pravidelné zálohování dat
2) Použití silného hesla
3) Nevyužívání soukromých telefonů a počítačů pro přihlašování do intranetové sítě a pro práci s podnikovými daty

Krizový scénář řešení pro případ ztráty či úniku dat

Směrnice by měla dále navrhovat způsob reakce na bezpečnostní incidenty, které souvisí s únikem dat. Organizace musí realizovat nejen preventivní opatření, ale také být schopná ihned reagovat na případná pochybení, což právě krizový scénář umožňuje. Cílem krizového scénáře by mělo být zmírnění následků bezpečnostních incidentů. Organizaci lze doporučit, aby připravila krizové scénáře pro:

- Kybernetický útok
- Phishingový útok
- Ztrátu/krádež služebního notebooku či jiných nosičů dat

Pravidla smazání souborů

Jako další je nutné definovat pravidla pro smazání souborů, aby zaměstnanec organizace nemohl smazat důležitá data. Lze doporučit, aby jakékoliv mazání dat bylo zakázáno řadovým zaměstnancům. Smazání souborů by měl provádět pouze manažer, a to u dat, které jsou zastaralé (pokud neexistuje nutnost jejich archivace) či zbytečné.

Tvorba přístupových hesel

Interní směrnice by měla definovat i pravidla pro tvorbu přístupových hesel, aby každý pracovník využíval silné heslo, které nemůže být předmětem úniku dat. Interní směrnice by měla přímo definovat základní pravidla pro tvorbu přístupových hesel. Je však zřejmé, že konkrétní podoba hesel nemůže být kontrolována, a proto lze v tomto případě pouze spoléhat na to, že zaměstnanci požadavek splní.

Ochrana prostorů před krádežemi a vstupem nepovolaných osob

V souvislosti s tvorbou interní směrnice by organizace měla vymezit i ochranu prostorů před krádežemi a vstupem nepovolaných osob. Je nutné zajistit, že budou datové nosiče organizace zabezpečené před krádeží (například uzamčením prostorů, kamerovým systémem apod.) Do prostor organizace se také nesmí dostat nepovolané osoby, které mohou provést krádež dat.

Pravidla využití služebních mobilů

Jako další je pak v rámci interní směrnice nutné definovat pravidla pro využití služebních mobilních telefonů. Tento telefon by neměl být využíván k soukromým účelům. To platí i obráceně, tedy pracovník nesmí využívat osobní mobilní telefon (který nemusí mít dostatečné zabezpečení) k pracovním účelům (například se jeho prostřednictvím přihlašovat do interního informačního systému apod.)

Návrh obsahu směrnice

Po vymezení základních oblastí a souvislostí se lze zabývat definicí konkrétního návrhu obsahu směrnice. Text směrnice (resp. návrh) je označen kurzívou.

Směrnice zálohování a archivace dat určuje pravidla pro zálohování a archivaci podnikových dat, tj. veškerých dat, které organizace shromažďuje. Obsah směrnice je rozdělen na kapitoly:

I. Úvodní ustanovení
II. Postupy zálohování a archivace dat
III. Kategorie dat a zálohování
IV. Personální odpovědnosti
V. Ochrana dat před únikem a ztrátou
VI. Sankce za porušení pravidel zálohování a archivace dat

I. Úvodní ustanovení

Zálohování a archivace dat je klíčovým předpokladem pro zajištění stability a konkurenceschopnosti organizace. Bez dispozice daty organizace nemůže relevantně fungovat a plnit svoji funkci. Z tohoto důvodu musí každý pracovník přistupovat k zálohování a archivaci aktivně, což znamená, že musí dodržovat zejména následující pravidla.

Každý pracovník musí v rámci výkonu svojí pracovní činnosti realizovat svoji práci takovým způsobem, aby bylo dosaženo kompletní zálohy potřebných dat a existovala možnost obnovení dat ze zálohy.

II. Postupy zálohování a archivace dat

Každý pracovník organizace je povinen pravidelně provádět zálohu dat, s kterými pracuje. Záloha se provádí na konci pracovního týdne, a to jak uložením nových dat na cloudové úložiště, tak uložením nových dat na externí harddisk. Každý pracovník má přidělen externí

harddisk, kam zálohu dat provede. Tento harddisk je nutné vždy po provedení zálohy odevzdat do předem vyhrazených prostor podniku.
Za archivaci dat, které se musí archivovat dle platných zákonů České republiky, nese odpovědnost finanční ředitel organizace. Finanční ředitel provede archivaci těchto dat jednou ročně, a to po zpracování účetní závěrky.
Za archivaci dalších typů dat nesou odpovědnost manažeři organizace, a to v rámci svých kompetencí (za archivaci marketingových dat odpovídá marketingový manažer apod.) Archivace těchto dat se provádí jednou ročně, a to vždy ke konci daného hospodářského roku. Archivace se provádí na cloudové úložiště a externí harddisk.

III. Kategorie dat a zálohování

Předmětem zálohování dat jsou veškerá elektronická data, která lze rozdělit do těchto kategorií:

- *Kategorie dat Účetnictví, mzdy*
- *Kategorie dat Hospodaření podniku (náklady, výnosy, ziskovost)*
- *Kategorie dat Zákazníci*
- *Kategorie dat Personalistika*
- *Kategorie dat Intranetový systém (data v intranetovém systému, včetně komunikace)*
- *Kategorie dat Interní směrnice*
- *Kategorie dat Know-how*

V jednotlivých kategoriích dat se nachází dílčí kategorie dat. To znamená, že se jednotlivé kategorie ještě rozdělují na veřejná data, interní data, diskrétní data a citlivá data. Zařazení dat do jednotlivých kategorií provádí manažer, který nese za danou oblast odpovědnost. Přístupy k diskrétním a citlivým datům jsou omezené přístupovými právy, které uděluje manažer či ředitel organizace.

IV. Personální odpovědnosti

Manažeři organizace nesou odpovědnost za: kategorizaci dat v rámci své oblasti práce do příslušných kategorií, za kontrolu realizace zálohování dat u svých podřízených.
Ostatní pracovníci organizace nesou odpovědnost za: pravidelné zálohování dat dle pravidel stanovených touto směrnicí.

V. Ochrana dat před únikem a ztrátou

a) Každý pracovník je povinen využívat silné heslo pro přihlášení do interního systému organizace a do dalších systémů, které v rámci práce využívá. Heslo bude obsahovat minimálně 12 znaků, kombinaci malých a velkých písmem a minimálně jeden speciální znak (tj. například: !).

b) Každý pracovník je povinen pravidelně aktualizovat (měnit) svoje heslo, a to vždy k 30. 6. daného roku.

c) Je zakázáno využívat stejné heslo pro přihlášení do více různých účtů.

d) Přístup k některým datům organizace je omezen přístupovými právy.

e) Mazání dat zaměstnanci je zakázáno. O případném smazání dat rozhoduje manažer (nadřízený) daného pracovníka. Smazání dat se řídí následujícími pravidly: je možné mazat pouze dat, která jsou zastaralá (tj. více než 5 let) a nemusí být archivována, či data nepotřebná.

f) Využití soukromých počítačů či mobilních telefonů pro přihlašování do intranetového systému, emailových účtů apod. je zakázáno.

g) V případě ztráty dat nebo jakéhokoliv bezpečnostního incidentu musí pracovník okamžitě nahlásit událost svému nadřízenému.

h) Do prostorů organizace je možné zajistit vstup pouze povolaným osobám. Nepovolané osoby se nesmí na pracovišti pohybovat. V případě jejich přítomnosti musí zaměstnanec ihned kontaktovat nadřízeného pracovníka či takovou osobu vykázat.

i) Při vzdáleném připojení k internímu informačnímu systému organizace je nutné využívat VPN.

VI. Sankce za porušení pravidel zálohování a archivace dat

a) Porušení pravidel této směrnice bude sankciováno dle vyhodnocení konkrétní situace a případu.

b) O udělení sankce rozhoduje generální ředitel organizace.

Implementace směrnice

Navrhovanou směrnici je následně nutné implementovat do praxe organizace, a proto se doporučuje tento postup:

1) Návrh a schválení textu směrnice
2) Proškolení zaměstnanců

3) Legislativní audit ochrany a použití dat
4) Zhodnocení efektivity směrnice

Návrh a schválení textu interní směrnice je krokem, ve kterém má dojít ke schválení výše uvedeného textu interní směrnice. Ředitel organizace a manažeři musí po vzájemné dohodě odsouhlasit text směrnice, aby se zvýšila pravděpodobnost reálného uplatnění směrnice v praxi organizace. Obsah směrnice může být v tomto kroku upraven dle individuálních požadavků a názorů jednotlivých manažerů.

V rámci implementace směrnice je dále nutné provést školení zaměstnanců. V rámci školení musí dojít nejen k seznámení pracovníků s textem směrnice, ale je nutné je také poučit o možnostech a pravidlech zabezpečení dat a celkově o přínosu a důležitosti ochrany dat. Zaměstnancům je nutné zdůraznit základní pravidla zálohování a způsoby zálohování dat, aby v praxi docházelo k realizaci zálohování a nedošlo k problémům v této oblasti.

Proškolení zaměstnanců je nutné, aby se zamezilo riziku, které představuje selhání lidského faktoru v rámci kyberbezpečnosti. Nejvhodnějším nástrojem je právě vzdělávání pracovníků v oblasti kyberbezpečnosti. V rámci vzdělávání je také možné předat pracovníkům relevantní znalosti, aby došlo k pochopení významu kyberbezpečnosti z jejich strany.

V oblasti ochrany dat je nutné také respektovat platnou legislativu, a proto by organizace měla využít možnost konzultace s advokátním specialistou na oblast ochrany dat, zejména osobních údajů. To se týká i problematiky archivace dat, kdy může existovat zákonná povinnost archivace některých dat (jako například účetních dokladů).

Z hlediska zhodnocení efektivity směrnice je nutné zabývat se kontrolou a monitoringem úspěšnosti přijatých opatření. Zabezpečení dat je trvalým a nepřetržitým procesem. Implementace směrnice nemůže být ojedinělou a nárazovou aktivitou, ale je nutné neustále kontrolovat a hodnotit, jestli nevznikají nová bezpečnostní rizika, jestli jsou přijatá opatření dostačující apod. V oblasti informačních a komunikačních technologií vznikají neustále nová bezpečnostní rizika, a proto nelze spoléhat na jednorázové řešení.

Je nutné pravidelně kontrolovat funkčnost bezpečnostních systémů a přijatých opatření, a také se zaměřovat na neustálou aktualizaci hardwaru a softwaru.

Tento proces implementace by měla organizace využít k tomu, aby byla směrnice respektována zaměstnanci organizace, ale také tím, aby každý zaměstnanec chápal základní souvislosti problematiky ochrany dat a realizoval aktivně opatření k zálohování a archivaci dat.

Ekonomické zhodnocení návrhů

Dále je vhodné provést ekonomické zhodnocení stanoveného návrhu. V souvislosti s pořízením služeb či vybavení od externích dodavatelů je nutné zmínit následující. V oblasti ochrany dat bude organizace využívat software a hardware od dodavatelů (třetích stran), a proto musí být při výběru dodavatele splněna určitá pravidla, aby nedošlo k pořízení hardwarového a softwarového vybavení, které bude z hlediska bezpečnosti nevhodné.

Nákup hardwaru pro zálohování:

- Externí pevný disk – organizace musí pro každého pracovníka pořídit externí pevný disk, na který bude provádět zálohu dat. Při nákupu se doporučuje určit konkrétní potřebu těchto zařízení a realizovat nabídkové řízení, aby došlo k výběru nákladově nejoptimálnější varianty.

Nákup software pro zálohování:

- Pronájem cloudového úložiště – za účelem zálohování dat musí organizace využívat cloudové úložiště. I v tomto případě se doporučuje definovat konkrétní potřebu a realizovat výběrového řízení nejvhodnějšího dodavatele.

Další náklady:

- Mzdové náklady zaměstnanců – zálohování dat budou provádět zaměstnanci v rámci své pracovní doby, a proto si zálohování vyžádá i mzdové náklady na realizaci tohoto opatření.
- Náklady na pronájem fyzických prostorů pro zálohování a archivaci – externí harddisky se zálohou budou uložené ve fyzických prostorech organizace, které si organizace pronajímá, a proto vznikne i tento náklad.
- Náklady na zabezpečení prostorů proti vstupu nepovolaných osob – prostory kanceláří organizace je nutné zabezpečit, aby nedošlo ke vstupu nepovolaných osob, což sebou také přinese náklady.
- Konzultace s advokátem (ohledně cloudových smluv, dodržování zákonů o archivaci dat, ochraně osobních údajů apod.)

Školení pro zaměstnance:

- Poplatek za externí školení – zaměstnancům je možné zprostředkovat i externí školení na téma ochrany a zabezpečení dat, zálohování a archivace dat apod.
- Administrativní náklady – v souvislosti s interním školením pro zaměstnance lze předpokládat, že dojde i ke vzniku administrativních nákladů.

Závěrečné zhodnocení návrhu a doporučení

Uvedené doporučení se zaměřuje na posílení kybernetické bezpečnosti organizace, aby byla lepším způsobem chráněna před kybernetickými útoky, ale také před problémy, které mohou souviset se ztrátou dat (ať už úmyslnou či neúmyslnou). Doporučení vytváří prostor pro zlepšení na straně každého ze základních prvků kybernetické bezpečnosti, mezi které se řadí procesy, technologie a lidé.

Návrh v podobě implementace interní směrnice splňuje základní doporučení pro malé podniky v oblasti zajištění kyberbezpečnosti (viz teoretická část práce). Je zajištěno proškolení pracovníků, ale také dochází k hodnocení rizik kybernetické bezpečnosti, na které je reagováno. Dále je reflektována nutnost využití antivirového software v organizaci. Vyšší důraz je kladen také na zajištění pravidelného zálohování souborů a omezení přístupu k citlivým informacím. V organizaci bude také využíváno šifrování a zabezpečení a bude zavedena politika silných hesel. Využití VPN by mělo vést k zajištění bezpečného přístupu k podnikové síti v rámci práce na dálku. Ochrana před fyzickou krádeží je zajištěna kamerovým systémem, alarmem či pravidly pro uzamykání prostorů. Je pamatováno i na problematiku mobilních zařízení a možností jejich ztráty či úniku dat jejich prostřednictvím. Za účelem zhodnocení ekonomické náročnosti implementace stanoveného návrhu došlo k realizaci nabídkového řízení mezi potenciálními dodavateli. V jednotlivých kategoriích došlo k oslovení potenciálních dodavatelů. Jejich nabídkové ceny jsou následně interními informacemi organizace, resp. interní vnitropodnikovou kalkulací. Jedná se o dodavatele:

- Externích pevných disků – z hlediska externích pevných disků je nutné, aby jejich kapacita pokryla očekávaný objem vygenerovaných dat v organizaci, a také plánovanou potřebu externích disků z hlediska interních procesů zálohování (každý pracovník by měl mít k dispozici dostatečné možnosti zálohy dat). Po konzultaci s vedením organizace bylo zjištěno, že organizace pravděpodobně bude nutné zajistit minimálně zálohu 350 TB dat. Z tohoto důvodu byl zvolen jako vhodný hardware WD Elements

5 TB, který bude nakoupen v počtu 70 kusů. Cenové nabídky od dodavatelů se pohybují na úrovni od 3 500 Kč za kus po 4 000 Kč za kus, tj. celkem 245 000 Kč až 280 000 Kč.

- Cloudového úložiště – u cloudového úložiště se nabízí několik různých variant výběru. V rámci výběrového řízení došlo k získání nabídky od OneDrive, Dropbox, Google. Organizace preferuje globální organizace XY, které považuje za stabilní a bezpečné. Bezplatná kapacita těchto cloudových úložišť nedokáže uspokojit potřebu organizace XY, a proto je pracováno s tím, že dojde k nákupu služeb. V tomto případě považuje organizace služby cloudových úložišť za srovnatelné, a proto se rozhoduje pouze na základě ceny, kdy potřebuje uložit minimálně 400 TB dat. V tomto případě je nejvhodnější služba Dropbox, která stanovila cenovou nabídku na 5 808 amerických dolarů, tj. přibližně 134 000 Kč.
- Zabezpečení vstupu do prostorů kanceláří – dále došlo k oslovení potenciálních dodavatelů zabezpečovacích systémů do prostorů kanceláří (tj. kamerový systém, systém zabezpečení vstupu apod.) Cenově nejvýhodnější nabídka byla stanovena na 90 000 Kč.
- Advokátního poradenství – u advokátního poradenství lze využít advokátní kancelář, s kterou spolupracuje mateřská společnost, a to při nákladech 30 000 Kč.
- Externího školení – nabídka externích školení je v tomto případě různorodá, ale lze využít kurz, který stanovuje náklady na proškolení jednoho zaměstnance ve výši 18 000 Kč, tj. (25 * 18 000 = 450 000 Kč).

Z těchto informací vyplývá, že organizace bude v rámci implementace doporučení generovat náklady ve výši 949 025 Kč. Tato výše může být pro organizaci důvodem k nepřijetí uvedených návrhů. Je však nutné zvažovat, že případná ztráta dat či jejich odcizení může vést k výrazně negativním důsledkům pro organizaci, které mohou skončit i bankrotem. Zároveň platí, že jde o náklady jednorázového charakteru, čili v dalších letech bude organizace platit pouze za pronájem cloudového úložiště, případně jen za pořízení části hardwarového zařízení. Z tohoto důvodu nebude z dlouhodobého hlediska podíl těchto nákladů výrazný na celkovém objemu nákladů.

V rámci závěrečného zhodnocení návrhu a doporučení se lze zabývat i odpověďmi na tyto otázky:

- Jak směrnice pomůže uživatelům zabezpečit data na svých počítačích před úmyslným či neúmyslným smazáním? Prostřednictvím pravidelné zálohy dojde k situaci, že bude možné obnovit smazaná data, či může dojít jen ke ztrátě dat v akceptovatelné míře.

Pro zaměstnance také přináší směrnice zákaz mazání dat, takže by nemělo docházet k úmyslnému smazání (toto je sankciováno). Pravidelná záloha dat je pak ochranou proti neúmyslnému smazání, protože pokud k takovému jevu dojde, tak stále bude existovat záloha dat na externím harddisku či cloudovém úložišti.

- Jak směrnice pomůže uživatelům zabezpečit data na svých počítačích před případným útokem hackerů? Zaměstnanci organizace budou nyní muset využívat různá bezpečnostní pravidla, čímž se zvýší pravděpodobnost neúspěchu případného útoku hackerů. Bude docházet k využití silnějších hesel, k omezení využití osobních počítačů a mobilů při plnění pracovních úkolů apod. Směrnice přináší základní pravidla ke zlepšení stávajícího stavu prevence a případné obrany.
- Jaké jsou k dispozici nástroje použitelné pro zabezpečení uživatelských dat? Interní směrnice kombinuje různé nástroje, které lze využít pro zabezpečení uživatelských dat.
- Jaké směrnice nabízí způsoby zabezpečení proti zneužití dat? Zejména směrnice vytváří prostor pro eliminaci rizika v podobě selhání lidského faktoru, protože definuje základní pravidla pro posílení bezpečnosti dat.

Závěr

Tato práce se zabývala problematikou zálohování, archivace dat a datovými úložišti v prostředí malého podniku XY. Jak se prokázalo, tak tuto oblast nemůže podceňovat žádná organizace, protože riziko ztráty a zneužití dat sebou přináší závažné důsledky, které mohou vést až k bankrotu organizace. Je tedy nutné, aby každá organizace kladla na tuto oblast vysoký důraz, i když například přímo nepodniká v odvětví informačních technologií. Zálohování a archivace dat se stává důležitou otázkou v dnešním podnikatelském prostředí.

Hlavním cílem bylo navrhnout řešení, které pomůže uživatelům zabezpečit data na svých počítačích před úmyslným i neúmyslným smazáním a případným útokem hackerů. Toto řešení je navrženo pro konkrétní organizaci a její zaměstnanci (jako uživatele). Klíčovým návrhem je návrh interní směrnice pro zálohování a archivaci dat, který sebou přináší i řadu dalších kroků, které souvisí s implementací směrnice, nákupem vhodného softwarového a hardwarového vybavení apod. Návrh směrnice je tedy komplexním opatřením, který reaguje na stávající situaci v organizaci.

Dílčím cílem byla analýza již existujících nástrojů použitelných k zabezpečení uživatelských dat. Dále bylo dílčím cílem navrhnout způsoby zabezpečení proti zneužití dat či sestavení návrhu a implementace řešení pro zvolenou firmu (malý až střední podnik).

Z rozboru existujících nástrojů použitelných k zabezpečení uživatelských dat v organizaci XY vyplynulo, že nedochází k systematickému a komplexnímu využití nástrojů, které mohou v tomto směru pomoci. To je dáno krátkou historií organizace, ale také i určitou mírou podcenění této problematiky. Z tohoto důvodu došlo k návrhu zlepšení situace, což je právě návrh způsobů zabezpečení proti zneužití dat a implementace řešení pro zvolenou firmu.

Výstupy z práce budou předložené managementu organizace XY, aby zvážil možnost jejich implementace v interním prostředí. Pro organizaci je výhodou, že návrh vychází z deskripce odborných zdrojů, ale také respektuje interní situaci organizace, tedy výstupy z analýzy interního prostředí. Návrh tímto přímo odpovídá potřebám a situaci organizaci, avšak také respektuje odborná doporučení.

Stávající vývoj informačních a komunikačních technologií nevytváří pouze pozitivní efekty, ale také právě rizika, která souvisí s kyberbezpečností. To vede k nutnosti neustále a aktivně přistupovat k řešení těchto rizik. Organizace, která problematiku podceňuje, může utrpět výrazné škody a ztráty. Výsledky práce mají přispět k eliminaci tohoto rizika v konkrétní organizaci.

Seznam použité literatury

Balabán, M. (2015). *Bezpečnostní systém ČR: problémy a výzvy*. Charles University in Prague, Karolinum Press.

Bašta, P. et al. (2019). CyberSecurity. CZ.NIC.

CRDR spol. s r. o. (2022). Kybernetická bezpečnost ve firmách. Tři pilíře pro efektivní ochranu před kyberútoky. https://www.bozp.cz/aktuality/kyberneticka-bezpecnost-ve-firmach/

Černý, M. (2019). Digitální kompetence v transdisciplinárním nahlédnutí. Masarykova univerzita.

Dinic, M. (2022). Top Trends in Enterprise Data Archiving for 2023. https://jatheon.com/blog/jatheon-enterprise-data-archiving-trends/

Gála, L., Šedivá, Z. & Pour, J. (2015). Podniková informatika. Grada Publishing.

Gandhi, S., Kaliyadan, F., Chatterjee, K., & Sharma, A. (2022). "Storage, Backup and Archiving of Images"-E-Dermatology Task Force (IADVL Academy). *Indian Dermatology Online Journal*, *13*(3), 321.

Hájek, M. (2022). Co je cloud a jak pro svou kancelář vybrat ten správný. https://www.firemniajtaci.cz/blog/uzitecne-rady-jak-pro-svou-kancelar-vybrat-vhodne-cloudove-uloziste/

Janeja, V. & Janeja, J. (2022). Data Analytics for Cybersecurity. Cambridge University Press.

Kaspersky. (2023). Cybersecurity for Small Businesses. https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security

Kolouch, J. (2016). CyberCrime. CZ. NIC.

Mašín, P. (2020). *Procesní management*. Vysoká škola ekonomie a managementu.

Můčka, J. (2022). Archivace dat vs. zálohování. https://www.master.cz/blog/archivace-dat-zalohovani-rozdily-pouziti/

Národní úřad pro kybernetickou a informační bezpečnost. (2022). Cloudy umožňují snížení nákladů a snadný vzdálený přístup, za cenu ztráty plné kontroly nad daty. https://www.nukib.cz/download/publikace/analyzy/Strategicka%20analyza%20cloudovych%20sluzeb.pdf

Národní úřad pro kybernetickou a informační bezpečnost. (2022b). Průvodce řízením aktiva a rizik dle vyhlášky o kybernetické bezpečnosti. https://www.nukib.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf

Nezmar, L. (2017). GDPR: Praktický průvodce implementací. Grada Publishing.

Nguyen, N. (2018). Essential Cyber Security Handbook in Czech. Nam H Nguyen.

Štětinová, B., Bernat, L. & Löffler, V. (2021). Big data a umělá inteligence pro manažery. Nakladatelství Vladimír Löffler.

Polanský, P. (2023). 5 výhod digitální archivace. https://www.exon.cz/cs/blog/vyhody-digitalni-archivace

Veber, J. et al. (2016). Management inovací. Albatros Media.

Vláda České republiky. (2021). Kybernetická bezpečnost. https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/#

Seznam obrázků a tabulek