UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2024 Kristýna Provázková

Univerzita Pardubice

Ekonomicko-správní

Řízení IT bezpečnosti zaměstnanců vybrané společnosti

Bakalářská práce

2024 Kristýna Provázková

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Kristýna Provázková**
Osobní číslo:	**E21740**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Řízení IT bezpečnosti zaměstnanců vybrané společnosti**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb ve vybrané organizaci z hlediska zaměstnanců, vyhodnocení slabých míst a návrh protiopatření.

Osnova:

- Teoretický základ IT bezpečnosti.
- Popis vybrané organizace.
- Průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb z hlediska zaměstnanců.
- Vyhodnocení slabých míst.
- Návrhy vhodných opatření.

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

Seznam doporučené literatury:

KIZZA, Joseph Migga. Guide to computer network security. Fifth edition. Cham, Switzerland: Springer Cham, 2020. ISBN 978-3-030-38141-7.
SEDLÁK, Petr a KONEČNÝ, Martin. Kybernetická (ne)bezpečnost. Brno: Akademické nakladatelství CERM, s.r.o., 2021. ISBN 978-80-7623-068-2.
SMEJKAL, Vladimír a RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 4. vydání. Praha: Grada Publishing, 2013. ISBN 978-80-247-4644-9.
SMEJKAL, Vladimír, SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
ŠULC, Vladimír. Kybemetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-737-5.

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

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 Řízení IT bezpečnosti zaměstnanců vybrané společnosti jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

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

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

V Pardubicích dne 30. 4. 2024

Kristýna Provázková v. r.

PODĚKOVÁNÍ

Moje poděkování patří vedoucí mé bakalářské práce, Ing. Renátě Máchové, Ph.D za její odborné rady, trpělivost, důslednost, zároveň pozitivní přístup a především inspirativní připomínky, které mi pomohly k sepsání této práce. Dále děkuji rodině a přátelům za jejich podporu při studiu a také všem kolegyním, kolegům z našeho studijního ročníku.

ANOTACE

Práce je zaměřena na průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb ve vybrané organizaci z hlediska zaměstnanců. Vyhodnotí slabá místa v IT zabezpečení organizace z hlediska zaměstnanců a navrhne protiopatření.

KLÍČOVÁ SLOVA

IT bezpečnost, zaměstnanci, klasifikace informací, phishing, ransomware

TITLE

IT security management of employees of the selected company.

ANNOTATION

The work is focused on researching the set preventive measures in the field of IT security and possible threats in the selected organization from the point of view of employees. It will evaluate the weaknesses in the organization's IT security from the point of view of employees and propose countermeasures.

KEYWORDS

IT security, employees, classification of information, phishing, ransomware

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

CEO	Chief executive officer
ČNB	Česká národní banka
ČR	Česká republika
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
EAP	Extensible Authentication Protocol
EDIT	Aplikace pro vyhledání závazných interní předpisů
ICT	Informační a komunikační technologie
ID	Identification
IT	Informační technologie
IP	Interní předpis
IS	Informační systém
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Personal Computer

ÚVOD

Často si lidé ani neuvědomují, jak snadno zneužitelná a lehce dostupná data o nás samých v kybernetickém světě jsou. Roste objem a rafinovanost škodlivých programů a množství různých podvodných technik včetně technik tzv. sociálního inženýrství-podvodných metod slibů a výhrůžek. Kybernetický svět se stal nedílnou součástí našich pracovních i osobních životů. V osobním čase i při pracovních aktivitách je využíván ke komunikaci, sdílení informací, může dojít k otevření i potenciálně nebezpečné stránky, e-mailu a dokumentu. Běžně jsou používány kreditní karty, bankovní účet, slevové a jiné benefitní karty atd. Kyberzločinci spoléhají na uživatelskou neznalost a důvěřivost jako na živnou půdu pro své útoky na bezpečnost. Obecná znalost v oblasti IT bezpečnosti je jedním ze základů pro zabezpečení informací a dat. Současné hrozby cílí hlavně na koncové uživatele, kteří si někdy ani nemusí všimnout, že stanici či mobilní zařízení napadl škodlivý program, tzv. malware, nebo se snadno mohou stát obětí rafinovaného phishingového útoku. Každé bezpečnostní řešení je jen tak bezpečné, jak bezpečný je jeho nejslabší článek. A nejslabším článkem každého počítačového systému je tradičně člověk (běžný uživatel či zaměstnanec).

Téma této práce je zaměřeno na IT bezpečnost vybrané společnosti z hlediska zaměstnanců. Cílem práce je průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb ve vybrané organizaci z hlediska zaměstnanců, vyhodnocení slabých míst a návrh protiopatření. V rámci tohoto cíle bude práce zaměřena na teoretický základ IT bezpečnosti, popis vybrané organizace, průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb z hlediska zaměstnanců, vyhodnocení slabých míst v IT zabezpečení organizace a návrh vhodných protiopatření.

1 TEORETICKÝ ZÁKLAD IT BEZPEČNOSTI

Pro pochopení problematiky bezpečnosti v oblasti informačních technologií (IT) je nutné vymezit základní pojmy. Tato kapitola je zaměřena na definici oblastí, ve kterých může být organizace ohrožena v důsledku činnosti zaměstnanců.

1.1 Bezpečnost

V současné legislativě a v odborné literatuře existuje více definic pro pojem bezpečnost a nelze je obecně sjednotit. (1) Podle Jiráska a kol. lze informační systém považovat jako objekt za bezpečný, pokud je do určitého stupně chráněn proti ztrátám. Ochrana je v IT bezpečnosti zaměřena na důvěrnost, integritu a dostupnost zásahu do informačního systému (IS). (2)

1.2 Informační bezpečnost

Informační bezpečnost se zabývá souborem zabezpečení v informačních a komunikačních technologiích (ICT), které slouží k ochraně dat a informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace. Zabezpečení v ICT mohou být fyzická, logická, technická, programová a organizační. (3)

Cílem informační bezpečnosti je zajištění důvěrnosti dat, integrity dat a dostupnosti dat. Zajištění důvěrnosti dat umožní, aby neautorizovaný subjekt nemohl vniknout do systému. Nastavením bezpečnostních opatření je zajištěn přístup do IS pouze oprávněným konkrétním osobám, a především je zajištěna ochrana před neoprávněným únikem dat z IS.

Triáda kybernetické bezpečnosti je tvořena následujícími prvky:

Důvěrnost

Význam zjištění důvěrnosti informace je ten, že informace a data uložená v systémech nebo uchovávaná v jiné formě je třeba zajistit, aby se nedostaly do nesprávných rukou, nebyly vyzrazeny a zneužity. (4) To by mohlo mít vážné obchodní, právní, reputační (ztrátu důvěry klientů a jejich odchod) a podobné důsledky. Zajištění důvěrnosti je proto velmi důležité a informace je tedy třeba uchovávat tak, aby byly dostupné jen povolaným, a naopak nedostupné nepovolaným osobám.

Integrita

Zajištění integrity dat odráží správnost a úplnost informací, dále spolehlivost informačního systému, přítomnost ochranných mechanismů k zabránění neautorizovaného přístupu nebo

nepatřičné změny informací. (4) Ochrana integrity dat zabraňuje modifikaci informace nebo proniknutí jiným než autorizovaným subjektům.

Dostupnost

Zajištění dostupnosti dat poskytuje včasný přístup ke spolehlivým údajům (nebo službám IS) v okamžiku potřeby. (4) Dostupnost znamená, že autorizovaným uživatelům nebude odmítnut přístup a systém bude zpracovávat příkazy autorizovaných subjektů.

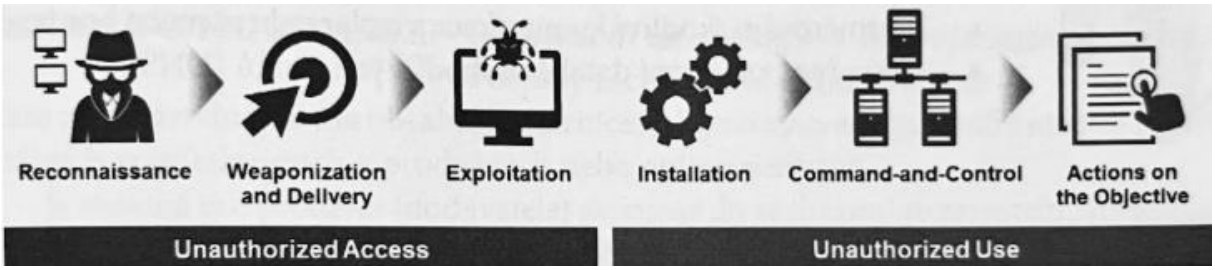
1.3 Kybernetické útoky

Útok, nebo také bezpečnostní incident, je úmyslné využití zranitelného místa, které má za cíl způsobit škodu či ztrátu na aktivech IS, nebo neúmyslné uskutečnění akce, která způsobí škodu na aktivech. Provedení útoku spočívá v odposlechu, přerušení, změnou nebo přidáním jiné hodnoty k původnímu datu. (3) Náklady na realizaci kybernetických útoků jsou zanedbatelné oproti škodě, kterou mohou způsobit.

Životní cyklus kybernetického útoku

Kybernetický útok definuje Sedlák a kol. jako sled po sobě jdoucích událostí. Rozděluje jej na dvě základní fáze. První fází je neautorizovaný přístup (Unauthorized Access), který má další tři fáze, a to rekognoskaci sítě[1], služeb a aplikací; zvolení strategie a způsobu vedení útoku; aktivace škodlivého kódu. Další fází kybernetického útoku je zneužití (Unauthorized Use), který má opět tři fáze, a to adaptaci na prostředí; vybudování zázemí pro útok; vytvoření komunikačního kanálu pro zadávání příkazů a samotný útok. (5)

Jednotlivé fáze kybernetického útoku jsou ilustrovány na Obrázek 1.



Obrázek 1: Fáze kybernetického útoku

Zdroj: (5)

[1]Rekognoskace znamená systematický průzkum sítě s cílem získat informace o konfiguraci, zařízeních, službách a potenciálních bezpečnostních hrozbách. Tento proces může být prováděn různými způsoby, včetně automatických nástrojů (například skenovací software) nebo manuálního zkoumání síťové infrastruktury.

Dále jsou vyjmenovány vybrané typy kybernetických útoků:

Malware

Jedná se o běžný typ kybernetického útoku pomocí škodlivého softwaru (malicious software, zkr. malware). Malware cílí v podstatě na cokoliv a na infikovaném zařízení se projevuje různě ve snaze zůstat skrytý. (4) Společným cílem pro malware jsou krádež identity, špionáž a narušení služeb.

Dle Sedláka a kol. (5) do této rozsáhlé skupiny škodlivého softwaru patří viry, červy (worms), trojský kůň, spyware, ransomware, scareware nebo malware cryptominers:

- **spyware**-má za cíl stopovat, špehovat, sledovat aktivity uživatele. Často dochází k tomu, že je sám uživatel upozorněn v licenčním ujednání softwaru o shromažďování, odesílání a využívání citlivých informací o uživatelů. Tato licenční ujednání při instalaci aplikace takřka nikdo nečte, a přesto jej odsouhlasí. Spyware je např. keylogger využívaný ke krádežím hesel.
- **ransomware**-software, který se pokouší o identifikaci zranitelných cílů, zašifrování dat na disku či zablikání koncových zařízení a následné vydírání uživatele pod hrozbou trestu či ztráty dat.
- **scareware**-má za cíl vyděsit uživatele. Jedná se o podvodné antiviry, které jsou doporučovány uživateli ke stažení a instalaci na infikované webové stránce. (4)

1.4 Sociální inženýrství

Šulc uvádí, „*pokud jde o bezpečnost, stále platí, že zaměstnanci jsou nejslabším článkem*.“ Sociální inženýrství je proces získávání citlivých informací, jako např. hesel a přístupových údajů od uživatelů s využitím manipulace nebo i zastrašování. Podvodník, sociální inženýr, chce získat nějakou informaci nebo uživatele donutit k provedení nějaké akce a použije k jejímu získání různých kliček, různých metod manipulace, časové tísně nebo se vydává za výše postaveného ve společenské hieararchii. (4) Nejlepší způsob obrany proti výše uvedenému je zdravý úsudek a povědomí o tom, kam se obrátit v případě nejistoty. Mezi dva běžné typy postupů vedeného sociálním inženýrem je prostřednictvím ICT, nebo postup využívající lidský faktor. Sociální inženýrství využívající lidský faktor je způsob, kdy sociální inženýr použije telefonický kontakt mezi dvěma osobami, nebo přímý kontakt k získání citlivých informací. Může se jednat o prosbu kolegy, který žádá o sdělení osobních údajů či zaslání peněz, nebo telefonát od pracovníka IT oddělení, který po zaměstnanci vyžaduje pod

různými záminkami sdělení přihlašovacích údajů do IS. Případný úspěch hackera je vždy závislý na tom, zda zaměstnanec spolupracuje.

Phishing

Mezi nejčastější útoky využívající sociální inženýrství lze zařadit phishing. Phishingové útoky mají za cíl krádež uživatelských dat, přihlašovacích či platebních údajů, a to zneužitím e-mailových služeb, zneužitím online softwarových služeb (např. Google Workspace, Microsoft 365, Dropbox), nebo zneužití cloudových služeb pomocí podvržených doménových adres a certifikátů. (5) Tradiční phishing je charakteristický rozesíláním obrovského množství e-mailů často na špatné adresy, kdy tyto e-maily obsahují gramatické a stylistické chyby a odkaz na internet. (4)

Spear phishing

Spear phishing je cílený sofistikovaný útok na konkrétního uživatele formou rafinovaného podvodného e-mailu se škodlivou přílohou či podvodným odkazem. Byly evidovány případy, kdy uživatel jako příjemce dokonce e-mail od odesílatele očekával. (4)

1.5 Řízení informační bezpečnosti v organizaci

Podle Šulce je nutno k vytvoření systému řízení informační bezpečnosti v organizaci v prvním kroku jmenovat odpovědnou osobu za řízení informační bezpečnosti. V dalším kroku by měly všechny organizace bez rozdílu ve velikosti, předmětu podnikání nebo odvětví zavést základní bezpečnostní opatření týkající se organizačního a technické zajištění. Dále navázat analýzou rizik, navrhnout vhodný způsob zvládání rizik a implementovat další bezpečnostní opatření. (4)

Vhodná metodika pro řízení informační bezpečnosti bez ohledu na velikost organizace a odvětví působnosti je ošetřena normou ISO/IEC 27001 (6) a příslušná bezpečnostní opatření organizační a technické povahy jsou uvedeny v katalogu opatření v ISO/IEC 27002 (7).

Aktivum

Aktivum představuje hmotné či nehmotné vyjádření určité hodnoty pro subjekt. Hodnota aktiva může být zmenšena uskutečněním hrozby. Hmotná aktiva jsou například nemovitosti, zboží, hardware, ceniny, finanční prostředky. Nehmotná aktiva jsou například kvalita personálu, pověst firmy, data, informace, znalosti, software, objekty autorského nebo průmyslového práva. (8)

Hrozba

Definice hrozby dle McQuade je náhodná či úmyslně vyvolaná událost s negativním dopadem na důvěrnost, integritu a dostupnost aktiv. (9)

Riziko

Kolouchem a kol. je riziko vymezeno jako možnost využití zranitelnosti aktiva či skupiny aktiv určitou hrozbou za účelem způsobit organizaci škodu. V oblasti kyberbezpečnosti jsou terčem rizika jednak uživatelé, tak i systémy a aplikace, které jsou uživateli využívány. (10) Riziko lze definovat jako pravděpodobnost narušení vyhovujícího stavu realizací hrozby. (8) Riziko lze vyhledávat nebo se mu lze vyhnout, v nějakých situacích nezbývá než riziko akceptovat. Předcházení hrozby dochází ke snížení rizika, k ochraně aktiv organizace a tím ke zvýšení bezpečnosti. V reálném světe lze mapovat z pohledu bezpečnosti podobné situace jako ty v IT oblasti. Zamykat zámek ve dveřích je stejné jako uzamykat obrazovku počítače. Nestahovat a neinstalovat programy, co lze objevit jako nabízené zdarma ke stažení. Rozhlížet se na křižovatce podobně jako udržovat počítač aktualizovaný a tím chráněný, nebo kontrolovat odesílatele e-mailů.

Zranitelnost

Požár definuje zranitelnost jako „*nedostatek nebo slabinu bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv. Každé aktivum je zranitelné, protože jeho hodnotu ohrožují různé vlivy.“* (3) Původcem zranitelnosti, obdobně jako hrozby, mohou být technická závada, živel či jednání člověka. (10) Systémová zranitelnost jsou slabiny v softwaru nebo hardwaru na zařízení uživatele či serveru, které může zneužít odhodlaný vetřelec k získání přístupu do sítě nebo k jejímu vypnutí. (11) Pipkin definuje zranitelnost systému jako stav, slabost nebo absenci bezpečnostní procedury nebo technických, fyzických nebo jiných kontrol, které by mohly být zneužity hrozbou. (12) Zranitelnosti existují nejen v hardwaru a softwaru, které tvoří IS, ale také v zásadách a postupech, zejména v bezpečnostních zásadách a postupech, které jsou používány jejich uživateli, nejčastěji zaměstnanci organizací. Vzhledem k tomu, že zranitelnosti lze nalézt v mnoha oblastech IS, zranitelností zabezpečení je skutečně cokoli v počítačové síti, co má potenciál způsobit nebo být zneužito ve prospěch útočníka. (11)

Zdroje zranitelností

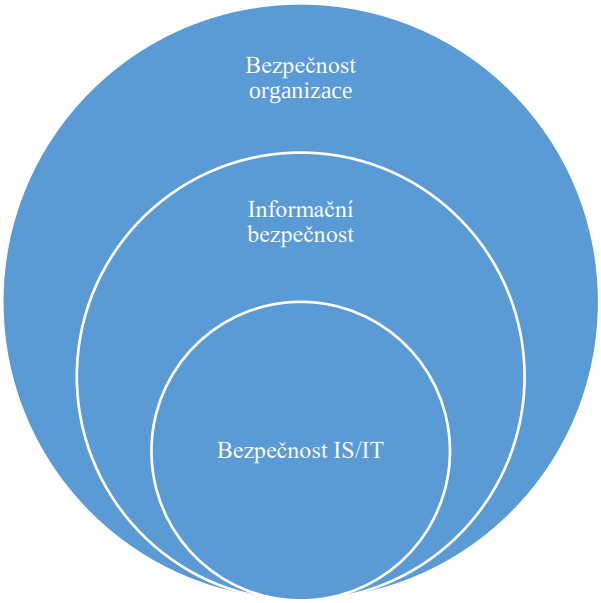
Četnost a rychlost šíření kybernetických útoků v posledních několika letech naznačují vážné problémy se zranitelností v IS. Podle Kizza neexistuje žádný definitivní seznam všech možných zdrojů zranitelností systémů. Mnohými odborníky a agenturami pro hlášení bezpečnostních incidentů, jako je například koordinační centrum Computer Emergency Response Team (CERT), nebo Computer Security Incident Response Team (CSIRT), je upozorňováno na více faktorů, které přispívají k bezpečnostním problémům a představují překážky pro bezpečnostní řešení. Mezi nejčastěji zmiňované zdroje problémů se zranitelností v systémech patří konstrukční chyby, slabý bezpečnostní management, nesprávná implementace bezpečnostních opatření, zranitelnost internetových technologií, obtížnost oprav zranitelných systémů, omezení účinnosti reaktivních řešení, povaha činnosti narušitelů a sociální inženýrství. (11)

Bezpečnost v organizaci

Bezpečnost organizace nebo firmy je komplexní koncept, který zahrnuje opatření a strategie navržené k ochraně různých aktiv organizace, včetně lidí, majetku, informací a procesů, před různými hrozbami a nebezpečím. Těmito hrozbami mohou být fyzické, jako jsou přírodní katastrofy, krádeže nebo vandalismus, a také digitální, jako jsou kybernetické útoky, malware nebo krádež dat.

Vztah úrovní bezpečnosti v organizaci je znázorněn na Obrázek 2. Podle Požára je bezpečnost organizace hierarchicky nejvyšší kategorií. Zahrnuje objektovou bezpečnost, bezpečnost majetku organizace jako je ostraha přístupů apod. Kontrolou oprávnění fyzického přístupu do budov je zároveň zajištěna bezpečnost IS a ICT. Další její součástí je informační bezpečnost. Informační bezpečnost je zaměřena specificky na ochranu informací organizace. To zahrnuje identifikaci, klasifikaci a ochranu citlivých informací, jako jsou osobní údaje zákazníků, obchodní tajemství a strategické plány, před neoprávněným přístupem, manipulací nebo zneužitím. Informační bezpečnost se zabývá také ochranou informačních technologií a systémů před kybernetickými hrozbami, včetně útoků na síťovou bezpečnost, phishingu, ransomwaru a dalších forem digitálních útoků. Bezpečnost IS a ICT je zaměřena na ochranu aktiv, která jsou součástí IS organizace podporovaného informačními a komunikačními technologiemi. Z toho důvodu je bezpečnost IS a ICT v hierarchii řízení bezpečnosti organizace tou nejužší oblastí. (3) Bezpečnost IS a ICT je úzce spojena s technologií, a proto za ni obvykle nese odpovědnost samostatné IT oddělení nebo bezpečnostní tým. Jelikož jsou

zapotřebí specializované znalosti o počítačových sítích, softwaru, šifrování a bezpečnostních hrozbách, je tato oblast vyhrazena specialistům s těmito dovednostmi. I když je bezpečnost IS a ICT vnímána jako úzce specializovaná oblast, je stále zásadní pro ochranu organizace před kybernetickými hrozbami a zajištění stability a důvěryhodnosti jejich informačních systémů.



Obrázek 2: Vztah úrovní bezpečnosti v organizaci

Zdroj: vlastní zpracování dle (3)

Celkově řečeno, bezpečnost organizace zahrnuje jak fyzické, tak digitální aspekty, a informační bezpečnost je klíčovou součástí celkové bezpečnostní strategie organizace.

1.6 Metoda ohodnocení rizik PNH

Metoda ohodnocení rizik PNH je jednoduchá semikvantitativní metoda analýzy rizika, která kombinuje prvky kvantitativního a kvalitativního přístupu. Tato metoda využívá číselné hodnoty nebo stupně k vyjádření určitých aspektů rizika, které nemusí dosahovat úrovně detailního matematického modelování charakteristické pro úplně kvantitativní metody. Za použití třech složek je vyhodnoceno příslušné riziko. (13)

Tato metoda vychází z rovnice analýzy rizik:

$$\boldsymbol{R = P \times N \times H}$$

Obrázek 3: Vzorec výpočtu metody ohodnocení rizik PNH

Zdroj: (13)

kde je:

R - celková míra rizika;

P - pravděpodobnost vzniku situace;

N - možné následky rizika pro objekt;

H - názor hodnotitelů na míru.

Jednotlivé složky metody PNH jsou ohodnoceny na bodové škále 1-5. Ohodnocené složky metody jako je *P*, *N*, *H* jsou dány do vztahu k hrozbám a provede se ohodnocení hrozeb. Tím dojde k určení pravděpodobnosti vzniku situace, k ohodnocení vážnosti následků rizika pro objekt a ke zjištění názoru hodnotitelů na míru závažnosti rizika. Hodnoty jednotlivých složek jsou následně dosazeny do vzorce Obrázek 3.

Výsledná hodnota *R* celkového hodnocení rizika vyjadřuje dle příslušné hodnotící stupnice v Tabulka 1 úroveň nutnosti zavedení protiopatření. (13)

Tabulka 1: Celkové hodnocení rizika metody PNH

Rizikový stupeň	**R**	**Míra rizika**
I.	>100	Nepřijatelné riziko
II.	51 - 100	Nežádoucí riziko
III.	11 - 50	Mírné riziko
IV.	3 - 10	Akceptovatelné riziko
V.	<3	Bezvýznamné riziko

Zdroj: vlastní zpracování dle (13)

Pomocí metody ohodnocení rizik PNH má organizace možnost identifikovat a analyzovat různé druhy rizik, pravděpodobnost jejich vzniku a lépe porozumět jejich potenciálním dopadům. Na základě výsledků použití této metody může organizace rozhodnout, jakým způsobem s riziky naložit-buď je přijmout, snížit, přenést nebo se jim vyhnout-a vytvořit plán řízení rizik, kterým lze minimalizovat nežádoucí dopady a maximalizovat příležitosti.

2 POPIS VYBRANÉ ORGANIZACE A PRŮZKUM NASTAVENÝCH PREVENTIVNÍCH OPATŘENÍ Z HLEDISKA ZAMĚSTNANCŮ

Obsahem kapitoly je popis vybrané organizace a průzkum nastavených preventivních opatření IT bezpečnosti z hlediska zaměstnanců v organizaci.

2.1 Popis vybrané organizace

Vybranou organizací je pojišťovna se sídlem v Praze. V roce 1991 vznikla jako akciová společnost a nyní je součástí mezinárodní pojišťovací skupiny. Její základní kapitál má 4 000 000 000 Kč a má největší klientský kmen, který obsahuje 4 miliony klientů. Klienty organizace jsou jednak fyzické osoby, tak i právnické osoby. Organizace zaměstnává 3096 osob. S ohledem na klientský kmen je prioritou organizace být spolehlivým a důvěryhodným partnerem. Vizí společnosti je, aby byla svým klientům oporou v nepříznivých životních okamžicích. (14)

Průzkum nastavených preventivních opatření IT bezpečnosti je zaměřen na zaměstnance pojistně-technického útvaru. Pracoviště útvaru je umístěno v kancelářských budovách v Praze, Brně a v Pelhřimově, kde mají v oddělených sekcích sídlo i jiné firmy.

2.2 Průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb z hlediska zaměstnanců

Následující kapitola se bude zabývat nastavením preventivních opatření v oblasti IT bezpečnosti ve vybrané organizaci a případných hrozeb z hlediska zaměstnanců.

2.2.1 Způsoby zajištění důvěrnosti informací

Následující část bude věnována netechnickým příkladům zajištění důvěrnosti informací v organizaci.

Objektová bezpečnost

Kontrola vstupu je pro bezpečnost organizace stejně důležitá jako ochrana informací a dalších aktiv. K identifikaci každého zaměstnance slouží vstupní karta, která v prostorách uvnitř budovy odlišuje oprávněné osoby od těch nepovolaných. V identifikační kartě je umístěn čip, jehož kód je elektronicky snímán. Určuje vstupní práva pro přístup do zabezpečených prostor na individuální úrovni každého zaměstnance v závislosti na stupni zodpovědnosti a pracovních povinnostech. Pro případné návštěvníky je zřízena kniha hostů, kam je každý

návštěvník zapsán. Zaměstnanec nese za svého návštěvníka odpovědnost a zajišťuje doprovod po celou dobu návštěvy v prostorách organizace tak, aby se nedostal do nepovolených prostor. (15)

Spořič (uzamknutí) obrazovky

Zablokuje počítač a zabrání nepovolané osobě v přístupu k pracovním, interním nebo důvěrným údajům v době, kdy uživatel není u svého zapnutého pracovního počítače. Počítač lze znovu použít po zadání (důvěrného) hesla zaměstnance. (15)

Čistý pracovní stůl

Čistý pracovní stůl bez citlivých nebo důvěrných materiálů jako jsou dokumenty, sestavy, paměťová média apod. zanechaných na stole bez dohledu po opuštění pracoviště. Zaměstnanec před odchodem od stolu by měl vyprázdnit přihrádku na dokumenty a došlou poštu, uzamknout zásuvky u stolů a kartoték a klíče uložit na bezpečném skrytém místě. Z flipchartů a z dalších prezentačních pomůcek by měl odstranit citlivé informace. Počítač by měl být před odchodem z pracoviště uzamčený nebo vypnutý. (15)

Místo a vybavení pro bezpečné ukládání informací

Je to místo, kde mohou být důvěrné dokumenty uzamčeny (trezor, uzamykatelná zásuvka, skříňka). (15)

Bezpečná likvidace médií a dokumentů

Pokud již informace nejsou nadále využitelné, je třeba je bezpečně zlikvidovat. V případě výpočetního zařízení je předat oddělení IT k vyřazení. Papírové dokumenty obsahující osobní nebo důvěrné firemní informace je třeba zničit skartací. (15) Ze zákona je ovšem nutné některé dokumenty uchovat. (16; 17) Důvěrná data na přenosných médiích je třeba před vyhozením nosičů odstranit a fyzické nosiče jako např. CD, flash disk je třeba fyzicky zničit. Odstranění není to samé jako vymazání dat z médií. Pro odstranění dat z média je nutný speciální software. Pokud není tento software k dispozici, je bezpečné odstranění dat zajištěno zničením nosiče. (15)

Hesla

Heslo je spojeno s osobním uživatelským jménem každého zaměstnance. Uživatelské jméno je elektronické jméno, které je zaměstnanci přiděleno při nástupu. Uživatelské jméno je elektronická identita a heslo je zvolený identifikační kód, který zná pouze uživatel.

Uživatelské jméno je systémem rozpoznáno po přihlášení, následně po zadání hesla porovná uživatelem zadané údaje s těmi, které jsou v systému uloženy. Pokud je zadané heslo správné, systém umožní uživateli přístup k datům a informacím. Při vytváření hesla by se měl uživatel vyhýbat běžným slovům, datům nebo číslům, zvláště těm, která vyvolávají osobní asociace, např. datum narození nebo příjmení. Dále by nemělo být voleno heslo jako nějaká posloupnost, protože jsou potom snadno odhadnutelná. Uživatel by měl délku hesla volit minimálně z dvanácti znaků, ale zároveň tak, aby neměl problém si jej zapamatovat. Je nežádoucí někam zapisovat heslo (papírek, nalepovací proužek, zadní strana klávesnice), protože je možné i pravděpodobné jeho vyzrazení. Heslo musí obsahovat zástupce alespoň tři z kategorií znaků jako je velké písmeno, malé písmeno, číslice a speciální znak. Heslo by mělo být v pravidelných intervalech obměňováno, v organizaci je nastaven interval na 90 dní. (15)

Zásady informační bezpečnosti

Zásady informační bezpečnosti vyžadující zakotvení závazku zachování důvěrnosti informací (mlčenlivosti) se všemi zaměstnanci organizace a spolupracujícími právnickými a fyzickými osobami souvisí se skupinovou politikou, která byla přeložena jako „Skupinový prováděcí pokyn bezpečnosti informací“ (18). Z ní vychází i závazný interní předpis pro koncové uživatele „Pravidla IT Bezpečnosti pro koncové uživatele“, kdy zaměstnanec musí potvrdit seznámení s interním předpisem (IP) v aplikaci pro vyhledání závazných interní předpisů (EDIT). (19)

2.2.2 Způsoby zajištění integrity informací

V této podkapitole bude vysvětlen význam integrity (neporušenosti) informací a bude uvedeno, jaké organizační a technické způsoby k zajištění integrity informací jsou organizací používány.

Chod kterékoli organizace je závislý na správném zpracování potřebných a relevantních informací (dat) souvisejících s její činností. Každá složka, oddělení, útvar a tým potřebuje jiné, pro něj nepostradatelné, informace a data. Chybné nebo chybějící informace mohou v procesu přijímání rozhodnutí nebo při reakcích na potřeby klientů způsobit společnosti velkou škodu. Zajištění integrity dále uvedenými metodami má data a informace ochránit před jejich neautorizovanou změnou nebo ztrátou. Existuje zde pak i přesah až k zajištění dostupnosti (poškozená data nelze zpřístupnit). Ochrana integrity informací a informačních systémů s cílem minimalizovat riziko poškození je tedy vysokou prioritou organizace.

Způsoby zajištění integrity informací jsou vytvořeny na ochranu integrity systémů a informací v nich uložených. (19)

Procesy zálohování

Pravidelné zálohování poskytuje ochranu proti neočekávanému zničení systémů nebo dat. Zálohy dat musí být aktuální a spolehlivé. Na těchto zálohách jsou zaměstnanci a ostatní zpracovatelé v případě výpadku systému závislí. Zálohování sdílených disků na serverech je obvykle automatické, přesto je však třeba zálohovat i soubory vytvořené na PC přiděleném zaměstnanci. V organizaci jsou uživatelům zálohovány automaticky osobní disky H a sdílené disky X, což je preferovaný prostor pro ukládání pracovních dat. Tyto disky však mají omezené kapacity, proto je v organizaci běžnou praxí, že kupříkladu archiv pošty je ukládán na lokální disky (např. notebooku), nikoliv na vyměnitelná média (USB disky). V zálohování dat existují tři základní pravidla dané interním předpisem „Pravidla IT Bezpečnosti pro koncové uživatele“: vědět, kdo je za co zodpovědný, provádět pravidelné zálohování a zálohy ukládat na bezpečném místě. (19)

Integrita systému

Zaměstnanci by neměli provádět změny v systému bez patřičného oprávnění. Ani by se neměli bez oprávnění pokoušet opravovat žádnou část IS. V případě problému s informačním systémem (aplikací, počítačem, periferií) mají k dispozici aplikaci Helpdesk nebo kontaktní telefon na operátory Helpdesku, kteří konečným uživatelům v celé organizaci zajišťují IT podporu. (19)

Antivirová ochrana

Používání antivirových programů slouží k identifikaci virů a k eliminaci poškozených programů a dat ještě předtím, než mohou viry způsobit jakoukoliv škodu. Počítačové viry představují velmi reálnou a neustálou hrozbu pro bezpečnost informací. V současné době je reálná nákaza přes sítě nepřeberným množstvím virů. Některé jsou víceméně zábavné než doopravdy škodlivé, ale některé jsou velmi nebezpečné, především pokud se dostanou do korporátního prostředí. Znalost toho, co mohou viry způsobit, odkud pochází a jak se proti nim chránit, je proto velmi důležitá. Viry mohou pocházet z příloh e-mailů, kde mohou být maskovány jako obrázek či dokument, dále mohou pocházet ze souborů načtených z internetu, z infikovaných přenosných nosičů dat, nebo z levných pochybných software. Antivirová kontrola všech přicházejících a odcházejících dat je osvědčeným způsobem

k zabránění šíření virů v systému organizace. Používání antivirových programů vede k identifikaci virů a k eliminaci poškozených programů a dat ještě předtím, než mohou viry způsobit jakoukoliv škodu. Organizace má ve svých systémech nastavenou automatickou detekci a odstranění známých virů. Proto je důležitá aktuálnost antivirového programu, což je zajišťováno servisní společností. Od zaměstnanců je potřeba ostražitost a nespoléhat, že každý škodlivý program musí být rozpoznán. S odvoláním na to, že ještě nemusí být znám a v tom případě jen připravenost uživatele je ochranou. (19)

Ochrana proti virům – email

Pomocí e-mailu se může informace dostat k lidem rychleji a zefektivnit vyřešení problémů, pokud je používán správně. E-mail není bezpečný způsob pro zasílání důvěrných zpráv, pokud nejsou přidána bezpečnostní opatření jako např. šifrování obsahu. E-mail svými přílohami může nakazit počítač viry. Nezáleží jen na antivirové ochraně, ale také na opatrnosti uživatele. Obsah e-mailu může být použit v soudním řízení jako elektronický důkaz, proto by měl být zaměstnanec obezřetný a používat jej pouze pro obchodní či služební účely. Zaměstnanec by se měl vyhýbat zasílání citlivých a důvěrných dokumentů v otevřené podobě elektronickou poštou. Dokument by měl zkomprimovat programem WinZip (nebo jiným obdobným programem) za použití hesla. Toto heslo následně sdělit adresátovi jiným komunikačním kanálem. Jakýkoliv podezřelý e-mail byl měl zaměstnanec okamžitě nahlásit na Helpdesk. (19)

Bezpečné používání internetu

Internet dává hackerům potenciálně otevřený přístup k jakýmkoliv informacím, které má uživatel ve svém PC, pokud není jeho PC chráněno. Informace stažené z internetu mohou obsahovat viry stejně jako jakákoliv jiná forma počítačových dat. Za účelem ochrany před napadením internetovými viry organizace nastavuje kontrolní mechanismy, aby zajistila antivirovou kontrolu veškerých příchozích dat při jejich stahování. Přesto ale nezaručuje 100% bezpečnost. Úplně nové viry nemusí být v systémech dočasně podchyceny. Proto je pro zaměstnance vždy lepší vyhnout se stahování dat z internetu a navštěvovat jen důvěryhodné webové servery. Zaměstnancům je povoleno využívat internet k soukromým účelům v omezené míře, ale přednostně je určen pro pracovní účely. Zaměstnanci nesmí vstupovat na nevhodné webové stránky nebo na diskuzní fóra, jejichž obsah by mohl být interpretován jako hanlivý, obtěžující či jinak urážlivý. Z neznámé webové stránky mohou být do systému přenesena data, aniž by o tom uživatel věděl. Proto by měl uživatel navštěvovat jen

důvěryhodné webové servery. Prezentace informací o organizaci na internetu je zásadní s ohledem na fakt, že je internet veřejná doména. Na internet nelze vystavovat informace, které jsou pro organizaci a z hlediska zákonů důvěrné, osobní a citlivé. Publikováním dat o organizaci na internetu jsou pověřeny určité osoby. Kupříkladu v diskuzních fórech nesmí být zveřejňovány interní nebo důvěrné informace o organizaci. (19)

Bezpečnost mimo pracoviště

Pravidla práce z domova nebo jiných externích míst je organizací ošetřena pracovní směrnicí „Pravidla IT bezpečnosti pro koncové uživatele“, jejíž součástí je i vzdálený přístup k datům společnosti, např. z domova, kde je uvedeno, že primárním přístupem je prostřednictvím vzdálené plochy Citrix. Pokud je zaměstnanec mimo kancelář, veškeré vybavení jako například notebook, mobilní telefony, bezpečnostní karty a tablety (i soukromá zařízení zaměstnanců) vyžadují zabezpečený přístup pomocí aplikace Microsoft Intune. Tato aplikace spravuje a zabezpečuje přístup uživatelů a jejich zařízení k prostředkům organizace. Dále automatizuje nasazení zásad pro aplikace, zabezpečení, konfiguraci zařízení, dodržování předpisů, podmíněný přístup a integruje se službami ochrany před mobilními hrozbami. (20) Zaměstnanec by měl citlivé informace převážet v příručním zavazadle, neměl by nechávat v automobilu zařízení jako notebook, tablet viditelně položené, i když je vozidlo uzamčeno. Dále by měl zaměstnanec, pokud možno, vozidlo vždy uzamknout a vždy uzamykat svůj mobilní telefon tak, aby bylo nutné před jeho použitím zadat PIN kód. Pokud zavazadlo disponuje zámkem, používat jej. Zaměstnanec by si měl s sebou brát pouze ty technické prostředky, které pro cestu či jednání potřebuje. A konečně by měl dbát na ostražitost, když do něj například někdo vrazí, nebo vylije nápoj, protože může jít o pokus o krádež. Mezi další bezpečnostní pravidla je zařazeno vymazat z pracovního notebooku všechny staré soubory, chránit heslem citlivé/důvěrné soubory a provádět pravidelné zálohování dat. Zaměstnanci by měli dávat pozor, aby se jim při práci nikdo nedíval přes rameno a neprojednávali citlivé/důvěrné záležitosti na veřejnosti. (19)

Plány obchodní kontinuity

Plánování procesů obnovy dat zajišťuje společnosti možnost pokračovat v provozu i v případě selhání systémů nebo jiné poškozující události (povodeň, požár) náhradním způsobem. (19)

Pravidla instalace a řízení změn

Stanovené postupy pomáhají kontrolovat, jaké změny byly v systému provedeny a kdo je provedl. (19)

2.2.3 Způsoby zajištění dostupnosti informací

Zaměstnanci používají informační zdroje (data) a nástroje organizace (hardware, software, IS) k tomu, aby mohli vykonávat svoji práci. Pokud je přístup k příslušným informacím a zařízením přerušen, nemohou vykonávat svou práci. V závažných případech, např. při výpadku hlavních systémů, může nedostupnost informací zcela paralyzovat chod organizace. Právě proto je důležité udržovat a chránit dostupnost informací a dalších zdrojů.

Základním cílem bezpečnostních opatření organizace je zajistit maximální dostupnost informací a systémů autorizovaným osobám a ty ostatní (neautorizované) k informacím nepustit následujícími způsoby (18):

- dostatečně silným heslem, který je znám jen vlastníkovi účtu,
- klasifikací informací, což je zařazení informací, dat, dokumentů apod. do skupin, které je ohodnocují a ke kategoriím dávají přístup jen autorizovaným osobám a systémům,
- fyzickou bezpečností, která zajistí, že se k informaci a systému nedostane neautorizovaná osoba,
- pravidelným školením zaměstnanců.

Školení informační bezpečnosti

Nastavená preventivní opatření shrnuje školení informační bezpečnosti, které je organizací pojato jako budování povědomí o informační bezpečnosti (Information Security Awareness). Školení a test je vyžadováno u všech pracovníků organizace. Školení je opakováno obvykle každý jeden až dva roky. Určitou formou je prováděno i u externistů. Je to součástí požadavků regulátora České národní banky (ČNB). Jiné instituce mohou mít jiný dohled, např. Národní bezpečnostní úřad (NBÚ), Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), pokud spadají pod Zákon o kybernetické bezpečnosti a auditů finančních institucí. Být si vědom bezpečnosti neboli „mít bezpečnostní povědomí“ znamená, že uživatel bude vědět, že existuje zranitelnost i hrozba, tj. možnost, že by někdo mohl náhodně nebo záměrně poškodit či zneužít informace, uložené v informačním systému. Informace, jinak také informační aktiva v majetku organizace, je zapotřebí chránit, snažit se hrozby odhalit a zastavit dříve než se popsané věci jako poškození, zneužití či zničení

nastanou. Hrozbou je zde myšlena událost, při které dojde k popisovanému poškození, ztrátě, vyzrazení. Cílem budování povědomí o bezpečnosti by mělo být dosažení posunu v přístupu pracovníků k IT bezpečnosti, tedy k zabezpečení informací a majetku organizace. (15)

Klasifikace informací

Organizací je využívána klasifikace informací, což je proces kategorizace informací do kategorií podle jejich hodnoty pro organizaci a míry závažnosti negativního dopadu v případě jejich úniku. Hlavní cíle procesu klasifikace informací je snížení rizika neoprávněného zpřístupnění informace, zajištění souladu s relevantními právními předpisy a standardy, zachování provozní efektivity za současné přiměřené ochrany informací organizace. (15)

Stěžejní role a odpovědnosti v procesu klasifikace informací jsou následující:

Specialista klasifikace informací

Je to osoba pověřená osobou odpovědnou za klasifikaci informací. Udržuje kompletnost a aktuálnost interního pravidla klasifikace informací. Udržuje ve spolupráci s vlastníky dat/informací a jejich zástupci aktuálnost katalogu klasifikovaných informací. Poskytuje nezbytnou podporu a konzultaci vlastníkům dat/informací a jejich zástupcům. Vyřizuje na žádosti o udělení výjimky z pravidel klasifikace informací, přijímá všechna oznámení a podněty v souvislosti s porušením důvěrnosti informací společnosti. Podílí se na řešení bezpečnostních incidentů proti pravidlům klasifikace informací. (15)

Vlastník dat/informací

Je to osoba v postavení ředitele, v korporátním prostředí je používáno označení Chief executive officer (CEO), který odpovídá za zajištění přístupu uživatelů ke klasifikovaným informacím v souladu s principem „need to know“ včetně pravidelné revize. Tato osoba je odpovědna za definování a zajištění odpovídajících bezpečnostních požadavků na ochranu klasifikované informace v souladu s jinými interními předpisy společnosti. (15)

Zástupce vlastníka dat/informací

Je to osoba pověřená vlastníkem dat/informací, definuje a aktualizuje katalog klasifikovaných informací. Podporuje uživatele informací v dodržování interních pokynů a vhodným způsobem kontroluje dodržování pravidel nakládání s informacemi. Písemně informuje

specialistu o jakémkoliv porušení pravidel klasifikace informací, o kterém se dozví a které významně ohrozí či poruší důvěrnost informací společnosti. (15)

Uživatel dat/informací

Seznamuje se a dodržuje pravidla klasifikace informací, klasifikuje informace stupněm důvěrnosti. Při nakládání s informacemi společnosti dodržuje stanovená pravidla. Zajišťuje ochranu informací před neoprávněným přístupem. Neprodleně oznamuje bezpečnostní incidenty, jejichž důsledkem je porušení důvěrnosti informací. Zachovává mlčenlivost o záležitostech týkající se pravidel klasifikace informací.

Na Obrázek 4 je znázorněn katalog klasifikovaných informací, na kterém je patrný souhrn všech vytvořených a zpracovávaných informací v rámci určité organizační oblasti. Každá organizační oblast čili útvar organizace je podřízen vlastníkovi dat/informací. K tomu je vázán určitý stupeň důvěrnosti, který jim byl ze strany vlastníka dat přidělen. (15) Pro ilustraci bude uveden jeden příklad z katalogu klasifikovaných informací. Proces pro kontrolní činnosti prováděné ve vztahu k problematice prevence legalizace výnosu z trestné činnosti spolu s přiřazenými nástroji jsou v gesci útvaru bezpečnostního managementu. Tento proces a přiřazené nástroje mají přidělen stupeň klasifikace důvěrné. Katalog klasifikovaných informací je dostupný v autentizačním protokolu, Extensible Authentication Protocol (EAP). (21)

Společnost	Úroveň 1	Úroveň 2	Proces	Klasifikovaná informace	Stupeň klasifikace	Přiřazené komponenty
ČP	Útvar bezpečnostního managementu	Tým AML a spolupráce s třetími stranami	AML/CTF	Informace o kontrolní činnosti prováděné ve vztahu k problematice prevence legalizace výnosu z trestné činnosti a financování terorismu	Důvěrné	APO MF, APO PC, CDA(Citrix), CPDS, DA, DA Upload, EDIT, GOLEM, INKAS/EXKAS (GLI ČR), Intranet, JOK/CZP, JOK/EIB, JOK/PK, KDP, Kukátko Pegas, LN_ePoint (GLI ČR), MS Exchange, ProAS, SAP FI (GLI ČR), SYNPAC (GLI ČR), Sybila, TIA, VIAS
ČP	Útvar bezpečnostního managementu	Tým AML a spolupráce s třetími stranami	Kontrola dodržování mezinárodních sankcí	Informace o kontrolní činnosti prováděné ve vztahu k problematice dodržování mezinárodních sankcí	Důvěrné	APO MF, APO PC, CDA(Citrix), CPDS, DA, DA Upload, EDIT, GOLEM, INKAS/EXKAS (GLI ČR), Intranet, JOK/CZP, JOK/EIB, JOK/PK, KDP, Kukátko Pegas, LD, LN_ePoint (GLI ČR), MS Exchange, ProAS, SAP FI (GLI ČR), SYNPAC (GLI ČR), Sybila, TIA, VIAS
ČP	Útvar bezpečnostního managementu	Tým AML a spolupráce s třetími stranami	Spolupráce s třetími stranami	Komunikace s třetími stranami	Důvěrné	APO MF, APO PC, CCD, CDA(Citrix), CDU2, CPDS, DA, DA Upload, DDU, DWH, E-regresy, EDIT, GOLEM, HelpDesk (Tivoli), INKAS/EXKAS (GLI ČR), Intranet, JOK/CZP, JOK/DMO, JOK/PK, KDP, Kukátko Pegas, LD, MS Exchange, ProAS, SAP ERP (HR), SAP ERP (MM), SAP HR portál, SYNPAC (GLI ČR), TIA, VIAS, ePohledávky
ČP	Útvar bezpečnostního managementu	Tým objektové a technické bezpečnosti	Objektová bezpečnost	Informace o zabezpečení objektů ČP a GLI	Důvěrné	CDA(Citrix), CDU2, CDU3, EDIT, HelpDesk (Tivoli), Intranet, MS Exchange, SAP FI (GLI ČR), SAP HR portál
ČP	Útvar bezpečnostního managementu	Tým objektové a technické bezpečnosti	Bezpečnostní monitoring	Výstupy bezpečnostního monitoringu	Přísně důvěrné	CDA(Citrix), MS Exchange
ČP	Útvar bezpečnostního managementu	Tým objektové a technické bezpečnosti	Recepční činnosti	Informace vznikající v rámci činnosti recepcí	Interní	CDA(Citrix), EDIT, Intranet, MS Exchange, SAP ERP (FI)
ČP	Útvar bezpečnostního managementu	Tým analytické podpory vyšetřování	Analytická podpora vyšetřování	Analytické datové výstupy	Důvěrné	Aquarius.NET, CCD, CDA(Citrix), CDU2, CDU3, DA, DWH, ICMS (GLI ČR), INKAS/EXKAS (GLI ČR), JOK/APH, JOK/CZP, JOK/EIB, JOK/ISP, JOK/PK, KCČ, KDP, Kukátko Pegas, MS Exchange, ProAS, Reise, SYNPAC (GLI ČR), Sybila, TIA, VIAS

Obrázek 4: Katalog klasifikovaných informací

Zdroj: (21)

Uživatel dat/informací klasifikuje informace společnosti do jednoho z následujících stupňů důvěrnosti:

Veřejné

Neoprávněné zpřístupnění má zanedbatelný dopad na podnikání, aktiva, jednotlivce, image společnosti či obchodní partnery. Informace zařazené do kategorie „Veřejné“ jsou přirozené ve veřejné doméně a z tohoto důvodu nemusí být zvláštním způsobem chráněny. Příklady: finanční reporting (publikovaný), schválená rozvaha (publikovaná), tiskové zprávy (publikované), materiály pro veřejné akce, korporátní a marketingové informace (publikované).

Interní

Neoprávněné zpřístupnění má omezený dopad na podnikání, aktiva, jednotlivce, image společnosti či obchodní partnery. Příklady: politiky, postupy, prováděcí pokyny, interní sdělení, adresář společnosti, organizační schémata.

Důvěrné

Neoprávněné zpřístupnění může mít významný dopad na podnikání, aktiva, jednotlivce, image společnosti či obchodní partnery. Příklady: osobní údaje zákazníků/zprostředkovatelů (např. datum narození, adresa, telefonní číslo, e-mailová adresa, zdravotní údaje poškozených atd.), osobní složky zaměstnanců a mzdové údaje, interní výpočty týkající se produktů a tvorby cen, účetní a rozpočtové údaje. (15)

Přísně důvěrné

Neoprávněné zpřístupnění může mít vážný či tragický dopad na podnikání, aktiva, jednotlivce, image společnosti či obchodní partnery. Příklady: v podstatě se jedná o privilegované informace, např. informace týkající se aktivit v oblasti fúzí a akvizic, „cenově citlivé“ finanční dokumenty, materiály určené výhradně pro potřeby top managementu.

V závislosti na stupni důvěrnosti informace jsou v dokumentu „Manuál zacházení s informacemi společnosti“, který je přílohou IP „Pravidla klasifikace informací“, definována pravidla nakládání s informacemi společnosti s poznámkou v případě, že je uživateli dostupný proces/nástroj k zajištění souladu svého zacházení s danými pravidly. (15) Manuál zacházení s informacemi společnosti je ilustrován Obrázek 5, ze kterého je patrné, že pro zabezpečenou tiskárnu společnosti s omezením použití je dovolen tisk

dokumentů s klasifikací C2-interní až C4-přísně důvěrné. Informace klasifikované jako přísně důvěrné lze tisknout pouze na tiskárně, kde je přístup k ní logicky či fyzicky řízen, tj. za autentizace prostřednictvím přístupové karty či jiného prostředku a za stálé přítomnosti toho, kdo tisk zadal.

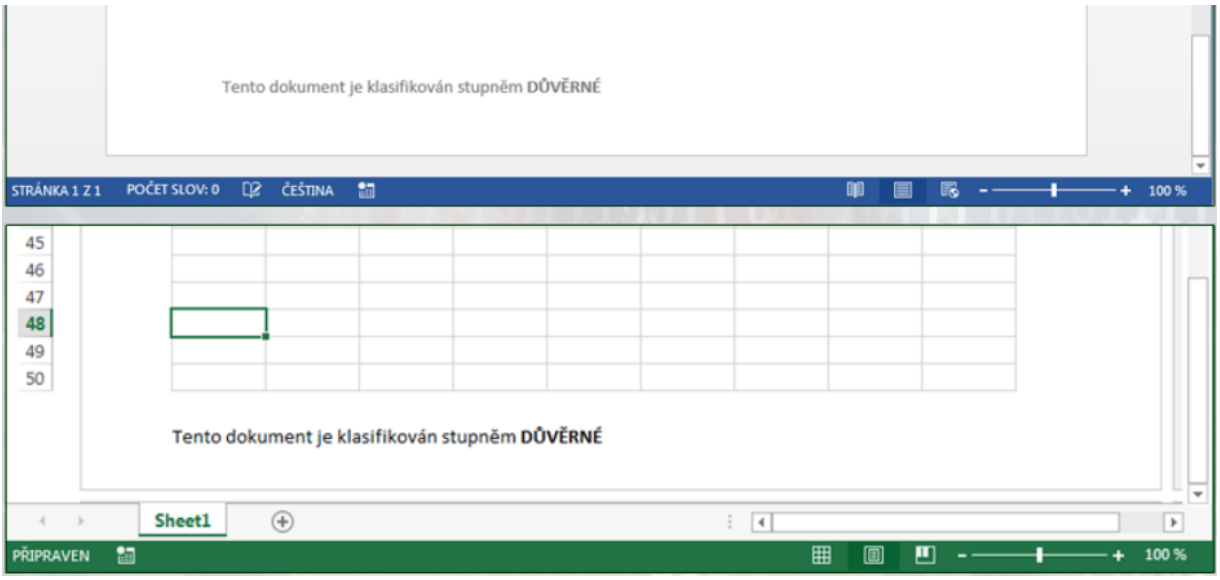
ČINNOST	NÁSTROJ/ KATEGORIE MÉDIA	NÁSTROJ/MÉDIA	C2 - INTERNÍ	C3 - DŮVĚRNÉ	C4 - PŘÍSNĚ DŮVĚRNÉ	STATUS	NÁSTROJ/PROCES DOSTUPNÝ PRO UŽIVATELE
Tisk	Tiskárny	Externí tiskárny	Dovoleno	Nedovoleno	Nedovoleno	Implementováno	Tisk informace klasifikované jako DŮVĚRNÉ a PŘÍSNĚ DŮVĚRNÉ na tiskárně mimo vlastnictví společnosti a bez omezeného přístupu uživatelů je zakázáno.
		Tiskárny společnosti (včetně zařízení užívaných v rámci outsourcingu) bez možnosti omezení přístupu	Dovoleno	Dovoleno	Nedovoleno	Implementováno	Každý uživatel by měl z preventivních důvodů minimalizovat tisk informace klasifikované jako DŮVĚRNÉ na tiskárně společnosti bez omezeného přístupu uživatelů (včetne zařízení užívaných v rámci outsourcingované činnosti).
		Zabezpečené tiskárny společnosti s omezením použití	Dovoleno	Dovoleno	Dovoleno	Implementováno	Informace klasifikované jako PŘÍSNĚ DŮVĚRNÉ lze tisknout pouze na tiskárně, kde je logicky nebo fyzicky řízen přístup (za autentizace prostřednictvím přístupové karty či jiného prostředku a za stálé přítomnosti toho, kdo tisk zadal).

Obrázek 5: Manuál zacházení s informacemi společnosti

Zdroj: (15)

Za jedno z pravidel nakládání s osobními údaji lze považovat, že společnost jako správce a zpracovatel osobních údajů přijala technická a organizační opatření k zajištění odpovídající úrovně zabezpečení osobních údajů. Tato opatření zahrnují i bezpečné nakládání s osobními údaji, kdy jsou zaměstnanci povinni při nakládání s osobními údaji dodržovat pravidla, která se vztahují na informace klasifikované jako důvěrné. Dále jsou zaměstnanci povinni při nakládání se zvláštními kategoriemi osobních údajů dodržovat pravidla, která se vztahují na informace klasifikované jako přísně důvěrné. (15)

Všichni uživatelé mají povinnost všechny dokumenty v elektronické či papírové podobě, které obsahují informace klasifikované jako důvěrné nebo přísně důvěrné viditelně označit příslušným klasifikačním stupněm dle metodického pokynu k označování informací. Příklad označení dokumentu je znázorněn na Obrázek 6. Povinnost označování se nevztahuje na smluvní dokumentaci, vybranou klientskou korespondenci, komunikaci s orgány činnými v trestním řízení a orgány veřejné správy. (15)



Obrázek 6: Klasifikace a označení dokumentů

Zdroj: (15)

2.2.4 Legislativní opatření

Obecně platí, že zákony zabývající se informační bezpečností vyžadují od organizací přijetí takových opatření, aby měly jejich používání pod kontrolou včetně informačních systémů, a to zavedením kontrol zajišťujících omezený přístup k informacím, zavedením procesů zajišťujících možnost obnovení informací. Dále jsou zavedeny kontroly zajišťující, aby zpracovávané a uchovávané informace byly přesné, a konečně i monitorování toku informací s cílem odhalit porušení pravidel informační bezpečnosti.

Porušení pravidel zaměstnancem v souvislosti se závaznými interními pravidly může vést i k rozvázání pracovního poměru. Dále může porušení pravidel vycházejících z platných zákonů může vést až k trestnímu stíhání. (15) Též může být udělena pokuta nebo vymáhána náhrada škody. Proto je v nejlepším zájmu každého zaměstnance brát otázky bezpečnosti informací vážně. Nejen kvůli možné způsobené škodě nebo porušení předpisů, ale i kvůli důsledkům, kterým by bylo nutné čelit, pokud by došlo k porušení zákona.

Mezi nejdůležitější zákony související s IT bezpečností společnosti patří Zákon č. 89/2012 Sb., občanský zákoník v platném znění, zejména pak ustanovení §504 (obchodní tajemství) (22), Zákon č. 277/2009 Sb., o pojišťovnictví v platném znění, zejména pak ustanovení §127 (povinnost mlčenlivosti) (23), Zákon č. 101/2000 Sb., o ochraně osobních údajů (24), který byl v r. 2019 nahrazen Zákonem č. 110/2019 Sb., o zpracování osobních údajů (GDPR) (25) a konečně Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění (26).

3 VÝSLEDKY PRŮZKUMU A VYHODNOCENÍ SLABÝCH MÍST

Průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb v organizaci z hlediska zaměstnanců byl proveden nejprve tak, že byla určena aktiva, hrozby a zranitelnosti. Následně bylo provedeno jejich ohodnocení metodou PNH popsanou v kapitole 1.6, ze které vzešly výsledná slabá místa.

3.1 Aktiva organizace

Definice aktiv vybrané organizace byla provedena na základě skupinové politiky organizace a interních materiálů organizace. Dále byly poznatky čerpány z vlastní znalosti pracoviště, které byly následně konzultovány s expertními pracovníky organizace. V Tabulka 2 jsou uvedena vybraná aktiva, která představují pro organizaci hodnotu.

Tabulka 2: Aktiva organizace a hodnota následků

Aktiva organizace		Použití aktiv	**Výše hodnoty následků (N)**
A1	**databáze**	údaje o klientech a smlouvách	**5**
A2	**pověst firmy**	obchodní výsledek	**4**
A3	**software**	operační systémy (OS), aplikace, nástroje	**2**
A4	**finanční zdroje**	přístup k účetnímu systému, platbám	**5**
A5	**zálohy**	zálohovaná data uživatelů IS, OS, databází	**5**
A6	**koncová zařízení**	notebooky, telefony, tiskárny, monitory	**2**
A7	**uživatelé IS**	zaměstnanci s přístupem do IS, databází	**3**

Zdroj: vlastní zpracování

Tabulka 2 obsahuje popis použití aktiv v organizaci a kvalitativní ohodnocení aktiv organizace na bodové škále 1-5, kdy nižší hodnota znamená nižší důležitost aktiva a tím i nižší důležitost aktiva pro organizaci. Z toho vyplývá hodnota následků (*N*) pro organizaci.

3.2 Hrozby pro aktiva organizace

Spektrum hrozeb, jež cílí na koncové uživatele, je celkem široké. Řádně proškolený zaměstnanec jako uživatel IS může hrozbu snáze rozpoznat a ubránit se. Ochrání tak sebe, svou práci a pomůže ochránit i informace, které vlastní společnost, u které je uživatel zaměstnán. Určení hrozeb v Tabulka 3 bylo provedeno na základě aktuálních nebezpečí, která se vyskytují v kyberprostoru (27) a která ovlivňují chod korporátních organizací (28).

Tabulka znázorňuje matici hrozeb ve vztahu k jednotlivým aktivům, kdy jejich vzájemný průnik označuje, jaká hrozba ohrožuje jaké aktivum. Dále je obsahem tabulky ohodnocení hrozeb na bodové škále 1-5, kdy vyšší hodnota znamená vyšší významnost hrozby pro organizaci. Stanovením číselné hodnoty jednotlivých hrozeb je umožněna kvantifikace hrozby a tím stanovuje pravděpodobnost vzniku (*P*).

Tabulka 3: Matice hrozeb a aktiv

	aktiva	**pravděpodobnost vzniku (P)**	databáze	pověst firmy	software	finanční zdroje	zálohy	koncová zařízení	uživatelé IS
	hrozby		A1	A2	A3	A4	A5	A6	A7
H1	neoprávněný vstup na pracoviště	**3**		X				X	X
H2	chybná klasifikace dat	**4**	X	X			X		X
H3	nechtěný zásah do integrity dat	**2**	X		X		X		X
H4	phishing útok	**5**	X	X	X	X	X		X
H5	ransomware	**4**	X	X	X	X	X	X	X
H6	chyba/ztráta/odcizení HW	**1**			X	X	X	X	
H7	zneužití zaměstnancem	**2**	X	X	X	X		X	X

Zdroj: vlastní zpracování

3.3 Zranitelnosti a výpočet pomocí metody PNH

Na základě znalosti útvaru organizace a konzultace s expertními pracovníky útvaru byly stanoveny zranitelnosti, které jsou shrnuty v Tabulka 4. Tabulka obsahuje ohodnocení míry ohrožení (*H*) jednotlivými zranitelnostmi na bodové škále 1-5, kdy vyšší hodnota vyjadřuje vážnou zranitelnost a tím i vyšší hodnotu míry ohrožení (*N*).

Tabulka 4: Matice hrozeb a zranitelností

	hrozby	**míra ohrožení (H)**	neoprávněný vstup na pracoviště	chybná klasifikace dat	nechtěný zásah do integrity dat	phishing útok	ransomware	chyba/ztráta/odcizení HW	zneužití zaměstnancem
	zranitelnosti		H1	H2	H3	H4	H5	H6	H7
Z1	slabé heslo	**3**			X	X	X		X
Z2	nedostatečná fyzická kontrola přístupu na pracoviště	**1**	X			X		X	X
Z3	neproškolení zaměstnanci	**5**	X	X	X	X		X	X
Z4	nedostupnost svěřeného HW	**2**	X		X	X	X	X	X
Z5	neaktuálnost SW	**4**			X	X	X		

Zdroj: vlastní zpracování

Ohodnocení hrozeb bylo provedeno rozsáhlým výpočtem dle metody PNH za použití vzorce na Obrázek 3 v kapitole č. 1. Výpočet je uveden v Tabulka 5.

Výsledné hodnoty míry rizika (*R*) byly vyhodnoceny příslušnou hodnotící stupnicí dle Tabulka 1 v kapitole č. 1, kterou byla určena úroveň nutnosti zavedení protiopatření. Škálování hodnot míry rizika (*R*) bylo v tabulce pro přehlednost barevně odlišeno.

Tabulka 5: Výpočet míry rizika (*R*) dle metody PNH

aktivum	hrozba	zranitelnost	N	P	H	R
A1	H2	Z3	5	4	5	100
A1	H3	Z1	5	2	3	30
A1	H3	Z3	5	2	5	50
A1	H3	Z4	5	2	2	20
A1	H3	Z5	5	2	4	40
A1	H4	Z1	5	5	3	75
A1	H4	Z2	5	5	1	25
A1	H4	Z3	5	5	5	125
A1	H4	Z4	5	5	2	50
A1	H4	Z5	5	5	4	100
A1	H5	Z1	5	4	3	60
A1	H5	Z4	5	4	2	40
A1	H5	Z5	5	4	4	80
A1	H7	Z1	5	2	3	30
A1	H7	Z2	5	2	1	10
A1	H7	Z3	5	2	5	50
A1	H7	Z4	5	2	2	20
A2	H1	Z2	4	3	1	12
A2	H1	Z3	4	3	5	60
A2	H1	Z4	4	3	2	24
A2	H2	Z3	4	4	5	80
A2	H4	Z1	4	5	3	60
A2	H4	Z2	4	5	1	20
A2	H4	Z3	4	5	5	100
A2	H4	Z4	4	5	2	40
A2	H4	Z5	4	5	4	80
A2	H5	Z1	4	4	3	48
A2	H5	Z4	4	4	2	32
A2	H5	Z5	4	4	4	64
A2	H7	Z1	4	2	3	24
A2	H7	Z2	4	2	1	8
A2	H7	Z3	4	2	5	40
A2	H7	Z4	4	2	2	16
A3	H3	Z1	2	2	3	12
A3	H3	Z3	2	2	5	20
A3	H3	Z4	2	2	2	8
A3	H3	Z5	2	2	4	16
A3	H4	Z1	2	5	3	30
A3	H4	Z2	2	5	1	10
A3	H4	Z3	2	5	5	50
A3	H4	Z4	2	5	2	20
A3	H4	Z5	2	5	4	40
A3	H5	Z1	2	4	3	24

aktivum	hrozba	zranitelnost	N	P	H	R
A3	H5	Z4	2	4	2	16
A3	H5	Z5	2	4	4	32
A3	H6	Z2	2	1	1	2
A3	H6	Z3	2	1	5	10
A3	H6	Z4	2	1	2	4
A3	H7	Z1	2	2	3	12
A3	H7	Z2	2	2	1	4
A3	H7	Z3	2	2	5	20
A3	H7	Z4	2	2	2	8
A4	H4	Z1	5	5	3	75
A4	H4	Z2	5	5	1	25
A4	H4	Z3	5	5	5	125
A4	H4	Z4	5	5	2	50
A4	H4	Z5	5	5	4	100
A4	H5	Z1	5	4	3	60
A4	H5	Z4	5	4	2	40
A4	H5	Z5	5	4	4	80
A4	H6	Z2	5	1	1	5
A4	H6	Z3	5	1	5	25
A4	H6	Z4	5	1	2	10
A4	H7	Z1	5	2	3	30
A4	H7	Z2	5	2	1	10
A4	H7	Z3	5	2	5	50
A4	H7	Z4	5	2	2	20
A5	H2	Z3	5	4	5	100
A5	H3	Z1	5	2	3	30
A5	H3	Z3	5	2	5	50
A5	H3	Z4	5	2	2	20
A5	H3	Z5	5	2	4	40
A5	H4	Z1	5	5	3	75
A5	H4	Z2	5	5	1	25
A5	H4	Z3	5	5	5	125
A5	H4	Z4	5	5	2	50
A5	H4	Z5	5	5	4	100
A5	H5	Z1	5	4	3	60
A5	H5	Z4	5	4	2	40
A5	H5	Z5	5	4	4	80
A5	H6	Z2	5	1	1	5
A5	H6	Z3	5	1	5	25
A5	H6	Z4	5	1	2	10
A6	H1	Z2	2	3	1	6
A6	H1	Z3	2	3	5	30
A6	H1	Z4	2	3	2	12
A6	H5	Z1	2	4	3	24

aktivum	hrozba	zranitelnost	N	P	H	R
A6	H5	Z5	2	4	4	32
A6	H6	Z2	2	1	1	2
A6	H6	Z3	2	1	5	10
A6	H6	Z4	2	1	2	4
A6	H7	Z1	2	2	3	12
A6	H7	Z2	2	2	1	4
A6	H7	Z3	2	2	5	20
A6	H7	Z4	2	2	2	8
A7	H1	Z2	3	3	1	9
A7	H1	Z3	3	3	5	45
A7	H1	Z4	3	3	2	18
A7	H2	Z3	3	4	5	60
A7	H3	Z1	3	2	3	18
A7	H3	Z3	3	2	5	30
A7	H3	Z4	3	2	2	12
A7	H3	Z5	3	2	4	24
A7	H4	Z1	3	5	3	45
A7	H4	Z2	3	5	1	15
A7	H4	Z3	3	5	5	75
A7	H4	Z4	3	5	2	30
A7	H4	Z5	3	5	4	60
A7	H5	Z1	3	4	3	36
A7	H5	Z4	3	4	2	24
A7	H5	Z5	3	4	4	48
A7	H7	Z1	3	2	3	18
A7	H7	Z2	3	2	1	6
A7	H7	Z3	3	2	5	30
A7	H7	Z4	3	2	2	12

Zdroj: vlastní zpracování

3.4 Výsledky průzkumu a vyhodnocení slabých míst

Pomocí metody PNH bylo zjištěno, s jakou pravděpodobností může dané riziko nastat a jak velký dopad může mít na fungování organizace a na bezpečné použití jejích aktiv. Vyhodnocení nejzávažnějších rizik, s dosaženým rizikovým stupněm I. nepřijatelné riziko a stupněm II. nežádoucí riziko, je zpracováno v Tabulka 6. Největším rizikem pro IT bezpečnost v organizaci z hlediska zaměstnanců jsou hrozby jako phishingový útok, chybná klasifikace dat, ransomware a neoprávněný vstup na pracoviště. Společným jmenovatelem těchto hrozeb jsou nedostatky v proškolení IT bezpečnosti zaměstnanců organizace, v aktualizaci SW a používání slabých hesel. Identifikované hrozby ohodnocené pomocí metody PNH by měla organizace s ohledem na jejich potenciální dopady analyzovat

a rozhodnout, jakým způsobem s riziky naložit. Organizace by měla nastavit protiopatření a tím minimalizovat nežádoucí dopady na svá aktiva.

Tabulka 6: Vyhodnocení nejzávažnějších rizik metodou PNH

aktivum	hrozba	zranitelnost	R	rizikový stupeň
databáze (A1)	phishing útok (H4)	neproškol. zaměst. (Z3)	125	I.
finanční zdroje (A4)	phishing útok (H4)	neproškol. zaměst. (Z3)	125	I.
zálohy (A5)	phishing útok (H4)	neproškol. zaměst. (Z3)	125	I.
databáze (A1)	chybná klasifik. dat (H2)	neproškol. zaměst. (Z3)	100	II.
databáze (A1)	phishing útok (H4)	neaktuálnost SW (Z5)	100	II.
pověst firmy (A2)	phishing útok (H4)	neproškol. zaměst. (Z3)	100	II.
finanční zdroje (A4)	phishing útok (H4)	neaktuálnost SW (Z5)	100	II.
zálohy (A5)	chybná klasifik. dat (H2)	neproškol. zaměst. (Z3)	100	II.
zálohy (A5)	phishing útok (H4)	neaktuálnost SW (Z5)	100	II.
databáze (A1)	ransomware (H5)	neaktuálnost SW (Z5)	80	II.
pověst firmy (A2)	chybná klasifik. dat (H2)	neproškol. zaměst. (Z3)	80	II.
pověst firmy (A2)	phishing útok (H4)	neaktuálnost SW (Z5)	80	II.
finanční zdroje (A4)	ransomware (H5)	neaktuálnost SW (Z5)	80	II.
zálohy (A5)	ransomware (H5)	neaktuálnost SW (Z5)	80	II.
databáze (A1)	phishing útok (H4)	slabé heslo (Z1)	75	II.
finanční zdroje (A4)	phishing útok (H4)	slabé heslo (Z1)	75	II.
zálohy (A5)	phishing útok (H4)	slabé heslo (Z1)	75	II.
uživatelé IS	phishing útok (H4)	neproškol. zaměst. (Z3)	75	II.
pověst firmy (A2)	ransomware (H5)	neaktuálnost SW (Z5)	64	II.
databáze (A1)	ransomware (H5)	slabé heslo (Z1)	60	II.
pověst firmy (A2)	neopr. vst. na pracov. (H1)	neproškol. zaměst. (Z3)	60	II.
pověst firmy (A2)	phishing útok (H4)	slabé heslo (Z1)	60	II.
finanční zdroje (A4)	ransomware (H5)	slabé heslo (Z1)	60	II.
zálohy (A5)	ransomware (H5)	slabé heslo (Z1)	60	II.
uživatelé IS (A7)	chybná klasifik. dat (H2)	neproškol. zaměst. (Z3)	60	II.
uživatelé IS (A7)	phishing útok (H4)	neaktuálnost SW (Z5)	60	II.

Zdroj: vlastní zpracování

Pro komplexní řešení IT bezpečnosti v organizaci z hlediska zaměstnanců by měly být monitorovány všechny nalezené hrozby dle Tabulka 5, protože při navýšení pravděpodobnosti jejich vzniku by došlo k nárůstu míry rizika.

Na základě provedeného průzkumu, jak jsou zabezpečena aktiva, se kterými pracují zaměstnanci organizace, byla v organizaci nalezena tato slabá místa včetně uvedení příslušných hrozeb:

1. Pro identifikaci a autentizaci je používáno pouze jednofaktorové přihlášení (hrozba phishing útoku, ransomware).

2. Vstup na pracoviště pouze pomocí identifikace předmětem, ID kartou (hrozba neoprávněného vstupu na pracoviště).
3. Nevyužívání možnosti zálohování e-mailových schránek zaměstnanců na cloudovém úložišti (hrozba phishing útoku a ransomware).
4. Možnost odložit plánovanou aktualizaci SW na koncovém zařízení. Pro přihlášení do účetního systému na zpracování případů jsou používány stejné přihlašovací údaje jako do celého IS organizace (hrozba phishing útoku, ransomware a zneužití zaměstnancem).
5. Možnost zásahu do databáze stavebního ceníku v expertním systému zaměstnancem při používání expertního systému (hrozba nechtěného zásahu do integrity dat a zneužití zaměstnancem).
6. Pořádání firemních soutěží pro zaměstnance a jejich prezentace pomocí e-mailů (hrozba phishing útoku a ransomware).
7. Zastaralé školení IT bezpečnosti zaměstnanců z roku 2016 s dvouletým cyklem opakování, které dostatečně nepodporuje angažovanost a motivaci zaměstnanců v dodržování pravidel IT bezpečnosti v organizaci (hrozba phishing útoku, neoprávněného vstupu na pracoviště, chybné klasifikace dat, nechtěného zásahu do integrity dat, chyby/ztráty/odcizení HW a zneužití zaměstnancem).

4 NÁVRHY VHODNÝCH PROTIOPATŘENÍ

Návrhy protiopatření v oblasti IT bezpečnosti z hlediska zaměstnanců byly vypracovány na základě zjištěných slabých míst pomocí metody PNH, které jsou uvedeny v závěru kapitoly 3. Organizace by měla návrhy protiopatření použít a tím minimalizovat nežádoucí dopady na svá aktiva. S ohledem na zaměření na IT bezpečnost zaměstnanců organizace byly některé návrhy protiopatření podrobněji rozpracované.

1. Zavedení dvoufaktorového přihlášení zaměstnanců do všech IS organizace.
2. Zavedení biometrické autentizace při vstupu na pracoviště.
3. Využívání možnosti zálohování e-mailových schránek zaměstnanců na cloudovém úložišti (např. Microsoft OneDrive).
4. Upravit nastavení automatických aktualizací SW na koncových zařízeních, které zaměstnanci používají. Dále diverzifikovat přihlašování uživatelů do SW nástrojů organizace, aby v případě prolomení hesla do IS útočníkem nedošlo k volnému přístupu do účetního systému organizace. Zaměstnanci by neměli kopírovat a distribuovat licencovaný software a používat software bez licence.
5. Změnit nastavení rolí uživatelů v databázích, aby nemohlo dojít k neoprávněnému zásahu do databází expertních systémů.
6. Zaměření managementu organizace na IT bezpečnost zaměstnanců a aktuální kybernetické útoky. Organizace by měla v tomto kontextu učinit preventivní kroky v běžném chodu organizace, aby předcházela nebezpečným situacím, například nepořádat vnitrofiremní soutěže pro zaměstnance a neposílat e mailem soutěžní vyplňovací formuláře. Organizace by měla zrevidovat nastavená opatření kybernetické bezpečnosti z hlediska zaměstnanců dle normy zabývající se problematikou kybernetické bezpečnosti ČSN ISO/IEC 27032 (369790) Informační technologie-Bezpečnostní techniky-Směrnice pro kybernetickou bezpečnost, příloha A. (29)
7. Úprava a aktualizace kurzu školení IT bezpečnosti zaměstnanců s uvedením konkrétních aktuálních příkladů ransomware a phishingových útoků, se kterými se zaměstnanci mohou při své práci reálně setkat. Zkrátit interval povinného absolvování interního školení IT bezpečnosti zaměstnanců na 1 rok.

5 ZÁVĚR

Předcházení kybernetickým bezpečnostním hrozbám a snižování následků hrozeb, kterým se předejít nepodaří, je rozsáhlou činností. Řešit IT bezpečnost a ochranu důvěrných dat pouze z pohledu ICT, nebo jako právní problém nestačí. Je vlastním zájmem každé organizace, aby její vedení znalo aktuální hrozby, trendy a praxi v IT bezpečnosti i z pohledu jejich zaměstnanců. Aby zaměstnanci dodržovali pravidla IT bezpečnosti, nestačí pouhé formální podepsání protokolu o seznámení s interními směrnicemi a metodikami. Pro jakoukoliv organizaci je nezbytné mít proškolené a motivované pracovníky, protože ti běžně pracují nebo mají přístup k chráněným aktivům nebo mohou být jakýmkoliv způsobem účastni kybernetického incidentu (mohou jej způsobit, zjistit, odvrátit).

Cílem této práce je průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb ve vybrané organizaci z hlediska zaměstnanců, vyhodnocení slabých míst a návrh protiopatření. V rámci tohoto cíle je práce zaměřena nejprve na teoretický základ IT bezpečnost. Následuje popis vybrané organizace, průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb z hlediska zaměstnanců. Práce obsahuje vyhodnocení slabých míst v IT zabezpečení organizace z hlediska zaměstnanců a návrh vhodných protiopatření.

Obsah první kapitoly tvoří teoretický základ IT bezpečnosti, který je klíčovým prvkem pro porozumění a aplikaci bezpečnostních opatření v organizacích. Jsou zde definovány základní pojmy jako bezpečnost, informační bezpečnost a její triáda – důvěrnost, integrita, dostupnost, Dále jsou vysvětleny vybrané kybernetické útoky s potenciálem ohrozit zaměstnance vybrané organizace. Tyto útoky mohou zahrnovat různé formy, včetně sociálního inženýrství, které využívá lidské chyby nebo nedostatky ve společnosti. V podkapitole o řízení informační bezpečnosti v organizaci je důraz kladen na pojmy jako aktivum, hrozba, riziko, zranitelnost, také jsou zmíněny nejčastější zdroje problémů se zranitelností. Součástí je i vysvětlení vztahu jednotlivých úrovní bezpečnosti v organizaci. V závěru první kapitoly je definována metoda ohodnocení rizik PNH, která slouží k identifikaci a hodnocení potenciálních hrozeb a zranitelností v organizaci, což umožňuje lépe porozumět rizikům a prioritizovat opatření k jejich řešení.

Druhá kapitola popisuje vybranou společnost a provádí v ní podrobný průzkum nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb z hlediska zaměstnanců. Nastavená bezpečnostní opatření v organizaci jsou rozčleněna na způsoby zajištění důvěrnosti

informací, způsoby zajištění integrity informací, způsoby zajištění dostupnosti informací a legislativní opatření.

Třetí kapitola se zabývá vlastním vyhodnocením výsledků z průzkumu nastavených preventivních opatření v oblasti IT bezpečnosti a případných hrozeb v organizaci z hlediska zaměstnanců. Nejprve byla určena a obodována aktiva, hrozby a zranitelnosti. Následně bylo provedeno jejich ohodnocení metodou PNH, ze které vzešla dle míry rizika výsledná slabá místa. Analýza výsledků průzkumu a vyhodnocení slabých míst vychází z identifikovaných aktiv organizace, možných hrozeb a zranitelností. Metoda PNH umožňuje kvantifikovat rizika a díky rizikovým stupňům identifikovat prioritní oblasti pro zlepšení. Na základě provedeného průzkumu, jak jsou zabezpečena aktiva, se kterými pracují zaměstnanci organizace, jsou vyjmenovaná konkrétní nejrizikovější slabá místa včetně uvedení příslušných hrozeb.

Na základě těchto výsledků jsou v závěrečné kapitole navržena ke každému slabému místu příslušná vhodná protiopatření, která mají za cíl zvýšit úroveň IT bezpečnosti organizace z hlediska zaměstnanců a minimalizovat rizika pro organizaci a její zaměstnance. Tato protiopatření zahrnují technologická opatření, změny procesů nebo politiky a další formy zlepšení ochrany dat a systémů organizace. Celkově je úspěch v oblasti IT bezpečnosti v organizaci závislý na kombinaci správně nastavených technologií, účinného řízení a osvěty zaměstnanců.

Přínosem této práce je poskytnutí komplexního pohledu na problematiku IT bezpečnosti v konkrétní organizaci zaměřenou na zaměstnance, protože se publikace či jiné analýzy zabývají spíše obecnou problematikou IT bezpečnosti nebo se zaměřením na oblast firem a organizací. Tato práce přispívá k posílení bezpečnostního povědomí samotných zaměstnanců vybrané organizace, zlepšení bezpečnostních postupů a ochraně informačních aktiv organizace, což má pozitivní dopad na celkovou úroveň bezpečnosti a spolehlivost pracovního prostředí pro zaměstnance. Díky této práci jsem získala širší povědomí o procesech a postupech v IT bezpečnosti velké korporátní společnosti. Také jsem si upevnila a prohloubila znalosti z tohoto oboru. Je možné, že se můj profesní rozvoj bude ubírat právě do oblasti zajištění IT bezpečnosti společností.

V souladu s cílem práce formulovaným v úvodní části mohu konstatovat, že jsem cíl práce splnila.

6 POUŽITÁ LITERATURA

1. **SMEJKAL, Vladimír, SOKOL, Tomáš a KODL, Jindřich.** *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň : Aleš Čeněk, 2019. 978-80-7380-765-8.

2. **JIRÁSEK, Petr a NOVÁK, Luděk a POŽÁR, Josef.** Výkladový slovník kybernetické bezpečnosti. [Online] 2015. [Citace: 29. únor 2024.] https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf.

3. **POŽÁR, Josef.** *Manažerská informatika.* Plzeň : Aleš Čeněk, 2010. 978-80-7380-276-9.

4. **ŠULC, Vladimír.** *Kybernetická bezpečnost.* Plzeň : Aleš Čeněk, 2018. 978-80-7380-737-5.

5. **SEDLÁK, Petr a KONEČNÝ, Martin a kolektiv.** *Kybernetická (ne)bezpečnost.* Brno : Akademické nakladatelství CERM, s.r.o., 2021. 978-80-7623-068-2.

6. **ČSN ISO/IEC 27001 (369797).** ***Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky.*** **Praha : Český normalizační institut, 2023.**

7. ČSN EN ISO/IEC 27002 (369798). ***Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti.*** **Praha : Český normalizační institut, 2023.**

8. SMEJKAL, Vladimír a RAIS, Karel. ***Řízení rizik ve firmách a jiných organizacích. 4. vydání.*** **Praha : Grada Publishing, 2013. 978-80-247-4644-9.**

9. McQuade, Samuel. ***Encyclopedia of Cybercrime.*** **Westport : Greenwood Press, 2008. 978-0313339745.**

10. KOLOUCH, Jan a BAŠTA, Pavel a kol. ***CyberSecurity.*** **Praha : CZ.NIC, z.s.p.o., 2019. 978-80-88168-31-7.**

11. KIZZA, Joseph Migga. ***Guide to Computer Network Security.*** **[Dokument] Fifth edition, Cham, Switzerland : Springer International Publishing, 2020. 978-3-030-38141-7.**

12. Pipkin, Donald L. ***Information Security: Protecting the Global Enterprise.*** **New Jersey : Prentice Hall, 2000. 978-0-130-17323-2.**

13. Šefčík, Vladimír. ***Analýza rizik*** **. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 978-80-7318-696-8.**

14. Generali Česká pojišťovna. ***O nás.*** **[Online] 2024. [Citace: 29. únor 2024.] https://www.generaliceska.cz/o-nas#vize-mise-hodnoty.**

15. Metodický útvar organizace II. Interní materiály. ***Školení informační bezpečnosti.***

16. AION CS, s.r.o. Zákony pro lidi. ***Zákon č. 235/2004 Sb. Zákon o dani z přidané hodnoty.*** **[Online] 2010-2024. [Citace: 24. březen 2024.] https://www.zakonyprolidi.cz/cs/2004-235.**

17. —. Zákony pro lidi. ***Zákon č. 582/1991 Sb. Zákon České národní rady o organizaci a provádění sociálního zabezpečení.*** **[Online] 2010-2024. [Citace: 24. březen 2024.] https://www.zakonyprolidi.cz/cs/1991-582.**

18. Metodický útvar organizace. Interní materiály organizace I. ***Skupinový prováděcí pokyn bezpečnosti informací.***

19. —. Interní materiály organizace. ***Pravidla IT Bezpečnosti pro koncové uživatele.***

20. Microsoft. Zabezpečení od Microsoftu. ***Základní funkce služby Microsoft Intune.*** **[Online] 2024. [Citace: 23. březen 2024.] https://www.microsoft.com/cs-cz/security/business/endpoint-management/microsoft-intune#tabxf3e200c1290442a594fbcbc3a22b12cf.**

21. Útvar IT bezpečnosti organizace. Interní materiály. ***Extensible Authentication Protocol.***

22. AION CS, s.r.o. Zákony pro lidi. ***Zákon č. 89/2012 Sb., občanský zákoník v platném znění.*** **[Online] 2010-2024. [Citace: 12. duben 2024.] https://www.zakonyprolidi.cz/cs/2012-89.**

23. —. Zákony pro lidi. ***Zákon č. 277/2009 Sb., o pojišťovnictví v platném znění.*** **[Online] 2010-2024. [Citace: 12. duben 2024.] https://www.zakonyprolidi.cz/cs/2009-277.**

24. AION CS s.r.o. Zákony pro lidi. ***Zákon č. 101/2000 Sb., o ochraně osobních údajů.*** **[Online] 2010-2024. [Citace: 20. duben 2024.] https://www.zakonyprolidi.cz/cs/2000-101.**

25. —. Zákony pro lidi. ***Zákon č. 110/2019 Sb., o zpracování osobních údajů (GDPR).*** **[Online] 2010-2024. [Citace: 20. duben 2024.] https://www.zakonyprolidi.cz/cs/2019-110.**

26. AION CS, s.r.o. Zákony pro lidi. ***Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).*** **[Online] 2010-2024. [Citace: 20. duben 2024.] https://www.zakonyprolidi.cz/cs/2000-121.**

27. Národní úřad pro kybernetickou a informační bezpečnost. Zprávy o stavu kybernetické bezpečnosti. ***Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022.*** **[Online] 19. červenec 2023. [Citace: 23. duben 2024.] https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick e_bezpecnosti_CR_za_rok_2022.pdf.**

28. BNP Media. Security Magazine. ***5 biggest cybersecurity threats.*** **[Online] 3. únor 2021. [Citace: 23. duben 2024.] https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats.**

29. ČSN ISO/IEC 27032 (369790). ***Informační technologie, bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost.*** **Praha : Český normalizační institut, 2023.**