

Řízení incidentů bezpečnosti informací

Bc. Petr Skřivánek

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Petr Skřivánek
Osobní číslo:	L23050
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Řízení incidentů bezpečnosti informací

Zásady pro vypracování

- Zpracujte teoretický vstup do řešené problematiky s důrazem na monografie.
- Pojednejte o doporučených postupech k zajištění informační bezpečnosti subjektů.
- Identifikujte vhodné postupy k řízení incidentů bezpečnosti informací.
- Navrhněte a modelujte konkrétní postup řízení vybraného incidentu bezpečnosti informací.

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

Seznam doporučené literatury:

1. CLARK, Robert M. a HAKIM, Simon. *Cyber-Physical Security*. 3rd ed. New York: Springer International Publishing, 2017. ISBN 978-3-319-32822-5.
 2. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
 3. NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Právní monografie. Praha: Wolters Kluwer, 2023. ISBN 978-80-7676-515-3.
 4. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
 5. WATTERS, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023. ISBN 9781032524511.
- Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**

Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

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

Prohlašuji, že

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

V Uherském Hradišti, dne: 24. 4. 2025

.....
podpis autora

ABSTRAKT

Diplomová práce se zaměřuje na problematiku, posouzení a zhodnocení systému řízení incidentů bezpečnosti informací vybraného subjektu. Je členěna do dvou, na sebe navazujících, částí. V teoretické části vymezuje základní pojmy, rešerše a přehled dostupných zdrojů v oblasti systému řízení incidentů. Dále se zabývá procesem řízení a identifikací vybraných incidentů, kontinuitu činností, analýzou dopadů, plány, strategií a dalšími opatřeními. Praktická část pojednává o základní charakteristice organizace, analýze a zhodnocení vhodných postupů řízení incidentů bezpečnosti informací. Následně je provedena analýza rizik a navržen model konkrétního postupu řízení vybraného incidentu.

Klíčová slova: řízení bezpečnosti informací, phishing, malware, organizace, hrozby, rizika.

ABSTRACT

The thesis focuses on the issues, assessment, and evaluation of the information security incident management system of a selected organization. It is divided into two interrelated parts. The theoretical part defines key concepts, includes a literature review, and provides an overview of available sources in the field of incident management systems. Furthermore, it addresses the process of incident management and identification of selected incidents, business continuity, impact analysis, planning, strategy, and other related measures.

The practical part discusses the basic characteristics of the organization and the analysis and evaluation of appropriate information security incident management procedures. Subsequently, a risk analysis is conducted, and a model for a specific incident response procedure is proposed.

Keywords: information security management, phishing, malware, organization, threats, risks.

Na tomto místě bych rád poděkoval vedoucímu své práce, panu Ing. Petru Svobodovi za odborné rady, cenné připomínky, trpělivost, a především drahocenný čas při vedení diplomové práce.

V neposlední řadě patří mé poděkování rodině, spolupracovníkům a nejbližšímu okolí za podporu a porozumění po celou dobu studia, zpracování této práce nevyjímaje.

Motto:

„Ten, kdo se ve jménu bezpečnosti vzdává svobody, nezaslouží si ani svobodu, ani bezpečnost.“

Benjamin Franklin

OBSAH

ÚVOD	11
CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE.....	13
I TEORETICKÁ ČÁST.....	14
1 ROZBOR MONOGRAFIE A ANALÝZA ODBORNÝCH ZDROJŮ	15
1.1 CYBER-PHYSICAL SECURITY	15
1.2 CYBERSECURITY	16
1.3 KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT 3D: IT, PRÁVO A COMPLIANCE.....	16
1.4 KYBERNETICKÁ (NE)BEZPEČNOST: PROBLEMATIKA BEZPEČNOSTI V KYBERPROSTORU	17
1.5 CYBERCRIME AND CYBERSECURITY	17
2 ZÁKLADNÍ POJMY	19
2.1 MODERNÍ HROZBY PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST.....	22
2.1.1 Phishing.....	23
2.1.2 Spam.....	24
2.1.3 Malware	24
2.1.4 Útok typu MiTM.....	24
2.1.5 Hrozba zevnitř.....	24
2.2 JAK SE BRÁNIT KYBERNETICKÝM ÚTOKŮM S VYUŽITÍM UMĚLÉ INTELIGENCE?	25
2.2.1 Zákonné normy a regulace	25
2.2.2 Směrnice NIS2	25
3 REAKCE NA INCIDENTY	27
3.1 PLÁN REAKCE NA INCIDENTY.....	27
3.1.1 Řízení rizik.....	29
3.1.2 Kontrolní mechanismy kybernetické bezpečnosti	29
3.1.3 Hodnocení závažnosti.....	30
3.1.4 Úroveň hodnocení závažnosti.....	30
3.1.5 Taktika, technika a postupy	30
3.1.6 Záznamy o událostech (uchování logů).....	31
3.1.7 Sběr a uchovávání důkazního materiálu.....	31
3.1.8 Obnovení provozu.....	31
3.2 KOORDINACE, SDÍLENÍ A OZNÁMENÍ.....	31
3.2.1 Závěrečná zpráva	32
3.2.2 Struktura závěrečné zprávy	32
4 POSTUPY ZAJIŠTĚNÍ INFORMAČNÍ BEZPEČNOSTI.....	35
4.1 KOMPLEXNÍ PŘÍSTUP K INFORMAČNÍ BEZPEČNOSTI A ŘÍZENÍ KYBERNETICKÝCH RIZIK	35
4.2 PŘÍSTUP A VZTAHY K EXTERNÍM SUBJEKTŮM PŘI ŘÍZENÍ KYBERNETICKÝCH HROZEB	37

5	DÍLČÍ ZÁVĚR.....	39
II	PRAKTICKÁ ČÁST	40
6	ANALYTICKO-EMPIRICKÁ ČÁST	41
6.1	POPIS A CHARAKTERISTIKA ORGANIZACE	41
6.2	PRIMÁRNÍ AKTIVA	42
6.3	PODPŮRNÁ AKTIVA.....	42
6.4	BEZPEČNOST OBJEKTU	44
6.5	ŘÍZENÝ ROZHOVOR	44
6.6	ANALÝZA PROSTŘEDÍ ORGANIZACE	45
6.7	VYHODNOCENÍ A OŠETŘENÍ RIZIK ORGANIZACE.....	47
6.8	FMEA	49
6.9	VÝSTUPY ANALÝZY FMEA.....	51
7	STANOVENÍ HYPOTÉZ A NÁVRH OPATŘENÍ	52
7.1	NAVROVANÁ OPATŘENÍ A DOPORUČENÍ	52
7.2	POSTUP ŘÍZENÍ KONKRÉTNÍHO BEZPEČNOSTNÍHO INCIDENTU – PŘÍKLAD	57
7.3	IDENTIFIKACE POSTUPŮ K ŘÍZENÍ INCIDENTŮ	60
8	VHODNÉ POSTUPY K ŘÍZENÍ INCIDENTŮ BEZPEČNOSTI INFORMACÍ	62
8.1	POSTUP PŘI ŘÍZENÍ INCIDENTŮ – PHISHING	62
8.2	NÁVRH ŘÍZENÍ INCIDENTU – PHISHINGOVÉHO ÚTOKU, MODEL PICERL.....	64
8.3	MODEL ŠÍŘENÍ PHISHINGOVÉHO ÚTOKU	67
8.4	KONTROLNÍ SEZNAM – CHECKLIST (PHISHING)	69
9	DISKUZE VÝSLEDKŮ VÝZKUMU	71
9.1	VÝSLEDKY ŘÍZENÉHO ROZHOVORU.....	71
9.2	VÝSLEDKY ANALÝZY RIZIK.....	71
	ZÁVĚR.....	73
	SEZNAM POUŽITÉ LITERATURY.....	75
	SEZNAM OBRÁZKŮ	80
	SEZNAM TABULEK.....	81
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	82
	SEZNAM PŘÍLOH.....	85

ÚVOD

Oblast kybernetické a informační bezpečnosti se vyvíjí stejně dynamicky jako naše společnost. Klade důraz na inovace, změnu přístupu a směrem k vzdělávání populace napříč generacemi, přináší i nové výzvy.

V digitální éře, kdy se moderní technologie stávají nedílnou součástí každodenního života, narůstá riziko hybridních a kybernetických hrozeb. Ochrana dat, systémů a uživatelů dávno není doménou IT specialistů, ale stává se klíčovou dovedností pro širokou veřejnost a zejména pro firmy a instituce. Dynamika vývoje nových technologií přináší nejen pokrok, ale také úskalí v podobě zranitelnosti a dalších rizik, které mohou být zneužity k útokům na jednotlivce, organizace nebo kritickou infrastrukturu.

Z tohoto důvodu je nutné rozvíjet programové a technické vybavení, posilovat povědomí o kybernetické bezpečnosti a podporovat vzdělávání v této oblasti.

Mezi nejvýznamnější komodity v digitální éře řadíme informace, data a čas. Informace a její dopady na lidskou společnost, vysvětluje v knize *„The Information: A History, a Theory, a Flood“* autor James Gleick, kdy poukazuje na mnohoznačnost pojmu informace a různých přístupech k jeho chápání. Poukazuje na teorie Samuela Morse, Alana Turinga a dalších významných osobností, které přispěli k rozvoji informační teorie (James Gleick, 2011).

Data jsou považována za základní prvky informací, představují čísla, znaky nebo symboly zaznamenané v digitální podobě, určené pro zpracování počítačem. Např. v knize *„Artificial Intelligence: A Modern Approach“* od Stuarta Russella a Petera Norviga je věnována značná pozornost etickým otázkám umělé inteligence. Zaměřuje se na výzvy, rizika a zejména dopady pro lidstvo a společnost (Stuart Russell a Peter Norvig, 2020).

Čas představuje fyzikální veličinu, která udává sled událostí, umožňuje měřit dobu trvání a vzájemné vztahy. Obklopuje nás a stejně tak odráží i oblast kybernetické bezpečnosti. Zde ovlivňuje reakční doby na incidenty, šifrování dat nebo monitorování systémových aktivit.

Známý citát, který je často připisován Benjaminu Franklinovi: „Když nemáš plán, plánuješ, že selžeš.“ (v originálu *„If you fail to plan, you are planning to fail.“*), přesně vystihuje důležitost strategie a přípravy v řízení incidentů.

Praktická část se ve svém úvodu zaměřuje na základní charakteristiku organizace. Dále je v této části provedena analýza a zhodnocení vhodných postupů řízení incidentů bezpečnosti informací. Následně je provedena analýza rizik a vypracován návrh modelu konkrétního postupu řízení vybraného incidentu. Součástí praktické části je vytvoření kontrolního seznamu a vypracování modelu dopadu a šíření vybraného incidentu, který znázorňuje rozdíl mezi řízenou reakcí na bezpečnostní incident a pasivním přístupem.

CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Hlavním cílem diplomové práce je analyzovat klíčové subprocessy vedoucí k řešení vybraného kybernetického bezpečnostního incidentu za využití modelování. Dílčími cíli práce jsou, s ohledem na dřívější zkušenost organizace s phishingovým útokem a její současný stav – zhodnocení systému řízení kybernetických bezpečnostních incidentů vybrané organizace, identifikace oblastí pro zlepšování kybernetické bezpečnosti a návrh opatření ke zmírnění dopadů a zvýšení efektivity reakce na kybernetické bezpečnostní incidenty.

K naplnění tohoto cíle bylo využito údajů poskytnutých vybraným subjektem, který si nepřál být jmenován. První, v teoretické části, použitou metodou je **rešerše a sběr informací**. Tato metoda byla využita v prvotní fázi, před samotným zahájením psaní diplomové práce.

Pro definování základních pojmů a vymezení oblastí zájmu charakteristických pro systém řízení bezpečnosti informací byla použita metoda **popisu**. V praktické části byla stanovena oblast a kritéria pro naplnění hlavního cíle diplomové práce. Při setkání se zástupci organizace byly uplatněny metody **dotazování, pozorování a řízeného rozhovoru**.

Mezi další metody využití při zpracování práce patří **analýza a komparace**. Pomocí analýzy rizik byl zhodnocen systém řízení konkrétního typu kybernetického bezpečnostního incidentu, stanovena míra rizika a identifikovány nejzávažnější hrozby. Tyto hrozby byly následně porovnány s údaji charakterizujícími stav před a po přijetí opatření u organizace.

I TEORETICKÁ ČÁST

1 ROZBOR MONOGRAFIE A ANALÝZA ODBORNÝCH ZDROJŮ

Kybernetická bezpečnost se stala jedním z nejdůležitějších témat digitálního věku, kdy informační technologie každodenně vstupují do našich životů a jsou jeho nedílnou součástí. Pochopení principů kybernetické bezpečnosti, řízení incidentů a dopadů kyberkriminality je proto klíčové pro efektivní ochranu digitálního prostředí, a to nejen pro jednotlivce, organizace, státní instituce, ale zejména pro kritickou infrastrukturu.

Následující kapitola se nezaměřuje na výčet všech dostupných zdrojů zabývajících se tématikou kybernetické bezpečnosti, ale vybranými monografiemi, které tvoří základ práce.

Výběr odborné literatury byl podmíněn důrazem na aktuálnost, odbornou relevanci a přímou souvislost s problematikou řízení kybernetických bezpečnostních incidentů. Upřednostněné zdroje představují kombinaci praktického přístupu a teoretického rámce.

Jednotlivé monografie se zaměřují na komplexní přehled o zásadách ochrany informačních systémů, přičemž zdůrazňují, že bezpečnostní strategie musí zahrnovat nejen technologická opatření, ale i organizační a právní aspekty. Propojují digitální a fyzický svět, upozorňují na rostoucí zranitelnost systémů vůči kybernetickým hrozbám a důležitost proaktivní ochrany a monitoringu.

V souvislosti s rostoucím počtem kybernetických hrozeb se stále více diskutuje problematika kyberkriminality, ať finančních podvodů, ransomwarových útoků či zneužití umělé inteligence pro sofistikované hackerské útoky. Pomineme-li etický rámec, vyvstává otázka nutnosti systematického řízení rizik, nepřetržitého monitoringu hrozeb a odpovídajících právních rámců, které organizacím umožňují efektivně reagovat na bezpečnostní incidenty. Aktuální jsou výzvy spojené s hrozbami v digitálním prostředí, včetně sociálního inženýrství a geopolitických konfliktů.

1.1 Cyber-Physical Security

Tato kniha od Roberta M. Clarka a Simona Hakima se zaměřuje na kybernetická rizika ohrožující státní a místní infrastrukturu. Autoři analyzují zranitelnost klíčových služeb, např. zásobování vodou, dopravu, veřejnou bezpečnost nebo komunikační služby a zdůrazňují nutnost efektivních bezpečnostních opatření proti kybernetickým útokům. Publikace poukazuje na rostoucí význam informačních a komunikačních technologií (dále ICT), jejichž vzájemné propojení může v případě narušení způsobit rozsáhlé škody a další negativní

dopady. Kybernetické útoky, včetně manipulace s daty, odmítnutí služby nebo narušení provozu, představují hrozbu nejen pro organizace, ale i pro národní bezpečnost a ekonomiku. Tradičně byla pozornost věnována především kybernetickým hrozbám na vyšší úrovni, přičemž ochrana místní infrastruktury zůstávala v pozadí. Autoři upozorňují, že právě tyto úrovně správy hrají klíčovou roli v zajištění každodenních služeb pro občany, a proto by měly být lépe chráněny. Kniha obsahuje příspěvky předních odborníků v oblasti kybernetické bezpečnosti, je určena zejména pro státní a místní úředníky, ústavní činitele, akademiky a specialisty na veřejnou politiku, kteří se zabývají ochranou kritické infrastruktury. (Clark a Hakim, 2017)

1.2 Cybersecurity

Monografie reflektuje skutečnost a poukazuje na fakt, že: *„Život bez informačních a komunikačních technologií je pro naši společnost nemyslitelný, respektive nemožný.“*. Dále poskytuje komplexní přehled o problematice kybernetické bezpečnosti.

Autoři se zaměřují na aktuální hrozby v digitálním světě a nabízejí praktické rady pro ochranu před nimi. Publikace je rozdělena do několika tematických celků, které pokrývají široké spektrum oblastí kybernetické bezpečnosti, přes seznámení s různými typy kybernetických útoků, metodami jejich provádění a způsoby, jak se proti nim účinně bránit. Důraz je kladen na praktické aspekty, což z knihy činí užitečný zdroj informací pro odborníky i laiky. Autoři také diskutují o významu bezpečnostní politiky a postupech, které by měly být implementovány v organizacích pro zajištění bezpečnosti informačních systémů. Kniha obsahuje řadu příkladů z praxe, které ilustrují teoretické koncepty a poskytují čtenářům lepší pochopení dané problematiky.

Kniha slouží jako cenný průvodce pro všechny čtenáře, kteří chtějí získat hlubší informace pro porozumění kybernetické bezpečnosti a hledají praktické rady pro ochranu systémů a pochopení fungování v digitálním prostředí. (Kolouch a Bašta, 2019)

1.3 Kybernetický bezpečnostní incident 3D: IT, právo a compliance

Kniha poskytuje komplexní pohled na problematiku kybernetických incidentů z perspektivy informačních technologií, právního rámce a compliance, což chápeme jako soulad s bezpečnostními standarty. Publikace je strukturována do tří klíčových částí zahrnující:

- **technickou stránku** – kdy se věnuje různým typům kybernetických incidentů, jejich prevenci a řešení. Zároveň představuje relevantní mezinárodní normy a bezpečnostní standardy.
- **právní pohled** – rozebírá právní důsledky kybernetických incidentů včetně povinností organizací při jejich hlášení a evidenci, a to jak z pohledu soukromého, tak veřejného práva.
- **compliance** – přibližuje strategie pro vytvoření efektivního IRT (incident response týmu) a začlenění řízení kybernetických incidentů do širšího rámce organizace. Kniha je zaměřena na praktické využití a nabízí konkrétní doporučení a osvědčené postupy, které mohou pomoci při prevenci a řešení bezpečnostních incidentů. Nalezneme zde cenné informace a praktické rady pro efektivní prevenci a řešení kybernetických bezpečnostních incidentů v organizacích různého typu. (Nonnemann, Červený a Vitek, 2022)

1.4 Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru

Monografie se věnuje aktuálním výzvám v oblasti kybernetické bezpečnosti. Navazuje na předchozí titul "*Problematika ISMS v manažerské informatice*" a rozšiřuje jeho obsah o nové poznatky týkající se ochrany digitálního prostoru. Hlavním cílem publikace je poukázat na rostoucí význam kybernetické bezpečnosti a přiblížit její různé aspekty, které ovlivňují odbornou i širší veřejnost. Kniha je určena IT manažerům, správčům sítí a dalším odborníkům působícím v oblasti informačních a komunikačních technologií.

Autoři zasazují pojem kybernetické bezpečnosti do širších souvislostí a zkoumají jej z pohledu současných řešení bezpečnosti v kyberprostoru a vývoje nových technologií, včetně systémové integrace kybernetické bezpečnosti. (Sedlák a Konečný, 2021)

1.5 Cybercrime and Cybersecurity

Kniha představuje komplexní úvod do problematiky kriminality v kybernetickém prostoru a kybernetické bezpečnosti. Je koncipována tak, aby byla srozumitelná nejen pro studenty a začátečníky v oboru, ale také pro zkušené odborníky, kteří chtějí získat hlubší vhled do bezpečnostních strategií a opatření.

Publikace se zaměřuje na běžné kybernetické hrozby a zásady řízení rizik v této oblasti. Rozebírá tři klíčové pilíře kybernetické bezpečnosti: lidi, procesy a technologie. Věnuje se roli lidského faktoru, včetně náboru specialistů, psychologického aspektu bezpečnosti, školení a osvěty. Dále se soustředí na význam bezpečnostních procesů, jako jsou strategie, řízení, zásady a fyzická ochrana systémů. V poslední části kniha analyzuje technologické aspekty, mezi něž patří zabezpečení systémů, správa identit, autentizace, řízení přístupu a kryptografie. Autor knihy Dr. Paul A. Watters je uznávaný odborník v oblasti kyberkriminality a kybernetické bezpečnosti s více než dvacetiletou praxí v akademické sféře i v konzultacích pro státní a soukromé instituce. Publikace představuje důležitý zdroj informací pro všechny, kteří se zajímají o kybernetickou bezpečnost, a poskytuje komplexní pohled na klíčové koncepty, teorie a osvědčené postupy v této oblasti. (Watters, 2023)

2 ZÁKLADNÍ POJMY

Úvodem této kapitoly budou používány následující klíčové termíny a pojmy. V závorce jsou uvedeny jejich anglické ekvivalent

- **Kybernetický bezpečnostní incident (Cyber Security Incident)** je chápán jako neočekávaná, nenadálá událost nebo série událostí, která může vést k ohrožení nebo narušení informačního systému, sítě, služby nebo IT infrastruktury. Pojem označuje rozpoznaný výskyt stavu systému, služby nebo sítě, který může signalizovat porušení bezpečnostních zásad, selhání ochranných opatření, popř. událost s potenciálně vážnými důsledky pro bezpečnost (Jirásek, Novák a Požár, 2022).

S touto událostí je neoddělitelně spjata podrobné šetření a analýza nastalé situace, označovaná jako **reakce na incident**.

- **Systém řízení incidentů bezpečnosti informací (Information Security Incident Management System)** je soubor procesů, postupů a technologických opatření, které organizace využívá k detekci, analýze, reakci, řešení a prevenci bezpečnostních incidentů. Je úzce spjatý s normami **ISO/IEC 27001** a **ISO/IEC 27035**.
- **Systém řízení bezpečnosti informací ISO/IEC 27001 (zkratka ISMS - Information Security Management System)** – je přístup ke správě a neustálému zlepšování ochrany informací v organizaci s cílem naplnit její strategické záměry. Řadu norem ISO/IEC 2700X lze vnímat jako „metodický rámec“ pro řízení bezpečnosti informačních aktiv. (ČSN ISO/IEC 27000, 2017)
- **ISO/IEC 27035 – Řízení bezpečnostních incidentů (Information security incident management)** se na rozdíl od ISO/IEC 27001 zaměřuje na reaktivní přístup k informační bezpečnosti a poskytuje postupy pro detekci, hlášení, analýzu a reakci na bezpečnostní incidenty, včetně jejich následného vyhodnocení a poučení se z nich. Hlavním cílem je minimalizace dopadů kybernetických hrozeb prostřednictvím konkrétních postupů pro detekci, hlášení, analýzu a reakci na ně. Poskytuje organizacím možnost rychle a efektivně reagovat na kybernetické incidenty (ISO/IEC 27035, 2023).
- **Hrozba (Threat)** jedná se o jakoukoli hrozbu, příčinu nežádoucího incidentu nebo události, která může nepříznivě ovlivnit aktiva, tj. cíleně mění stav systému,

konzistenci dat nebo počítačové sítě. Důsledkem takového útoku může být úprava zpráv, vkládání falešných informací, vydávání se za jiného uživatele nebo odmítnutí poskytované služby. Jeden z autorů rozděluje hrozby podle jejich původu na **objektivní**, které zahrnují technické a přírodní vlivy, popř. vyšší moc a **subjektivní**, jejichž původcem je člověk – a mohou být úmyslné nebo neúmyslné. Riziko tak představují oba typy hrozeb (Jirásek, Novák a Požár, 2022).

- **Zranitelnost (Vulnerability)** označuje slabiny, kterou mohou potenciální hrozby využít (ČSN ISO/IEC 27000, 2017).
- **Riziko (Risk)** v oblasti informační bezpečnosti označuje pravděpodobnost, že hrozby zneužijí zranitelnosti informačního aktiva, což může vést ke škodám. Riziko je určeno kombinací pravděpodobnosti vzniku takové události a závažnosti jejích dopadů (ČSN ISO/IEC 27000, 2017).
- **Detekce incidentu (Incident detection)** je proces identifikace a reakce možného bezpečnostního incidentu prostřednictvím monitorovacích systémů, uživatelských hlášení nebo jiných bezpečnostních mechanismů. Je uzákoněna a je součástí několika norem a předpisů (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a Vyhláška o kybernetické bezpečnosti (č. 82/2018 Sb.)).
- **Reakce na incident (Incident Response)** je souhrn opatření, která organizace přijímá k minimalizaci dopadu incidentu, zastavení jeho šíření a obnovení normálního stavu. Odezva zahrnuje identifikaci, izolaci, analýzu a eliminaci hrozby. Organizace mají jasně definované povinnosti a postupy pro odezvu na různé typy incidentů, což pomáhá zlepšovat bezpečnost a ochranu v různých oblastech (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti).
- **Evidence a hlášení incidentů (Incident Recording and Reporting)** je systematická dokumentace bezpečnostních incidentů, včetně detailního popisu, časového průběhu, přijatých opatření a výsledků vyšetřování. Hlášení incidentů umožňuje organizaci učit se z minulých událostí a zlepšovat bezpečnostní opatření (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, European Parliament and Council, 2022 a ISO/IEC 27035, 2023).
- **Obnova po incidentu (Incident Recovery)** soubor opatření k obnovení systémů a služeb po bezpečnostním incidentu. Cílem je zajistit návrat k běžnému provozu

s co nejmenším dopadem na organizaci (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti).

- **Plán obnovy po havárii (Disaster Recovery Plan)** představuje soubor postupů a opatření, jejichž cílem je co nejrychlejší obnova klíčových prvků informačních systémů po výpadku způsobeném bezpečnostním incidentem nebo jinou krizovou událostí. Zaměřuje se na technickou obnovu IT infrastruktury (Gregory, 2022).
- **Plán kontinuity činností (Business Continuity Plan)** je dokument obsahující soubor opatření a scénářů, které umožňují organizaci pokračovat v provozu i během krizových situací. Zaměřuje se na zajištění fungování klíčových procesů a služeb nejen v oblasti IT, ale také v personálních, organizačních nebo provozních oblastech (Watters, 2023).
- **Aktivum (Asset)** lze chápat jako jakýkoli prvek, který má pro správní orgán určitou hodnotu. Tato aktiva mohou mít různou podobu – zahrnují například technické vybavení, poskytované služby nebo samotnou reputaci organizace. Mezi aktiva se řadí také zaměstnanci, kteří tvoří personální základ dané organizace. V rámci této práce jsou klíčová především aktiva související s informačními technologiemi, které představují prostředky umožňující organizaci plnit její úkoly (Jirásek, Novák a Požár, 2022).
- **Kybernetická bezpečnost (Cyber security)** je stav ochrany informačních systémů před narušením bezpečnostních pravidel, obecně uznávaných bezpečnostních zásad a standardů. Zahrnuje soubor postupů a opatření zaměřených na eliminaci rizik, zajištění integrity, důvěrnosti a dostupnosti dat (tzv. CIA triáda).

Je definována jako „soubor právních, organizačních, technických a vzdělávacích opatření zaměřených na ochranu kybernetického prostoru.“. V kontextu této práce je kybernetická bezpečnost vnímána jako specifická oblast informační bezpečnosti, která se zaměřuje na ochranu digitálního prostředí a technologií (Požár, 2005).

- **Informační bezpečnost (Information security)** zahrnuje ochranu informací, informačních systémů před neoprávněným přístupem, zneužitím, změnou nebo zničením. Jinými slovy ji lze chápat jako vlastnost objektu nebo organizace, která stanovuje úroveň ochrany před potenciálními hrozbami a jejich následky (Jirásek, Novák a Požár, 2022).

- **Důvěrnost (Confidentiality)** znamená, že informace jsou dostupné pouze oprávněným osobám (jednotlivcům, skupinám, procesům nebo entitám).
- **Integrita (Integrity)** zajišťuje správnost, úplnost a ochranu dat a metod jejich zpracování.
- **Dostupnost (Availability)** umožňuje autorizovaným uživatelům přístup k informacím.
- **Událost (Event)** označuje identifikovatelný jev v digitálním prostředí. Mezi typické příklady patří uživatelské přihlášení, připojení uživatele ke sdílení souborů, požadavek serveru na načtení webové stránky, odeslání e-mailu nebo zásah firewallu při blokování nežádoucího připojení (ČSN ISO/IEC 27000, 2017).
- **Výstraha (Alert)** je obvykle generována z aktiv detekce hrozeb nebo postupů jejich vyhledávání. Výstrahy mohou být důsledkem negativního jevu a obvykle vyžadují následnou analýzu a reakci. Mezi typické příklady patří selhání systému, zneužití administrátorských práv nebo neoprávněný přístup k citlivým informacím, spuštění škodlivého kódu nebo úmyslné zničení dat (ČSN ISO/IEC 27000, 2017).
- **Opatření (Control)** představuje proces, nástroj nebo zavedený postup, který upravuje nebo snižuje riziko (Ibidem).

2.1 Moderní hrozby pro kybernetickou a informační bezpečnost

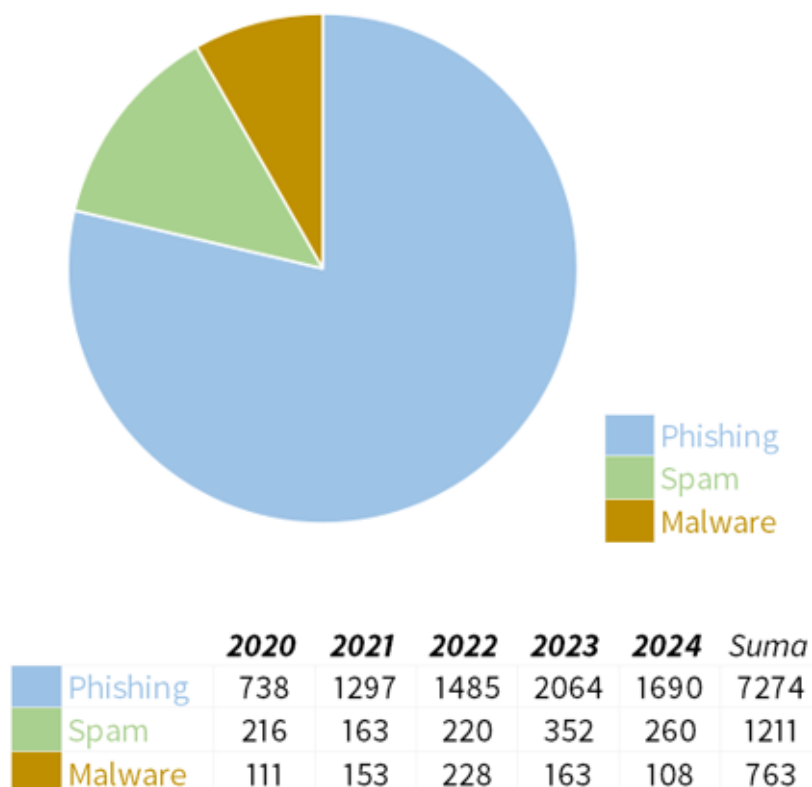
Snahou útočníků je získat přístup k datům organizace nebo společnosti, vyřazení systémů apod. S rostoucím vlivem a využitím umělé inteligence ve všech oblastech lidské činnosti, nevylučuje kybernetickou kriminalitu, se objevují nové hrozby a způsoby zneužití této technologie. Na jedné straně přináší AI v oblasti kybernetické bezpečnosti řadu výhod, ale zaznamenáváme také možná rizika, např. provádění sofistikovaných útoků.

Dalším faktorem, který významně ovlivňuje kybernetickou bezpečnost, je sám člověk. Pomineme-li, že ztrátou kritického myšlení usnadňuje útočníkům jejich činnost, můžeme se zaměřit na konkrétní typy incidentů, jako jsou:

- Phishing.
- Spam.
- Malware.

- Útok typu MiTM.
- Hrozba zevnitř.

V následující tabulce (obr. 1) jsou uvedeny tři nejčastější typy incidentů zaznamenaných ve statistikách za období let 2020 až 2024, a to včetně grafického znázornění vybraných typů incidentů (otevřené a zavřené) za uvedené období.



Obrázek 1 Statistika řešených incidentů z let 2020 až 2024
(zdroj: CSIRT.cz, 2024)

2.1.1 Phishing

Je formou sociálního inženýrství a psychologické manipulace, při níž se útočník prostřednictvím e-mailu, textové zprávy nebo telefonátu vydává za důvěryhodnou osobu či organizaci se záměrem vyvolat strach nebo pocit naléhavosti a tím donutit uživatele k okamžité reakci. Klasický phishing bývá rozesílán masově v naději, že osloví aspoň jednu potenciální oběť, zatímco pokročilejší verze, tzv. cílený (spear) phishing, je zaměřen na konkrétní osobu nebo organizaci. Útočník předem provádí detailní průzkum, aby zpráva působila důvěryhodně a byla přizpůsobena konkrétní oběti (Microsoft, 2025).

V této oblasti může AI analyzovat obrovské množství osobních dat a vytvářet cílené útoky, např. generovat podvodné e-maily, napodobovat hlasy a reportážní videa (deepfake). Dle statistiky ze sledovaného období se jedná o nejčastější hlášenou formu incidentu (CSIRT.cz, 2024).

2.1.2 Spam

Tento termín se používá pro nevyžádané zprávy a podle statistik z období let 2020 až 2024 se řadí mezi nejčastěji hlášené incidenty. A i když se definice tohoto pojmu často rozcházejí, pomáhají popsat podstatu spamu – tedy masové rozesílání nevyžádaných zpráv, často s reklamním nebo škodlivým obsahem. Pro zajímavost lze uvést, že tento pojem byl zmíněn v pořadu Monty Python, kde byla konzerva téhož jména neustále opakována v písni, což symbolizovalo nevyhnutelnost a otravnost – ostatně podobně jako nevyžádané zprávy.

2.1.3 Malware

Nezkráceně malicious software, je jakýkoliv škodlivý software, který je navržen za účelem páčání škod. Mezi nejběžnější typy malwaru patří viry, červi, trojské koně, spyware, adware, ransomware. Moderním způsobem je zneužití AI – může generovat sofistikované malware útoky, které se přizpůsobují bezpečnostním opatřením, např. Emotet, který využívá strojové učení a své oběti si cíleně vybírá. Současně efektivně obchází sledovací systémy, jako jsou botnet a honeypot (Cisco Systems, Inc., 2025).

2.1.4 Útok typu MiTM

Útok typu Man-in-the-Middle (MiTM) nastává, když se útočník tajně vloží do komunikace mezi dvěma stranami, přičemž odposlouchává, mění nebo přesměrovává přenášené informace, aniž by si to účastníci uvědomili. Tento druh útoku je často využíván k získání přihlašovacích údajů, dešifrování důvěrných informací nebo manipulaci s obsahem komunikace (Kolouch a Bašta, 2019).

I u tohoto typu útoku lze využít AI, ať už pro analýzu síťového provozu, generování certifikátů, kombinací s malware pro snazší přizpůsobení se bezpečnostním opatřením v reálném čase apod. (Watters, 2023).

2.1.5 Hrozba zevnitř

Přestože většinu kybernetických útoků mají na svědomí osoby mimo organizaci, je nezbytné, aby bezpečnostní týmy věnovaly pozornost také vnitřním hrozbám. Zaměstnanci či jiné

osoby s oprávněným přístupem k chráněným zdrojům mohou být příčinou úniku citlivých informací, a to buď neúmyslně, například kvůli nedbalosti, nebo záměrně, s úmyslem poškodit organizaci (Microsoft, 2025).

2.2 Jak se bránit kybernetickým útokům s využitím umělé inteligence?

Protikladem využití umělé inteligence (dále AI) k ochraně kybernetických systémů se jeví behaviorální analýza uživatelů a entit (UEBA), která využívá strojového učení k odhalování bezpečnostních hrozeb. Může detekovat neobvyklé chování, například pokusy o přihlášení z nových lokací nebo jiných aktivit, které se odchylují od běžného chování uživatelů či systémů. (Visitech a.s., 2024).

2.2.1 Zákonné normy a regulace

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále ZoKB) v současné době explicitně neřeší kybernetické útoky s využitím umělé inteligence. Nicméně se dá předpokládat, že s rostoucím významem AI je pravděpodobné, že budoucí novelizace tohoto zákona bude hrozby a technologie spojené s AI zohledňovat.

Na evropské úrovni byl Evropským parlamentem schválen „Akt o umělé inteligenci“ (angl. „AI Act“), což je první nařízení týkající se regulace umělé inteligence a omezení rizik s ní spojených. Jedním z hlavních bodů „Aktu o AI“ je stanovení odpovědnosti za bezpečnostní incidenty a také prevence nebezpečného použití AI. To může vyústit v zavedení přísnějších postupů pro reakci na incidenty a nutnost implementace pokročilých mechanismů pro detekci a eliminaci kybernetických hrozeb. Ačkoli jde o významný historický milník, je nutné si uvědomit, že jeho důsledky budou patrné až časem (Miloslav Lujka, 2024).

2.2.2 Směrnice NIS2

Network and Information Security 2 (dále NIS2) nahrazuje směrnici NIS vydanou roku 2016. Jejím hlavním cílem je posílení kybernetické bezpečnosti organizací a firem v rámci Evropské unie, jejichž činnost by v případě kybernetického útoku mohla ovlivnit životy a zdraví občanů.

Směrnice NIS2 se vztahuje na klíčové organizace působících v oblasti energetiky, zdravotnictví, dopravy, v bankovním sektoru a dalších odvětvích. Směrnice stanoví povinnosti v oblasti kybernetické bezpečnosti, systém hlášení incidentů Národnímu úřadu

pro kybernetickou a informační bezpečnost (dále NÚKIB), testování odolnosti proti průnikům, plány pro řízení rizik, reakce na incidenty apod. (Gordic, 2025)

Výše uvedená normativa představují zákonný a regulační rámec pro bezpečné a odpovědné nasazení technologií umělé inteligence do více oblastí, kybernetickou bezpečnost nevyjímaje. Tyto předpisy vymezují povinnosti organizací v oblasti prevence, detekce a zvládání bezpečnostních incidentů.

Z hlediska využití AI vůči kybernetickým útokům se jedná o moderní nástroje, které umožňují včasnou detekci hrozeb a rychlou reakci na vzniklé incidenty (AI-driven response). Reakce řízená umělou inteligencí přináší zkrácení doby reakce na incident a zvyšuje odolnost systémů vůči kybernetickým útokům. Může zahrnovat automatickou detekci hrozeb, klasifikaci incidentů, návrh vhodné reakce a adaptivní funkce založené na strojovém učení.

3 REAKCE NA INCIDENTY

Z pohledu kybernetické bezpečnosti představuje klíčovou součástí systému řízení incidentů bezpečnosti informací. Cílem této fáze je minimalizovat dopady incidentu, obnovit běžný provoz a zabránit jeho opakování. Efektivní reakce vyžaduje jasně definované postupy, stanovení odpovědnosti a připravenost týmů. V kontextu narůstající složitosti hrozeb hraje stále významnější roli také automatizace a využití prvků AI.

Tato kapitola se zaměřuje na plán reakce na incidenty, principy a metodiky, které se uplatňují při řízení kybernetických bezpečnostních incidentů.

3.1 Plán reakce na incidenty

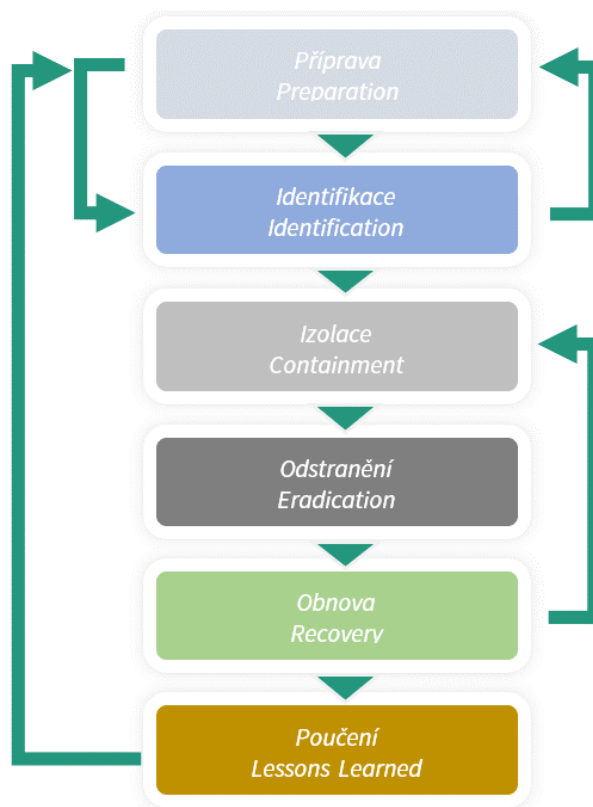
Směrnice NIS2 a stále rostoucí počet kybernetických útoků přináší pro organizace a firmy nové požadavky v oblasti řízení kybernetické bezpečnosti. Tím je povinnost vytvořit plán reakce na incidenty (IRP – Incident Response Plan), který bude klíčový pro řízení a reakci na ně. Bude sloužit pro ochranu dat a zachování kontinuity organizace (implementace IRP např. s využitím implementační smyčky, obr. 2). Hlavním cílem takového plánu je snížení rizik/dopadu na organizaci a následně obnova informačních aktiv, v co nejkratším časovém úseku. Pro sestavení plánu reakce na incidenty využívá např. model PICERL (obr. 3) sloužící jako vodítko pro sestavení jednotlivých fází (reakce na incident).



Obrázek 2 IRP – Schéma OODA a „Incident Response Plan“ (zdroj: EC Council, 2024)

Systematický přístup k řízení bezpečnostních incidentů a kontinuity činností v organizacích usnadňující řízení incidentů (obr. 3).

Model je široce využíván v oblasti řízení informační bezpečnosti a krizového řízení, protože poskytuje strukturovaný rámec pro efektivní reakci na incidenty a jejich následnou analýzu, s důrazem na poučení se z této události a následným posilováním odolnosti vůči budoucím bezpečnostním hrozbám (NCI, 2024).



Obrázek 3 Přístup k řízení incidentů, model PICERL (zdroj: NCI, 2024)

Vysvětlení jednotlivých položek modelu PICERL je následující:

- **Příprava (Preparation)** zahrnuje preventivní opatření a připravuje organizaci na potencionální kybernetické incidenty. V tomto kontextu se jedná např. o školení, zavádění bezpečnostních opatření, zpracování reakčních plánů.
- **Identifikace (Identification)** zjištění a následné potvrzení bezpečnostního incidentu na základě monitorování a analýzy dat.
- **Izolace (Containment)** nebo také zabránění šíření (v kontextu kybernetické bezpečnosti označuje opatření ke zmírnění dopadu incidentu na aktiva a zabránění dalšího šíření).

- **Odstranění (Eradication)** zahrnuje proces eliminace (odkazuje na úplné odstranění hrozby, například škodlivého kódu nebo kompromitovaných součástí systému).
- **Obnova (Recovery)** stav, kdy dochází k obnovení systémů a služeb do původního stavu a zajištění jejich bezpečnosti.
- **Poučení se (Lessons Learned)** je analýza průběhu incidentu, vyhodnocení účinnosti reakce na incident a zavedení preventivních opatření.

3.1.1 Řízení rizik

Postup řízení rizik chrání informační aktiva kontrolními mechanismy a procesy před porušením bezpečnostní politiky organizace, stanovením pravidel pro přijatelné používání. Zodpovědnost za implementaci těchto opatření v souladu s klíčovými funkcemi řízení rizik ponese osoba/tým odpovědn-á/ý za definování strategií řízení rizik. Proces zahrnuje klíčové fáze (ČSN ISO/IEC 27000, 2017 a COBIT, 2019):

- **Identifikace** – analýza dopadů a rizik, kterým organizace čelí a na které se zaměřuje, tj. důležité procesy a hodnocení možných dopadů při jejich přerušení;
- **Ochrana** s cílem stanovení opatření, které minimalizují riziko kybernetických incidentů a chrání systémy, data a služby organizací;
- **Detekce** rozpoznání anomálií a bezpečnostních událostí, které organizacím napomáhají rychle reagovat na hrozby a minimalizovat jejich dopady;
- **Reakce** zajišťuje prevenci a efektivní reakci na kybernetické bezpečnostní incidenty, minimalizovat jejich dopad a obnovit běžný provoz organizace;
- **Obnova** zajišťuje rychlé řešení bezpečnostních incidentů a návrat k normálnímu provozu.

3.1.2 Kontrolní mechanismy kybernetické bezpečnosti

Jsou stanoveny pravidelným prověřováním efektivitu těchto mechanismů. Slouží k detekci a prevenci incidentů, pro zajištění jejich připravenosti. Odpovědnost za řešení případných chyb, výpadků nebo snížení výkonnosti IT prostředků a bezpečnostních opatření nese CSIRT (Computer Security Incident Response Team), který zpracovává zprávy o stavu připravenosti těchto prostředků a výsledky kontrol. CSIRT dále poskytuje doporučení pro zlepšení bezpečnostních opatření a prevenci budoucích incidentů. Tyto zprávy

se zpravidla uchovávají po dobu nejméně jednoho roku. Další významnou roli plní pracovníci odpovědní za informační bezpečnost ISO (Information Security Officer), ať už jde o jednotlivce nebo tým, jedná se o osoby, které jsou odpovědné za realizaci a účinnost Plánu reakce na incidenty (IRP) (Nonnemann, Červený a Vitek, 2023).

3.1.3 Hodnocení závažnosti

Hodnocení závažnosti kybernetických incidentů je klíčovým procesem, který umožňuje organizacím efektivně řídit a stanovovat priority pro reakci na bezpečnostní hrozby. Tento proces zahrnuje analýzu rozsahu dopadu na systémy a data, povahy útoku, pravděpodobnosti zneužití a celkového rizika pro organizaci. Závažnost incidentu se často hodnotí na základě předem definovaných kritérií – důvěrnost, integrita a dostupnost (CIA triáda), a používají se stupnice od nízké po kritickou úroveň ohrožení. (Nonnemann, Červený a Vitek, 2023).

3.1.4 Úroveň hodnocení závažnosti

Slouží ke stanovení potřebného rozsahu opatření a určuje priority při přidělování zdrojů pro řešení a zvládnutí incidentu. Role jednotlivých týmů – CSIRT má odpovědnost za provedení úvodního vyhodnocení závažnosti bezpečnostního incidentu, tedy stanovení jeho klasifikace. Poté pracovník odpovědný za informační bezpečnost (ISO) posuzuje toto hodnocení a potvrzuje jeho správnost, případně jej v dle potřeby upravuje. ISO je povinen detailně přezkoumat a definitivně schválit všechna hodnocení incidentů, jejichž úroveň závažnosti dosahuje nebo přesahuje kategorii „Vysoká“, aby byla zajištěna adekvátní reakce při řešení incidentu (Nonnemann, Červený a Vitek, 2023).

3.1.5 Taktika, technika a postupy

Týmy CSIRT a ISO budou disponovat kvalifikovanými specialisty na informační bezpečnost a využívat vhodné kybernetické nástroje a bezpečnostní opatření, která umožní efektivně čelit a předcházet specifickým taktikám, technikám a metodám útočníků. K tomu využívají MITRE ATT&CK Framework, což je rozsáhlá znalostní databáze popisující taktiky, techniky a postupy (TTPs – tactics, techniques, and procedures), které útočníci využívají během kybernetických útoků. Slouží k pochopení chování útočníků, pomáhají s detekcí hrozeb a zlepšováním obranných mechanismů v kybernetické bezpečnosti (Nonnemann, Červený a Vitek, 2023).

3.1.6 Záznamy o událostech (uchování logů)

Tým ISO bude odpovídat za to, že záznamy o událostech (log data) získávané z jednotlivých aktiv budou bezpečně uchovány, chráněny a spravovány po dobu jednoho roku. Tato činnost napomáhá k efektivní analýze bezpečnostních incidentů, umožňuje dohledání příčin a rozsahu narušení, zajišťuje soulad s regulatorními a právními požadavky v této oblasti. S tím souvisí i následující kapitola, která se věnuje reakcím na výstrahy a vyhledávání hrozeb. CSIRT reaguje na výstrahy, pravidelně analyzuje stav sítě, identifikuje bezpečnostní hrozby a systémové anomálie, přičemž tým dále provádí audit logů/dat za účelem prevence kompromitace jednotlivých aktiv (Nonnemann, Červený a Vítek, 2023).

3.1.7 Sběr a uchovávání důkazního materiálu

Tým CSIRT vytvoří elektronické úložiště důkazů, které zajistí bezpečné uchovávání důkazů získaných při řešení kybernetických incidentů. Rovněž je odpovědný za vedení deníku, ve kterém bude zaznamenávat aktivity spojené se sběrem důkazů. Dále zajistí vedení záznamů o všech přesunech těchto důkazů z úložiště autorizovaným osobám či na jiná média. Každý záznam by měl obsahovat datum, popis, odesílatele a příjemce.

ISO je pak pověřen schvalováním všech přesunů důkazních materiálů autorizovaným příjemcům nebo na jiná média. Měl by zajistit ochranu a uchování důkazů shromážděných během bezpečnostního incidentu v úložišti po dobu jednoho roku od data první detekce incidentu. Stejným způsobem odpovídá za ochranu a uchování zprávy o incidentu včetně všech souvisejících komunikačních záznamů, taktéž po dobu jednoho roku od data počáteční detekce incidentu (Nonnemann, Červený a Vítek, 2023).

3.1.8 Obnovení provozu

Jednou z klíčových činností týmu je obnova provozního stavu. Než k tomu dojde, má ISO povinnost ověřit, zda jsou aktiva postižená bezpečnostním incidentem způsobilá k obnovení do běžného provozu, a to až poté, co budou realizována nápravná opatření, která eliminují riziko další kompromitace a narušení bezpečnosti (Clark a Hakim, 2017).

3.2 Koordinace, sdílení a oznámení

Úspěšné zvládnutí bezpečnostního incidentu nekončí jeho technickým vyřešením. Nedílnou součástí celého procesu je následná koordinace, sdílení poznatků a oznamovací povinnost, která umožňují z incidentu vyvodit poučení, posílit obranné mechanismy a zajistit soulad

s legislativními požadavky. V rámci této fáze se zpracovávají závěrečné právy (Post–Mortem analýza, Incident Reports), které shrnují průběh incidentu, přijatá opatření a doporučení pro zlepšení. Efektivní komunikace mezi zúčastněnými stranami – interními týmy (koordinace mezi rolemi CSIRT a ISO), vedením organizace, případně externími subjekty (např. dozorčími orgány, partnery nebo zákazníky) – je klíčová pro transparentní a odpovědný přístup k bezpečnostnímu řízení (Nonnemann, Červený a Vítek, 2023).

3.2.1 Závěrečná zpráva

Tuto zpracuje tým CSIRT a detailně popisuje průběh a okolnosti kybernetického incidentu. Obsah zprávy je průběžně doplňován v průběhu reakce na incident. Jakékoliv další šíření podléhá schválení ze strany pracovníka odpovědného za informační bezpečnost ISO. Jeho role pak spočívá v odpovědnosti za to, že pokud to situace vyžaduje, jsou relevantní informace o incidentu včas sdíleny s oprávněnými pracovníky. Toto sdílení by mělo proběhnout bez zbytečného odkladu, pokud ISO vyhodnotí, že takový krok podpoří efektivní reakci na incident a zároveň bude v souladu s interními pravidly pro klasifikaci a ochranu dat. V případě, že dojde k bezpečnostnímu incidentu, je dále ISO povinen zajistit včasné informování všech zúčastněných – kontrolních a dozorčích orgánů, fyzických osob, zákazníků a dalších subjektů. Tato oznamovací povinnost se liší časovým rámcem dle adresáta oznámení. Zpravidla k oznámení dochází bez zbytečného odkladu nebo musí být učiněno do 72 hodin od zjištění incidentu, přičemž ISO vyhodnocuje a posuzuje následky, přínos, pravidla a právní rámec každého konkrétního případu (Nonnemann, Červený a Vítek, 2023).

Cílem této zprávy je:

- **rekapitulovat incident** – co se stalo, kdy, jak a proč;
- **zhodnotit detekci a reakci** – jak byla situace detekována a jak zvládnuta;
- **zachovat důkazy** – pro opakující se incidenty a případné právní kroky;
- **poučit se** – jak incidentu předejít v budoucnu a jak zlepšit procesy.

3.2.2 Struktura závěrečné zprávy

Zpráva typu Post–Mortem (nebo také Incident Report) představuje důležitý výstup po zvládnutí kybernetického bezpečnostního incidentu. Jejím hlavním cílem je zpětná analýza, co se stalo, jakým způsobem byl incident detekován a řešen, jaké byly jeho příčiny.

Dále zohledňujeme dopady a jaká opatření byla přijata pro minimalizaci budoucích incidentů. Taková zpráva umožňuje nejen lepší pochopení celého incidentu, ale zejména systematické zlepšování procesů bezpečnosti celé organizace (Nonnemann, Červený a Vítek, 2023).

Součástí zprávy bývá uvedena časová osa událostí (timeline), technická analýza, zapojené týmy, přehled přijatých nápravných opatření a preventivních doporučení. Je také nástrojem pro sdílení zkušeností v rámci organizace a zajištění souladu s regulačními požadavky. Kvalitně zpracovaná zpráva je klíčovým krokem v budování odolnosti a zralosti bezpečnostního řízení (Watters, 2023).

Zpráva typu Post–Mortem (nebo Incident Report) by měla obsahovat (Nonnemann, Červený a Vítek, 2023), př.:

1. **Základní informace o incidentu** (Název incidentu, datum a čas detekce, datum a čas vyřešení, zodpovědné týmy, jedinečný identifikátor incidentu);
2. **Popis incidentu** (Co se stalo, stručné shrnutí incidentu – včetně typu útoku, kdy a kde k němu došlo, specifikace času, postižených systémů, aktiv nebo uživatelů, jak byl incident detekován);
3. **Dopad incidentu** (Technické, obchodní dopady a právní a důsledky);
4. **Kořenová příčina** (Root Cause Analysis – RCA) (Jak k incidentu došlo, míra lidského nebo technického zavinění, zda incident odhalil slabinu v řízení bezpečnosti nebo kontrole);
5. **Průběh řešení incidentu** (Časová osa událostí a přijatá opatření);
6. **Důkazní materiál** (Kde jsou uchovány logy další důkazy, opatření na zajištění integrity důkazů, přenos a schválení (kdo, kdy, jak));
7. **Zpráva pro vedení / externí oznámení** (Zda a komu byl incident oznámen (NÚKIB, partneři, zákazníci), shrnutí pro vedení organizace);
8. **Poučení a doporučená opatření** (Co bylo zjištěno – pozitivní i negativní poznatky, jakým způsobem lze incidentům tohoto typu v budoucnu předejít a nápravná a preventivní opatření);
9. **Zodpovědné osoby** (Člen/ové týmu, externí partneři);

10. Přílohy (Logy, časové osy, síťová schémata, forenzní výstupy, záznamy komunikace apod.).

4 POSTUPY ZAJIŠTĚNÍ INFORMAČNÍ BEZPEČNOSTI

Doporučené postupy k zajištění informační bezpečnosti zahrnují soubor technických, organizačních a procesních opatření, jejichž cílem je ochrana důvěrnosti, integrity a dostupnosti informací. Klíčovými prvky je zavedení systému řízení informační bezpečnosti (např. dle ISO/IEC 27001), řízení přístupových práv, šifrování dat, pravidelné zálohování a monitorování systémů. Tento rámec umožňuje pravidelně hodnotit rizika, definovat bezpečnostní cíle a zavádět odpovídající kontroly včetně přesné dokumentace a odpovědností. Nedílnou součástí je také ochrana aktiv – ať už fyzických (např. serveroven) nebo technických (systémů a dat) prostřednictvím řízení přístupů, šifrování a zálohování (ČSN ISO/IEC 27001, 2017).

Nedílnou součástí je včasná detekce a reakce na incidenty prostřednictvím specializovaných týmů, zpracování analýz, vzdělávání zaměstnanců a splnění právních požadavků (např. zákona o zpracování osobních údajů (GDPR) nebo zákona o kybernetické bezpečnosti). Celý proces by měl být kontinuálně vyhodnocován a přizpůsobován aktuálním hrozbám a vývoji technologií (Kolouch a Bašta, 2019).

4.1 Komplexní přístup k informační bezpečnosti a řízení kybernetických rizik

Efektivní bezpečnostní strategie vyžaduje kontinuální monitorování a detekci hrozeb pomocí specializovaných technických prostředků a nástrojů usnadňující detekci (firewall, antivirus atd.), forenzní analýzu (záznamy – logy, paměťové výpisy, síťový provoz) a jejich následný a pravidelný audit. V případě incidentu je nezbytné mít připravený Plán reakce na incidenty (IRP), definované role odpovědných osob a schopnost zpracovat analýzu vedoucí k nápravným opatřením. Klíčovou roli hraje také vzdělávání zaměstnanců formou pravidelných školení a simulací kybernetických útoků (Nonnemann, Červený a Vitek, 2023).

Nezbytné opatření pro ochranu aktiv zahrnují:

- implementace bezpečnostních opatření v organizaci;
- klíčové prvky účinné strategie informační bezpečnosti;
- integrace technických, organizačních a právních aspektů kybernetické ochrany;
- proaktivní bezpečnostní přístup a role odpovědných subjektů.

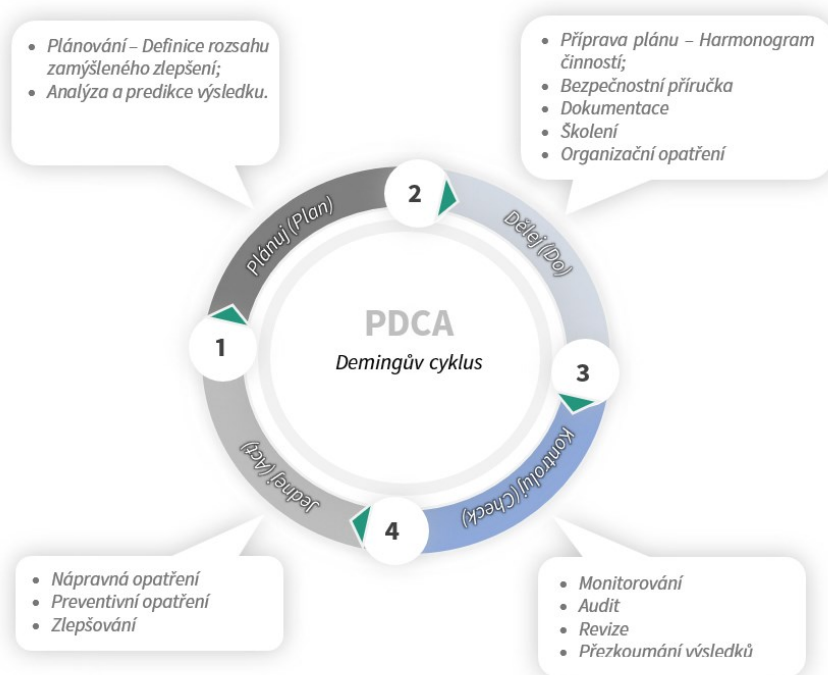
Implementace bezpečnostních opatření v organizaci – zahrnuje striktní opatření, která jsou zavedená a platná pro každého zaměstnance, kdy má přístup pouze k systémům a datům, které potřebuje ke své práci, a to na základě principu nejmenších oprávnění. Až do narušení systému zůstávají opatření zpravidla neměnná.

Klíčové prvky účinné strategie informační bezpečnosti – jsou jasně ohraničeny, s řízeným Plánem reakce na incidenty (IRP), definováním role a odpovědnosti týmu (CSIRT, CERT, ISO), pravidelné hodnocení rizik, postupy při detekci a řešení incidentu, způsob vedení dokumentace apod.

Integrace technických, organizačních a právních aspektů kybernetické ochrany – je dána spoluprací interních oddělení při nastavování bezpečnostních opatření a posuzování jejich dopadů s ohledem na soulad s legislativou při zavádění bezpečnostních opatření a technologií.

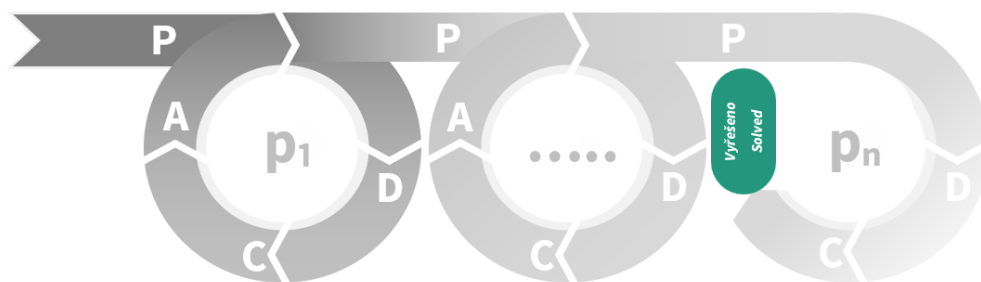
Proaktivní bezpečnostní přístup a role odpovědných subjektů – aktivní vyhledávání příznaků možného napadení, přestože nedošlo k žádné výstraze a pravidelné revidování bezpečnostní politiky a hodnocení nových rizik.

Základní rámec pro zlepšování informační bezpečnosti, který je zároveň součástí několika norem je úzce provázán s principy modelu PDCA (Plan–Do–Check–Act), známého jako Demingův model (obr. 4).



Obrázek 4 Demingův cyklus PDCA (zdroj: Techportal.cz, 2012)

Tento model identifikuje informační aktiva, hrozby a zranitelnost. Po provedení analýzy rizik organizace připravuje plán nebo harmonogram činností stanovených pro řízení rizik. Poté probíhá monitorování bezpečnostních opatření a revidování účinnosti implementovaných opatření. Posledním krokem je reakce na zjištěné nedostatky a aktualizace opatření. Tento cyklus je iterativní, tedy opakovaný od p_1 p_n dokud není dosaženo požadovaného výsledku (obr. 5).



Obrázek 5 Opakovaný cyklus PDCA (zdroj: *Praxisframework.org*, 2023)

4.2 Přístup a vztahy k externím subjektům při řízení kybernetických hrozeb

Organizace by měla ve vztahu s externími subjekty – prověřovat důvěryhodnost partnerů, smluvně definovat bezpečnostní požadavky a sdílet s nimi informace. V neposlední řadě dbá na plnění právních povinností, zejména v rámci GDPR, zákona o kybernetické bezpečnosti a souvisejících vyhlášek, přičemž důležitou roli hrají osoby odpovědné za bezpečnost a ochranu osobních údajů (Sedlák a Konečný, 2021).

Každá organizace má zavedené opatření a stanovené priority pro snížení rizik, což je klíčovým krokem v rámci řízení informační bezpečnosti. Tímto způsobem dochází k efektivnímu přidělování zdrojů s cílem zaměřit se na nejzásadnější hrozby – určit, která rizika vyžadují okamžitou reakci, která je možné akceptovat a které lze řešit v delším časovém horizontu. Tento proces vychází z analýzy rizik, při níž se posuzuje pravděpodobnost výskytu hrozby a závažnost jejího dopadu na organizaci. Rizika jsou pak rozdělena dle úrovně (př. nízká, střední, vysoká, kritická) a na jejich základě jsou pak stanoveny priority. Při určování priorit je důležité zohlednit technické a další aspekty (právní, ekonomické, provozní apod.). Do rozhodovacího procesu jsou kromě specialistů na IT a kybernetickou bezpečnost zapojeni také zástupci organizace (vedení, právní oddělení apod.), pro stanovení opatření a jejich soulad se strategickými cíli organizace. Tato se podle stanovených priorit nejdříve snaží o mitigaci rizik s nejvyšší

prioritou (kritická, vysoká) a poté řeší střední a nízká rizika (tab. 1). Tento systematický přístup pomáhá efektivně alokovat zdroje a zaměřit se na oblasti s nejvyšším bezpečnostním významem (Nonnemann, Červený a Vítek, 2023).

Tabulka 1 Stanovení priorit mitigace rizik řízení bezpečnostních incidentů

<i>Riziko / Incident</i>	<i>Pravděpodobnost výskytu</i>	<i>Dopad na organizaci</i>	<i>Úroveň rizika</i>	<i>Doporučená opatření</i>	<i>Priorita řešení</i>	<i>Zodpovědná osoba / tým</i>
Neoprávněný přístup k citlivým datům	Vysoká	Kritický	Kritické	Zavést vícefaktorovou autentizaci, audit přístupů	Okamžitá	ISO / IT
Ransomwarový útok, server	Střední	Vysoký	Vysoké	Pravidelné zálohování, školení zaměstnanců, AV ochrana	Vysoká	CSIRT / IT
Phishingový útok, e-mail	Vysoká	Střední	Vysoké	Osvěta uživatelů, antispamová filtrace, simulace útoků	Vysoká	Bezpečnostní tým
Dočasný výpadek webové služby	Střední	Nízký	Střední	Monitoring dostupnosti, plán obnovy	Střední	Správce IT
Ztráta mobilního zař.	Nízká	Střední	Střední	Šifrování zařízení, možnost vzdál. vymazání dat	Střední	Uživatel / IT
Nesprávná konfigurace systému	Střední	Střední	Střední	Pravidelné bezpečnostní audity	Střední	IT oddělení
Zastaralý software (bez aktualizace)	Nízká	Vysoký	Střední	Aktualizace systému, patche	Vysoká	IT / ISO

(zdroj: ISO/IEC 27005, 2018)

5 DÍLČÍ ZÁVĚR

Závěr teoretické části shrnuje nejpodstatnější poznatky jednotlivých kapitol v návaznosti na téma „Řízení incidentů bezpečnosti informací“. Hlavním úkolem tohoto procesu je účinné zvládnutí incidentu, minimalizace jeho dopadů na chod organizace a co nejrychlejší obnova běžného provozu. Klíčovou roli zahrnuje plánování, včasná detekce, jasně definované postupy a stanovení zodpovědnosti.

Organizace, která si uvědomuje význam investic do vzdělávání, transparentní komunikace a budování důvěry uvnitř týmu, je odolnější vůči rizikům a nejistotám nejen v kybernetickém prostředí. Subjekty veřejného nebo soukromého sektoru by proto měly bezpečnost chápat jako kontinuální proces, nikoli jednorázovou investici nebo projekt.

Teoretické poznatky uvedené v této části práce tvoří výchozí rámec pro následnou analýzu konkrétního typu bezpečnostního incidentu a návrh postupu jeho řešení v prostředí organizace.

II PRAKTICKÁ ČÁST

6 ANALYTICKO-EMPIRICKÁ ČÁST

Tato část práce na základě dostupných dat poskytnutých organizací analyzuje dopad a závažnost phishingového útoku, kterému organizace v minulosti čelila a zároveň vyhodnocuje rozsah a účinnost opatření, které byly po tomto útoku zavedeny. Výsledky šetření organizace jsou podrobeny SWOT analýze přizpůsobené kontextu kybernetické bezpečnosti. Tato metoda byla zvolena pro svou srozumitelnost, nízkou náročnost na vstupní data a možnost kombinace s dalšími analytickými metodami. V tomto případě slouží k identifikaci silných, slabých stránek organizace a k určení příležitostí a hrozeb v oblasti kybernetických bezpečnostních incidentů. Jejím cílem je stanovit klíčové faktory ovlivňující odolnost organizace vůči incidentům. Metoda FMEA (Failure Mode and Effects Analysis) je následně využita pro stanovení míry rizika a identifikaci nejzávažnějších hrozeb.

Klíčovým ukazatelem této metody je RPN (Risk Priority Number), který je součinem tří faktorů – závažnosti dopadu (Severity), pravděpodobnosti výskytu (Occurrence) a schopnosti detekce (Detection). Výsledná hodnota RPN pomáhá určit pořadí rizik podle jejich závažnosti a napomáhá při návrhu opatření. (Fernández-Alemán, Lozoya a Toval, 2018).

$$RPN = S \cdot O \cdot D$$

6.1 Popis a charakteristika organizace

Úvodem této kapitoly je nutné zdůraznit, že při řešení otázek kybernetické a informační bezpečnosti, s částečným přesahem do dalších bezpečnostních oblastí si vybraný subjekt, který pro svou činnost zpracovává množství citlivých údajů, nepřál být jmenován. Při prvotním dohovoru a následném řízeném rozhovoru byla stanovena podmínka zachování anonymity. Z tohoto důvodu práce neobsahuje objektové a stavební (půdorysná) schémata a popis činnosti organizace není podrobněji popsán.

Jedná se o organizaci nekomerčního charakteru s kombinovanou funkcí v oblasti veřejných a podpůrných služeb, přičemž se na některé její činnosti (přesah do veřejné nebo kritické infrastruktury) může vztahovat směrnice NIS2. V rámci evropské klasifikace a s ohledem na prostředí ČR ji lze zařadit do kategorie středně velkých subjektů. Mezi primární aktiva této organizace patří služby, které jsou klíčové pro její činnost. Narušení těchto aktiv by mělo zásadní dopad na provoz organizace, kontinuitu a důvěryhodnost.

Podpůrná aktiva pak zahrnují prostředky nezbytné pro poskytování těchto služeb – informace, hardware, software a peopleware. Do této skupiny patří rovněž další služby, které podmiňují chod organizace, například zajištění energie, stravování nebo úklid.

Organizace je připravená na řešení krizových situací, které by na ni mohly mít negativní dopad (přerušení dodávek elektrické energie, konektivity / dostupnosti tradičních způsobů připojení apod.). Objektová bezpečnost je zajištěna vlastním (režimovým) podpůrným prvkem zařazeným v organizaci pro efektivní zajištění ochrany objektů.

6.2 Primární aktiva

Z pohledu zajištění činnosti organizace patří mezi nejdůležitější a nejvýznamnější aktiva služby, které organizace poskytuje.

- **Služby** představují klíčovou oblast pro naplnění poslání organizace, jejichž narušení by mohlo vést k omezení provozu nebo schopnosti naplňovat její hlavní úkoly. Vzhledem k tomu, že tyto služby jsou poskytovány v režimu, je kladen důraz na jejich vysokou dostupnost a provozní spolehlivost. S ohledem na primární zaměření se jedná o služby informační podpory, vzdělávací aktivity a provoz specifických systémů určených k interním účelům, u některých činností s částečným přesahem do veřejného prostoru.

6.3 Podpůrná aktiva

Zahrnují data – informace nezbytné pro zajištění služeb a provozu organizace, hardware, software, fyzickou infrastrukturu a v neposlední řadě také peopleware. Tato aktiva jsou důležitá pro správné fungování primárních aktiv – služeb, které jsou zásadní pro chod organizace. Selhání některého z podpůrných aktiv může vést k narušení nebo způsobit nedostupnost primárního aktiva (NÚKIB, 2021).

- **Informace** jak osobní, o zaměstnancích, tak klientská data by představovala ohrožení pro činnost a reputaci organizace. Jejich únik by měl za následek nejen ztrátu důvěryhodnosti organizace, ale především renomé. O porušení předpisů týkajících se ochrany osobních údajů (GDPR) nemluvě. Zneužití citlivých dat, mezi které osobní údaje patří, spadá mezi nejvýznamnější bezpečnostní hrozby.
- **Strategicky významné informace** mezi tyto aktiva patří databáze zahrnující plány, publikace, revizní činnost a další aktiva s vysokou informační a bezpečnostní

hodnotou. Dále pak nabídky, výběrová řízení a jejich výsledky. Jejich zneužití by přispělo k ohrožení strategického významu organizace.

- **Hardware** představuje v organizaci prostředky pro zabezpečení pracovních náplní zaměstnanců a možnosti pro zajištění telekomunikačních a datových služeb. Zahrnuje: mobilní zařízení, stacionární PC v kancelářích a notebook pro práci na cestách nebo v domácím prostředí. Zařízení jsou zaměstnancům vydána proti podpisu jako nepřenositelné (z osoby na osobu), a to na základě podané žádosti. Další periférie tvoří multifunkční zařízení, které jsou využívány jako sdílené a nakonec projektory. Vnější paměťová zařízení (USB disky) jsou organizací striktně zakázány. Ostatní statická média, dokumentace apod. je uložena v uzamykatelných kartotékách nebo uložena v archivu.
- **Software** je instalován pouze IT oddělením organizace před převzetím hardwaru. Zaměstnancům, aby uživatelům není umožněn jakýkoliv zásah do systému. Operační systém je pravidelně aktualizován. Software, který zaměstnanci využívají ke své práci, je zapsán na evidenčním listu. Pokud zaměstnanec vyžaduje pro svou pracovní činnost další specializovaný software, je tento nainstalován pracovníkem IT oddělení po zakoupení licence a doplněn na evidenční list.
- **Infrastruktura** je nezbytná pro zabezpečení fungování a zajištění služeb organizace. Stacionární PC jsou připojena síťovým kabelem RJ-45 do vnitřní sítě organizace která slouží k bezpečnému sdílení informací a dalších zdrojů mezi zaměstnanci organizace (intranet). Zaměstnanci využívající pro práci na cestách nebo z domova notebooky se mohou připojit do vnitřní sítě organizace zabezpečeným spojením prostřednictvím internetu, a to softwarem společnosti Fortinet.
- **Lidský faktor** peopleware představuje pro organizaci ve vztahu ke kybernetické bezpečnosti klíčový prvek. Nejdůležitějším faktorem ovlivňující tuto oblast je prevence a výběr lidských zdrojů. To zahrnuje pravidelné testování v rozsahu stanoveném organizací, pro zajištění bezpečnosti informací a zajištění kontinuity činnosti organizace. Dále vzdělávání a osobní rozvoj pro zvýšení povědomí a efektivní interakce mezi členy organizace. Tento bod byl označen při řízeném rozhovoru jako nejvýznamnější, kdy selhání jedince může vést k dopadu na celou organizaci.

V této souvislosti je třeba zmínit, že než k těmto opatřením došlo, organizace se potýkala s nedbale zabezpečeným systémem, kdy nereflektovala na doporučení bezpečnostního analytika upozorňujícího na rizika a hrozby s nevyřešenými a přetrvávajícími bezpečnostními incidenty.

6.4 Bezpečnost objektu

Z hlediska fyzické bezpečnosti lze konstatovat, že této oblasti je věnována náležitá pozornost a fyzická bezpečnost je řešena s ohledem na bezpečnostní situaci rozdělením organizace do perimetrů, které zaručují nerušenou činnost organizace a zajištění kontinuity. Organizace je rozdělena na zabezpečené oblasti, kanceláře, konferenční a prezentační prostory a technické zázemí.

Tyto informace byly získány pozorováním, při řízeném rozhovoru s vedením organizace, specialistou IT oddělení a bezpečnostním analytikem organizace.

Bezpečnost je u organizace zajištěna vlastním režimovým prvkem, který je zodpovědný za dodržování zásad, kontroly vstupu a vjezdu do areálu a kontrolní činnost zaměřenou na zajištění bezpečnosti u organizace.

6.5 Řízený rozhovor

Pro účely řízeného rozhovoru, který byl zmiňován v předchozích kapitolách, byli osloveni klíčoví zástupci organizace, konkrétně členové vedení, IT specialista a bezpečnostní analytik. Výběr respondentů byl zaměřen na osoby, které se přímo podílejí řízení kybernetických bezpečnostních incidentů nebo za tuto oblast nesou zodpovědnost. Omezený počet respondentů byl dán organizační strukturou a současně probíhající restrukturalizací organizace.

Získání prvotního přehledu a dalších informací bylo možné díky nastaveným pravidlům a otevřenosti ze strany organizace. Odpovědi byly poskytnuty následujícími respondenty: zástupcem vedení (A), specialistou IT (B) a bezpečnostním analytikem organizace (C). Snadnější průběh rozhovoru byl zajištěn zasláním otázek předem. V průběhu rozhovoru docházelo k názorovým a odborným konfrontacím, což přispělo k vyjasnění problematiky, zlepšení vnímání a komunikace mezi jednotlivými zaměstnanci organizace. Řízený rozhovor je přílohou I této práce.

6.6 Analýza prostředí organizace

U organizace v minulosti došlo k pochybení, které bylo způsobeno selháním lidského faktoru, jehož důsledkem byla ovlivněna reputace a pozitivní vnímání celé organizace. Tato událost přispěla ke změně pohledu a vnímání kybernetické a informační bezpečnosti.

Při tomto kybernetickém útoku došlo k úniku dat zahrnující citlivé informace, včetně osobních údajů (adres, dat narození, telefonních čísel), ale také uživatelských jmen a přístupů. Došlo rovněž k odcizení interní dokumentace, smluv a souvisejících materiálů apod.

Jelikož útok vedl k úniku osobních údajů, byl pro tuto skutečnost zařazen do zóny vysokého až kritického rizika. V následující tabulce je uvedena matice rizik (dopadů a pravděpodobnosti útoku – tab. 2).

Tabulka 2 Matice rizik

Dopad / Pravděpodobnost	Nízká	Střední	Vysoká
<i>Nízký dopad</i>		 	
<i>Střední dopad</i>	 		
<i>Vysoký dopad</i>			



Nízké riziko: Sleduj, bez potřeby zásahu.



Střední riziko: Vyžaduje plánování a kontrolu.



Vysoké riziko: Aktivní opatření, rychlá reakce.



Kritické riziko: Okamžitý zásah, prioritní.

(zdroj: Management organizace, 2023)

Pro stanovení silných a slabých stránek organizace byla využita SWOT analýza (obr. 6) ve vztahu k bezpečnostním incidentům – phishingový útok, který u organizace proběhl. Hodnoty jednotlivých prvků (silných stránek a příležitostí) jsou vyjádřeny kladnými hodnotami, zatímco slabé stránky a hrozby zápornými, vždy v rozsahu ± 1 až ± 5 . Pro větší objektivitu byly tyto váhy stanoveny s bezpečnostním analytikem organizace. (obr. 7). Následně byla rizika (slabé stránky a hrozby) analyzována metodou FMEA.

Silné stránky (Strengths)	Slabé stránky (Weaknesses)
<i>Zavedena politika informační bezpečnosti</i>	<i>Nízká míra povědomí zaměstnanců</i>
<i>Princip minimálních oprávnění</i>	<i>Chybějící testování uživatelů formou simul. útoků</i>

Zálohování a obnova dat	Neexistující scénáře a plány IRP
Používání filtru e-mailu	Nedostatečná detekce pokročilých technik
Příležitosti (Opportunities)	Hrozby (Threats)
Zavedení pravidelných školení a simulací	Rychle se vyvíjející techniky útočníků
Automatizace detekce a reakce	Kompromitace účtů ke škodlivým aktivitám, zneužití
Spolupráce s CERT/CSIRT týmy	Sankce (po incidentu)
Využití nových technologií	Nedůvěra klientů po úniku informací

Obrázek 6 Stanovení rozsahu pro SWOT analýzu
(zdroj: Informace managementu organizace, 2023)

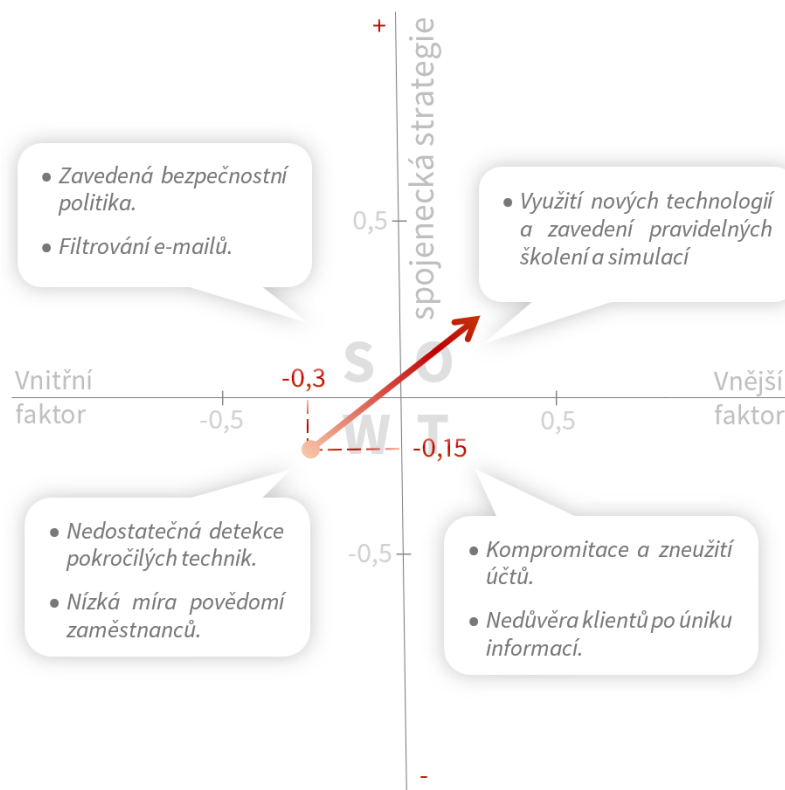
Kategorie	Faktor	Váha (0-1)	Hodnocení (-5 až +5)	Součin	Součet
Silné stránky (Strengths)	S1 - Zavedena politika informační bezpečnosti	0,25	3	0,75	3,7
	S2 - Princip minimálních oprávnění	0,2	3	0,6	
	S3 - Zálohování a obnova dat	0,4	4	1,6	
	S4 - Používání filtru e-mailu	0,15	5	0,75	
		1			
Slabé stránky (Weaknesses)	W1 - Nizká míra povědomí zaměstnanců	0,15	-4	-0,6	-4
	W2 - Chybějící testování uživatelů formou simul. útoků	0,3	-4	-1,2	
	W3 - Neexistující scénáře a plány IRP	0,35	-4	-1,4	
	W4 - Nedostatečná detekce pokročilých technik	0,2	-4	-0,8	
		1			
Příležitosti (Opportunities)	O1 - Zavedení pravidelných školení a simulací	0,15	5	0,75	4,45
	O2 - Automatizace detekce a reakce	0,35	4	1,4	
	O3 - Spolupráce s CERT/CSIRT týmy	0,3	5	1,5	
	O4 - Využití nových technologií	0,2	4	0,8	
		1			
Hrozby (Threats)	T1 - Rychle se vyvíjející techniky útočníků	0,25	-4	-1	-4,6
	T2 - Kompromitace účtů ke škodlivým aktivitám, zneužití	0,3	-5	-1,5	
	T3 - Sankce (po incidentu)	0,15	-4	-0,6	
	T4 - Nedůvěra klientů po úniku informací	0,3	-5	-1,5	
		1			

Obrázek 7 Analýza před nápravnými opatřeními
(zdroj: Informace managementu organizace, 2023)

Výpočet hodnot pro vektorové znázornění

Tento výpočet vychází z rozdílů mezi pozitivními a negativními faktory identifikovanými ve SWOT analýze. Konkrétně se jedná o rozdíl silných a slabých stránek vnesených na osu x, příležitostí a hrozeb na osu y. Tyto hodnoty jsou uvedeny ve sloupci „Součet“ v předchozí

tabulce (obr. 7), výsledné hodnoty vnitřních (interních) a vnější (externích) faktorů pro znázornění strategie (obr. 8) jsou průsečíkem $-0,3$ (x) a $-0,15$ (y).



Obrázek 8 Grafické znázornění výsledků
(zdroj: *Informace managementu organizace, 2023*)

Organizace disponuje zdroji a prostředky, které ji umožňují pokrýt identifikované slabiny, a proto je vhodné uvažovat o spojenecké strategii. Ta vyjadřuje aktivní přístup organizace a směřuje ke zlepšení vnitřních schopností. Nedostatky nejsou řešeny izolovaně, ale jako reakce na vnější prostředí s cílem posílit odolnost vůči budoucím hrozbám. Vektor směřuje z kvadrantu vnitřních slabin do vnějšího kvadrantu příležitostí. Tato strategie podporuje rozvoj organizace v oblasti posilování bezpečnosti a nezaměřuje se pouze na obranu proti hrozbám.

6.7 Vyhodnocení a ošetření rizik organizace

Na základě výsledků, které vyplynuly z analýzy (obr. 7), došlo v organizaci nejen ke změnám v oblasti řízení lidských zdrojů, ale především vnímání důležitosti kybernetické a informační bezpečnosti. Došlo k přehodnocení cílového stavu a do investičního plánu byla zahrnuta oblast posílení IT, zavedení nových technologií, pravidelných školení, revidování reakčních plánů a dohled nad jejich dodržováním.

Na prvotní analýzu, která sloužila k identifikaci silných, slabých stránek, příležitostí a hrozeb, navázala metoda FMEA (tab. 3), umožňující konkrétní vyhodnocení rizik vyplývajících ze slabých stránek a hrozeb (Gregory, 2022).

Negativní faktory identifikované ve SWOT analýze, například nízké povědomí zaměstnanců o phishingu, chybějící nebo nedostatečné testování pomocí simulačních útoků nebo absence jednotného postupu pro řešení incidentu – byly dále rozpracovány v rámci FMEA jako možné body selhání.

Přestože metodiky doporučují udržovat ve SWOT analýze rovnováhu mezi jednotlivými kategoriemi, tato numerická symetrie se do FMEA nepřenáší. Na základě skutečných poznatků o stavu řízení bezpečnosti v organizaci zde byla analyzována širší oblast rizik, než jakou vymezuje SWOT. Ta sloužila jako výchozí rámec pro definování oblastí slabých stránek a hrozeb.

Dalším krokem bylo stanovení priorit podle závažnosti, výskytu a možnosti detekce s cílem zpracování návrhu opatření pro snížení rizik (tab. 4).

6.8 FMEA

Tabulka 3 FMEA před přijetím opatření (po provedeném útoku)

Stav před přijetím opatření (po kybernetickém útoku)						
Faktory (ze SWOT)	Možný následek	Závažnost (S)	Výskyt (O)	Detek. (D)	RPN	Doporučené opatření
Nízké povědomí zaměstnanců (W1)	Kompromitace účtu	9	7	6	378	Školení a simulace phishingu
Chybějící testování uživatelů (W2)	Neodhalení rizik. zaměstnanců	8	6	7	336	Pravidelné simulace útoků
Neexistující IRP (W3)	Chaos, zpoždění reakce	10	4	8	320	Zavedení a testování IRP
Nefunkční det. pokročilých technik (W4)	Obcházení filtrů, malware v síti	9	5	7	315	Investice do pokročilé detekce
Rychlý vývoj technik útočníků (T1)	Neaktuální obranné mechanismy	8	6	5	240	Spolupráce s CSIRT apod.
Kompromitace účtů (T2)	Únik a zneužití dat	10	5	6	300	Monitoring účtů, včasné varování
Sankce po inc. (např. GDPR) (T3)	Právní dopady, reputace	9	3	8	216	Prevence incidentů, dokumentace
Nedůvěra klientů (T4)	Ztráta důvěry, odliv klientů	8	4	7	224	Komunikační plán a obnova důvěry
Doplňující faktory						
Nejasné vymezení kompetencí	Zpožděná reakce, duplicita činností	8	6	7	336	Vyjasnění rolí a koordinace, Aktualizace IRP
Zpožděné informování vedení	Nesprávná rozhodnutí, zhorš. reputace	9	5	6	270	Nastavení pravidel
Neprovázanost s právním odd., HR, PR	Chybné zacházení s citlivými daty	8	5	5	200	Zahrnutí odd. k řešení incidentu
Chybně nastavené filtry e-mailů	Neodhalení phishingu	8	7	4	224	Revize, nastavení a testování
Nedostatečná archivace důkazů	Nemožnost analýzy	9	6	6	324	Centralizace záznamů
Absence post-incident review	Opakování stejných chyb	8	6	6	288	Zavedení analýzy po incidentu
Neaktuální scénáře v testech	Přecenění připravenosti	8	5	7	280	Tvorba scénářů simul. reálných hrozeb

(zdroj: Informace managementu organizace, 2023)

Tabulka 4 Výsledky FMEA po přijetí opatření

Očekávaný stav (po přijetí opatření)						
Faktory (ze SWOT)	Opatření	Závažnost ppo	Výskyt ppo	Detek. ppo	RPN ppo	Zlepšení RPN
Nízké povědomí zaměstnanců (W1)	Školení a simulace phishingu	6	5	4	120	258
Chybějící testování uživatelů (W2)	Pravidelné simulace útoků	6	4	5	120	216
Neexistující IRP (W3)	Zavedení a testování IRP	7	3	5	105	215
Nefunkční det. pokročilých tech. (W4)	Investice do detekce	7	4	5	140	175
Rychlý vývoj technik útočníků (T1)	Spolupráce s CSIRT apod.	6	5	4	120	120
Kompromitace účtů (T2)	Monitoring účtů a včasné varování	8	4	4	128	172
Sankce po inc. (např. GDPR) (T3)	Prevence incidentů, dokumentace	7	2	5	70	146
Nedůvěra klientů (T4)	Komunikační plán a obnova důvěry	6	3	5	90	134
Doplňující faktory						
Nejasné vymezení kompetencí	Vyjasnění rolí a koordinace, Aktualizace IRP	6	4	5	120	216
Zpožděné informování vedení	Nastavení pravidel	7	3	5	105	165
Neprovázanost s právním odd., HR, PR	Zahrnutí odd. k řešení incidentu	6	3	4	72	128
Chybně nastavené filtry e-mailů	Revize, nastavení a testování	6	5	3	90	134
Nedostatečná archivace důkazů	Centralizace záznamů	7	5	4	140	184
Absence post-incident review	Zavedení analýzy po incidentu	5	4	4	80	208
Neaktuální scénáře v testech	Tvorba scénářů simul. reál. hrozeb	6	4	5	120	160

(zdroj: Informace managementu organizace, 2023)

6.9 Výstupy analýzy FMEA

Výstupy z provedené analýzy zobrazují výskyt rizik v organizaci a úspěšný kybernetický útok byl vyústěním přehlížení skutečností, na které bylo vedení organizace upozorňováno bezpečnostním analytikem. V následující tabulce je uvedeno shrnutí před a po zavedením nápravných opatření (tab. 5).

Tabulka 5 Výstupy analýzy před a po přijetí opatření

Stanovená rizika	RPN (před)	RPN (po)
<i>Nízké povědomí zaměstnanců</i>	378	120
<i>Chybějící testování uživatelů</i>	336	120
<i>Neexistující IRP</i>	320	105
<i>Nefunkční detekce pokročilých technik</i>	315	140
<i>Rychlý vývoj technik útočníků</i>	240	120
<i>Kompromitace účtů</i>	300	128
<i>Sankce (např. GDPR)</i>	216	70
<i>Nedůvěra klientů</i>	224	90
<i>Nejasné vymezení kompetencí</i>	336	120
<i>Zpožděné informování vedení</i>	270	105
<i>Neprovázanost s právním odd., HR, PR</i>	200	72
<i>Chybně nastavené filtry e-mailů</i>	224	90
<i>Nedostatečná archivace důkazů</i>	324	140
<i>Absence zpětné analýzy, vyhodnocení průběhu a dopadů inc.</i>	288	80
<i>Neaktuální scénáře v testech</i>	280	120

(zdroj: Informace managementu organizace, 2023)

 **0 – 100 Akceptovatelné riziko**
(je nízké, řízení postačuje, doporučuje se:
monitorovat, bez nutnosti zásahu)

 **101 – 200 Významné riziko**
(by mělo být sledováno, doporučení: zvážit
preventivní opatření)

 **201 – 300 Nežádoucí riziko**
(může ovlivnit provoz – doporučuje se zásah
a přijmout nápr. opatření)

 **≥ 301 Nepřijatelné riziko**
(kritické s vysokou závažností – okamžitě
reagovat, vysoká priorita)

Rozšířené výsledky analýzy FMEA potvrzují výstupy ze SWOT. Nejvýraznější snížení hodnot rizikového čísla (RPN) se týká oblasti slabín a hrozeb, což odpovídá zvolené spojenecké strategii.

7 STANOVENÍ HYPOTÉZ A NÁVRH OPATŘENÍ

Pro návrh struktury postupu pro řízení bezpečnostních incidentů je vhodné úvodem definovat hypotézy (tab. 6), které mohou být dále ověřovány (studie, rozhovory, simulace apod.). Pro praktickou aplikaci předpokládáme, že jsou disponibilní preventivní opatření, aktivní a připravené týmy pro řízení reakce na incidenty.

Stanovené hypotézy jsou:

Tabulka 6 Stanovení hypotéz

P.č.	Hypotéza	Zaměření
1.	Organizace, mají formálně definovaný Plán reakce na incidenty (IRP), = zvládají BI efektivněji.	Znalost a efektivita řízení BI
2.	Organizace, používají standardizovaný rámec (např. ISO/IEC 27035), = nižší míra rekurentních incidentů.	Použ. norem při řízení BI
3.	Zapojení odpovědných rolí (např. ISO, CSIRT) = urychluje reakční dobu na incident.	Efektivní využití rolí a zdrojů organizace
4.	Pravidelné školení zaměstnanců = významně snižuje počet BI způsobených lidskou chybou.	Prevence selhání lidského faktoru
5.	Včasná post-mortem analýza = zlepšení bezpečnostních opatření v organizaci.	Poučení a zvýšení odolnosti organizace

(zdroj: ISO/IEC 27035, 2023)

V souladu s NIS2 – Směrnice Evropské unie o kybernetické bezpečnosti (EU 2022/2555), která byla předmětem kapitoly 3 a pojednává o rozšířeném okruhu subjektů s cílem harmonizace kybernetické odolnosti, regulace a dozoru, je nemalá část této směrnice věnována hlášení incidentů a posuzování rizik.

Tématem hlášení bezpečnostních incidentů se zabývá Národní úřad pro kybernetickou a informační bezpečnost (dále NÚKIB), který na svých stránkách přináší metodiku, formuláře, další možnosti jejich hlášení a stanovuje podmínky jejich využití.

7.1 Navrhovaná opatření a doporučení

Na základě výsledků provedené SWOT a FMEA analýzy, které odhalily převažující slabé stránky v interním nastavení a současně identifikovaly externí hrozby, je pro organizaci vhodné přijmout spojeneckou strategii. Tento přístup je zaměřen na posílení vnitřních kapacit organizace a spolupráce s externími subjekty. Spojenecká strategie umožňuje stabilizaci bezpečnostního prostředí, snižuje rizika a vytváří podmínky pro další rozvoj a zvyšování odolnosti vůči hrozbám. Současně napomáhá postupnému budování vyšší míry samostatnosti organizace v oblasti kybernetické bezpečnosti.

Opatření pro spojeneckou strategii:

- **Posílení vnitřních kapacit organizace** – představuje pro organizaci krok směrem k rozvoji zázemí v oblasti kybernetické bezpečnosti, a to v rovině materiální, technické a personální. Součástí je zajištění kvalifikovaného personálu, zavedení pravidelných školení a realizace simulací incidentů, které reflektují aktuální poznatky kybernetických útoků. Cílem tohoto opatření je posílit samostatnost organizace a snížit její závislost na externích subjektech při zvládání incidentů.
- **Prohloubení externí spolupráce** – pro dosažení požadované úrovně kybernetické bezpečnosti může organizace navázat spolupráci s externími subjekty – bezpečnostní týmy, poradenské firmy nebo školicí instituce. Taková spolupráce umožňuje přístup k novým poznatkům, pokročilým technologiím nebo zajištění odborné podpory při řešení incidentů. Toto opatření přispívá ke zvýšení připravenosti a odolnosti organizace vůči kybernetickým hrozbám.
- **Zavedení pravidelných školení a simulací** – pro zvýšení odolnosti organizace vůči kybernetickým útokům je vhodné zavést systém pravidelných a povinných školení, který podpoří průběžné vzdělávání zaměstnanců prostřednictvím online kurzů a prezenčních forem školení. Nedílnou součástí tohoto opatření je provádění realistických simulací útoků pro zvýšení povědomí zaměstnanců a posílit jejich schopnost reagovat na skutečné hrozby. Opakovaným školením a praktickým nácvikem lze významně snížit riziko selhání lidského faktoru, které bývá častým původcem kybernetických incidentů.
- **Využití moderních technologií** – organizace by se měla zaměřit na nasazení nástrojů pro detekci hrozeb a varování. Zároveň je důležité provádět pravidelné testování systémů, aktualizaci a následného vyhodnocování účinnosti zavedených opatření. Moderní technologie představují prvek ochrany, které mohou zlepšit schopnost organizace včas reagovat a omezit dopady incidentů.
- **Zlepšení komunikace** – pro vytvoření přehledné komunikační struktury by měla organizace definovat role a zodpovědnost za jednotlivé fáze řízení incidentu bezpečnosti informací. Dále zajistit evidenci, následné vyhodnocování incidentů a jejich dopadů. V rámci interní i externí komunikace nastavit formální pravidla s partnery, veřejností, médii a dalšími orgány. Transparentnost a včasnost informací jsou klíčové pro minimalizaci škod, udržení důvěry a zajištění kontinuity.

V kategorii slabých stránek a hrozeb došlo ke zlepšení, které jsou doložitelné dle údajů uvedených (na obr. 9 a obr. 10). Organizace se na tento pozitivní vývoj snaží navázat dalšími proaktivními kroky, které mají za cíl posílení odolnosti vůči hrozbám a postupné snižování přetrvávajících slabin. Zároveň si je vědoma stávajících rezerv v oblasti kybernetické bezpečnosti a na tyto se cíleně zaměřuje. V rámci dlouhodobé strategie organizace přistupuje k této oblasti kontinuálně, pravidelně přehodnocuje a přizpůsobuje opatření aktuálním hrozbám.

Osvědčil se princip, který jasně definuje fáze přípravy, identifikace, analýzy, reakce, obnovy a vyhodnocení. Nejde přitom o složitý systém, ale funkční, přehledný a průběžně aktualizovaný postup, který zohledňuje rizika a v němž každý zaměstnanec ví, jak postupovat.

Existuje přímá souvislost mezi mírou školení zaměstnanců a počtem úspěšně zablokovaných útoků. Významnou roli přitom hraje také skutečnost, zda organizace pravidelně investují do technického vybavení, simulačních nástrojů a rozvoje svých týmů.

Tímto krokem dochází ke snižování míry dopadu – zaměstnanci si více uvědomují rizika a dokážou na ně adekvátně reagovat.

Přehled navrhovaných opatření

Navržená opatření (tab. 7) jsou zaměřena na konkrétní oblasti řízení incidentů a přinášejí orientační odhad nákladů, technické požadavky a očekávaný dopad na organizaci. Výsledný přehled tvoří základní rámec pro další zlepšování:

Tabulka 7 Přehled navrhovaných opatření

	<i>Název opatření /Očekávaný dopad/</i>	<i>Popis</i>	<i>Technické řešení</i>	<i>Orientační náklady</i>
1.	Posílení vnitř. kapacit organizace /Zvýšení samostatnosti, snížení závislosti na exter. subjektech/	• Vyčlenění odpovědné osoby za kyber. bezp. • Školení nebo vytvoř. pozice.	• Interní pracovník, případně školení (NÚKIB, ESET)	• Školení: 5 000–10 000 Kč, externí: 35 000 Kč/měs.
2.	Prohloubení externí spolupráce /Přístup k analýzám, cvičením/	• Navázání spolupráce s CSIRT/CERT týmy nebo bezpečnostním konzultantem.	• CSIRT.CZ nebo jiný externí konzultant	• 1 200–1 800 Kč/hod. • 150 000 Kč/rok
3.	Zavedení pravidelných školení a simulací /Zvýšení povědomí zaměstnanců/	• Dvě povinná školení ročně • Simulace se zpět. vazbou čtvrtletně.	• LMS systém Moodle • ESET Cybersecurity Awareness Train.	• Online školení: 25 000 Kč/rok • Simulace: 15 000 Kč/rok

4.	Využití moderních technologií /Zkrácení doby detekce, pokrytí hrozeb /	• Nasazení technologií pro analýzu a reakci.	• MS Sentinel, Wazuh, Splunk	• Wazuh: 40 000 Kč/rok. • Sentinel: 70–120 000 Kč/rok
5.	Zlepšení komunikace /Eliminace informačního šumu/	• Vypracování komun. plánu.	• Interní metodika. • Pravidelné testování	• Interní – mezi týmy, • Externí – PR, případně konzultant (cca. 35 000 Kč)

(zdroj: vlastní)

Posílení vnitřních kapacit organizace – organizace by měla vyčlenit pracovníka odpovědného za kybernetickou bezpečnost, případně využít služeb externích subjektů. Náklady na školení se pohybují v rozmezí 5 000–10 000 Kč, případně lze uvažovat o externí spolupráci, formou částečného úvazku, přičemž náklady se pohybují okolo 35 000 Kč.

Prohloubení externí spolupráce – navázání spolupráce s externími subjekty (např. CSIRT.CZ) může organizaci poskytnout cenné know-how a podporu při řešení bezpečnostních incidentů. Nabízené služby zahrnují konzultační hodiny, penetrační testování, technickou asistenci či přístup k přednostní zákaznické podpoře. Tato spolupráce přispívá k posílení odolnosti organizace a zkrácení doby reakce na incidenty. Orientační náklady na spolupráci s externími subjekty se mohou pohybovat v rozmezí 150 000 Kč až 2 000 000 Kč v závislosti na typu nabízených služeb (CZNIC.cz, 2025).

Zavedení pravidelných školení a simulací – implementace systému pravidelných školení a realistických simulací přispívá ke zvýšení odolnosti organizace vůči kybernetickým útokům. Doporučuje se kombinace online školení pro stávající zaměstnance (realizované každé pololetí) a prezenční forma pro nastupující zaměstnance. Školení by doplňovaly realistické simulace útoků. K tomuto účelu lze využít platformy typu Titan HQ nebo ESET Cybersecurity Awareness Training, kde se náklady pohybují v rozmezí 250 USD až 350 USD za 10 uživatelů (ESET a Titan HQ, 2025).

Využití moderních technologií – nasazení moderních nástrojů pro detekci a reakci na hrozby výrazně zvyšuje schopnost organizace včas reagovat na bezpečnostní incidenty. Organizace může využít komerční řešení, jako např. Microsoft Sentinel, které nabízí cloudové řešení a cenový model založený na objemu zpracovaných dat (Microsoft, 2024) nebo open-source nástroje, např. Wazuh (Wazuh, 2024). Roční náklady uvedených řešení se pohybují v rozmezí 40 000 až 100 000 Kč. Volba tohoto řešení by měla vycházet z požadavků organizace a její technické vyspělosti.

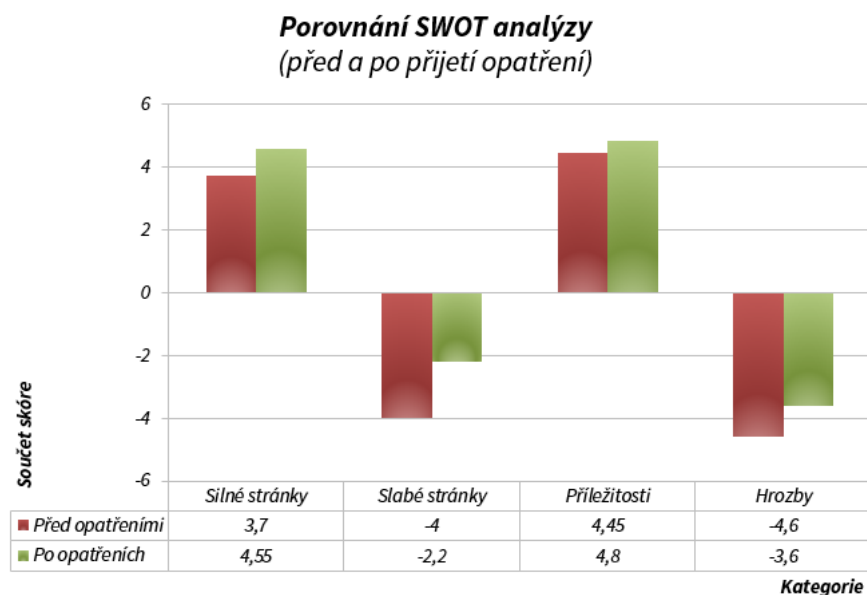
Zlepšení komunikace – organizace by se měla soustředit na zlepšení interní komunikace mezi týmy, ale také na externí komunikaci směrem k veřejnosti, sdělovacím

prostředkům apod. Zvládání incidentů vyžaduje vypracování komunikačního plánu, který bude obsahovat seznam kontaktních osob, stanovené role a odpovědnost v jednotlivých fázích řízení incidentu. Orientační náklady na školení zaměstnance organizace se pohybují mezi 5 000 až 10 000 Kč, zatímco náklady na externího specialistu mohou činit 35 000 Kč měsíčně.

Porovnání výsledků

Výsledky přijatých opatření byly ověřeny auditem organizace a následnou analýzou (obr. 10), která ukázala, že opatření přispěla – ke snížení slabin (45 %) a hrozeb (21,7 %). Tento výsledek odpovídá zvolené strategii. Tuto skutečnost potvrzují výsledky analýzy FMEA, kde rizika spojená s těmito oblastmi dosahovala nejvyššího RPN a byla cílem navržených opatření. Obě provedené analýzy jsou ve vzájemném souladu a potvrzují vhodnost a účinnost zvolených opatření.

Posun v oblasti kybernetické bezpečnosti je znázorněn na grafu (obr. 9) a odráží skutečnost, že u organizace nebyl od té doby hlášený další bezpečnostní incident.



Obrázek 9 Porovnání výsledků analýzy (před/po přijetí opatření)
(zdroj: *Informace managementu organizace, 2023*)

Kategorie	Faktor	Váha (0-1)	Hodnocení (-5 až +5)	Součin	Součet
Silné stránky (Strengths)	S1 - Zavedena politika informační bezpečnosti	0,25	4	1	4,55
	S2 - Princip minimálních oprávnění	0,2	4	0,8	
	S3 - Zálohování a obnova dat	0,4	5	2	
	S4 - Používání filtru e-mailu	0,15	5	0,75	
		1			
Slabé stránky (Weaknesses)	W1 - Nízká míra povědomí zaměstnanců	0,15	-2	-0,3	-2,2
	W2 - Chybějící testování uživatelů formou simul. útoků	0,3	-2	-0,6	
	W3 - Neexistující scénáře a plány IRP	0,35	-2	-0,7	
	W4 - Nedostatečná detekce pokročilých technik	0,2	-3	-0,6	
		1			
Příležitosti (Opportunities)	O1 - Zavedení pravidelných školení a simulací	0,15	5	0,75	4,8
	O2 - Automatizace detekce a reakce	0,35	5	1,75	
	O3 - Spolupráce s CERT/CSIRT týmy	0,3	5	1,5	
	O4 - Využití nových technologií	0,2	4	0,8	
		1			
Hrozby (Threats)	T1 - Rychle se vyvíjející techniky útočníků	0,25	-3	-0,75	-3,6
	T2 - Kompromitace účtů ke škodlivým aktivitám, zneužití	0,3	-4	-1,2	
	T3 - Sankce (po incidentu)	0,15	-3	-0,45	
	T4 - Nedůvěra klientů po úniku informací	0,3	-4	-1,2	
		1			

Obrázek 10 Výsledky analýzy po přijetí nápravných opatření
(zdroj: *Informace managementu organizace, 2023*)

Na základě výsledků, které z analýzy vyplynuly (obr. 11), došlo v organizaci k dalšímu přehodnocení stavu a vytyčení nových cílů, které budou zahrnovat směřování organizace v oblasti kybernetické a informační bezpečnosti.

	Silné stránky	Slabé stránky	Příležitosti	Hrozby
Před opatřeními	3,7	-4	4,45	-4,6
Po opatřeních	4,55	-2,2	4,8	-3,6
Rozdíl	0,85	1,8	0,35	1
% vyjádření	23,0%	45,0%	7,9%	21,7%

Obrázek 11 Porovnání výsledků analýzy
(zdroj: *Informace managementu organizace, 2023*)

7.2 Postup řízení konkrétního bezpečnostního incidentu – příklad

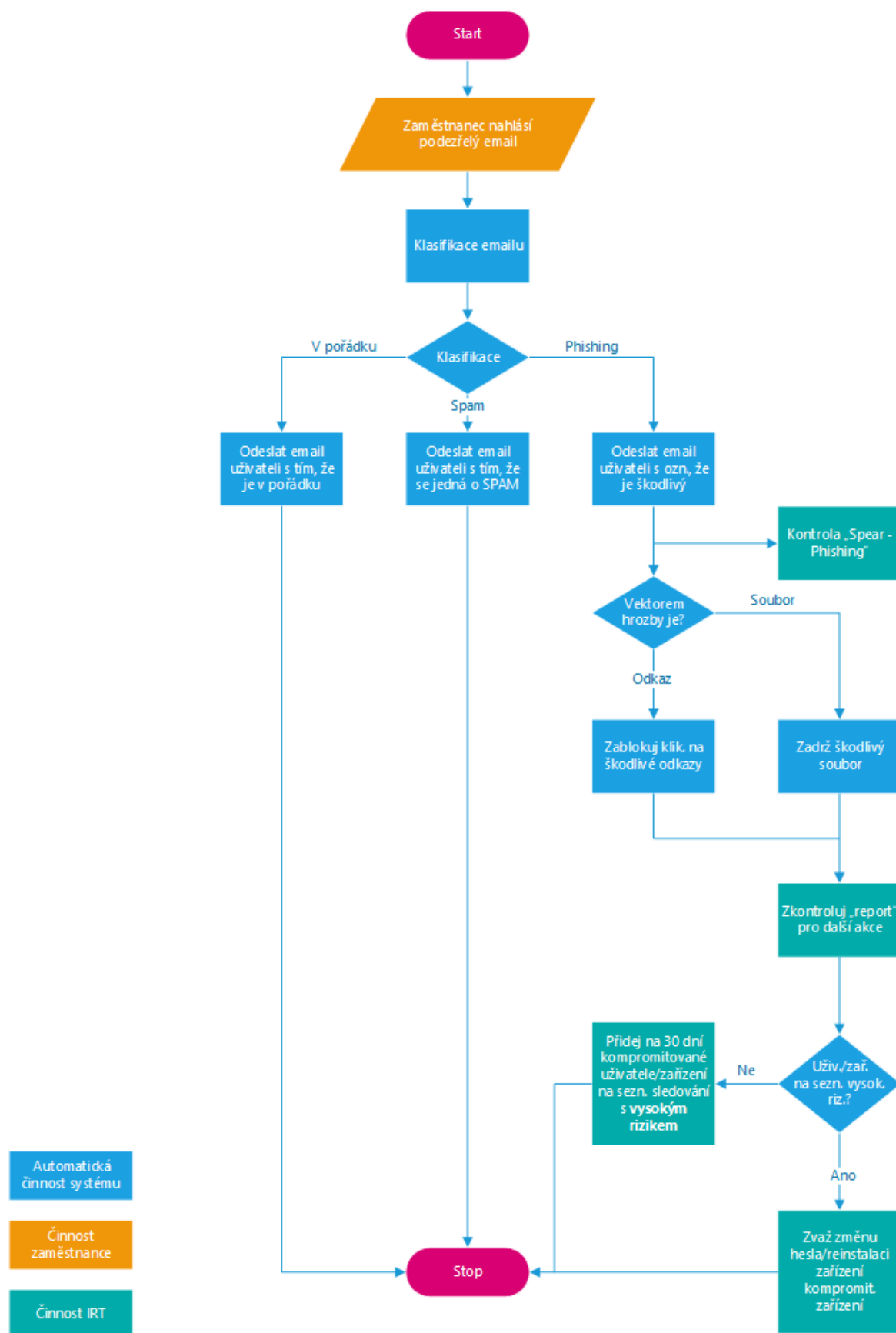
Znázorňuje postup na bezpečnostní incident, který byl popisován v kapitole 6 a představuje přístup k identifikaci a řešení e-mailových hrozeb, phishingu (obr. 12). Tento postup využívá organizace při jeho zachycení s cílem identifikovat nežádoucí zprávu, informovat uživatele a případně zahájit opatření k omezení dopadu této hrozby.

Klíčovým prvkem je zapojení zaměstnanců do detekce hrozeb, popř. probíhá na úrovni systému. Tento proces začíná nahlášením podezřelé zprávy zaměstnancem, po kterém následuje automatické rozpoznání zprávy systémem. Ten email vyhodnotí a na tomto základě dochází k dalšímu postupu – uživatel je informován, zda je zpráva bezpečná či nikoliv.

Při identifikaci škodlivého e-mailu vstupuje do procesu tým pro reakci na incidenty (IRT), který posuzuje typ hrozby (např. škodlivý odkaz, přílohu apod.) a aplikuje vhodná opatření – zablokování odkazů, zadržení souboru a vyhodnocuje další rizika spojené s kompromitací zařízení.

Dalším krokem spadajícím mezi zásady řízení rizik je sledování, tj. zařazení uživatele nebo zařízení na seznam pozorovaných objektů. V případě vysokého rizika jsou prováděna opatření k zamezení dalšího šíření (např. změna hesla, přeinstalování systému nebo eskalace incidentu). Tento postup zajišťuje efektivní reakci a omezení dopadů bezpečnostních hrozeb.

Následující schéma (obr. 12) znázorňuje postup řízení bezpečnostního incidentu z úrovně základních aktérů – koncového uživatele (zaměstnance), systému a bezpečnostního týmu. Rozlišuje odpovědnost a návaznost jednotlivých činností a znázorňuje průběh detekce, klasifikace a řešení incidentu. Umožňuje sledovat proces od okamžiku vzniku incidentu až po jeho uzavření.



Obrázek 12 Postup řízení bezpečnostního incidentu – phishing
(zdroj: Medium, 2019)

7.3 Identifikace postupů k řízení incidentů

Začněme slovy, která jsou připisovány Tomáši Prouzovi: „*Když selže prevence, nastupuje reakce.*“ a vystihují podstatu řízení bezpečnostních incidentů. I přes veškeré úsilí o prevenci nelze zcela vyloučit, že ke kompromitaci bezpečnosti informací dojde (Prouza, n.d.).

Právě proto je nezbytné mít efektivní postupy pro zvládání a řízení incidentů bezpečnosti informací, které jsou pro organizace klíčovým procesem a umožňují tak rychle reagovat, minimalizovat dopady a obnovit běžný provoz.

Reakce nastává, když preventivní opatření selžou (FR Secure, 2024). V této fázi je klíčové mít připravený plán reakce (tab. 8), který zahrnuje:

- **Rychlou identifikaci příčiny incidentu**, která zahrnuje posouzení a hodnocení.
- **Koordinovanou komunikaci mezi týmy**, zaznamenání a sdílení informací. Pokud je to možné, komunikace je šifrována.
- **Proces zahrnující sběr dat, jejich uchovávání a izolaci**, kdy je izolace jedním z nejdůležitějších opatření během reakce na incident.
- **Analýzu incidentu pro zlepšení budoucích / preventivních postupů** – rozbor a následné využití zkušeností z incidentu pro zlepšení preventivních opatření do budoucna.

Tabulka 8 Jednotlivé fáze tvorby IRP

<i>Fáze</i>	<i>Cíl</i>	<i>Hlavní úkoly</i>
1. Příprava na incident	Nastavení procesů a nástrojů k reakci na incident.	Školení zaměstnanců. Simulace incidentu. Nastavení nástrojů detekce.
2. Identifikace (detekce) incidentu	Rychle rozpoznat a potvrdit incident a určit jeho příčinu.	Monitoring, ověření, analýza, klasifikace, evidence.
3. Analýza a reakce (izolace, zadržení)	Eliminovat hrozbu a obnovit provoz. Zabránit šíření, minimalizovat škody.	Izolace, odstranění hrozby (odpojení, blokace).
4. Odstranění	Odstranění příčin incidentu.	Vyčištění infikovaných zařízení. Aktualizace. Změna přihlašovacích údajů.
5. Obnova	Obnovení běžného provozu. Zajištění kontroly systému.	Obnovení systémů ze záloh. Monitorování účtů. Komunikace s dotčenými stranami.
6. Poučení	Zlepšit prevenci pomocí poučení z incidentu. Zajistit zpětnou vazbu.	Revize reakce, aktualizace IRP, školení, zpráva.

(zdroj: Cyber Incident Response Plan Guidance, 2023)

Efektivní řízení vyžaduje, aby každá zainteresovaná strana měla přesně definované role, stanovenou zodpovědnost a jejich činnost byla koordinovaná (Příloha II). Právě souhra

těchto činností a jejich správné načasování hraje zásadní roli v minimalizaci dopadů útoku, bez ohledu na to, o jaký typ incidentu se jedná.

8 VHODNÉ POSTUPY K ŘÍZENÍ INCIDENTŮ BEZPEČNOSTI INFORMACÍ

Klíčovým předpokladem pro stanovení vhodných postupů k řízení kybernetických bezpečnostních incidentů je vymezení rozsahu činnosti zainteresovaných stran v jednotlivých fázích řešení incidentu. Fáze jsou definované v souladu s mezinárodními standardy (např. NIST SP 800-61 nebo ISO/IEC 27035) a zahrnují postupné kroky, např. dle modelu PICERL.

8.1 Postup při řízení incidentů – Phishing

Úvodem jsou definovány úrovně dopadu (tab. 9) a klasifikace závažnosti (tab. 10). Tím získáme vhodný nástroj pro hodnocení dopadu, závažnosti incidentu a úrovně reakce na něj (FR Secure, 2024).

Tabulka 9 Úroveň dopadu bezpečnostního incidentu

Úroveň dopadu	Definice	Činnost / reakce
Žádný	Incident nemá zásadní dopad na schopnost organizace poskytovat služby uživatelům v plném rozsahu.	Evidovat, monitorovat, bez aktivního zásahu
Nízký	Incident s minimálním dopadem na schopnost organizace poskytovat všechny klíčové služby, ale s nižší efektivitou.	Vyhodnotit, zaznamenat a dále sledovat, kontrolovat zařízení, informovat uživatele
Střední	Organizace ztratila schopnost poskytovat některou z klíčových služeb pro skupinu uživatelů.	Analyzovat přístup, resetovat heslo, zaznamenat a dále sledovat. Informovat vedoucího IT
Kritický	Organizace není schopna poskytovat jednu či více klíčových služeb všem uživatelům.	Aktivovat CSIRT, vedoucího IT, provést forenzní analýzu a zvážit plán obnovy

(zdroj: FR Secure – Information Security Experts, 2024)

Klasifikace (tab. 10) napomáhají určit naléhavost přijatých opatření pro zabezpečení bezpečnosti (FR Secure, 2024).

Tabulka 10 Stanovení klasifikace závažnosti incidentu

Klasifikace závažnosti		Ovlivňující informační bezpečnost			
		Nízká	Střední	Vysoká	Kritická
Ovlivňující funkčnost	Nízká	Úroveň 4	Úroveň 3	Úroveň 2	Úroveň 1
	Střední	Úroveň 3	Úroveň 3	Úroveň 2	Úroveň 1
	Vysoká	Úroveň 2	Úroveň 2	Úroveň 2	Úroveň 1
	Kritická	Úroveň 1	Úroveň 1	Úroveň 1	Úroveň 1

(zdroj: FR Secure – Information Security Experts, 2024)

Aplikace úrovní dopadu a závažnosti (tab. 11) při řešení phishingového útoku na organizaci umožňuje vhodné nastavení reakčních časů (FR Secure, 2024):

Tabulka 11 Dopad a závažnost bezpečnostního incidentu

Úroveň dopadu	Definice	Příklad	Úroveň závažnosti	Činnost / reakce
Žádný	Incident nemá zásadní dopad na schopnost organizace poskytovat služby uživatelům v plném rozsahu.	E-mail byl zablokován filtrem, žádný uživatel jej neotevřel ani nenahlásil.	Nízká (4)	Evidovat, monitorovat, bez aktivního zásahu
Nízký	Incident s minimálním dopadem na schopnost organizace poskytovat všechny klíčové služby, ale s nižší efektivitou.	Uživatel otevřel podezřelý e-mail, klikl na odkaz, ale nevyplnil žádné údaje.	Střední (3)	Vyhodnotit, zaznamenat a dále sledovat, kontrolovat zařízení, informovat uživatele
Střední	Organizace ztratila schopnost poskytovat některou z klíčových služeb pro skupinu uživatelů.	Uživatel vyplnil přihl. údaje do podvodného formuláře.	Vysoká (2)	Analyzovat přístup, resetovat heslo, zaznamenat a dále sledovat. Informovat vedoucího IT
Kritický	Organizace není schopna poskytovat jednu či více klíčových služeb všem uživatelům.	Účet byl kompromitován a použit k dalším útokům nebo došlo k úniku citlivých dat. Dopad na provoz nebo reputaci.	Kritická (1)	Aktivovat CSIRT, vedoucího IT, provést forenzní analýzu a zvážit plán obnovy

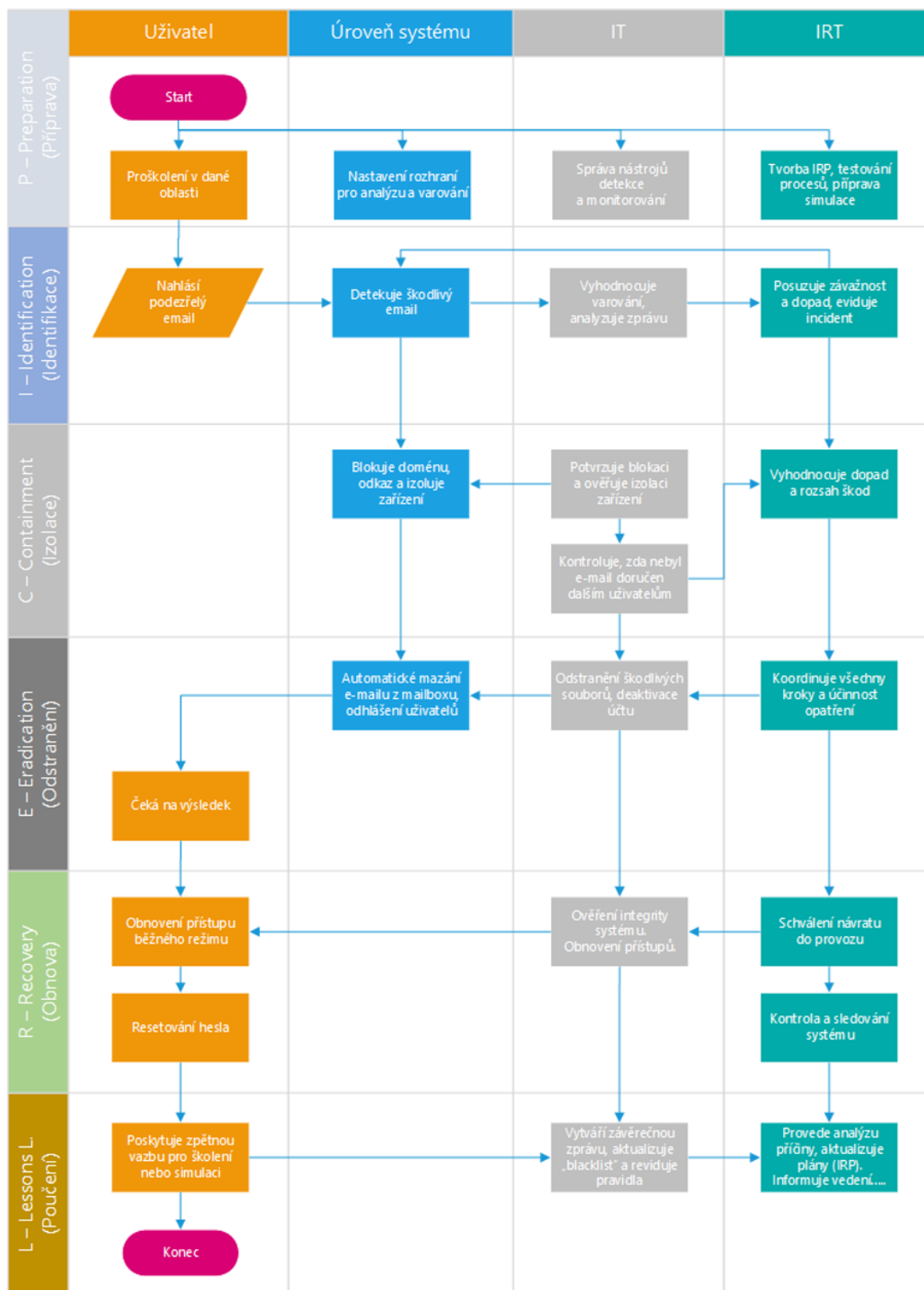
(zdroj: FR Secure – Information Security Experts, 2024)

Pro jednotlivé úrovně je stanoven čas pro detekci, reakci a vyřešení incidentu (Johansen, 2020), např.:

- **Kritická úroveň závažnosti (úroveň 1)** incident musí být detekován do 15 minut, reakce na něj provedena do 60 minut a vyřešen do 4 hodin;
- **Vysoká úroveň závažnosti (úroveň 2)** incident musí být detekován do 30 minut, reakce na něj provedena do 120 minut a vyřešen do 8 hodin;
- **Střední úroveň závažnosti (úroveň 3)** incident musí být detekován do 60 minut, reakce na něj provedena do 4 hodin a vyřešen do 1 dne;
- **Nízká úroveň závažnosti (úroveň 4)** incident musí být detekován do 120 minut, reakce na něj provedena do 8 hodin a vyřešen do 2 dnů;

Předem připravený IRP formulář (pro phishingové incidenty, příloha III) nebo rychlý checklist slouží jako dokumentace incidentu.

8.2 Návrh řízení incidentu – phishingového útoku, model PICERL



Obrázek 13 Návrh řízení incidentu pomocí modelu PICERL
(zdroj: vlastní)

Mezi další nástroje, které napomáhají rozhodovacímu procesu je tzv. „**Two Minute Incident Assessment Reference**“, což je dvouminutové hodnocení incidentu s cílem zamezit podcenění situace a připravit se na vlastní řešení incidentu (FR Secure, 2024). Tato metoda je vhodná pro pracovníky helpdesku organizace nebo slouží pro stručné shrnutí incidentu pro vedení organizace – bez uvedení technických detailů.

Dvouminutové hodnocení incidentu – phishing

Krok 1: Potenciální dopad

Cíl: Rychle zjistit, jaké důsledky incident nese.

- **Jaká je hodnota aktiva** – *např. napadený účet patří účetní / vysoké riziko (přístup k citlivým údajům).*
- **Nejhorší scénář, který může nastat** – *únik osobních údajů, poškození reputace.*
- **Jaká je jeho pravděpodobnost** – *např. uživatel klikl na odkaz, ale nic nezadal = nízké riziko, nebo naopak zadal přihlašovací údaje = vysoké riziko úniku.*

Krok 2: Pravděpodobná příčina

Cíl: Získat rychlou představu, co se stalo a jaký je původ problému.

- **Uživatel obdržel podezřelý e-mail** – *klikl na odkaz a byl přesměrován na falešnou stránku.*
- **E-mail nezachytil firewall / filtr na SPAM** – *možné selhání detekce.*

Krok 3: Nápravná opatření

Cíl: Zabránit dalším škodám co nejdříve.

- **Okamžité kroky** – *reset hesla, zablokování přístupu, izolování zařízení.*
- **Zmírnění dopadu** – *analýza přístupu, monitoring účtu, izolace příloh.*

Krok 4: Komunikace s vedením

Cíl: Stručně a věcně informovat klíčové osoby (Vedení).

- **Co se stalo:** *phishingový útok na účetní, kliknutí na podezřelý e-mail, možný únik dat.*
- **Co to znamená:** *možné ohrožení přístupu, riziko neoprávněných fakturací.*
- **Co děláme:** *účet je zablokován, přístup odebrán, komunikace zahájena.*

Z uvedených kroků dále vyplývá postup pro technická nebo organizační opatření. Dochází k restriktivním a bezpečnostním zásahům zabráňujícím dalšímu šíření škodlivého mailu (kódu, URL), kupříkladu:

- **Zablokování a omezení přístupu kompromitovaného účtu s cílem ukončení aktivních relací.**
- **Odstranění phishingového mailu jako prevence snížení dalšího šíření.**
- **Zablokování podvodných URL a IP adres pro zabránění sekundárního kontaktu se zdrojem.**
- **Prověření zařízení na backdoor / malware detekce a odstranění dalších potencionálních hrozeb.**
- **Síťový dohled nad účtem a systémem, zda nedochází k opětovnému pokusu o jeho zneužití.**
- **Oznámení incidentu splnění oznamovací povinnosti vůči správním orgánům.**

Přehled správních orgánů pro hlášení incidentů v ČR pro oblast kybernetické a informační bezpečnosti jsou uvedené dále (tab. 11):

Tabulka 12 Vybrané správní orgány pro hlášení incidentů

Organizace	Kdy se incident hlásí?	Typ hlášených incidentů	Pro koho je určeno?
NÚKIB (Národní úřad pro kybernet. a informační bezpečnost)	Spadá-li organizace pod zákon č. 181/2014 Sb. o KB	Kybernetické incidenty, s dopadem na funkčnost nebo dostupnost syst. klíč. pro chod státu (kritickou infrastrukturu)	Organizace oblasti kritické infrastruktury (KI), veřejné spr., nemocnice apod.
ÚOOÚ (Úřad pro ochranu osobních údajů)	Došlo-li k úniku osobních údajů v důsledku BI (např. phishing, ransomware)	Porušení zásad zabezp. osobních údajů (dle GDPR – čl. 33)	Organizace, které zpracovávají osobní údaje. Povinnost hlášení do 72 hodin od zjištění incidentu.
Policie ČR NCOZ	Je-li incident trestným činem – např. podvod, vydírání.	Kriminální kybernetická činnost (např. phishing s finančním dopadem)	Trestní oznámení může podat jednotlivec nebo organizace
CERT.CZ (Národní tým CSIRT – provoz. CZ.NIC)	Nepovinné hlášení – sdílení inf. o útocích a hrozbách, spolupráce při řešení.	Bezpečnostní incidenty – malware, phishing, DoS útoky apod.	Soukromý i veřejný sektor, ISP, univerzity apod.

(zdroj: vlastní)

Následně jsou stanoveny role a odpovědnost pro reakci na bezpečnostní incidenty (ISO/IEC 27035, 2023). Velmi účinný nástroj pro jejich stanovení je v rámci řízení bezpečnostních incidentů je model RACI (PMI, 2017):

- **R (Responsible)** – označuje výkonnou roli (kdo je vykonavatelem odpovědným za daný úkol).
- **A (Accountable)** – Kdo nese odpovědnost za výsledek.
- **C (Consulted)** – S kým je aktivita konzultována (pro upřesnění informací).
- **I (Informed)** – Kdo má být informován o průběhu nebo výsledku.

Tyto vychází z postupů a organizační struktury organizace a pro řízení incidentu – phishingového útoku jsou role a zodpovědnost stanoveny takto (tab. 12):

Tabulka 13 RACI model phishingového útoku

<i>Fáze incidentu / Role</i>	<i>Koncový uživatel/-é</i>	<i>Helpdesk</i>	<i>IT oddělení</i>	<i>Vedoucí IT</i>	<i>Právní odd., HR, PR</i>	<i>Management organizace</i>
<i>Identifikace – nahlášení incidentu</i>	<i>R</i>	<i>I</i>	<i>C</i>	<i>A</i>	<i>I</i>	<i>I</i>
<i>Analýza dopadu (škod)</i>	<i>I</i>	<i>C</i>	<i>R</i>	<i>A</i>	<i>I</i>	<i>I</i>
<i>Informování uživatelů</i>	<i>I</i>	<i>R</i>	<i>C</i>	<i>A</i>		<i>I</i>
<i>Zablokování šíření škodlivého obsahu</i>		<i>I</i>	<i>R</i>	<i>A</i>	<i>I</i>	
<i>Odstranění – odebrání přístupu</i>		<i>I</i>	<i>R</i>	<i>A</i>		<i>I</i>
<i>Obnova – ze záloh a návrat k běžnému provozu</i>	<i>I</i>	<i>I</i>	<i>R</i>	<i>A</i>	<i>I</i>	<i>I</i>
<i>Zajištění důkazů</i>		<i>C</i>	<i>R</i>	<i>A</i>	<i>C</i>	<i>I</i>
<i>Vyhodnocení – Lessons Learned</i>	<i>C</i>	<i>C</i>	<i>R</i>	<i>A</i>	<i>C</i>	<i>I</i>

(zdroj: vlastní)

8.3 Model šíření phishingového útoku

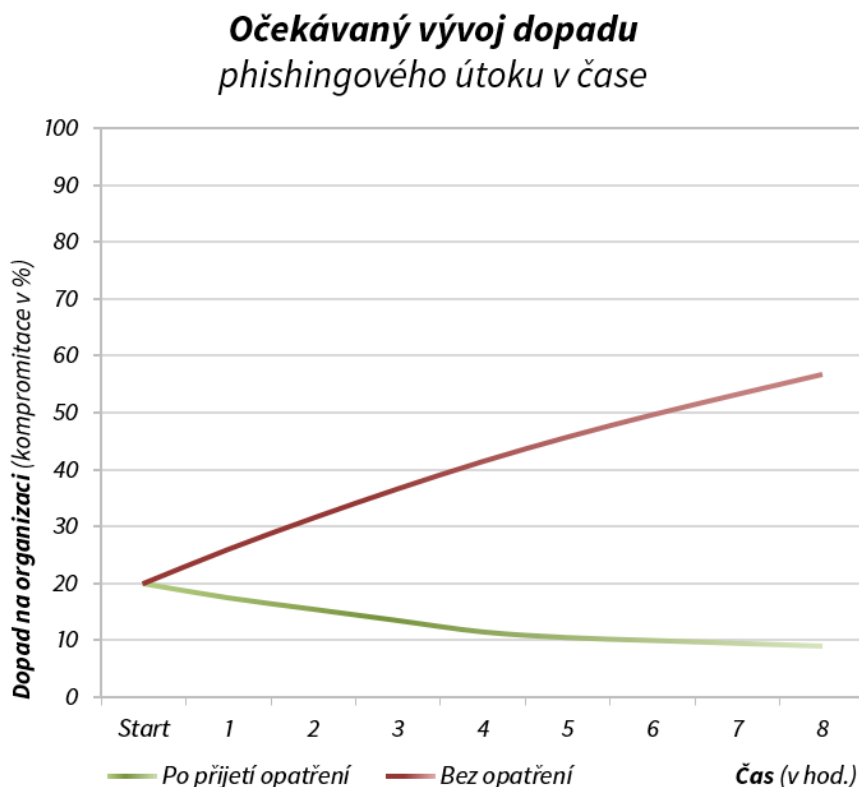
Pro ilustraci očekávaného dopadu bezpečnostního incidentu a jeho následného šíření v organizaci byl vytvořen model, který znázorňuje dva rozdílné scénáře (obr. 14):

- První, znázorňující dopad na organizaci bez přijetí opatření, kdy se phishing volně šíří organizací bez aktivní reakce.
- A druhý, se správně nastavenými opatřeními, kdy je u organizace incident včas detekován a řízen.

Tento model slouží k pochopení dynamiky vývoje incidentu a důležitosti přijatých opatření.

Pro výpočet dopadu incidentu na organizaci vycházíme z předpokladu, že se jedná o středně velkou organizaci s celkovým počtem 400 zaměstnanců. Přičemž v okamžiku odhalení incidentu (označeno jako „Start“) bylo kompromitováno 80 zařízení, tj. 20 % celé organizace. Tento údaj vychází z řízeného rozhovoru, příloha I.

Následně je předpokládáno, že v každé následující hodině dojde ke kompromitování 7,5 % dosud neinfikovaných zařízení.



Obrázek 14 Očekávaný vývoj dopadu útoku
(zdroj: Informace managementu organizace, 2023)

Přístup reflektuje důležitost a včasnost reakce a znázorňuje vývoj incidentu v závislosti na čase a demonstruje rozdíl mezi včasným zásahem a pasivitou.

Stanovení výpočtu: Po prvotním odhalení útoku, došlo ke kompromitování 80 zařízení. V následující hodině k napadení dalších 24 zařízení, což představuje 7,5 % z dosud nezasažených zařízení. Celkový počet kompromitací tak po první hodině vzrostl na 104, což představuje 26 % z celkového počtu. Hodnoty znázorňující další vývoj v čase jsou uvedeny (v tab. 14):

Tabulka 14 Model vývoje phishingového útoku v čase

Čas	Nové komprom.	Zbývající nezasaž.	Bez opatř. (v %)	Celkem komprom.	Přij. opatř. (v %)	Celkem komprom.
Start	0	320	20	80	20	80
1	24	296	26	104	17,5	70
2	22	274	31,5	126	15,5	62
3	21	253	36,8	147	13,5	54
4	19	234	41,5	166	11,5	46
5	18	216	46	184	10,5	42
6	16	200	50	200	10	40
7	15	185	53,8	215	9,5	38
8	13	171	57,2	229	9	36

(zdroj: vlastní s využitím dat organizace)

Vyhodnocení: Tento model poskytuje rámec pro posouzení, jak kritická může být každá hodina prodlení v reakci na incident. Rozdíl mezi výpočty ukazuje dopad na organizaci a ohrožení zbývajících, útokem nedotčených zařízení.

Umožňuje vizualizovat a kvantifikovat dopady, ale především demonstruje přínos přijatých opatření pro řízení incidentů.

8.4 Kontrolní seznam – checklist (phishing)

Kapitola obsahuje seznam (checklist), který slouží jako návod pro řízení incidentu bezpečnosti informací a napomáhá spolupráci všech zúčastněných stran. Postup je rozdělen do jednotlivých fází, počínaje přípravou, přes detekci, analýzu, izolaci, odstranění a obnovu, až po závěrečné vyhodnocení incidentu (tab. 15).

Cílem je zajištění rychlé, koordinované a co nejúčinnější reakce na provedený útok, a tím minimalizovat jeho dopady na organizaci.

Tabulka 15 Kontrolní seznam pro reakci na incident

Místo: _____

Č.	Popis	Poznámka
	<i>Připravit seznam kontaktů a distribuovat jej relevantním osobám</i>	
Identifikace		
1.	Nahlášení podezřelého e-mailu (Koncový uživatel/-é)	
2.	Zachycení a zaevidování incidentu (Helpdesk)	
Analýza		
3.	Ověření zpráv a rozsahu incidentu (IT oddělení)	
4.	Informování ved. IT a aktivace kriz. postupu (IT oddělení)	
Izolace		
5.	Odpojení kompromitovaného účtu/stanice od sítě (IT oddělení)	
6.	Informování postižených uživatelů (Helpdesk)	
Odstranění		
7.	Vymazání škodlivých e-mailů a změna hesel (IT oddělení)	
Obnova		
8.	Obnovení přístupů a systémových funkcí (IT oddělení)	
Vyhodnocení		
9.	Vypracování zprávy o incidentu (Vedoucí IT)	
10.	Revize školení a aktualizace postupů, Informování vedení organizace (Vedoucí IT)	

(zdroj: vlastní)

9 DISKUZE VÝSLEDKŮ VÝZKUMU

Cílem práce bylo pojednat o doporučených postupech k zajištění informační bezpečnosti, identifikování vhodných postupů, navržení a modelování konkrétního postupu pro řízení vybraného incidentu bezpečnosti informací. Požadované výsledky byly získány prostřednictvím řízeného rozhovoru, provedena identifikace a analýza rizik s následným porovnáním dosažených výsledků.

9.1 Výsledky řízeného rozhovoru

Nejslabším článkem organizace byl všemi dotazovanými označen lidský faktor. V jedné z odpovědí zástupce managementu zaznělo: „*Řetěz je tak silný, jak silný je jeho nejslabší článek*“ – a v tomto kontextu se význam opatření, informovanosti o aktuálních kybernetických hrozbách snoubí s nepozorností nebo rutinními pracovními návyky zaměstnanců, které zvyšují pravděpodobnost úspěšného útoku.

Ani organizace s účinnými technologickými opatřeními a postupy se bez aktivní spolupráce svých zaměstnanců neobejde. A právě lidský faktor tak zůstává klíčovým prvkem odolnosti vůči kybernetickým hrozbám.

V souladu s konstatováním respondentů a navrženými opatřeními vyvstala otázka četnosti simulace krizových situací, potřeby upřesnění některých postupů pro zajištění vyšší přehlednosti a rychlého předávání informací. Z rozhovorů vyplynula potřeba stanovit přesné komunikační postupy a pravidelné testování organizace na kybernetické incidenty. Bezpečnostní analytik se v této souvislosti vyslovil pro vytvoření jednotného rámce pro evidenci a vyhodnocení incidentů (*řízený rozhovor, 2024*). Tato databáze by následně sloužila jako základ pro návrhy simulačních cvičení, tak pro reálné útoky.

Organizace a její představitelé si uvědomují potřebu vzdělávání a dalšího rozvoje. Došlo ke změnám v oblasti řízení lidských zdrojů – od výběrových řízení, systému převzetí komunikační a výpočetní techniky až po zavedení pravidelných školení. Testování a následné vyhodnocování doznalo několika zásadních změn, které přispívá k rostoucímu povědomí zaměstnanců a jejich vnímání důležitosti kybernetické a informační bezpečnosti.

9.2 Výsledky analýzy rizik

Mezi nejvýznamnější oblasti lze jednoznačně zařadit řízení lidských zdrojů, který nese potenciál jak pro vznik rizik, tak příležitostí. Rizika – ke kterým se primárně řadí

nedostatečné nebo chybějící školení, případně nízká míra zapojení zaměstnanců a s ním související povědomí o bezpečnostních hrozbách. Příležitosti pak představují možnosti zavedení pravidelných školení a testování celé organizace a následné zažití postupů při řešení jednotlivých incidentů.

Další rizika představují rychle se vyvíjející postupy útočníků a možnost zapojení umělé inteligence, které vytváří prostředí, ve kterém je nutné přistupovat k bezpečnosti jako k dynamickému, rychle se rozvíjícímu procesu. Tyto trendy výrazně zvyšují nároky na systém detekce, ale především na rozvoj kritického myšlení zaměstnanců, např. prostřednictvím cílených školení a simulací.

ZÁVĚR

V průběhu získávání informací a následném vypracování práce vyvstaly otázky, které napomáhají naplnit jednotlivé cíle. V obecné rovině byla první z nich: „*Jaká je role lidského faktoru v řízení incidentů bezpečnosti informací v organizaci?*“

Lidský faktor má v řízení incidentů bezpečnosti informací nezaměnitelnou roli. Na jedné straně je nejzranitelnějším článkem v tomto procesu a na straně druhé také tím, kdo incident rozpozná, nahlásí, analyzuje a reaguje.

Paradox, kdy je v prvním případě zneužívána nepozornost, důvěřivost nebo nedostatek informací a v druhém pak snaha o zodpovědný a systematický přístup, aktivní spolupráci, rychlou komunikaci s cílem daný incident efektivně zvládnout.

Klíčem k úspěchu se tak jeví spojení technických opatření se vzděláváním.

Další, řekněme procesní otázkou: „*Jaké jsou hlavní překážky v implementaci účinného postupu reakce na incidenty?*“

Pomineme-li lidský faktor, který dominoval v předchozí otázce, dalším významným problémem se jeví nejasné rozdělení odpovědnosti při reakci na incident. Pro zefektivnění spolupráce mezi jednotlivými týmy by měl být nastaven komunikační systém tak, aby každý z týmu věděl, jaká je jeho role – znal svůj úkol a věděl, na koho se obrátit.

Další překážkou je absence pravidelných simulací útoků. Ty mohou být přínosné pro praktické procvičení reakce na incident, možnost zastavení a opakování scénářů, a to vše bez reálného stresu. Zaměstnanci si během simulace často uvědomí, co jim není jasné a kde se dopouštějí chyb.

Simulace mohou zároveň napomáhat k budování důvěry k nastavenému systému, a především pak mezi týmy samotnými. Lze konstatovat, že pokud incident neohrozí provoz nebo reputaci organizace, management tuto oblast zpravidla nepovažuje za prioritní – což však snižuje celkovou připravenost organizace.

Oblast školení by měla odrážet poznatky reálných útoků a nedostatků zjištěných při simulacích. Smysluplné školení má přidanou hodnotu pouze tehdy, pokud kombinuje teoretické základy s výsledky konkrétních scénářů, kdy se zaměstnanci aktivně podílí na procesech, které jim připomínají jejich vliv na bezpečnost celé organizace.

Poslední oblastí, při které vyvstala další z otázek měla aplikační charakter? „*Jaký model řízení incidentu bezpečnosti informací nejlépe vyhovuje podmínkám vybrané organizace?*“

Pozorování a rozhovory ukázaly, že je zapotřebí jednoduchého a pro všechny zaměstnance srozumitelného rámce pro řízení incidentů. Nejde ani tak o dokonale teoreticky zvládnutý model, ale spíše o jeho pochopení, tedy to, že jej zaměstnanci znají, rozumí mu a umí tyto postupy uplatňovat v praxi.

Dva přístupy k řízení incidentů bezpečnosti informací = jeden společný cíl, tím je efektivně zvládnout incident a omezit jeho dopad. Tím však určité znaky podobnosti nekončí. Ať už se organizace opírá o ISO/IEC 27035, nebo jiný, např. model OODA a PICERL, úspěch závisí na tom, zda a jak jednotlivé fáze fungují v praxi, jak jsou srozumitelné a vnímané napříč celou organizací.

Klíčem k úspěšnému řízení incidentu bezpečnosti informací zůstává nejen samotná existence postupu, ale především jeho zažití, souhra týmů a uvědomění si role každého jednotlivce. To vychází ze znalostí získaných prostřednictvím školení, nácviku a zejména důvěry. Důvěry nejen v systém, ale především člověka, který je jeho součástí.

Připravená organizace, která nestojí pouze na nástrojích a opatřeních, ale především na lidech, bude lépe připravená čelit kybernetickým hrozbám.

Bezpečnost dnes není jen otázkou technologií, ale otázkou kultury, sdílené odpovědnosti a schopnosti reagovat. Čím dříve se stane přirozenou, každodenní součástí celé organizace, tím větší je její šance čelit hrozbám s klidem a jistotou.

SEZNAM POUŽITÉ LITERATURY

AUSTRALIAN CYBER SECURITY CENTRE. *Cyber Incident Response Plan Guidance* [online]. Canberra: Australian Government, 2023. Dostupné z: https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf. [cit. 2025-02-20].

AXELOS. *ITIL Foundation: ITIL 4 Edition*. Norwich: The Stationery Office, 2019. ISBN 9780113316076.

CICHONSKI, P., MILLAR, T., GRANCE, T. a SCARFONE, K. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61 Revision 2 [online]. National Institute of Standards and Technology, 2012. Dostupné z: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final> [cit. 2025-02-10].

Cisco Systems, Inc. *What is malware?* [online]. Nedatováno. Dostupné z: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html> [cit. 2024-12-30].

CLARK, Robert M. a HAKIM, Simon. *Cyber-Physical Security*. 3rd ed. New York: Springer International Publishing, 2017. ISBN 978-3-319-32822-5.

CSIRT.CZ. *Statistiky kybernetických bezpečnostních incidentů* [online]. 2024. Dostupné z: <https://csirt.cz/cs/o-nas/statistiky/> [cit. 2024-12-10].

CZ.NIC. *Vzdělávací program CZ.NIC* [online]. 2025. Dostupné z: <https://vip.nic.cz/cs/> [cit. 2025-04-20].

ČESKÁ REPUBLIKA. *Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti*. Sbírka zákonů České republiky, 2018.

ČESKÁ REPUBLIKA. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů*. Sbírka zákonů České republiky, 2014.

ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik informační bezpečnosti*. Praha: Český normalizační institut, 2019.

EC COUNCIL. *What is Incident Response* [online]. Cybersecurity Exchange, 3.7.2024. Dostupné z: <https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response/> [cit. 2024-11-20].

ESET. *Cybersecurity Awareness Training* [online]. 2025. Dostupné z: <https://www.eset.com/us/business/cybertraining/> [cit. 2025-04-15]

ESET. *Man-in-the-Middle (MITM)* [online]. Nedatováno. Dostupné z: <https://www.eset.com/cz/slovník/co-je-to-man-in-the-middle-mitm/> [cit. 2024-12-30].

EUROPEAN PARLIAMENT AND COUNCIL. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. *Official Journal of the European Union*, L333, 2022.

FERNÁNDEZ-ALEMÁN, José L. a SEÑOR, Isabel C. a LOZOYA, Pedro Á. O. a TOVAL, Ambrosio. *Strengthening Information Technology Security through the Failure Modes and Effects Analysis Approach*. *Journal of Open Innovation: Technology, Market, and Complexity* [online]. 4(4), 55, 2018. Dostupné z: <https://jqualityinnovation.springeropen.com/articles/10.1186/s40887-018-0025-1> [cit. 2025-03-10].

FR SECURE. *FR Secure – Information Security Experts* [online]. Nedatováno. Dostupné z: <https://frsecure.com/> [cit. 2024-12-05].

GLEICK, James. *The Information: A History, a Theory, a Flood*. New York: Pantheon Books.

GORDIC spol. s r.o. *Začnete rok 2025 s CSA: 7 důvodů, proč je tento nástroj klíčový pro kybernetickou bezpečnost* [online]. 2025. Dostupné z: <https://kybez.cz/zacnete-rok-2025-s->

[csa-7-duvodu-proc-je-tento-nastroj-klicovy-pro-kybernetickou-bezpecnost/](#) [cit. 2025-01-25].

GRANCE, Tim a SCARFONE, Karen a MELL, Paul. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg: NIST, 2012. NIST Special Publication 800-61 Revision 2. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> [cit. 2025-03-01].

GREGORY, P. H. *Certified Information Security Manager All-in-One Exam Guide*. 2. vyd. McGraw-Hill Education, 2022. ISBN 978-1-260-02703-7.

INSMART. Zákon o umělé inteligenci očima experta na kybernetickou bezpečnost [online]. 2024. Dostupné z: <https://insmart.cz/zakon-akt-o-umele-inteligenci-ocima-experta-na-kybernetickou-bezpecnost/> [cit. 2024-12-30].

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association (ISACA), 2019.

ISO/IEC 27035. *Information security incident management*. Geneva: International Organization for Standardization, 2023.

JAHANKHANI, Hamid a BOWEN, Gordon a SHARIF, Mhd Saeed a HUSSIEN, Osama. *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation*. Cham: Springer Nature Switzerland, 2024. ISBN 978-3-031-52272-7.

JIRÁSEK, Petr a NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary*. 5. doplněné a upravené vydání. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, z.ú., 2022. ISBN 978-80-908388-4-0.

JOHANSEN, G. *Incident Response in the Age of Cloud: Techniques and Best Practices*. Birmingham: Packt Publishing, 2020.

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-31-7.

MICROSOFT. *Co je analýza chování uživatelů a entit (UEBA)?* [online]. Nedatováno. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-user-entity-behavior-analytics-ueba> [cit. 2025-02-05].

MICROSOFT. *Co je reakce na incidenty?* [online]. Nedatováno. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-incident-response> [cit. 2024-12-30].

MICROSOFT. *Microsoft Sentinel documentation* [online]. Redmond: Microsoft Corporation, 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/sentinel/> [cit. 2025-04-10].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB). *Základní pojmy v oblasti kybernetické bezpečnosti* [online]. Nedatováno. Dostupné z: <https://osveta.nukib.gov.cz/mod/page/view.php?id=4022> [cit. 2025-03-31].

NATIONAL CYBER SECURITY CENTRE. *Guidance on Cyber Security* [online]. 2023. Dostupné z: <https://www.ncsc.gov.uk/> [cit. 2025-01-05].

NONNEMANN, František a ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 1. vyd. Praha: Wolters Kluwer, 2022. ISBN 978-80-7676-515-3.

PMI. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. 6th ed. Newtown Square, PA: Project Management Institute, 2017. ISBN 978-1628251845.

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005.

PRAXIS FRAMEWORK. *Shewhart Cycle* [online]. Nedatováno. Dostupné z: <https://www.praxisframework.org/en/library/shewhart-cycle> [cit. 2025-01-05].

RAMAKRISHNAN, A. *Yet another phishing incident response playbook* [online]. Nedatováno. Dostupné z: <https://arjunramakrishnan.medium.com/yet-another-phishing-incident-response-playbook-83825326debb> [cit. 2024-12-20].

RUSSELL, Stuart a NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 4th US ed. Hoboken: Pearson, 2020. ISBN 9780134610993.

SANS Institute. *Incident Handler's Handbook* [online]. Nedatováno. Dostupné z: <https://www.sans.org/white-papers/incident-handlers-handbook/> [cit. 2025-02-10].

SARKER, Iqbal H. *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*. Cham: Springer Nature Switzerland, 2024. ISBN 978-3-031-54496-5.

SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. 1. vyd. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

TITAN HQ. *SafeTitan – Security Awareness Training* [online]. 2025. Dostupné z: <https://www.titanhq.com/safetitan-master-lp/> [cit. 2025-04-20].

VISITECH a.s. *Behaviorální analýza pro bezpečnost* [online]. 2024. Dostupné z: <https://www.visitech.cz/aktuality/behavioralni-analyza-pro-bezpecnost/> [cit. 2025-02-10].

WATTERS, Paul A. *Cybercrime and Cybersecurity*. 1st ed. Boca Raton: CRC Press, 2023. ISBN 978-1-032-52451-1.

WAZUH. *Wazuh: Open source security platform* [online]. Sunnyvale: Wazuh, Inc., 2024. Dostupné z: <https://wazuh.com/> [cit. 2025-04-10].

SEZNAM OBRÁZKŮ

Obrázek 1 Statistika řešených incidentů z let 2020 až 2024 (<i>zdroj: CSIRT.cz, 2024</i>)	23
Obrázek 2 IRP – Schéma OODA a „Incident Response Plan“ (<i>zdroj: EC Council, 2024</i>)	27
Obrázek 3 Přístup k řízení incidentů, model PICERL (<i>zdroj: NCI, 2024</i>)	28
Obrázek 4 Demingův cyklus PDCA (<i>zdroj: Techportal.cz, 2012</i>)	36
Obrázek 5 Opakovaný cyklus PDCA (<i>zdroj: Praxisframework.org, 2023</i>)	37
Obrázek 6 Stanovení rozsahu pro SWOT analýzu (<i>zdroj: Informace managementu organizace, 2023</i>)	46
Obrázek 7 Analýza před nápravnými opatřeními (<i>zdroj: Informace managementu organizace, 2023</i>)	46
Obrázek 8 Grafické znázornění výsledků (<i>zdroj: Informace managementu organizace, 2023</i>)	47
Obrázek 9 Porovnání výsledků analýzy (před/po přijetí opatření) (<i>zdroj: Informace managementu organizace, 2023</i>)	56
Obrázek 10 Výsledky analýzy po přijetí nápravných opatření (<i>zdroj: Informace managementu organizace, 2023</i>)	57
Obrázek 11 Porovnání výsledků analýzy (<i>zdroj: Informace managementu organizace, 2023</i>)	57
Obrázek 12 Postup řízení bezpečnostního incidentu – phishing (<i>zdroj: Medium, 2019</i>)	59
Obrázek 13 Návrh řízení incidentu pomocí modelu PICERL (<i>zdroj: vlastní</i>)	64
Obrázek 14 Očekávaný vývoj dopadu útoku (<i>zdroj: Informace managementu organizace, 2023</i>)	68

SEZNAM TABULEK

Tabulka 1 Stanovení priorit mitigace rizik řízení bezpečnostních incidentů	38
Tabulka 2 Matice rizik.....	45
Tabulka 3 FMEA před přijetím opatření (po provedeném útoku).....	49
Tabulka 4 Výsledky FMEA po přijetí opatření.....	50
Tabulka 5 Výstupy analýzy před a po přijetí opatření	51
Tabulka 6 Stanovení hypotéz	52
Tabulka 7 Přehled navrhovaných opatření.....	54
Tabulka 8 Jednotlivé fáze tvorby IRP	60
Tabulka 9 Úroveň dopadu bezpečnostního incidentu	62
Tabulka 10 Stanovení klasifikace závažnosti incidentu	62
Tabulka 11 Dopad a závažnost bezpečnostního incidentu	63
Tabulka 12 Vybrané správní orgány pro hlášení incidentů	66
Tabulka 13 RACI model phishingového útoku	67
Tabulka 14 Model vývoje phishingového útoku v čase.....	69
Tabulka 15 Kontrolní seznam pro reakci na incident	70

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3D	Trojrozměrné zobrazení (Three-Dimensional)
AI	Umělá inteligence (Artificial Intelligence)
BI	Bezpečnost informací
CERT	Tým pro řešení nouzových situací (Computer Emergency Response Team)
CIA	Důvěrnost, integrita, dostupnost (Confidentiality, Integrity, Availability)
CSIRT	Tým reakce na počítačové bezpečnostní incidenty
FMEA	Analýza možných poruch a jejich následků (Failure Mode and Effects Analysis)
GDPR	Nařízení o ochraně osobních údajů
HR	Lidské zdroje (Human Resources)
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDS/IPS	Systém detekce a prevence narušení (Intrusion Detection/Prevention System)
IP	Adresa, Internetový protokol
IRP	Plán reakce na incidenty (Incident Response Plan)
IRT	Tým reakce na incidenty (Incident Response Team)
ISMS	Systém řízení bezpečnosti informací (Information Security Management System)
ISO	Bezpečnostní manažer (Information Security Officer)
ISO/IEC	Mezinárodní norma pro IT a bezpečnost
IT	Informační technologie

IoC	Indikátory kompromitace (Indicators of Compromise)
MFA	Vícefaktorové ověřování (Multi-Factor Authentication)
MITM	Útok typu „člověk uprostřed“ (Man-in-the-Middle)
MITRE ATT&CK	Dostupná znalostní databáze technik, chování útočníků (MITRE Adversarial Tactics, Techniques, and Common Knowledge)
NCOZ	Národní centrála proti organizovanému zločinu
NIS2	Směrnice kybernetické bezpečnosti
NIST	Národní institut pro standardy a technologie (National Institute of Standards and Technology)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OODA	„Pozoruj, orientuj se, rozhodni, jednej“ (Observe, Orient, Decide, Act)
PDCA	Demingův cyklus „Plánuj, dělej, kontroluj, jednej“ (Plan-Do-Check-Act)
PICERL	„Příprava, identifikace, zadržení, odstranění, obnova, poučení“ (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned)
PR	Vztahy s veřejností (Public Relations)
RACI	Stanovení rolí a odpovědnosti (Responsible, Accountable, Consulted, Informed)
RCA	Analýza příčiny problému (Root Cause Analysis)
RJ-45	Standardizovaný konektor pro síťové připojení
RPN	Prioritní číslo rizika (Risk Priority Number)
TTPs	Taktiky, techniky a postupy (Tactics, Techniques, and Procedures)
UEBA	Analýza chování uživatelů a entit (User and Entity Behavior Analytics)
URL	Identifikátor zdroje, odkaz

ZoKB

Zákon o kybernetické bezpečnosti

ÚOOÚ

Úřad pro ochranu osobních údajů

SEZNAM PŘÍLOH

Příloha P I: Řízený rozhovor

Příloha P II: Návrh plánu řešení incidentu pro phishingový útok pomocí modelu PICERL

Příloha P III: Incident Response Plan (IRP) – Phishing aneb návrh formuláře „Plán reakce na bezpečnostní incident (IRP) typu phishing“

PŘÍLOHA P I: ŘÍZENÝ ROZHOVOR

Řízené rozhovory byly jedním z nejprínosnějších zdrojů informací pro získání uceleného přehledu na technickou a personální připravenost a schopnost rychlé reakce na bezpečnostní incidenty. Na základě požadavku organizace byla při zpracování rozhovorů stanovena podmínka pro zachování anonymity. Rozhovory proběhly s představitelem vedení organizace (A), specialistou IT (B) a bezpečnostním analytikem organizace (C).

Při rozhovoru byl kladen důraz na dodržení okruhů otázek a vytvořen prostor pro jejich doplnění příklady z praxe. Otázky byly rozděleny do dvou částí, kdy odpovědi u společných otázek umožnily porovnání a vymezení názorových rozdílů mezi respondenty. A cílené otázky pro oblast každého z respondentů.

1. Myslíte si, že je vaše organizace náležitě připravena na řešení incidentu bezpečnosti informací nebo spatřujete prostor pro zlepšení?

A: „Osobně si myslím, že ano, ale prostor pro zlepšení je, s ohledem na neustále se objevující nové hrozby, nutností. Bezpečnost musí být dynamický, nikoliv statický proces!“

B: „Z technického hlediska jsme poměrně dobře připraveni. Rezervy spatřuji v přípravě personálu.“

C: „Organizace stojí na dobrých základech. Zlepšit lze oblast připravenosti, simulace, pravidelných cvičení a systém vyhodnocení.“

2. Jaké bezpečnostní incidenty ohrozily v minulosti vaši organizaci a které typy považujete za nejzávažnější?

A: „Byl to phishingový útok, při kterém došlo k úniku citlivých informací. Mezi nejzávažnější považuji incidenty, které ohrožují naši pověst a důvěru klientů.“

B: „Ano, došlo k pochybení ze strany zaměstnance naší organizace a tento incident přispěl ke změnám přístupu a zásad v oblasti přidělování IT zařízení a systému pravidelných školení. Každému incidentu musí být věnována náležitá pozornost bez ohledu na to, o jaký typ se jedná!“

C: „Na nedostatečné opatření a porušování zásad bezpečnosti jsem upozorňoval, stačilo reflektovat naše doporučení. Nejzávažnější typy jsou ty, které se nedaří ihned odhalit – skrytý průnik, kompromitace účtů, postupné šíření uvnitř sítě.“

3. Jaké kroky k nápravě organizace učinila, aby se opět nestala cílem útoků a bezpečnostní incidenty ji opět neohrozily?

A: *„Došlo k aktualizaci reakčních plánů a užší spolupráci mezi našimi odděleními. Byl nastaven systém pravidelných školení formou e-learningových kurzů a simulace.“*

B: *„Plán pro reakci na bezpečnostní incidenty pravidelně aktualizujeme. Účastníme se odborných konferencí. Na základě bezpečnostní politiky organizace došlo k úplnému zákazu používání vyměnitelných zařízení a přenos dat probíhá prostřednictvím zabezpečeného úložiště.“*

C: *„Navrhl jsem vytvořit metodiku pro sjednocení postupů, systému komunikace a informování při řešení incidentu. Doporučil realizovat opatření pro nově příchozí zaměstnance a přezkoumávat plán pro reakci minimálně jednou ročně nebo ihned po závažném incidentu. Zapracovat do něj získané poznatky, a to včetně těch ze simulací.“*

4. Probíhají simulace reakce na incidenty (konkrétně phishing)? Jak často jsou prováděny? A jaký je na ně u organizace ohlas?

A: *„Ano, vedení je jim nakloněno, ale zároveň přiznávám, že to není úplně snadné, přesto mají v organizačním plánu své místo. Probíhají cca. dvakrát ročně se smíšeným ohlasem u zaměstnanců.“*

B: *„Prováděli jsme simulaci phishingu a obnovu ze záloh. Probíhají dvakrát ročně. Největší překážkou je zapojení netechnických týmů – které to považují za zbytečné. Technicky nám to odkrývá nedostatky a pomáhá najít slabá místa.“*

C: *„Simulace považuji za klíčové. Pravidelně je vyhodnocuji a spolupracuji s ostatními odděleními a výsledky předkládám vedení. Ohlasy se různí napříč celou organizací, ale většina zaměstnanců si uvědomuje jejich význam a důležitost.“*

5. Můžete zveřejnit jejich výsledky?

A: *„Ano, bylo mi sděleno, že pětina našich zaměstnanců klikla na podvržený odkaz. S ohledem na přijatá opatření to nepovažuji za ideální výsledek.“*

B: „Poslední výsledky ukazují, že přibližně 18% zaměstnanců zareagovalo na podvodný email. Nejčastěji se jednalo o nové kolegy a pracovníky administrativy.“

C: „Výsledek nedávné simulace byl znepokojující, 20% uživatelů nejenže kliklo na odkaz, ale 5% dokonce zadalo své přihlašovací údaje! Na základě těchto zjištění jsme upravili obsah dalších školení. V rámci naší organizace se snažíme udržovat pozitivní přístup a já mohu konstatovat, že tento trend má klesající tendenci.“

Otázky pro představitele vedení organizace:

1. Do jaké míry vnímáte kybernetickou bezpečnost jako vaši prioritu?

A: „V současnosti řadíme kybernetickou bezpečnost mezi klíčové oblasti. Několik varování, které jsme v minulosti nechali bez povšimnutí, nakonec vyústilo v reálný incident. Ten nám ukázal, že opomenutí a přehlížení této oblasti může mít vážné dopady na celou organizaci.“

2. Jaké máte zkušenosti s krizovou komunikací v souvislosti s bezpečnostními incidenty?

A: „S krizovou komunikací v souvislosti s bezpečnostními incidenty zkušenosti máme, avšak spoléháme na podporu našeho PR oddělení.“

3. Jakým způsobem je v organizaci zajištěna objektová a fyzická bezpečnost?

A: „Organizace má ve své struktuře vyčleněnou skupinu zodpovědnou za dodržování pravidel režimu vstupů a vjezdů do areálu. Přístup je umožněn pouze na základě povolení nebo přidělené čipové karty. Využíváme elektronické zabezpečovací systémy a jasně definovaný systém pro vstup do areálu a klíčových prostor organizace.“

4. Máte stanoveny pravidla pro zabezpečení zaměstnanců výpočetní a komunikační technikou?

A: „Ano, při nástupu zaměstnance dochází k přidělení výpočetní a komunikační techniky potřebné pro výkon jeho funkce, kterou si převezme proti podpisu na evidenčním listu. Stejný postup se uplatňuje při obměnách nebo při ukončení

pracovního poměru, kdy zařízení vrací. V rámci organizace využíváme koncová zařízení společnosti Apple.“

5. Má organizace stanovenou strategii pro řízení lidských zdrojů a zajištění stability na klíčových bezpečnostních pozicích?

A: „Ano, organizace má stanovenou strategii řízení lidských zdrojů, která se zaměřuje na všechny klíčové pozice. Snažíme se o personální stabilitu prostřednictvím motivačních prvků nebo a možností dalšího osobního rozvoje.“

Otázky pro IT specialistu:

1. Kdo je v rámci organizace primárně zodpovědný za řízení incidentů?

B: „Za řízení incidentů nese odpovědnost IT oddělení. První kontakt obvykle probíhá prostřednictvím helpdesku, poté je incident vyhodnocen a předán podle možného dopadu a závažnosti.“

2. Jak rychle např. izolujete napadené účty nebo zařízení?

B: „Dočasné zablokování uživatelského účtu zpravidla probíhá do 15 minut od potvrzení incidentu. Fyzické odpojení zařízení ze sítě pak bývá realizováno v řádu několika minut.“

3. Jaké nástroje používáte pro správu přístupových oprávnění a monitoring síťové aktivity?

B: „Infrastruktura na straně serveru je postavena na systémech Linux a Windows. Pro správu oprávnění využíváme kombinaci systémů Active Directory, Open LDAP a Kerberos. Sledování síťové aktivity zajišťujeme pomocí nástrojů Wireshark nebo Security Onion.“

4. Jakým způsobem máte nastaven systém zálohování a jak často zálohujete?

B: „Zálohování uživatelských dat probíhá primárně na lokální úložiště, a to denně v nočních hodinách. Kompletní zálohy jsou prováděny jednou týdně. Systém je nastaven tak, aby bylo možné obnovení systémů ze záloh do 24 hodin.“

Otázky pro bezpečnostního analytika:

1. Jaká je vaše role v rámci řízení incidentů?

C: „Koordinuji celý proces řízení incidentů – od identifikace, přes zadržení až po obnovu a následné vyhodnocení. Nastavuji pravidla a dohlížím nad jejich dodržováním.“

2. Jak probíhá klasifikace incidentů a určování jejich závažnosti?

C: „Incidenty klasifikujeme na základě jejich dopadu a závažnosti, kdy používáme rozmezí od nízké po kritickou úroveň. Hodnocení vychází z posouzení narušení důvěrnosti, integrity a dostupnosti. Kromě počáteční klasifikace zohledňujeme závěrečnou fázi, kdy analyzujeme příčiny a navrhujeme preventivní opatření.“

3. Využíváte při řízení incidentu bezpečnosti informací nějakou metodiku?

C: „Ano, máme připravené plány pro řízení bezpečnostních incidentů, které průběžně aktualizujeme. Využíváme metodický rámec dle ISO/IEC a postupujeme dle předem připravených kontrolních seznamů. Ve fázi detekce pracujeme s analýzou příčin (RCA) a maticí pro určení závažnosti incidentu. Pro hodnocení a plánování dalšího postupu pak základní analýzu rizik. Samotný proces řízení incidentu stavíme na kombinaci OODA nebo PDCA.“

4. Provádíte pravidelně testování odolnosti zařízení vůči útokům (např. penetrační test)?

C: „Ano, spolupracujeme s externí firmou, která provádí penetrační testy v pravidelných ročních intervalech. Výsledky těchto testů slouží pro interní potřebu organizace a podléhají mlčenlivosti. Víc bych se k této otázce nevyjadřoval.“

Poslední dvě otázky závěrem pro všechny respondenty:

1. Jaký význam přikládáte výběru, prevenci a vzdělávání lidských zdrojů v oblasti bezpečnosti informací? Může lidský faktor ovlivnit celkovou bezpečnost organizace?

A: „Naprostý základ. Pokud zaměstnanci nerozumí své roli v této oblasti nebo nejsou vhodně vybráni, je celý systém v ohrožení. Říká se, že řetěz je tak silný, jak silný je jeho nejslabší článek – a v našem případě to velmi často bývá lidský faktor.“

B: *„Můžeme mít sebelepší a nejvýkonnější technologie, ale když uživatel naletí, použije slabé heslo, jsme v problému. Podle mě je důležité testování, školení, ale nikdy nesmí být pouze formální.“*

C: *„Z pohledu bezpečnostních strategií je lidský faktor největší slabina i největší příležitost. Prevence, přezkoušení a cílené vzdělávání – to vše musí být nedílnou součástí systému. Selhání jedince může narušit činnost celé organizace.“*

2. Pokud byste mohl změnit jedinou věc v oblasti řízení bezpečnostních incidentů ve vaší organizaci, co by to bylo – a proč právě to?

A: *„Zavedl bych častější simulace krizových situací. Věřím, že by to všem zúčastněným pomohlo pochopit svou roli.“*

B: *„Zpřehlednil bych některé postupy. Občas nevíme, komu co předat a v krizové situaci nás to stojí cenný čas.“*

C: *„Jsem pro vytvoření jednotného systému evidence a vyhodnocování incidentů. Bez dat a historie se nemůžeme efektivně zlepšovat.“*

PŘÍLOHA P II: NÁVRH PLÁNU ŘEŠENÍ INCIDENTU PRO PHISHINGOVÝ ÚTOK POMOCÍ MODELU PICERL

Nedílnou součástí tohoto procesu je komunikace mezi jednotlivými stranami, kdy sdílení informací urychluje reakci na incident a snižuje riziko jeho dopadu. Zabraňuje také vzniku informačního šumu.

Zainterесované strany pro řízení incidentu bezpečnosti informací jsou:

- Koncový uživatel/-é.
- IT oddělení, helpdesk organizace a vedoucí oddělení IT.
- Oddělení pro řízení lidských zdrojů (HR), tiskové a komunikační oddělení (PR) a právní oddělení.
- Management organizace.

1. fáze – „Příprava na incident“ během této fáze týmy připravují prostředky a opatření pro rychlou reakci na vzniklý incident (Cyber Incident Response Plan Guidance, 2023).

<i>Tým / zainter. strana</i>	<i>Popis</i>	<i>Otázky</i>	<i>Akce</i>
<i>Koncový uživatel/-é</i>	-	-	-
<i>Helpdesk</i>	• Přípravenost reagovat na incidenty.	• Známe své povinnosti? • Potřebuji další školení?	• Reakce a postupy. • Absolvovat školení.
<i>IT oddělení</i>	• Zajišťuje funkčnost a aktualizaci syst.	• Jsou systémy aktuální? • Využíváme nové funkce? • Potřebujeme školení?	• Provéřit aktualizace. • Provéřit. • Účast na školeních.
<i>Vedoucí IT</i>	• Zajišťuje aktuálnost a funkčnost plánu IRP. • Příprava CSIRT týmu.	• Je plán aktuální? • Jsou lidé proškolení? • Vědí, co dělat?	• Provést cvičení. • Zajistit školení. • Pravidelné schůzky týmu.
<i>Právní odd., HR, PR</i>	• Zajišť. soulad s předpisy a zákony. • Vytváření komunikač. šablon.	• Je nutné doplnění právních podkladů? • Potřebujeme školení?	• Sledovat legislativu. • Připravit šablony. • Účast na školeních.
<i>Management organizace</i>	-	• Jsou nové zákony nebo vyhlášky, se kterými je potřeba se vypořádat?	-

2. fáze – „Identifikace (detekce) incidentu“ je vyhodnocením potencionálního incidentu a jakmile je tento detekován, je pro každý nahlášený incident vytvořen „Záznam o incidentu“ (Cyber Incident Response Plan Guidance, 2023).

Tým / zainter. strana	Popis	Otázky	Akce
Koncový uživatel/-é	• Může nahlásit podezř. chování nebo výpadky syst./služby. • Nahlásit incident.	• Obdržel jsem podezřelý e-mail? • Proč nefunguje přístup k datům nebo účtu?	• Nahlásit problém nebo podezření na phishing na helpdesk.
Helpdesk	• Monitoruje požadavky uživatelů a identifikuje možné bezpečnostní incidenty.	• Zaznamenali jsme více podobných hlášení? • Je třeba předat incident?	• Vytvoř. záznam o incidentu a přeposlat relevantnímu týmu k dalšímu posouzení.
IT oddělení	• Vyhodnocuje incident z pohledu technických událostí (např. firewall, IDS/IPS).	• Ovlivnění dat, služeb? • Detekovaly systémy podezřelé aktivity?	• Provést technickou analýzu, identifikovat poškozené prvky incidentu. • Spolupracovat s týmy.
Vedoucí IT	• Je informován při před. incidentu mezi týmy.	-	-
Právní odd., HR, PR	• Nezapojuje se, jen v příp. zajištění interní/externí komunikace.	-	-
Management organizace	• Je informován pouze při závažném incidentu.	-	-

3. fáze – „Analýza a reakce (Izolace, zadržení)“ týmy analyzují možný dopad a rozsah škod, který incident způsobí a podle těchto veličin se řešením incidentu pověří jeden nebo více týmů (Cyber Incident Response Plan Guidance, 2023).

Tým / zainter. strana	Popis	Otázky	Akce
Koncový uživatel/-é	• Poskytuje informace týkající se incidentu podle potřeby.	• Co incidentu předcházelo? • Jak jsem reagoval?	• Poskytnout inf. helpdesk.
Helpdesk	• Komunikují s uživatelem. • Klade otázky. • Incident dokumentuje. • Předává dále.	• Klikl uživatel na odkaz? • Otevřel přílohu? • Navštívil podezřel. URL? • Byl odepřen přístup?	• Aktualizovat záz. o inc. • Shromáždit informace. • Určit rozsah dopadu. • Předat IT oddělení. • Příp. incident uzavřít.
IT oddělení	• Provádí analýzu logů, hledá stopy a důkazy. • Koordinuje incident a vyhodnocuje rozsah škod.	• Byla identifikována podezřelá aktivita? • Jaký je rozsah dopadu? • Byl kompromitován server nebo zařízení?	• Provést analýzu loC. • Určit rozsah incidentu. • Hlásit při podezř. na TČ. • Příp. incident uzavřít.
Vedoucí IT	• Koordinuje komunikaci s vedením.	• Došlo ke ztrátě dat? • Je nutné spustit plán obnovy? • Byl incident TČ?	• Informovat vedení. • Schválit plán obnovy. • Vydat varování.

	Schvaluje zásadní rozhodnutí a aktivuje plán obnovy.		Koordinovat právní a HR podporu.
Právní odd., HR, PR	- Vyhodnocuje právní důsledky. - Porušení pravidel a dopad na reputaci.	- Došlo k právnímu porušení? - Kdo porušil pravidla? - Došlo k poškození značky?	- Posoudit odpovědnost zaměstnanců. - Připravit komunikaci (PR).
Management organizace	Je informován pouze při závažném incidentu.	- Byly ovliv. klíč. funkce? - Má incident dopad na reputaci? - Je třeba kontaktovat úřady?	- Koordinuje reakci. - Rozhoduje o hlášení. - Provádí alokaci zdrojů a komunikaci navenek.

4. fáze – „Odstranění“ je omezení dopadů incidentu a zabránění jeho šíření ve zbytku organizace (Cyber Incident Response Plan Guidance, 2023).

Tým / zainter. strana	Popis	Otázky	Akce
Koncový uživatel/-é	Pokračuje ve spolupráci s týmy.	-	Spolupracovat s řešiteli incidentu dle potřeby.
Helpdesk	- Udržuje komunikaci s dotčenými uživateli a informuje je o dopadu. - V případě potřeby zajišťuje náhradní zařízení.	- Je třeba informovat uživ. o nedostupnosti systémů nebo dat? - Je třeba vydat náhradní zařízení?	- Informovat uživatele o výpadech. - Udržovat kontakt po dobu řešení inc. - Připravit a vydat nové zařízení.
IT oddělení	- Koordinuje izolaci incidentu. - Odpojuje kompromit. zařízení a deaktivuje účty. - Odstraňuje příčiny inc. - Instaluje záplaty. - Připravuje nové servery a obnovuje systémy.	- Lze izolovat incident bez narušení provozu? - Které systémy byly zasaženy? - Zůstávají v síti napadené zař./účty? - Jsou systémy záplatovány?	- Odpojit zařízení, deaktivovat účty. - Změnit hesla. - Provést obraz systému. - Informovat zainteres. strany. - Odstranit malware. - Aplikovat záplaty. - Deaktivovat účty. - Zálohovat systémy. - Informovat vedoucího IT.
Vedoucí IT	- Hodnotí nedostatky v kontr. mechanismech a navrhuje zlepšení. - Schvaluje implementaci nových nebo aktualiz. bezpečnostních opatř.	- Jsou stávající bezp. opatření dostatečná? - Je třeba zavést nové nebo aktualizovat stávající bezp. kontroly?	- Informovat vedení, navrhnout posílení opatření. - Schválit dočasná řešení. - Schválit navržená opatření a řešení identif. slabín.
Právní odd., HR, PR	- PR komunikuje s veřejností. - Právní a HR oddělení pokračují v přijatých opatřeních. - Zvažuje nové nálezy a pokr. ve stávajících práv. a komunikač. krocích.	- Je třeba veřejné nebo cílené komunikace? - Musí pokračovat právní nebo HR kroky? - Vedou nové poznatky k aktualizaci právních nebo HR kroků?	- Pokračovat v právních a HR úkonech. - Veřejně komunikovat kroky k omezení dopadu incidentu. - Vyhodnotit nové nálezy a případně aktualizovat postupy, jinak pokr. dle zavedených procesů.

Management organizace	Rozhoduje o odstavení kritických systémů a schvaluje opatření dle potřeby.	- Musí být klíčové systémy odstaveny? - Kdo další musí být informován?	- Rozhodnout o odstavení systémů. - Schválit kroky pro komun. navenek. - Schvalovat zásadní opatření dle potřeby.
-----------------------	--	---	---

5. fáze – „Obnova“ týmy zahájí obnovení všech systémů (ze záloh, nová instalace, záplaty) zařízení nebo účtů dotčených incidentem. Po obnově systémů do normálního provozu ověří jejich funkčnost (Cyber Incident Response Plan Guidance, 2023).

Tým / zainteres. strana	Popis	Otázky	Akce
Koncový uživatel/-é	Pokračuje ve spolupráci s týmy.	-	Spolupracovat s IT týmem a helpdeskem dle pokynů.
Helpdesk	Komunikuje s uživateli, informuje je o obnovení provozu a případných změnách.	- Je třeba informovat uživatele? - Jsou informace v záznamu o incidentu aktuální?	- Informovat uživatele o obnovení provozu, změnách a nových postupech. - Vydat nové zařízení nebo přístupy. - Aktualizovat záz. o inc.
IT oddělení	Obnovuje systémy, provádí testování, zajišťuje návrat k běžnému provozu.	- Je třeba obnovit další systémy? - Byl incident vyřešen?	- Obnovit systémy. - Provést testování. - Informovat vedoucího IT o možných procesních změnách.
Vedoucí IT	Posuzuje kontrolní mechanismy a informuje vedení o obnovení provozu.	Je třeba upravit postupy nebo opatření?	Zrevidovat opatření, informovat vedení o obnovení provozu.
Právní odd., HR, PR	Dokončují související procesy, dokumentují opatření a případné důsledky.	- Je třeba zahájit disciplinární řízení vůči zaměstnancům? - Jak komunikovat výstupy incidentu?	- Právní: Uzavřít právní procesy. - HR: Zaznamenat kázeňská opatření. - PR: Informovat veřejnost o vyřešení incidentu.
Management organizace	Nemá přímé úkoly, ale zůstává informován a schvaluje klíčová rozhodnutí dle potřeby.	-	Informován vedením IT.

6. fáze – „Poučení“ zahrnuje analýzu příčin, kterou provádějí odpovědné týmy společně s dalšími zúčastněnými stranami. Při ní jsou vyhodnocovány záznamy o incidentu a veškeré dostupné informace (Cyber Incident Response Plan Guidance, 2023).

Tým / zainteresovaná strana	Popis	Otázky	Akce
Koncový uživatel/-é	Může poskytnout inf. pro zprávu o incidentu a účastnit se školení.	- Co se stalo? - Co se změnilo? - Co jsme se naučili?	- Zodpovědět případné dotazy. - Účastnit se školení a zvýšení povědomí.
Helpdesk	Účastní se zpětného vyhodnocení reakce na incident.	- Jak jsme reagovali? - Co by se dalo zlepšit?	- Účastnit se hodnotících schůzek. - Sdílet poznatky a aktual. procesy.
IT oddělení	Podporuje vyhodnocení incidentu a navrhuje zlepšení v IT procesech.	- Jak jsme reagovali? - Kde jsou slabiny v procesech?	- Účast na vyhodnocení incidentu. - Aktualizace záznamu. - Návrh zlepšení.
Vedoucí IT	Koordinuje vyhodnocení incidentu, organizuje schůzky a zajišťuje zápisy.	Jak lze zlepšit reakci na incident?	Zvážit potřebu hodnotící schůzky, určit účastníky, zajistit vedení záznamu.
Právní odd., HR, PR	Podporují týmy a řeší nové poznatky z vyhodnocení.	Vyžadují se úpravy v právních, HR nebo PR postupech?	- Účast na schůzkách. - Navazující kroky dle nových zjištění. - Komunikace výstupů incidentu.
Management organizace	Podporuje týmy, sleduje vyhodnocení a schvaluje preventivní investice.	Je třeba zlepšit rozhodovací nebo schvalovací procesy?	- Účastnit se jednání. - Schválit preventivní opatření.

Poučení z incidentu (Lessons Learned) uzavírá cyklus řízení phishingového incidentu v modelu PICERL.

PŘÍLOHA P III: INCIDENT RESPONSE PLAN (IRP) – PHISHING

Návrh plánu založen na (zdroj: ISO/IEC 27035, 2023 a FR Secure – Information Security Experts, 2024)

Plán reakce na bezpečnostní incident (IRP) „Phishing“

1. Identifikace incidentu

- **Datum a čas hlášení:** _____
- **Způsob detekce:**
 - ☐ Automatické varování (např. Gateway)
 - ☐ Nahlášené uživatelem
 - ☐ Jiné: _____
- **Zdroj e-mailu (odesílatel / doména):** _____
- **Předmět e-mailu:** _____
- **Příložené soubory / odkazy:**
 - ☐ Ano – popis: _____
 - ☐ Ne

2. Interakce uživatele

- **Otevřel uživatel e-mail?**
 - ☐ Ano
 - ☐ Ne
- **Klikl uživatel na odkaz?**
 - ☐ Ano
 - ☐ Ne
 - ☐ Není známo
- **Byly vyplněny údaje (např. přihlašovací)?**
 - ☐ Ano
 - ☐ Ne
 - ☐ Není známo
- **Došlo ke kompromitaci účtu nebo systému?**
 - ☐ Ano – popis: _____
 - ☐ Ne
 - ☐ Vyšetřuje se

3. Předběžné hodnocení dopadu

- **Dopad na informační bezpečnost:**
 - ☐ Žádný
 - ☐ Nízký (ve stádiu pokusu)
 - ☐ Střední (získány přístupové údaje)
 - ☐ Kritický (ztráta dat, přístup do systému)
- **Funkční dopad:**
 - ☐ Žádný
 - ☐ Nízký (narušení části služby)
 - ☐ Střední (ztráta přístupu pro některé uživatele)
 - ☐ Kritický (výpadek klíčových služeb)

4. Klasifikace závažnosti

- Úroveň závažnosti dle matice:
 - ☐ **Úroveň 1 – Kritická**
 - ☐ **Úroveň 2 – Vysoká**
 - ☐ **Úroveň 3 – Střední**
 - ☐ **Úroveň 4 – Nízká**

Klasifikace závažnosti		Ovlivňující informační bezpečnost			
		Nízká	Střední	Vysoká	Kritická
Ovlivňující funkčnost	Nízká	Úroveň 4	Úroveň 3	Úroveň 2	Úroveň 1
	Střední	Úroveň 3	Úroveň 3	Úroveň 2	Úroveň 1
	Vysoká	Úroveň 2	Úroveň 2	Úroveň 2	Úroveň 1
	Kritická	Úroveň 1	Úroveň 1	Úroveň 1	Úroveň 1

Zvolená úroveň: _____

5. Doporučená opatření

- ☐ Reset hesla
- ☐ Izolace zařízení
- ☐ Analýza e-mailu / URL / Soubor - příloha
- ☐ Blokace domény / IP
- ☐ Upozornění dalších uživatelů
- ☐ Notifikace / Vedení
- ☐ Zahájení forenzní analýzy
- ☐ Jiné: _____

6. Odpovědná osoba a časový rámec

- Vyplnil: _____
- Datum a čas vyplnění: _____
- Další krok do: _____
- Předáno komu: _____