Kompromitující vyzařování v kontextu kybernetické bezpečnosti

Michal Gardavský

Bakalářská práce
2023

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: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Michal Gardavský**
Osobní číslo:	**L20220**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kompromitující vyzařování v kontextu kybernetické bezpečnosti**

Zásady pro vypracování

1. Zpracujte teoretický vstup do dané problematiky.
2. Analyzujte současný stav zabezpečení ve vybraném objektu z hlediska ochrany proti úniku informací.
3. Na základě provedené analýzy navrhněte opatření ke zlepšení současného stavu.
4. Ověřte aplikovatelnost navržených opatření.

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

Seznam doporučené literatury:

1. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing. ISBN 978-80-88260-39-4.
2. KOLOUCH, Jan a Pavel BAŠTA. *Cybersecurity.* Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
3. MAISNER, Martin, 2015. *Zákon o kybernetické bezpečnosti: komentář.* Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 978-807-4788-178.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 5.5.2023

Jméno a příjmení studenta: Michal Gardavský

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá problematikou kompromitujícího vyzařování. Je rozdělena na dvě části, část teoretickou a část praktickou. V teoretické části se bakalářská práce zabývá legislativní problematikou ochrany utajovaných informací a kybernetické bezpečnosti. Teoretická část dále pojednává o možnosti zneužití kompromitujícího vyzařování a také způsobu, jakým se před ním chránit. Praktická část bakalářské práce je věnována aktuální zranitelnosti vybraného objektu vůči kompromitujícímu vyzařování, a je zde využita analýza hrozeb. Po analýze jsou následně navržena řešení jednotlivých hrozeb.

Klíčová slova: bezpečnost, elektromagnetické záření, informace, kompromitující vyzařování, kybernetická ochrana, kyberprostor, ochrana utajovaných informací.

ABSTRACT

The bachelor thesis deals with the issue of compromising radiation. It is divided into two parts, a theoretical part and a practical part. In the theoretical part, the bachelor thesis deals with legislative issues of protection of classified information and cyber security. The theoretical part also discusses the possibility of misuse of compromising radiation and also how to protect yourself from it. The practical part of the bachelor thesis is devoted to the current vulnerability of the selected object to compromising radiation, and threat analysis is used here. After the analysis, solutions to individual threats are proposed.

Keywords: compromising radiation, cyber protection, electromagnetic radiation, information, protection of classified information, security.

„Život je těžká zkouška a jen ten, kdo jeho výzvu přijme, opravdu ví, co znamená žít“.

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Petru Svobodovi Ph.D. za odborné vedení, za pomoc a rady při zpracování této práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Tato práce se zabývá problematikou kompromitujícího vyzařování v kontextu kybernetické bezpečnosti. Z dlouhodobého hlediska přináší vývoj informačních a komunikačních technologií lidem řadu výhod a přínosů. Lidé mohou jejich prostřednictvím komunikovat, nakupovat, spravovat svoje finance a další záležitosti. Zároveň se však objevují i rizika při využití informačních a komunikačních technologií, na která je nutné reagovat, aby nedocházelo k poškozování zájmů určitých osob, ke škodám apod. Uživatelům informačních a komunikačních technologií neustále hrozí rizika jako je ztráta dat, zneužití dat apod. Do této kategorie rizik se řadí i tzv. kompromitující vyzařování.

Tento jev s sebou přináší významné bezpečnostní riziko zejména kvůli tomu, že si uživatel informačních a komunikačních technologií, vůbec nemusí uvědomovat, že byl napaden

a jeho data jsou zneužívána. Útočník využívá elektromagnetického záření či „jiného“ typu vyzařování, aby získal přístup k citlivým informacím. Z tohoto důvodu se musí různé subjekty chránit aktivním způsobem i proti tomuto riziku.

V bakalářské práci se zabývám problematikou kompromitujícího vyzařování na konkrétním objektu, který se nachází v oblasti s dalšími budovami, kde sídlí jiné společnosti a v blízkosti lesního porostu. V rámci výzkumu jsem se zaměřil na literární rešerši, která mi poskytla ucelený pohled na otázku ochrany tajných informací z legislativního hlediska. Dále jsem využil metodu syntézy, abych sjednotil jednotlivé části práce do celku.

V praktické části mé bakalářské práce jsem použil analýzu a sběr dat prostřednictvím pozorování vybrané budovy a důkladného zkoumání, abych odhalil hrozby spojené s únikem tajných informací. Pro zhodnocení významnosti těchto hrozeb jsem použil metodu pravděpodobnosti, dopadu rizik a názoru hodnotitelů. V této části jsem identifikoval hrozby z různých oblastí, kde mohou unikat tajné informace. Kompromitující vyzařování a možnost úniku utajovaných informací mohou být využity nejen ve státních institucích, ale i v soukromých společnostech, kde by to mohlo poškodit společnost ve prospěch konkurence. Proto jsou opatření z praktické části relevantní pro jakoukoli společnost.

Výstupy z práce budou předložené managementu vybrané organizace, aby zvážil jejich uplatnění v praxi zajištění bezpečnosti budovy a kybernetické bezpečnosti v rámci organizace. Podnikatelský subjekt tímto získává možnost aktivní reakce a prevence na významné bezpečnostní riziko, které představuje právě zneužití kompromitujícího vyzařování.

I. TEORETICKÁ ČÁST

1 LEGISLATIVA A ZÁKLADNÍ POJMY

Teoretická část práce se zabývá kybernetickou bezpečností, kompromitujícím vyzařováním a legislativou či doporučeními pro oblast kompromitujícího vyzařování.

1.1 Zákony

Stěžejní standardy využívané pro hodnocení informačních systémů a zabezpečených oblastí v rámci kompromitujícího vyzařování vydává Severoatlantická aliance (NATO) a Evropská unie (EU). Lze je kategorizovat na standardy hodnocení informačních systémů, standardy hodnocení prostorů, standardy hodnocení instalace informačních systémů. V oblasti hodnocení informačních systémů se využívá standard NATO SDIP-27/2 či standard EU IASG 7-0,3 a částečně i Česká státní norma EN 55022 (pro hodnocení úrovně rušení komerčních zařízení). K hodnocení prostorů (určení zóny prostoru) se využívá standardu NATO SDIP-28/2 či standardu EU IASG 7-02. Hodnocení instalace informačních systémů

v zabezpečených oblastech je prováděno standardem NATO SDIP-29/2 či standardem EU IASG 7-01 (Národní bezpečnostní úřad, 2023).

V České republice pak platí v této oblasti zejména následující legislativa.

Zákon č. 412/2005 Sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zásadami pro zjišťování utajovaných informací se zabývá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dále specifikuje podmínky přístupu k těmto informacím a další požadavky na ochranu informací (Maisner, 2015). Zákon č. 412/2005 Sb., se zaměřuje na definici zásad pro stanovení informací jako utajovaných, dále určuje podmínky pro přístup k těmto informacím či další požadavky na jejich ochranu, zásady definování citlivých činností a podmínky pro jejich výkon, a s tím

i související výkon státní správy. Oblast kompromitujícího vyzařování tento zákon přímo upravuje v rámci paragrafu 45. Legislativa stanovuje povinnosti ochrany utajovaných informací v režimech přísně tajné, tajné či důvěrné před jejich únikem prostřednictvím kompromitujícího vyzařování (Česká republika, 2005).

Z hlediska institucionálního zajištění na úrovni státu řeší problematiku kompromitujícího vyzařování zejména Národní úřad pro kybernetickou a informační bezpečnost. To je dáno

i zákonem č. 421/2005 Sb., který stanoví, že tento úřad zjišťuje kompromitující vyzařování tam, kde se vyskytují či budou vyskytovat utajované informace. To neplatí pro případy oblastí či objektů, které jsou provozované či užívané zpravodajskými službami, zde jsou k měření oprávněné právě zpravodajské služby (Česká republika, 2005).

Vyhláška č. 523/2005 Sb., vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor

V této vyhlášce jsou stanovené požadavky na informační systémy nakládající s utajovanými informacemi, včetně oblasti problematiky jejich úniku kompromitujícím vyzařováním. Kompromitující vyzařování je ve vyhlášce definováno jako vyzařování elektrických

a elektronických zařízení, které by mohlo způsobit únik utajované informace stupně utajení přísně tajné, tajné nebo důvěrné. Ochrana proti kompromitujícímu vyzařování je zde chápána jako jedno ze základních opatření v oblasti bezpečnosti informačních systémů. Z tohoto důvodu musí být komponenty informačního systému (nakládající s utajovanými informacemi stupně utajení důvěrné či vyššího) zabezpečené takovým způsobem, aby kompromitující vyzařování nevedlo k úniku utajovaných informací. Konkrétní požadavky pak vychází ze stupně utajení utajované informace (Česká republika, 2005b).

Institucionální zajištění v České republice

Národní úřad pro kybernetickou a informační bezpečnost patří mezi ústřední správní orgány pro kybernetickou bezpečnost, kdy zajišťuje také ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Do portfolia činností úřadu patří i měření kompromitujícího vyzařování elektrických a elektronických zařízení, která slouží pro nakládání s utajovanými informacemi a hodnotí je z hlediska způsobilosti k ochraně utajovaných informací. Tímto měřením zároveň identifikuje i způsobilosti zabezpečených oblastí a objektů pro ochranu před únikem utajovaných informací kompromitujícím vyzařováním. Zde se řadí i certifikace stínících komor a zajišťování obranných prohlídek (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Stínící komora je *„uzavřený stíněný prostor zabraňující šíření elektromagnetického, optického a akustického vyzařování mimo tento prostor (Česká republika, 2005b).“*

Problematikou kompromitujícího vyzařování se zabývají i různé metodické materiály, které Národní úřad pro kybernetickou a informační bezpečnost vydává a publikuje. Materiály jsou

určené zejména pro potřeby státu a slouží pro zajištění jeho bezpečnosti (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

K dalším činnostem v oblasti kompromitujícího záření v rámci Národního úřadu pro kybernetickou a informační bezpečnost patří měření kompromitujícího záření. Měření provádí tento úřad dle standardů Severoatlantické aliance (SDIP), dle standardů Evropské unie (IASG 7) a dle metodiky bezpečnostních standardů Národního bezpečnostního úřadu. Objektem měření bývají zejména zařízení orgánů státu, a to včetně komerčních zařízení (pro účely výběrových řízení), či zařízení speciálních informačních systémů (zejména armády) (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Například v roce 2021 realizoval úřad přes 40 měření kompromitujícího vyzařování

u různých typů zařízení. Ve většině případů nebyl identifikován významnější problém a byl splňován standard SDIP-27/2. Další měření probíhala v rámci certifikace či akreditace informačních systémů pro zpracování utajovaných informací stupně utajení důvěrné či tajné, buď pro orgány státu či pro podnikatele. Ve většině případů se jednalo o požadavek Ministerstva obrany (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Souhrn měřených zařízení a objektů tímto úřadem poskytuje následující tabulka. V rámci zónového měření a obranných prohlídek došlo k měření objektů, kdy v rámci jednoho objektu bylo měřeno více místností či budov. U kryptografických prostředků šlo o ověřovací měření. U PC sestav třídy 1 a 2 šlo o měření v rámci výběrových řízení, například pro Ministerstvo obrany nebo Národní úřad pro kybernetickou a informační bezpečnost. Instalační záznamy jsou systémy, které mohou mít několik instalací, ať už v rámci České republiky, či mimo Českou republiku.

Tabulka 1: Přehled měření v oblasti kompromitujícího vyzařování v roce 2021 (Zdroj: Národní úřad pro kybernetickou a informační bezpečnost, 2022)

Typ měření[2]	Počet
Zónové měření	8 lokalit
Kryptografické prostředky	2 typy
Komponenty ICT	41 systémů
Audiotechnika	2 typy zařízení
Obranné prohlídky i v rámci certifikace IS	10 objektů
Mobilní systémy	8 systémů
Instalační záznamy	> 20 lokalit
Stínicí komory	27 certifikátů

Problematika kompromitujícího záření patří v rámci činnosti tohoto úřadu mezi prioritní oblasti. Úřad neustále rozvíjí výzkum a vývoj v oblasti kryptografické ochrany a ochrany proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování tak, aby reflektoval požadavky resortů státní správy, které musí prioritně zajišťovat tuto formu ochrany utajovaných informací. Tento úřad má také zřízeno odborné pracoviště oddělení TEMPEST, které se problematikou zabývá a realizuje různé projekty a výzkumy v této oblasti (Národní úřad pro kybernetickou a informační bezpečnost, 2022).

Bezpečnostní standard Národního bezpečnostního úřadu 2/2011

Bezpečnostní standard Národního bezpečnostního úřadu České republiky shrnuje legislativní a právní ukotvení problematiky kompromitujícího záření. Z přehledu je například patrné, že se kompromitující vyzařování v české legislativě řešilo již v roce 1998 prostřednictvím zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a vyhlášky

č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi. Byl však používán pojme parazitní elektromagnetické vyzařování. Jak vyplývá z dalšího obsahu standardu, tak je v současnosti problematika kompromitujícího vyzařování řešena různými legislativními předpisy (Národní bezpečnostní úřad, 2011).

1.2 Pojmy a doporučení

Doporučení z odborných studií

Odborná studie autorů Martin, Sunmola a Lauder (2022) se zabývala problematikou kompromitujícího záření z informačních technologií, které mohou ohrožovat bezpečnost v souvislosti s citlivými informacemi. Tímto zároveň identifikují různé souvislosti, kterými se musí organizace zabývat v rámci problematiky kompromitujícího vyzařování. Jde zejména o informace a sekundární kanály, zdroje elektromagnetického záření, aktéři hrozeb, protiopatření, testování (Martin, Sunmola, Lauder, 2022).

Informace a sekundární kanály

V rámci běžného provozu informačních technologií a jejich zařízení vznikají neúmyslně tzv. sekundární kanály, kterými mohou unikat různé informace. Jde například

o elektromagnetické záření, které způsobuje kompromitující záření (Martin, Sunmola, Lauder, 2022).

Zdroje elektromagnetického záření

Systémy informačních technologií mohou v důsledku využívání digitálních signálů a kvůli výpočetním činnostem (typu zpracování paměti) produkovat neúmyslné elektromagnetické záření. Potenciálně ohrožující je i možné kompromitující vyzařování prostřednictvím displejů, tiskáren, projektorů, klávesnic, spolu s jejich rozhraními – například digitální video rozhraní DVI, dále USB. Toto kompromitující vyzařování může být využito pro identifikaci konkrétních činností a typů zařízení (Martin, Sunmola, Lauder, 2022).

Obrázek 1: Keylogger (Zdroj: Safeguard-eshop, 2023)

Aktéři hrozeb

Aktéry hrozeb se rozumí potenciální útočníci, kteří se snaží zneužít data a informace. K tomuto využívají různé technické prostředky za účelem detekce, zachycení a rekonstrukce získaného vyzařování. K tomuto potřebují nejen technické prostředky, ale také technické schopnosti jako je zpracování signálů, znalost a využití algoritmů apod. Pro zachycování kompromitujícího vyzařování využívají různých přijímačů a softwarového vybavení. Negativně lze hodnotit, že náklady na vysoce výkonné přijímací systémy se neustále snižují, takže se rozšiřuje i okruh aktérů hrozeb, kteří k nim mají přístup (Martin, Sunmola, Lauder, 2022).

Protiopatření

Protiopatření se využívají pro eliminaci zneužití zranitelnosti a ztráty citlivých informací. Protiopatření mají snižovat sílu kompromitujícího vyzařování, zvětšovat vzdálenost mezi zdrojem kompromitujícího vyzařování a potenciálním útočníkem. Dále se využívá například architektonických úprav budov a konstrukce objektů, filtrací, izolací, které snižují sílu signálu jakéhokoliv vyzařování. Sílu vyzařovaného signálu lze také snížit prostřednictvím rušení kompromitujícího vyzařování přidáním šumu či rušivých signálů. Protiopatření mohou také směřovat k úpravě vyzařovaných informací, takže zachycené a obnovené obrazy nebudou odpovídat realitě (Martin, Sunmola, Lauder, 2022).

Testování

Testování se zaměřuje na zhodnocení fungování protiopatření, a to dle konkrétních požadavků na eliminaci kompromitujícího vyzařování (Martin, Sunmola, Lauder, 2022).

Doporučení Národního úřadu pro kybernetickou a informační bezpečnost pro TEMPEST

Národní úřad pro kybernetickou a informační bezpečnost formuluje doporučení pro zpracovávání utajovaných informací v rámci subjektů veřejné správy, a to dle různých stupňů utajení. U zpracovávání utajovaných informací stupně utajení Vyhrazené se nevyžadují žádná významná opatření v oblasti kompromitujícího vyzařování. Je nutné pouze prohlášení o shodě a umístění monitoru se doporučuje tak, aby nebylo opticky možné odezírání obsahu obrazovky monitoru. Při zpracovávání utajovaných informací stupně utajení důvěrné má být přihlíženo k charakteru organizace provozující informační systém

a k charakteru zpracovávaných informací, rozsahu informací, časovému rozložení a způsobu jejich zpracovávání. Rizika se vztahují zejména s vkládáním utajovaných informací prostřednictvím klávesnice, tiskem a uložením na zálohovací média. Pravidelné zpracovávání přináší i vyšší riziko. Pokud dochází ke zpracování utajovaných informací ve stupně tajné či přísně tajné, tak se je nutné provádět i zónové měření (Národní úřad pro kybernetickou a informační bezpečnost, 2023).

„Pokud jsou zpracovávány utajované informace stupně utajení „Důvěrné“, „Tajné“ nebo „Přísně tajné“, vyžaduje se u některých instalací, určených v bezpečnostních standardech, napájení ze síťového přívodu vybaveného vysokofrekvenčním filtrem. Pro zpracování utajovaných informací stupně utajení „Důvěrné“ je nutné použít vhodný typ s útlumem minimálně 30dB v kmitočtovém pásmu 100 kHz – 1 GHz. Pro zpracování utajovaných informací stupně utajení „Tajné“ nebo „Přísně tajné“ je nutná konzultace s oddělením TEMPEST NÚKIB. K využití útlumových vlastností zapojených filtrů je nutná jejich odpovídající instalace (patřičné oddělení vodičů vstupní a výstupní části) (Národní úřad pro kybernetickou a informační bezpečnost, 2023).“

Dále je také nutné dodržovat pravidla bezpečnosti při zacházení s komponenty informačních systémů, které obsahují paměti typu RAM. Informace v těchto pamětech mohou zůstávat

i po odpojení napájecího napětí, tedy v případě odeslání do servisu či jiné manipulace, je lze nějakým způsobem zneužívat (Národní úřad pro kybernetickou a informační bezpečnost, 2023).

2 KYBERNETICKÁ BEZPEČNOST

Kyberprostor lze chápat jako veřejný prostor. To samozřejmě znamená, že kyberprostor nemá žádné vlastníky. Není kontrolován úřady, jednotlivci ani zeměmi. Vzhledem k tomu, že kyberprostor nemá určeného přímého vlastníka, bezpečnostní prostředky musí být koordinovány mezi zúčastněnými stranami. Subjekty v kyberprostoru by měly mezi sebou sdílet informace o možných rizicích a anomáliích, které mohou narušit zabezpečený prostor (Doucek, Konečný, Novák, 2019).

Kyberprostor se skládá z prvků informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou globální počítačovou síť a jednotlivé počítačové systémy, které se připojují k této síti a interagují v rámci této sítě (Kolouch, Bašta, 2019).

Rozvoj moderních informačních technologií zvyšuje závislost dnešní společnosti na jejich řádném fungování, a proto musí být zajištěna bezproblémová funkčnost informačních technologií. To se vztahuje právě i ke kybernetické bezpečnosti, která má zajistit plnění tohoto cíle (Jansa et al., 2016, s. 416).

Informační technologie a jejich zařízení je určeno pro zpracování, ukládání a odesílání informací. V současnosti je již běžné, že jsou informační technologie pro každou organizaci velmi důležitým majetkem, což ještě prohlubuje rozvoj digitalizace, průmyslu 4.0 a další podobné trendy (Martin, Sunmola, Lauder, 2022).

Lidé i organizace využívají technologie pro celou řadu kritických úkolů, jako je například správa financí v rámci internetového bankovnictví, personální řízení, spolupráce s dalšími osobami a firmami. Informační technologie sice usnadňují plnění těchto úkolů, ale zároveň generují i závažné bezpečnostní problémy (Kavak et al., 2021).

Kybernetické hrozby představují rostoucí riziko pro celou řadu různých podnikatelských

i nepodnikatelských subjektů. Z tohoto pohledu je nutné klást vysoký důraz na zajišťování kybernetické bezpečnosti. Žádná organizace si v dnešní době rozvoje informačních

a komunikačních technologií nemůže dovolit podceňovat tuto hrozbu. Naopak, je nutné, aby se otázkami zajišťování kybernetické bezpečnosti aktivně zabývala, identifikovala hrozby

a rizika, včetně realizace správné reakce. Tato ambice však může být složitě splnitelná, a to zejména v prostředí organizací, které jsou velké, a v jejichž interním prostředí probíhají stovky různých procesů (Jalali, Kaiser, 2018).

Kybernetická bezpečnost je fenoménem dnešní informační doby. V současnosti již má daleko větší a širší rozpětí než pouze hrozbu zneužití informací. V reflexi bezpečnostních hrozeb a rizik v kyberprostoru vzniká celostní pohled na kybernetickou bezpečnost jako modelový stav, jenž je narušován různými typy fenoménů destruujících kybernetickou bezpečnost (Sak, 2018).

Bezpečnost počítačů, tabletů, mobilů či infrastruktury se musí neustále rozvíjet, protože s vývojem informačních technologií roste i důležitost kybernetické bezpečnosti.

Kybernetickou bezpečností se dnes musí zabývat nejen státy a podniky, ale i jednotlivci (Nezmar, 2017, s. 78).

Tento požadavek je dán aktuálním vývojem, kdy se neustále zvyšuje počet různých kybernetických útoků, které navíc necílí pouze na vládní instituce, ale také na podniky, či jednotlivce. Kybernetická bezpečnost se pro takové subjekty a jednotlivce stává prioritní oblastí zájmu (Snider et al., 2021).

Navzdory snahám vlád a jednotlivců o zajišťování kybernetické bezpečnosti se stále jedná

o obrovskou a neustále se rozvíjející výzvu, která zahrnuje řešení na úrovni fyzických, softwarových a lidských systémů (Kavak et al., 2021).

Z hlediska kyberbezpečnosti se však nelze setkat s jednotně uznávanou a obecně přijímanou definicí. Je zřejmé, že kybernetická bezpečnost je podmnožinou bezpečnosti jako takové, ale dále lze na tento jev nahlížet různými způsoby. O definici pojmu se snaží jak celá řada odborníků, tak i politici v rámci legislativních předpisů, které se kyberbezpečností zabývají. Z přehledu těchto definic lze potom kybernetickou bezpečnost vymezit jako soubor legislativních, organizačních, technických a vzdělávacích prostředků, které se zaměřují na zajištění ochrany počítačových systémů a dalších prvků informačně komunikačních technologií, aplikací, dat a uživatelů. Jedná se i o schopnost počítačových systémů

a využívaných služeb reagovat na kybernetické hrozby a útoky či na jejich následky, ale také jde o plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených (Bašta et al., 2019).

Cílem kybernetické bezpečnosti je obrana a ochrana kybernetického prostoru za účelem zajištění dostupnosti, integrity a důvěrnosti kybernetických systémů. Sestává z konkretizace cílů, identifikace hrozeb a realizace preventivních opatření. Z tohoto pohledu je kybernetická

bezpečnost praxí v ochraně kybernetických systémů a jejich operací před hrozbami prostřednictvím kombinace preventivních opatření (Kavak et al., 2021).

Zajišťování kybernetické bezpečnosti tedy nespadá pouze do prostoru kyberprostoru, ale také mimo něj (Bašta et al., 2019).

Organizace čelí kybernetickým bezpečnostním hrozbám z různých zdrojů, tedy respektive od různých útočníků. Nemusí se jednat pouze o jednotlivce, kteří patří do kategorie kybernetických zločinců, ale například i o zpravodajské služby, aktivity, teroristy či zaměstnance (vlastní či konkurence) (Martin, Sunmola, Lauder, 2022).

Cíle kybernetických útoků tvoří zejména kybernetické systémy, data a lidské zdroje, jejichž narušení či přístup k nim může přinést výhody neoprávněným uživatelům či stranám. Jde například o informační a komunikační technologie, datové systémy, či personál. Informační a komunikační technologie jsou fyzické a síťové systémy, které mají společné prvky typu výpočetního výkonu, zpracovávání informací a počítačových sítí, jejichž úkolem je poskytování prostředků pro snadnější plnění úkolů v oblasti síťové infrastruktury. Datové systémy zase obsahují důvěrné informace, a to dle konkrétní povahy datového systému. Může jít o důvěrné informace typu finančních údajů, osobních údajů, ale například

i informace o národní bezpečnosti (Kavak et al., 2021).

Z hlediska zajištění kybernetické bezpečnosti platí poučení, že nejlepší obrana je taková, která zabrání, aby ke kybernetickým útokům vůbec došlo. Tohoto je však v současnosti téměř nemožné dosáhnout, pokud jsou systémy propojené s jinými systémy prostřednictvím sítí či internetu. V rámci prevence je tak vhodné realizovat různá preventivní opatření, která lze rozdělit na kategorie technologických opatření, vzdělávacích opatření a opatření v oblasti politiky bezpečnosti (Kavak et al., 2021).

Technologická preventivní opatření

Technologie jsou jednou z klíčových oblastí zabezpečení kyberprostoru. V oblasti technologických preventivních opatření jde o nástroje, techniky a software, které kybernetický útok odhalí, zabrání mu či jej zastaví. Obvykle se jedná například o antivirový software, firewally, automatické aktualizace, systémy IDS (systémy detekce narušení). Antivirový systém dokáže identifikovat známé škodlivé programy jako počítačové viry, trojské koně apod., takže zároveň zabraňuje i jejich spuštění. Automatické aktualizace zajišťují, že mají systémy nejaktuálnější zabezpečení. Systémy detekce narušení se zaměřují

na monitoring počítačových a síťových událostí a jejich analýzu za účelem detekce známých incidentů, typu porušení zásad bezpečnosti, porušení zabezpečení apod. (Kavak et al., 2021).

Vzdělávací opatření

Vzdělávání a edukace je v oblasti kybernetické bezpečnosti zásadní. Může nabývat podoby školení uživatelů v základních bezpečnostních konceptech či v politice bezpečnosti (viz níže). Uživatel by měl mít informace o tom, jak bezpečně používat internet, jak rozpoznat podezřelé emailové a jiné zprávy, jak využívat zabezpečení heslem, chápat softwarová oprávnění a dokázat bezpečně likvidovat data, ale také například být schopen identifikovat kybernetickou hrozbu (zejména u pokročilých uživatelů). Vzdělávání by mělo směřovat

i k organizacím, což je realizováno velmi často prostřednictvím implementace a prosazování „zásad a postupů“ v kybernetické bezpečnosti (Kavak et al., 2021).

Opatření v oblasti politiky bezpečnosti

Ani špičková technologie nemusí zabránit kybernetickým útokům, protože v praxi platí, že velká část bezpečnostních incidentů vzniká v důsledku selhání lidského faktoru. Preventivní opatření se tedy musí zabývat právě i vzděláváním a nastavením politiky bezpečnosti (Kavak et al., 2021).

V souvislosti s kybernetickou bezpečností lze na lidi nahlížet jako na strůjce kybernetické bezpečnosti (jejich zájmem je prosadit a implementovat jednotlivé prvky kybernetické bezpečnosti), příjemce pravidel kybernetické bezpečnosti (zajišťují implementaci pravidel kybernetické bezpečnosti), subjekty ochrany před kybernetickými útoky, subjekty informování a proškolení o pravidlech a principech kybernetické bezpečnosti, dále jako na riziko a hrozbu v rámci tvorby a zajišťování kybernetické bezpečnosti (Bašta et al., 2019).

Analýza rizik kybernetické bezpečnosti

Zajišťování kybernetické bezpečnosti je v podstatě nepřetržitou analýzou rizik, které se v této oblasti objevují či působí, případně, se v budoucnosti mohou objevit. Celý proces začíná identifikací a detekcí rizik (hrozeb, incidentů a útoků, systémových událostí), následně pokračuje analýzou (standardní analýzou činnosti systémů a služeb, forenzní analýzou). Dále jde o aktivity v oblasti realizace opatření (to například za účelem obnovy funkčnosti systémů a služeb, doporučení na základě analýzy incidentů, best practices, školení či dalšího vzdělávání). Na toto navazuje krok v podobě monitoringu a podpory činnosti systémů a služeb systému, včetně podpory poskytované uživatelům. V další fázi

nastává kontrola, která má například podobu auditu či realizace opatření. Celý proces je však nepřetržitý, a proto musí po kontrole opět následovat identifikace a detekce rizik (Bašta et al., 2019).

Identifikace rizik tedy musí identifikovat veškerá podstatná rizika, pochopit jejich podstatu a popsat je v rámci vztahu mezi příčinou – rizikem – účinkem. V návaznosti na toto potom vzniká registr rizik a dochází k realizaci prvotních návrhů na ošetření rizik (Janíček, Marek, 2013, s. 323).

Analýzu rizik je pak vhodné založit na kvantifikaci rizika, tj. určení pravděpodobnosti jeho vzniku a míry dopadu na daný subjekt. Vychází se z registru rizik, *„do kterého je nyní potřeba určit (odhadnout) pravděpodobnost popsaného scénáře a stanovit (odhadnout) vážnost předpokládaného nepříznivého dopadu na projekt. Objektivitě zde velmi napomáhá výše uvedené stanovení úrovní pravděpodobnosti a dopadu (Doležal, 2016, s. 206).“*

3 KOMPROMITUJÍCÍ VYZAŘOVÁNÍ

Právě v dnešní informační společnosti jsou informace klíčovým a prioritním aktivem, nenahraditelnou součástí dnešního života, ať už jedinců, podniků či národních států. Bezpečnost informací se díky tomuto stává prioritní oblasti bezpečnosti a uživatelé musí realizovat aktivní opatření k tomu, ať eliminují riziko vystavení se hrozbám (Lee et al., 2022).

Elektromagnetické vlny vysílané elektronikou mohou způsobit únik zpracovávaných informací, a tedy i umožnit odposlech. Takové rádiové signály, označované právě jako kompromitující vyzařování, jsou studovány a kontrolovány bezpečnostními složkami různých států (jedná se o oblasti TEMPEST), a to v některých zemích již od šedesátých let minulého století (Kuhn, 2013).

V současnosti již nelze pochybovat o tom, že je nutné problematiku zranitelnosti v rámci kompromitujícího vyzařování zohledňovat při návrhu, výrobě, repasování, testování

a zajišťování kvality bezpečnosti různých systémů a procesů, včetně systému zabezpečení budovy/objektu (Martin, Sunmola, Lauder, 2022).

Informační a komunikační technologie mohou vyzařovat různé formy energie. Řada těchto emisí (vyzařování) vzniká neúmyslně v důsledku běžného provozu, tedy jako vedlejší provozní účinek. Pro bezpečnost těchto zařízení je problematické, že část neúmyslně vyzařované energie nese informace o zpracovávaných datech. Pokud jsou k tomu dobré podmínky, tak může důmyslný a kvalitní odposlech právě tato data zachytit a analyzovat. Kompromitující vyzařování tedy může vést k úniku dat (Kuhn, 2011).

Právě název TEMPEST se používá pro označení vyzařování kompromitujících elektromagnetických signálů. Takové vyzařování může útočníkům (i neúmyslně) pomoci k identifikaci polohy různých zařízení informačních technologií, čímž samozřejmě vzniká bezpečnostní riziko v podobě narušení důvěrnosti. Toto riziko vzniká, když může kompromitující záření vést ke škodlivým dopadům na organizaci, například ke ztrátě duševního vlastnictví, ke zhoršení výkonnosti, k finančním ztrátám. V konečném důsledku pak podcenění rizika povede ke ztrátě konkurenceschopnosti (Martin, Sunmola, Lauder, 2022).

TEMPEST byl původně kódový název amerického vládního projektu, který se zabýval hrozbou zneužití kompromitujícího vyzařování. V dnešní době se název stále používá

a označuje právě i aktivity prevence zneužití dat prostřednictvím kompromitujícího vyzařování (Zhang, 2022).

Klíčovou součástí TEMPEST je právě hodnocení kompromitujícího vyzařování, které je vyzařováno elektronickými zařízeními, jenž zpracovávají citlivé informace (Cazanaru, Cosereanu, Szilagyi, 2011).

Zdrojem kompromitujícího vyzařování může být jakékoliv elektromechanické či elektronické zařízení, které se využívá pro zpracování zabezpečovaných informací (Astrodynetdi, 2023).

Obrázek 2: Elekromechanické a elektronické zařízení (Zdroj: Monzas, spol. s.r.o., 2023)

Je prokázáno, že informační technologie jsou z bezpečnostního hlediska zranitelné právě prostřednictvím kompromitujícího vyzařování. Zařízení jako LCD monitory, klávesnice, dotykové obrazovky apod. vyzařují emise, pokud jsou vedené prostřednictvím kabelů, tak

i několik kilometrů. Útočníci mohou obnovovat takto vyzařované emise, čímž získávají citlivé údaje (Martin, Sunmola, Lauder, 2022).

Z hlediska šíření signálu kompromitujícího vyzařování existují čtyři základní způsoby, kterými k němu může docházet. Jde elektromagnetické vyzařování, elektrické vedení (vytváří signály a šumy), přenášené signály, akustika (například klávesnice, tiskárny apod. vytváří zvuky, které mohou být zdrojem ohrožení) (Astrodynetdi, 2023).

Záměrem útočníka není určení skutečného zdroje kompromitujícího vyzařování, ale zneužití tohoto vyzařování. Není tedy přímo podstatné, odkud konkrétně vyzařování vychází. Útočník zjednodušeně řečeno hledá signál, který může zneužít (Vuagnoux, Pasini, 2010).

Zabezpečení výpočetní techniky, aby z jejich kompromitujícího vyzařování nemohla speciální technika (na vzdálenost i několika stovek metrů) získat data je zpravidla velmi nákladné, ale v praxi se objevuje i další problém v tom, že si organizace takové riziko v podstatě vůbec neuvědomují. I samotné odhalení útočníka je prakticky nemožné. Proces je absolutně pasivní, nedochází k narušení budovy, činnost není zjistitelná (Keřkovský, Drdla, 2003, s. 158).

Obrázek 3: Záznamník zvuku v náramku a GSM odposlech/štenice skrýtá v PC myši (Zdroj: Safeguard-eshop, 2023)

Ochrana zařízení před zneužitím v oblasti kompromitujícího záření se realizuje různými způsoby. Může jít o odstup, stínění, filtrování či maskování. V řadě případů existují různé normy a metodická doporučení, která nařizují/doporučují využití prvků pro zajištění ochrany před tímto druhem zneužití. Jde například o vzdálenost zařízení od stěn, stínění v budovách, rozdělení utajovaných a neutajovaných informací atd. (Astrodynetdi, 2023).

Při návrhu řešení v oblasti prevence kompromitujícího vyzařování mohou být efektivními kroky následující (Astrodynetdi, 2023):

- Preventivní opatření – identifikace rizik v této oblasti a realizace preventivních opatření v reakci na rizika.
- Výběr informačních technologií s vhodnými funkcemi a ve vhodných formátech.
- Zajištění minimální úrovně signálu všech datových obvodů, aby se minimalizoval šíření kompromitujícího vyzařování.
- Stínění – oddělení různých oblastí tak, aby se při přechodu z jedné do druhé oslabilo elektrické a magnetické pole (například odrazem, absorpčními ztrátami).
- Filtrování – propouštění určité frekvence a utlumení všech ostatních.
- Izolace.

Efektivním způsobem ochrany proti úniku informací prostřednictvím kompromitujícího vyzařování může být například tzv. Faradayova místnost/klec. Jedná se o nejúčinnější legální způsob ochrany proti odposlechu a úniku informací technickou cestou (Mudroch Labs, 2011).

Obrázek 4: Faradayova místnost (Zdroj: Mudroch Labs s.r.o., 2011)

V oblasti zajišťování ochrany proti kompromitujícímu vyzařování je nutné, aby organizace chápala technické možnosti, které mohou potenciální útočníci zneužít, a také vzala do úvahy veškerá rizika, takže může dojít k posouzení pravděpodobnosti zneužití zranitelnosti (Martin, Sunmola, Lauder, 2022).

Kompromitující vyzařování lze zachytit pasivně prostřednictvím směrových antén, mikrofonů, vysokofrekvenčních zařízení, elektrického vedení, radiových přijímačů, osciloskopů a dalších zařízení, která jsou určená k snímání a zpracování signálů. V některých případech mohou útočníci získat informace prostřednictvím aktivního směřování radiových vln či světelných paprsků na zařízení a analýzu odrážené energie (Kuhn, 2011).

Proces analýzy rizik v oblasti kompromitujícího vyzařování má obvyklou podobu, která se v rámci analýzy rizik využívá i pro posouzení rizik jiného charakteru. Je nutné zhodnotit úroveň pravděpodobnosti vzniku rizika a míru zranitelnosti (dopadu) rizika na subjekt v případě, že by došlo ke vzniku identifikovaného rizika. Vzhledem k tomu, že jde o rozbor oblasti bezpečnosti, tak je nutné hodnocení provádět s důrazem na cíle bezpečnosti v podobě důvěrnosti, integrity a dostupnosti (Martin, Sunmola, Lauder, 2022).

K příkladům kompromitujícího vyzařování lze přiradit například (Kuhn, 2011):

- Zvuk a chování tiskáren – tiskárny mohou vydávat charakteristické zvuky u každého tištěného znaku, takže lze vytištěný text rekonstruovat dle odposlechu zvuku. Tento problém však byl spíše u historických typů tiskáren. V současnosti však mohou podobně fungovat magnetické a napájecí signály tiskáren.
- CRT monitory – jde o zobrazovací zařízení fungující na principu katodové trubice se stínítkem. Tyto monitory vysílají videosignál jako elektromagnetické vlny, které lze následně zachytit a rekonstruovat.
- Ploché displeje – některé ploché obrazovky je možné odposlouchávat prostřednictvím UHF radiostanic.
- Kabely RS-232 – data z kabelů RS-232 lze odposlouchávat na vzdálenost několika metrů s využitím jednoduchých krátkovlnných AM vysílaček.
- Klávesnice – dle zvuku stisku klávesy je možné v některých případech určit, jaká klávesnice byla použita.
- Čipové karty – čipové karty nahrazují klíče, ale mohou vykazovat i kompromitující vyzařování.

Zneužití kompromitujícího vyzařování je vztaženo zejména na hardwarové vybavení informačních technologií. Zranitelnost hardwaru je zpravidla dlouhodobější než u softwaru, protože softwarové programy jsou častěji aktualizované, a to včetně oblasti svojí

bezpečnosti. Naopak, u hardwarového vybavení často neexistuje žádná možnost bezpečnostních aktualizací. Vysoká cena těchto zařízení či neinformovanost uživatelů

o bezpečnostních problémech je pak právě často příčinou toho, že i hardware nevhodný z hlediska bezpečnosti je používán dlouhodobě (Vuagnoux, Pasini, 2010).

Specifickým záměrem útočníků je prostřednictvím kompromitujícího vyzařování získat informace typu kryptografických klíčů, informací o zobrazení či další typy citlivých informací (Lee et al., 2022).

Zároveň z výše uvedených informací vyplývá, že existuje velmi úzká souvislost mezi kybernetickou bezpečností a problematikou kompromitujícího vyzařování. Je zřejmé, že technologie, které mohou být napadené kybernetickými útoky ve většině případů vykazují

i kompromitující vyzařování, které právě může být nástrojem kybernetického útoku

a ohrožení kybernetické bezpečnosti. Jsou to právě počítače a další elektronická zařízení, která vysílají radiofrekvenční signály a elektromagnetické záření, které mohou kyberzločinci využít pro rekonstrukci dat (Zhang, 2022).

Teoretická část bakalářské práce se podrobněji zabývá problematikou kompromitujícího vyzařování na konkrétním objektu. V rámci výzkumu jsem se zaměřil na literární rešerši, která mi poskytla ucelený pohled na otázku ochrany tajných informací z legislativního hlediska. Dále jsem využil metodu syntézy, abych sjednotil jednotlivé části práce do celku.

V praktické části mé bakalářské práce jsem použil analýzu a sběr dat prostřednictvím pozorování vybrané budovy a důkladného zkoumání, abych odhalil hrozby spojené s únikem tajných informací. Pro zhodnocení významnosti těchto hrozeb jsem použil metodu pravděpodobnosti, dopadu rizik a názoru hodnotitelů. V této části jsem identifikoval hrozby z různých oblastí, kde mohou unikat tajné informace.

II. PRAKTICKÁ ČÁST

4 PROFIL ORGANIZACE A OBJEKTU

Praktická část práce představuje profil organizace a objektu, dále se věnuje analýze rizik kompromitujícího vyzařování u daného objektu, a to zejména v souvislosti s kybernetickou bezpečností. V závěru kapitoly dochází k návrhu opatření ke zlepšení aktuálního stavu.

Vybraná organizace XY je podnikatelským subjektem, konkrétně akciovou společností, která se zabývá nákupem a prodejem zlatých a stříbrných slitků, investičních zlatých

a stříbrných mincí, zlatých a stříbrných pamětních mincí. V současnosti organizace dokončuje rekonstrukci nových skladových a kancelářských prostorů, které si vyžadují

i řešení v oblasti kompromitujícího záření. Výstupy z této práce tedy budou využité přímo pro naplnění této potřeby.

Na trhu v České republice působí organizace od roku 2015 a v současnosti provozuje pouze internetový obchod bez kamenné pobočky. Na tomto internetovém obchodě nabízí přes 100 variant různých produktů. Denně expeduje přes deset zásilek různé hodnoty a ceny, ale zákazníkům umožňuje i osobní odběr (tento bude probíhat právě i v prostorech objektu).

Hodnota skladových zásob organizace činí více než deset milionů korun českých, dále organizace shromažďuje i citlivé informace nejen o svojí vlastní činnosti, ale i o zákaznících a jejich odběrech zboží. Veškeré informace jsou velmi citlivého obchodního charakteru

a jejich zneužití může vést nejen k poškození celé organizace, ale právě i klientů. Z tohoto důvodu je nutné klást velký důraz na zajištění kybernetické bezpečnosti, bezpečnosti celé budovy, včetně právě problematiky kompromitujícího záření.

Z důvodu požadavku na anonymitu bude organizace označována anonymní zkratkou XY,

a také nedojde k přesnému popisu lokality, ve které se řešená budova nachází. V majetku organizace se jedná o jedinou budovu, další stavby neprovozuje. Lze jen uvést, že se budova nachází v okrajové části jednoho z krajských měst České republiky.

Stavba budovy byla dokončena v roce 2023 a v současnosti probíhají závěrečné práce v rámci rekonstrukce. Jedná se o jednopodlažní budovu určenou pro skladovací, kancelářskou techniku a jinou techniku. Budova má dva vchody.

V bezprostředním okolí budovy se nachází chodník, který je volně přístupný všem osobám bez omezení. Dále je zde další budovy, parkoviště a zemědělská plocha, resp. lesní porost.

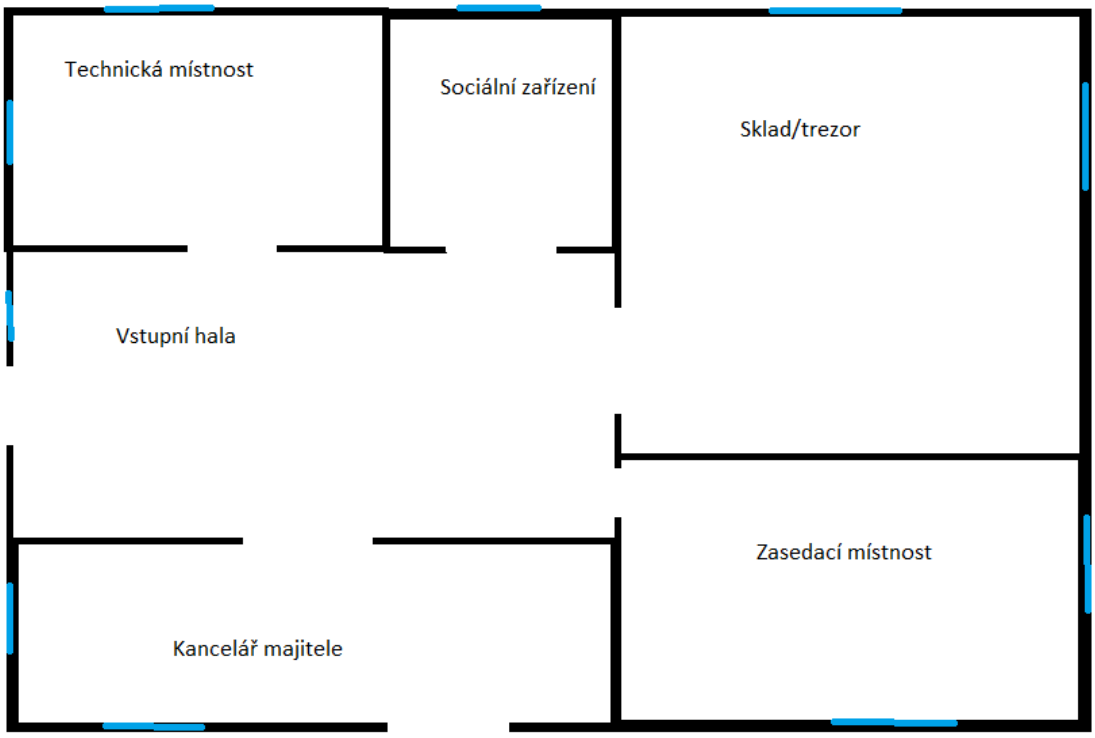
V budově se nachází celkem šest místností, včetně vstupní haly. Jejich rozložení má následující podobu (viz následující obrázek – modře jsou zvýrazněná okna). Jedná se

o místnosti:

- Vstupní hala – do této místnosti se vstupuje hlavním vchodem do objektu. Nachází se zde dva pracovní stoly, kde sedí zaměstnanci organizace (tj. po pravé straně vstupující osoby). Za těmito zaměstnanci se nachází vstup do kanceláře ředitele podniku. Po levé straně jsou vchody do technické místnosti a sociálního zařízení. Před vstupující osobou se nachází místnost sklad/trezor a zasedací místnost.
- Technická místnost – v této místnosti se nachází sklad různého materiálu od balícího materiálu a zařízení (jako například tiskárna apod.)
- Sociální zařízení – v místnosti se nachází WC a umyvadlo.
- Sklad/trezor – v této místnosti je naskladněno veškeré zboží na skladě, které není umístěno v bankovních schránkách. V místnosti probíhá příprava expedice zboží

  a je zde vždy uskladněno až do příjezdu kurýrní služby. Část zboží menší hodnoty je umístěna mimo trezor.
- Kancelář majitele – v této kanceláři má majitel zřízenou svoji kancelář. Specifikem místnosti je skutečnost, že se zde nachází samostatný vchod.
- Zasedací místnost – v této místnosti jsou realizována různá jednání, ať už v rámci pracovního týmu, nebo s obchodními partnery.

Plán objektu popisuje polohu jednotlivých místností. U kanceláře majitele a vstupní haly se nachází parkoviště pro návštěvníky a pracovníky. U místnosti sklad/trezor a zasedací místnosti je zemědělská plocha a lesní porost.



Obrázek 5: Plán objektu (Zdroj: Vlastní)

Vstup do těchto místností momentálně není nijak zabezpečen z hlediska přístupu (v provozní době). Pouze do místnosti sklad/trezor musí vstupující osoba disponovat klíčem od místnosti. To znamená, že pokud do budovy vstoupí cizí osoba, tak má volný přístup do všech ostatních místností. To není z bezpečnostního hlediska ideální řešení, a proto na něj bude reagováno v rámci návrhové části práce.

V organizaci se využívá následujících informačních a komunikačních zařízení:

- Služební mobilní telefony – jedná se o mobilní telefony určené výhradně ke služebním účelům. Mobilní telefony jsou zabezpečené antivirovým softwarem, který by měl zamezit riziku kybernetického útoku.
- Služební notebook – zaměstnancům je k dispozici služební notebook, který využívají k práci. Tento je vždy ponechán v objektu, tedy zaměstnanec si jej nesmí brát mimo pracoviště.
- Televizní obrazovka – v zasedací místnosti se nachází LCD televizní obrazovka, která je využívána při jednání k promítání různých informací, které souvisí s konkrétním jednáním.
- Multifunkční tiskárna – v technické místnosti se nachází multifunkční tiskárna.

- Wifi a příslušenství k internetu – objekt je pokryt signálem wifi, který je realizován prostřednictvím příslušného hardwarového vybavení.
- Stolní PC – část zaměstnanců využívá i stolních počítačů, které jsou umístěné ve vstupní hale. Stolní PC se nachází i v kanceláři majitele.
- Klávesnice – ke stolním počítačům náleží i klávesnice.
- Myš – ke stolním počítačům je k dispozici i myš.
- USB disky – pro rychlejší přenos dat mezi některými počítači a pro zálohování dat využívá organizace USB disků.
- Interní informační software – v organizaci je využíván interní informační systém.
- Digitální projektor – v zasedací místnosti je k dispozici i digitální projektor.

Z tohoto přehledu vyplývá, že organizace využívá různé informační a komunikační technologie. Z tohoto důvodu se musí otázkou kybernetického bezpečnosti

a kompromitujícího vyzařování zabývat. Tuto nutnost ještě zvyšuje skutečnost, že se bude v objektu nacházet zboží organizace, které je nemalé hodnoty. Bezpečnostní riziko zneužití dat ke krádeži je velmi vysoké. Z tohoto důvodu je dále provedena analýza rizik kompromitujícího vyzařování.

5 ANALÝZA RIZIK KOMPROMITUJÍCÍHO VYZAŘOVÁNÍ

Analýza rizik kompromitujícího vyzařování je provedena prostřednictvím expertního hodnocení tří osob na problematiku. Jde o nezávislého externího experta, který se zabývá poradenstvím v oblasti kompromitujícího vyzařování, dále o pracovníka bezpečnostní agentury, která také nabízí služby související s problematikou kompromitujícího vyzařování. Třetím hodnotitelem je autor práce. S odborníky byla uskutečněna prohlídka budovy, dále byl konzultován plán rozmístění nábytku a technického vybavení. Na základě tohoto pak proběhlo hodnocení. Náklady na tuto konzultaci pokryl majitel organizace XY, který souhlasil s využitím konzultačních služeb těchto osob a s realizací prohlídky objektu těmito osobami. Majitel si tedy uvědomuje, že musí řešit i rizika související s kompromitujícím vyzařováním, což lze hodnotit pozitivně.

Jako první jsou definována různá rizika, která mají souvislost s řešenou problematikou,

a která mohou v organizaci XY vzniknout. Jedná se pouze o rizika, která se vztahují k oblasti kompromitujícího vyzařování, případně rizika, která s touto oblastí nějakým způsobem souvisí. Rizika jsou identifikována prostřednictvím odborných zdrojů (tj. výstupů z teoretické části práce), dále prostřednictvím vlastního názoru na problematiku, a také byl zjišťován názor uvedených expertů.

Analýza rizik z tohoto pohledu umožňuje identifikovat veškerá podstatná rizika, která mohou potenciální útočníci zneužít pro svůj útok. Je využito obvyklého postupu při analýze rizik a jejich vyhodnocení.

Dále dochází k hodnocení těchto rizik dle míry pravděpodobnosti jejich vzniku

a potenciálnímu dopadu na organizaci. Toto hodnocení je kvantifikováno, tedy je využito stupnice pro hodnocení pravděpodobnosti i dopadu. U pravděpodobnosti vzniku rizika se jedná o škálu viz tabulka 2.

Tabulka 2: Pravděpodobnost vzniku (Zdroj: Vlastní)

velmi nízká pravděpodobnost vzniku	1
spíše nízká pravděpodobnost vzniku	2
střední pravděpodobnost vzniku	3
spíše vysoká pravděpodobnost vzniku	4
velmi vysoká pravděpodobnost vzniku	5

Potenciální dopad rizika na organizaci je pak také kvantifikován. Vzhledem k řešené problematice je vztažen dopad k úniku citlivých informací. Je využito následující škály viz tabulka 3.

Tabulka 3: Dopad rizika (Zdroj: Vlastní)

možnost náhodného úniku citlivých informací	1
nízká pravděpodobnost úniku citlivých informací	2
střední pravděpodobnost úniku citlivých informací	3
vysoká pravděpodobnost úniku citlivých informací	4
trvalý únik citlivých informací	5

Každý hodnotitel následně hodnotí pravděpodobnost a míru dopadu rizika na organizaci. Prostřednictvím součinu hodnot lze získat konečnou hodnotu rizika, čímž lze konkrétní riziko kategorizovat. To provedeme například následujícím postupem viz tabulka 4.

Tabulka 4: Celkové hodnocení hrozeb (Zdroj: Vlastní)

Stupeň rizika	**Stupnice**	**Kategorie hrozeb**
I.	<5 bodů	Rizika s nízkým vlivem, která nemusí být prioritně řešena
II.	6–10 bodů	Rizika s menším vlivem, která je vhodná sledovat a hodnotit
III.	11–15 bodů	Rizika se středním vlivem, která je nutná nějakým způsobem řešit či sledovat
IV.	16–20 bodů	Rizika s vyšším vlivem, která je nutné řešit, reagovat na jejich existenci
V.	> 21 bodů	Rizika s vysokým vlivem, která je nutné akutně a prioritně vyřešit

Kategorizace rizik pak umožní identifikovat u jednotlivých rizik jeho konkrétní kategorii. Je zřejmé, že s riziky s výrazným vlivem, musí být pracováno odlišně než s riziky s nízkým vlivem. Kategorizace tedy urychluje reakci a celý proces řešení rizika standardizuje.

Mezi identifikovaná rizika lze zařadit zejména následující:

1) Zachycení kompromitujícího vyzařování prostřednictvím vedení elektrického napětí.
2) Zachycení kompromitujícího vyzařování prostřednictvím zdrojů LAN.
3) Zachycení kompromitujícího vyzařování prostřednictvím odposlechů (či bez odposlechů – tenké zdivo může usnadnit zachycení konverzace v místnosti i bez techniky).
4) Zachycení kompromitujícího vyzařování prostřednictvím oken (ať už pohybu osob v místnosti, nebo obrazu z obrazovek, projektorů apod.).
5) Zachycení kompromitujícího vyzařování z informačních technologií a jejich komponent (jedná se o kompromitující vyzařování z periferních zařízení).
6) Zachycení kompromitujícího vyzařování z obrazovek.

Přítomnost těchto rizik v objektu organizace XY lze přiblížit následujícím způsobem.

1) Zachycení kompromitujícího vyzařování prostřednictvím vedení elektrického napětí

Elektrické napětí vytváří elektromagnetické vyzařování, které může být zachyceno

a útočníkem zneužito. Elektromagnetické vyzařování z elektrického napětí může útočník určitým způsobem detekovat.

2) Zachycení kompromitujícího vyzařování prostřednictvím zdrojů LAN

LAN (Local Area Network) je označení pro počítačovou síť, kterou organizace v objektu využívá. Tato je připojena k internetu, takže může být zneužita i útočníky pro zachycení kompromitujícího vyzařování.

3) Zachycení kompromitujícího vyzařování prostřednictvím odposlechů (či bez odposlechů – tenké zdivo může usnadnit zachycení konverzace v místnosti i bez techniky)

Jde o riziko, že bude využito odposlechu pro zachycení konverzace osob uvnitř objektu s využitím různých technologických nástrojů. Podobně, nelze vyloučit riziko, že do objektu pronese nepovolaná osoba odposlech.

4) **Zachycení kompromitujícího vyzařování prostřednictvím oken (ať už pohybu osob v místnosti, nebo obrazu z obrazovek, projektorů apod.)**

Okna v budově mohou být zneužita pro sledování pohybu a lokace osob v objektu, nebo pro sledování dění na obrazovkách počítačů, projektoru.

5) **Zachycení kompromitujícího vyzařování z informačních technologií a jejich komponent (jedná se o kompromitující vyzařování z periferních zařízení)**

Jedná se o riziko, že dojde k zachycení vyzařování, které vydávají klávesnice, myši, monitory apod.

6) **Zachycení kompromitujícího vyzařování z obrazovek**

Jde o riziko, že dojde k zachycení kompromitujícího vyzařování z obrazovky LCD, která se nachází v zasedací místnosti.

Výsledky expertního hodnocení pak mají následující podobu. Zároveň je v rámci vyhodnocení provedena i kategorizace zkoumaných rizik. U jednotlivých rizik je uvedeno hodnocení hodnotitelů (E1 = expert 1, E2 = expert 2, A = autor práce). Hodnocení těchto tří hodnotitelů je následně zprůměrováno a dochází k součinu (tj. zjištění celkové hodnoty rizika) a zařazení rizika do kategorie.

Z výsledků vyplývá, že dle hodnotitelů má většina rizik velmi vysokou pravděpodobnost vzniku, což je dáno tím, že jde o rizika, která souvisí s využívanými informačními

a komunikačními technologiemi v organizaci. Dále i s tím, že prozatím organizace nerealizovala žádné aktivní kroky v prevenci kompromitujícího vyzařování, a proto je pravděpodobnost jejich vzniku vyšší, než kdyby už v minulosti k některým preventivním krokům došlo. I v rámci dopadu dosahují rizika negativního hodnocení, které je ve formě buď trvalého úniku citlivých dat nebo vysoké pravděpodobnosti úniku citlivých dat.

Tabulka 5: Výsledky hodnocení rizik kompromitujícího vyzařování (Zdroj: Vlastní)

Identifikovaná hrozba	Pravděpodobnost				Dopad				Součin	Kategorie
	E1	E2	A	Průměr	E1	E2	A	Průměr		
1) Zachycení kompromitujícího vyzařování prostřednictvím vedení elektrického napětí	5	5	5	5	5	5	5	5	**25**	Vysoké riziko
2) Zachycení kompromitujícího vyzařování prostřednictvím zdrojů LAN	5	5	5	5	4	4	4	4	**20**	Vyšší riziko
3) Zachycení kompromitujícího vyzařování prostřednictvím odposlechů	5	5	5	5	5	5	5	5	**25**	Vysoké riziko
4) Zachycení kompromitujícího vyzařování prostřednictvím oken	4	5	4	4,33	4	5	4	4,33	**18,78**	Vyšší riziko
5) Zachycení kompromitujícího vyzařování z informačních technologií a jejich komponent	5	5	5	5	5	5	5	5	**25**	Vysoké riziko
6) Zachycení kompromitujícího vyzařování z obrazovek	4	5	5	4,67	4	4	4	4	**18,67**	Vyšší riziko

Z výsledků vyplývá, že polovina identifikovaných rizik spadá do kategorie vysokého rizika. Z tohoto důvodu musí dojít k aktivní reakci na tato rizika, protože jsou velmi závažná a mohou ohrozit fungování a stabilitu organizace. Jejich působení může vést k trvalému úniku citlivých dat z organizace, a to navíc dlouhodobému úniku, protože se jen složitě identifikuje, že dochází ke zneužití kompromitujícího vyzařování útočníkem. Nelze ovšem podceňovat ani rizika v kategorii vyšší riziko.

Návrhy ke zmírnění rizik se zabývá následující část práce.

6 NÁVRH OPATŘENÍ KE ZLEPŠENÍ

Na základě shrnutí veškerých informací a jejich vyhodnocení lze nyní definovat návrhy a opatření ke zlepšení aktuálního stavu. Informace uvedené v rámci této práce jednoznačně poukazují na to, že je kompromitující vyzařování výraznou a významnou bezpečnostní hrozbou. Organizace se vůči jeho působení musí aktivně chránit a realizovat veškerá opatření, aby došlo k eliminaci této bezpečnostní hrozby. Útočníci mají v dnešní době přístup k celé řadě sofistikovaných technologií, které mohou kompromitující vyzařování zneužívat. Jejich cílem pak mohou být právě organizace jako XY, které se zabývají internetovým obchodováním (tedy na internetu lze zjistit, jaké mají skladové zásoby a v jaké výši, kde jsou uskladněné apod.) Prostředí internetového obchodování umožňuje útočníkům získat základní informace o podobě organizace, které pak doplní daty získanými kompromitujícím vyzařováním. Pak už mají usnadněnou pozici pro realizaci krádeže či jiného nekalého jednání. Prevence je v tomto směru velmi žádoucí a nutná. Toto zjištění potvrzuje i skutečnost, že ochranu proti kompromitujícímu vyzařování řeší česká legislativa, avšak pouze u subjektů veřejné správy. Podnikatelské subjekty musí tuto problematiku řešit ve vlastní režii a ve vlastním zájmu.

Prostřednictvím následujících návrhů a doporučení může organizace posílit ochranu svých citlivých dat před zneužitím, zlepšit vlastní bezpečnost (zejména v rámci kyberprostoru), ochránit se lepším způsobem před odposlechy, přijmout bezpečnost v interních procesech jako nezbytnou a důležitou součást činnosti, ale také získá možnost, jak se bránit vzniku mimořádných nákladů souvisejících se ztrátami dat a dalšími problémy.

K návrhům ke zlepšení se řadí následující:

- Protiopatření proti působení výrazných rizik.
- Protiopatření proti působení vyšších rizik.
- Identifikace citlivých dat a režimů práce s těmito kategoriemi.
- Sestavení provozního řádu v oblasti bezpečnosti a kompromitujícího vyzařování.
- Zabezpečení vstupu do budovy a jednotlivých místností s využitím čipů a klíčů.
- Testování a nepřetržitá analýza rizik v oblasti kompromitujícího vyzařování.

Jednotlivé návrhy lze nyní popsat detailnějším způsobem, a to následovně.

6.1 Ochrana proti úniku citlivých dat

Protiopatření proti působení vysokých rizik

Jako první lze navrhnout konkrétní opatření proti působení výrazných rizik v oblasti kompromitujícího vyzařování v budově. Jde o zachycení kompromitujícího vyzařování prostřednictvím vedení elektrického napětí, dále o zachycení kompromitujícího vyzařování prostřednictvím odposlechů či bez odposlechů, či zachycení kompromitujícího vyzařování z informačních technologií.

V oblasti kompromitujícího vyzařování prostřednictvím vedení elektrického napětí lze organizaci doporučit, aby se zaměřila na kontrolu tohoto vyzařování a využívala standardizované a certifikované řešení v této oblasti. Organizace by měla využít odborné poradenství v této oblasti a konzultovat návrh a konstrukci elektrického vedení v objektu s expertem na tuto oblast. Je nutné minimalizovat emise elektromagnetického záření, což lze také ochrannými prostředky jako jsou různé kryty, filtry apod. Veškerá elektronická zařízení musí být také v certifikována.

Zachycení kompromitujícího vyzařování prostřednictvím odposlechů či bez odposlechů je významným rizikem, protože může vést k trvalému úniku citlivých dat. Útočník tímto získá informace o dění v organizaci a plánech organizace, což je kritickým bezpečnostním rizikem. Z tohoto důvodu je nutné aktivně reagovat. Zejména, pak prostřednictvím prohlídek místností za účelem odhalení umístěných odposlechů. K tomuto slouží specializovaná zařízení ve formě detektorů odposlechů. Majitel organizace by měl v pravidelných intervalech provádět kontrolu každé místnosti tímto detektorem. Dále je nutné zamezit vstupu do budovy osobám, které zde mohou odposlouchávací zařízení umístit. To lze zabezpečením vstupu do budovy a jednotlivých místností s využitím čipů a klíčů (tj. jeden z dalších návrhů) a tvorbou pravidel pro vstup a pohyb osob v objektů (tj. jeden z dalších návrhů). Problém může nastat i kvůli odposlechu přes tenké zdivo, jenž může usnadnit zachycení konverzace v místnosti i bez techniky. Prostor mimo objekt budou snímat bezpečnostní kamery, takže by mělo dojít k identifikaci osob, které mohou případně stát

u oken nebo u zdi ve venkovním prostoru. Ve vnitřním prostoru lze riziku zabránit právě tím, že budou formulována pravidla pro pohyb osob v objektu.

Zachycení kompromitujícího vyzařování z informačních technologií a jejich komponent (periferních zařízení) představuje další výrazné riziko, na které je nutné reagovat. Zařízení

typu klávesnic, tiskáren apod. je v organizaci aktivně využíváno v rámci každodenního plnění pracovních úkolů. Zároveň se jedná o zařízení, která vyzařují kompromitující data,

a proto je nutné klást důraz na případně riziko jejich zneužití. Jako řešení rizika (protiopatření) se jeví možnost pořízení počítačových sestav a dalšího vybavení, které má certifikaci v oblasti TEMPEST, tedy jde o počítačové sestavy, které jsou vhodné pro zpracování citlivých dat.

Protiopatření proti působení vyšších rizik

Dále se doporučuje realizovat protiopatření proti působení vyšších rizik, která ještě nenabývají kritický charakter, ale i přesto mohou vést k výraznému ohrožení. Z tohoto důvodu je nutné na tato rizika reagovat.

Zachycení kompromitujícího vyzařování prostřednictvím zdrojů LAN vytváří právě takové vyšší riziko, které může vést k úniku citlivých informací, i když nemusí jít o dlouhodobý únik, protože existují různá protiopatření za účelem detekce narušení LAN. Jako opatření se navrhuje zabezpečit kabely sítě před napadením, a to například jejich umístěním a rozvodem ve zdech objektu, aby se ztížila možnost jejich narušení, ztížil se přístup k těmto kabelům. Z hlediska opatření proti zneužití přenosu dat lze organizaci doporučit, aby využívala šifrování dat (například formou různých protokolů a zabezpečení, antivirových programů), dále by měla umožnit přístup do LAN pouze oprávněným osobám (na základě hesla, PIN kódu apod.) Možností je také omezení využít bezdrátové sítě wifi a využití pouze kabelové sítě.

Dalším rizikem je v oblasti kompromitujícího vyzařování zachycení kompromitujícího vyzařování prostřednictvím oken (ať už pohybu osob v místnosti, nebo obrazu z obrazovek, projektů apod.) Jako základní opatření lze doporučit, aby nedošlo k nasměrování monitorů a obrazovek vůči oknům, tímto by bylo zamezeno takovému kompromitujícímu vyzařování. Dalším řešení je možnost využití poloprůhledných okenních fólií, které absorbují či odráží elektromagnetické vlny, případně využití okenních žaluzií. V místnosti sklad/trezor lze uvažovat o kompletním zatemnění oken, aby nebylo možné, jakkoliv pozorovat z vnějšku pohyb osob v této místnosti.

Dalším výrazným rizikem je zachycení kompromitujícího vyzařování z obrazovky v zasedací místnosti, která je umístěna naproti oknu, a která je poměrně velká, takže umožňuje snímání obsahu i z větší vzdálenosti (navíc je namířena na zemědělskou plochu

a lesní porost). Toto riziko lze vyřešit přesunem obrazovky na jinou zeď, kde nebude namířena proti oknu. Případně, se doporučuje pořízení poloprůhledných okenních fólií (to souvisí i s dalším návrhem), zatemnění oken v průběhu přítomnosti osob v zasedací místnosti.

Identifikace citlivých dat a režimů práce s těmito kategoriemi

Vzhledem k tomu, že je organizace XY podnikatelským subjektem, tak se neřídí legislativními nařízením platnými pro subjekty veřejné správy, které vedou k nutnosti rozdělení zpracovávaných informací do různých kategorií dle citlivosti. To však neznamená, že si organizace XY nemůže provést vlastní identifikaci citlivých dat a zvolit různé režimy práce s těmito daty v rámci svého interního prostředí. Tímto dojde k identifikaci citlivých dat, které musí být chráněné ve větší míře než ostatní data a informace. V současnosti není situace zcela ideální, když mají všichni zaměstnanci přístup k většině informací a dat, ať už o zákaznících, objednávkách, objemech prodejů, dodavatelích apod. Tímto se zvyšuje pravděpodobnost jejich úniku či zneužití.

Organizaci se doporučuje sestavit seznam veškerých dat a informací, s kterými je v organizaci pracováno. Následně provést jejich kategorizaci na citlivá data a běžná data. Běžná data budou dostupná všem zaměstnancům v rámci informačních systémů organizace. Citlivá data však budou dostupná pouze vybraným pracovníkům a majiteli organizace. Tímto se zvýší ochrana důvěrnosti dat a sníží se riziko zneužití dat. Organizace určí konkrétní data, která budou vyžadovat vyšší stupeň ochrany. Tímto stupněm ochrany může být, že budou přístupné pouze po zadání hesla, PIN kódu, případně budou oddělená od informačního systému nebo LAN.

S citlivými daty bude například pracováno v místnostech – kancelář ředitele a sklad/trezor. Obě místnosti je tedy nutné ve větší míře zabezpečit proti úniku citlivých dat formou kompromitujícího vyzařování. Zde se může konkrétně jednat například o objednávky zákazníků ve výši nad 500 000 Kč. Pokud organizace takovou objednávku přijme, tak ji obdrží přímo majitel organizace a bude si ji moci zobrazit pouze na PC ve své kanceláři. Expedici objednávky pak připraví ve skladu, kde také bude pracovat s daty z objednávky (dodací adresa apod.) Informace o této objednávce se tak nedostanou k jiným zaměstnancům, ani nebudou zpracovávané v jiných místnostech, kde mohou být odhalené kompromitujícím vyzařováním.

V rámci tohoto by mělo být dosaženo stavu, kdy budou mít zaměstnanci přístup pouze k informacím, které pro výkon svojí práce potřebují. Tvorba konkrétních režimů práce s běžnými a citlivými daty posílí ochranu citlivých dat před zneužitím, včetně kybernetických útoků a úniku prostřednictvím kompromitujícího vyzařování.

Sestavení provozního řádu v oblasti bezpečnosti a kompromitujícího vyzařování

Selhání lidského faktoru patří k nejčastějším bezpečnostním rizikům, a to platí i v oblasti kybernetické bezpečnosti. Ať už úmyslně, či neúmyslně, tak lidé svým jednáním představují hrozbu pro bezpečnost. Vybavenost organizace XY nejmodernějšími technologiemi nebude efektivní, když budou zaměstnanci porušovat elementární bezpečnostní pravidla.

Z tohoto důvodu je nutné sestavit provozní řád v oblasti bezpečnosti a kompromitujícího vyzařování, který budou zaměstnanci dodržovat, a jehož dodržování bude kontrolováno majitelem organizace.

Provozní řád by měl zaměstnancům vysvětlit problematiku kompromitujícího vyzařování, aby došlo k lepšímu pochopení významu realizovaných opatření. Měl by definovat potenciální rizika úniku (lze vycházet z realizované analýzy rizik v rámci práce) a objasnit způsoby, jak se preventivně chránit proti těmto rizikům.

Z hlediska objektu by pak mělo dojít k identifikaci prostorů, které jsou nejvíce vystavené rizikům kompromitujícího vyzařování, a tedy zároveň i zde identifikovat způsoby ochrany a snižování rizika. V tomto případě lze vycházet z návrhů protiopatření vůči rizikům.

Provozní řád by měl formulovat i pravidla používání mobilních telefonů zaměstnanců. Soukromé mobilní telefony se mohou stát cílem kybernetických útoků, a pokud je zaměstnanci využívají i k řešení pracovních záležitostí, tak může dojít právě i k úniku citlivých podnikových informací. V objektu by měl zaměstnanec využívat pouze služební mobilní telefon, který bude dostatečně zabezpečen proti zneužití kompromitujícího vyzařování.

Dodržování pravidel je pak samozřejmě nutné neustále kontrolovat a případně sankciovat jejich porušení. Problematiku nelze podceňovat, což si musí pracovníci uvědomit. Jako vhodný nástroj pro podporu zájmu zaměstnanců o dodržování těchto pravidel a řádu se jeví uspořádání školení, kde bude pracovníkům vysvětleno vše, co se týká řešené problematiky.

Zabezpečení vstupu do budovy a jednotlivých místností s využitím čipů a klíčů

Dalším doporučením je potom zabezpečení vstupu do budovy a jednotlivých místností s využitím čipů a klíčů, aby se zamezilo riziko pohybu nepovolaných osob v místnostech objektu. Nepovolané osoby zde mohou instalovat například odposlechy, kamery apod. V současnosti není zabezpečení vstupu do budovy příliš dostačující. V provozní době se může do objektu dostat prakticky každý návštěvník. Z tohoto důvodu se doporučuje implementovat systém využití čipů a klíčů pro přístup do objektu a jeho jednotlivých místností, aby došlo k minimalizaci rizika přítomnosti nežádoucí osoby v objektu. Tímto se zvýší i ochrana informací, s kterými organizace pracuje.

Testování a nepřetržitá analýza rizik v oblasti kompromitujícího vyzařování

Dále se organizaci doporučuje provádět pravidelné testování v oblasti prevence kompromitujícího vyzařování. K tomuto lze využívat externí poradenské služby, kdy testování provedou odborníci s kvalitními znalostmi v této oblasti a s využitím moderních technologií. Mělo by docházet například ke kontrole toho, jakým způsobem organizace dodržuje doporučení z různých norem apod. Testování se musí zaměřit na zhodnocení fungování protiopatření, a to dle konkrétních požadavků na eliminaci kompromitujícího vyzařování v organizaci.

S tímto pak souvisí i návrh na nepřetržitou analýzu rizik v oblasti kompromitujícího vyzařování. Organizace by měla i nadále neustále identifikovat rizika v této oblasti, včetně oblasti kybernetické bezpečnosti, aby zabránila zneužití dat prostřednictvím kybernetického postupu. Celý proces analýzy rizik by měl tedy probíhat v pravidelných intervalech.

V rámci obsahu analýzy rizik je také vhodné věnovat se rizikům i z dalších oblastí. Jako jsou například finanční rizika, provozní rizika apod. V této práci byla předmětem primárního zájmu zejména rizika související s kyberbezpečností a kompromitujícím zářením, ale v podnikatelské praxi se nelze omezovat pouze na analýzu vybraných rizik. Je nutné hodnotit a sledovat veškerá možná rizika, která mohou organizaci ohrožovat.

6.2 Náklady na realizaci opatření

V souvislosti s návrhy je vhodné věnovat pozornost i nákladové stránce jejich realizace. Organizace dosahuje ziskovosti přesahující několik milionů korun ročně, a proto nebudou celkové náklady pro organizaci příliš vysoké. Navíc mají opatření vést ke snižování rizik

zneužití citlivých dat. Takové zneužití citlivých dat může v konečném důsledku ohrozit další existenci organizace, a proto jsou takové náklady vždy účelné a přínosné.

Část nákladů na navrhovaná opatření má také podobu personálních, časových a administrativních nákladů, takže nevznikají konkrétní finanční náklady (ekonomické náklady). Takové náklady tedy nelze přímo kvantifikovat, ale je nutné počítat s jejich existencí. Jde například o časové a personální náklady na identifikaci dat v organizaci

a jejich rozřazení do kategorií citlivé a běžné, dále o personální a časové náklady na tvorbu interní bezpečnostní směrnice apod.

Z finančních nákladů pak lze kalkulovat zejména s následujícími položkami:

- Využití poradenských a konzultačních služeb – jedná se o využití různých poradenských a konzultačních služeb v rámci oblasti prevence zneužití kompromitujícího vyzařování.
- Pořízení filtrů, krytů pro ochranu elektrického napětí – jde o prvky, které mají eliminovat riziko zachycení kompromitujícího vyzařování prostřednictvím elektrického vedení.
- Pořízení detektorů odposlechů a bezdrátových kamer – jedná se o nákup detektoru odposlechů a bezdrátových kamer (na trhu se prodávají detektory v rámci jednoho produktu).
- Pořízení okenních fólií (poloprůhledné) – jde o náklady na nákup a instalaci poloprůhledných fólií do oken objektu.
- Instalace zatemnění oken – jedná se o instalaci kompletního zatemnění oken v místnosti sklad/trezor.
- Pořízení počítačových sestav pro práci s citlivými údaji – zde jde o nákup počítačových sestav, které jsou v souladu s certifikací TEMPEST.
- Nákup software pro eliminaci rizik (antivir, firewall) – v tomto případě jde o pořízení softwarových řešení, které jsou určené pro eliminaci kybernetických rizik.

Očekávané náklady potom shrnuje následující tabulka. Odhady nákladů vychází z konzultace s majitelem organizace, dále z vlastního průzkumu trhu. Celkové finanční náklady jsou na úrovni 199 000 Kč, včetně práce.

Tabulka 6: Náklady na realizaci opatření (Zdroj: Vlastní)

Náklady na realizaci opatření	
Využití poradenských a konzultačních služeb	50 000 Kč
Pořízení filtrů, krytů pro ochranu elektrického napětí	10 000 Kč
Pořízení detektorů odposlechů a bezdrátových kamer	25 000 Kč
Pořízení okenních fólií (poloprůhledné)	4 000 Kč
Instalace zatemnění oken	10 000 Kč
Pořízení počítačových sestav pro práci s citlivými údaji	90 000 Kč
Nákup software pro eliminaci rizik (antivir, firewall)	10 000 Kč
Celkem	199 000 Kč

Podobně jako vznikají i neekonomické náklady na realizaci navrhovaných opatření, tak vznikají i mimoekonomické přínosy z jejich realizace. Preventivní opatření v oblasti proti úniku dat kompromitujícím vyzařováním vytváří prostředí, ve kterém dochází k ochraně citlivých dat a informací. Organizace tímto získává větší míru jistoty, že není bezprostředně ohrožena různými kybernetickými riziky. Celkově tímto systémem může získat i větší důvěryhodnost u svých obchodních partnerů, jejichž data jsou také v rámci prevence chráněné. V konečném důsledku tedy navržená opatření zvyšují i spokojenost zákazníků

a mohou vést k vyšším tržbám organizace.

Organizace XY využívá aktivně a každodenně moderní informační a komunikační technologie. Jsou nezastupitelnou součástí práce zaměstnanců a managementu organizace. Nevytváří však pouze výhody, ale také nevýhody, protože jejich využití je rizikové z hlediska bezpečnosti. Kybernetické hrozby představují významné riziko, které nesmí být nikterak podceněno. Počet kybernetických útoků neustále roste a cílí právě i na podnikatelské subjekty. Cílem organizace v oblasti kybernetické bezpečnosti musí být

zajištění obrany a ochrany vlastního kybernetického prostoru za účelem zajištění dostupnosti, integrity a důvěrnosti kybernetických systémů.

Kompromitující vyzařování představuje právě jedno z rizik v oblasti kybernetické bezpečnosti, které musí být akceptováno, identifikováno a hodnoceno, aby mohlo dojít k realizaci nápravných opatření. Problematika je podstatná i z toho hlediska, že v dnešní době může být zdrojem kompromitujícího vyzařování jakékoliv elektromechanické či elektronické zařízení, které se využívá pro zpracování zabezpečovaných informací. Ochranu proti zneužití kompromitujícího vyzařování pak mohou organizace realizovat různými způsoby. Právě výstupy z této práce poskytují konkrétní příklady a návrhy, jak se může organizace XY bránit tomuto riziku. Jedná se o kombinaci preventivních opatření, výběru relevantních informačních technologií s vhodnými funkcemi a ve vhodných formátech, zajištění minimální úrovně signálu všech datových obvodů, stínění, filtrování a izolace. To znamená, že dochází k využití efektivních kroků pro prevenci kompromitujícího vyzařování tak, jak je doporučují i odborné zdroje.

Po implementaci navrhovaných opatření lze očekávat výrazné zlepšení aktuální situace v organizaci. To znamená, že dojde ke snížení pravděpodobnosti vzniku identifikovaných rizik, protože organizace přijme preventivní opatření.

Ověření aplikovatelnosti navržených opatření

Veškerá navržena opatření byla konzultována s experty i majitelem. Oba experti zhodnotili navržená opatření a tato posoudili jako aplikovatelná. V závěru lze tedy doporučit organizaci, aby realizovala uvedené návrhy a doporučení ke zlepšení.

ZÁVĚR

Tato práce se zabývala problematikou kompromitujícího vyzařování v kontextu kybernetické bezpečnosti a podnikatelského sektoru. Je to právě kompromitující vyzařování, které představuje závažné bezpečnostní riziko, ale v řadě případů si to organizace nemusí uvědomovat a mohou toto riziko podceňovat. Je však zřejmé, že dnešní vývoj informačních technologií vede k tomu, že obsahují široké spektrum různých citlivých obchodních informací a osobních údajů, které mohou být zneužité. Tímto se rozšiřují i možnosti pro útočníky, kteří mohou přicházet se stále novými způsoby ohrožení kyberbezpečnosti

a zneužití kompromitujícího vyzařování. Zajišťování bezpečnosti v těchto oblastech je tedy neustálou výzvou, ať už pro subjekty ve veřejném či soukromém sektoru, nebo jednotlivce.

Protiopatření proti působení vysokých rizik a vyšších rizik mají různorodou podobu a jsou uvedené v příslušné části práce. Na jednu stranu vychází z odborných doporučení z odborných zdrojů, ale zároveň respektují i konkrétní situaci ve zkoumané organizaci. Dále se doporučuje provést identifikaci citlivých dat a nastavit režimy práce s těmito kategoriemi, protože v současnosti mají všichni zaměstnanci organizace přístup k téměř všem informacím, což není zcela vhodné. Tímto se zvyšuje riziko úniku dat. Dále se doporučuje provést lepší zabezpečení vstupu do budovy a jednotlivých místností s využitím čipů a klíčů, což lze chápat jako bezpečnostní opatření snižující riziko pohybu nepovolaných osob v objektu. Posledním návrhem je provádět pravidelné testování úrovně kompromitujícího vyzařování, a také neustále realizovat analýzu rizik v oblasti kompromitujícího vyzařování.

Kompromitující vyzařování je v oblasti kybernetické bezpečnosti pojmem poměrně zavedeným a historickým, protože se o něm hovoří prakticky již od šedesátých let minulého století. V současnosti je také diskutován, ale řada informačních zdrojů, které se tomuto pojmu věnují, je spíše starší, což komplikovalo zpracování teoretické části práce.

I v současnosti však musí organizace přistupovat k řešení tohoto rizika aktivně. Významná rizika v oblasti kompromitujícího vyzařování ve zvoleném podniku jsou pak identifikována v příslušné části práce, kde se nachází i jejich vyhodnocení.

Všechna tato rizika pak dle vyhodnocení patří do kategorie vysokých či vyšších rizik, na které musí být reagováno. Tato reakce má podobu právě definice návrhů a doporučení k minimalizaci jejich působení.

Výstupy z práce budou předložené managementu vybrané organizace, aby provedl jejich implementaci do praxe. Závěry z práce slouží nejen k tomu, aby management získal povědomí o závažnosti této bezpečnostní hrozby, ale také k tomu, aby přijal konkrétní a funkční opatření proti hrozbě a rizikům.

SEZNAM POUŽITÉ LITERATURY

ASTRODYNETDI. What is TEMPEST? *Www.astrodynetdi.com* [online]. 2023 [cit. 2023-04-20]. Dostupné z: https://www.astrodynetdi.com/blog/tempest-emi-filters

BAŠTA, P. et al. CyberSecurity. Praha: Cz.nic, 2019. ISBN 9788088168324.

CAZANARU, Daniela; COSEREANU, Liviu; SZILAGYI, Andrei. Evaluation of the compromising radiation by electromagnetic compatibility tests. *University" Politehnica" of Bucharest Scientific Bulletin, Series A: Applied Mathematics and Physics*, 2011, 73.2: 185-192.

ČESKÁ REPUBLIKA. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.* 2005.

ČESKÁ REPUBLIKA. *Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.* 2005b.

DOLEŽAL, Jan. *Projektový management: komplexně, prakticky a podle světových standardů*. Praha: Grada Publishing, 2016. Expert (Grada). ISBN 978-80-247-5620-2.

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

JALALI, Mohammad S.; KAISER, Jessica P. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical internet research*, 2018, 20.5: e10059.

JANÍČEK, Přemysl a Jiří MAREK. *Expertní inženýrství v systémovém pojetí*. Praha: Grada, 2013, 592 s. Expert (Grada). ISBN 978-80-247-4127-7.

JANSA, Lukáš et al. *Internetové právo*. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

KAVAK, Hamdi, et al. Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, 2021, 7.1: tyab005.

KEŘKOVSKÝ, Miloslav a Miloš DRDLA. *Strategické řízení firemních informací: teorie pro praxi*. Praha: C.H. Beck, 2003. C.H. Beck pro praxi. ISBN 80-7179-730-8.

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

KUHN, Markus. Compromising Emanations. *Link.springer.com* [online]. 2011 [cit. 2023-04-24]. Dostupné z: https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_188

KUHN, Markus G. Compromising emanations of LCD TV sets. *IEEE Transactions on Electromagnetic Compatibility*, 2013, 55.3: 564-570.

LEE, Euibum, et al. A Quantitative Analysis of Compromising Emanation From TMDS Interface and Possibility of Sensitive Information Leakage. *IEEE Access*, 2022, 10: 73997-74011.

MAISNER, Martin, 2015. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 978-807-4788-178.

MARTIN, Maxwell; SUNMOLA, Funlade; LAUDER, David. Unintentional compromising electromagnetic emanations from IT equipment: A concept map of domain knowledge. *Procedia Computer Science*, 2022, 200: 1432-1441.

MONZAS, spol. s r.o.*: Divize slaboproudých a bezpečnostních systémů* [online]. [cit. 2023-04-26]. Dostupné z: https://monzas.cz/strediska/divize-zabezpecovaci-a-komunikacni-systemy

MUDROCH LABS s.r.o.*: Faradayova místnost* [online]. [cit. 2023-04-29]. Dostupné z: http://www.triangulace.cz/konstrukce-faradayovy-mistnosti-bezpecna-kancelar/

MUDROCH LABS. *Ochrana proti odposlechu, odposlouchávací zařízen*í v praxi. *Www.triangulace.cz* [online]. 2011. [cit. 2023-04-23]. Dostupné z: http://www.triangulace.cz/ochrana-proti-odposlechu-odposlouchavaci-zarizeni-v-praxi/

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Bezpečnostní standard Národního bezpečnostního úřadu 2/2011. 2011.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Standardy. *Www.nbu.cz* [online]. 2023 [cit. 2023-04-23]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/kompromitujici-vyzarovani/1000-standardy/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Metodické pokyny. *Nukib.cz/* [online]. 2023 [cit. 2023-04-25]. Dostupné z: https://nukib.cz/cs/ochrana-ui-v-ict/tempest/metodicke-pokyny/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o činnosti 2021*. 2022.

NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

SAFEGUARD-ESHOP: Špionážní technika [online]. [cit. 2023-04-29]. Dostupné z: https://www.safeguard-eshop.net/c/spionazni-technika

SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. [Praha]: Petrklíč, 2018. ISBN 978-80-7229-652-1.

SNIDER, Keren LG, et al. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 2021, 7.1: tyab019.

VUAGNOUX, Martin; PASINI, Sylvain. An improved technique to discover compromising electromagnetic emanations. In: *2010 IEEE International Symposium on Electromagnetic Compatibility*. IEEE, 2010. p. 121-126.

ZHANG, Alex. What Is TEMPEST and How Does It Relate to Cybersecurity? *Blog.enconnex.com* [online]. 2022 [cit. 2023-04-25]. Dostupné z: https://blog.enconnex.com/what-is-tempest

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A	Autor práce
AM	Amplitudová modulace
CRT	Cathode Ray Tube
dB	decibel
DVI	Digital Visual Interface
E1	Expert 1
E2	Expert 2
EU	Evropská Unie
GHz	Gigahertz
IDS	Systémy detekce narušení
kHz	Kilohertz
LAN	Local Area Network
LCD	Liquid Crystal Display
NATO	North Atlantic Treaty Organization
NÚKIB	Národní úřad pro kybernetickou bezpečnost
PC	Personal Computer
PIN	Personal Identification Number
RAM	Random Access Memory
SDIP	Označení bezpečnostního standartu NATO
TCP/IP	Transmission Control Protocol/ Internet Protocol
UHF	Ultra High Frequency
USB	Universal Seriál Bus
WC	Water Closet
Wi-Fi	Wireless Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK