

Ochrana financí v kyberprostoru: Rizika, hrozby a strategie pro efektivní management

Bc. Jiří Valenta

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Jiří Valenta
Osobní číslo:	A23368
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní management
Forma studia:	Prezenční
Téma práce:	Ochrana financí v kyberprostoru: Rizika, hrozby a strategie pro efektivní management
Téma práce anglicky:	Protecting Finances in Cyberspace: Risks, Threats and Strategies for Effective Management

Zásady pro vypracování

- Provedte literární rešerši tématu.
- Provedte analýzu rizik s ohledem na bezpečnost financí a prostředí kyberprostoru.
- Porovnejte dostupná řešení a navrhněte způsoby ochrany financí z pohledu efektivního řízení rizik.
- Implementujte své návrhy do podoby doporučení pro konkrétní specifické případy.
- Provedte kritickou diskusi nad vytvořenými návrhy a jejich skutečným využitím.

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

Seznam doporučené literatury:

1. NARAYANAN, Arvind; BONNEAU, Joseph; EDWARD, Felten; MILLER, Andrew a GOLDFEDER, Steven. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, [2016]. ISBN 978-0-691-17169-2.
2. PŘÁDKA, Michal a KALA, Jan. *Elektronické bankovníctví: rady a tipy. Praxe manažera*. Praha: Computer Press, 2000. ISBN 8072263285.
3. NOVÁK, Michal. *Lightning network: platby budoucnosti*. [Praha]: Braiins Systems, 2023. ISBN 978-80-908709-4-9.
4. GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy. Zip*. Praha: Argo, 2013. ISBN 9788073635220.
5. KORYČANSKÁ, Martina. *Informační technologie v bankovníctví*. Vedoucí Zelinka, Stanislav. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav elektroniky a měření, 2020. Dostupné také z: <http://hdl.handle.net/10563/47908>.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 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.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Diplomová práce se zabývá kybernetickou bezpečností zaměřenou na finance českých koncových uživatelů a má za úkol představit rizika a jak se k těmto rizikům stavět a pracovat. V teoretické části je představena a popsána bezpečnost spolu s riziky, které se v kyberprostoru vyskytují a konkrétní útoky, které se staly a měly značný dopad na finance. Taktéž je to doplněno o legislativu týkající se kyberbezpečnosti a financí. V praktické části jsou uvedeny opatření pro zvýšení bezpečnosti a porovnání některých dostupných produktů na trhu. Dále jsou v práci zanalyzovány rizika a ty největší hrozby jsou následně rozebrány. V závěru jsou vypracovaná doporučení, která mají za úkol preventivně snížit počet kybernetických útoků na koncové uživatele.

Klíčová slova: kybernetická bezpečnost, finance, management, bezpečnost, legislativa, rizika, kryptoměny

ABSTRACT

The thesis deals with cybersecurity focused on the finances of Czech end users and aims to present risks and how to approach them and work with these risks. The theoretical part presents and describes security along with the risks that occur in cyberspace and specific attacks that have occurred and had a significant impact on finances. It is also extended by legislation related to cybersecurity and finances. The practical part presents measures to increase security and a comparison of some available products on the market. The thesis also analyses risks and discusses the biggest threats. In the conclusion, recommendations are developed that aim to preventively reduce the number of cyber attacks on end users.

Keywords: cybersecurity, management, finance, security, legislation, risks, cryptocurrencies

Chtěl poděkovat mému vedoucímu práce prof. Mgr. Roman Jašek, Ph.D., DBA za rady a pomoc se zpracováním diplomové práce.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 KYBERNETICKÁ BEZPEČNOST	15
1.1 BEZPEČNOST	15
1.2 INFORMAČNÍ BEZPEČNOST.....	15
1.3 VÝZNAM KYBERNETICKÉ BEZPEČNOSTI	16
1.4 KYBERNETICKÁ BEZPEČNOST VE FINANČNÍM SEKTORU	17
1.5 VÝZNAM KYBERNETICKÉ BEZPEČNOSTI VE FINANCÍCH	17
1.5.1 Ochrana citlivých dat	17
1.5.2 Prevence finančních ztrát	18
1.6 CIA TRIÁDA	18
1.6.1 Důvěrnost	18
1.6.2 Integrita	19
1.6.3 Dostupnost.....	19
1.7 ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI	20
1.7.1 Aktiva.....	20
1.7.2 Hrozby.....	20
1.7.3 Zranitelnost	22
1.8 SPOTŘEBITELÉ V KYBERNETICKÉ BEZPEČNOSTI	22
2 REGULACE A LEGISLATIVNÍ OPATŘENÍ.....	24
2.1 DORA.....	25
2.2 MiCA.....	26
2.3 PSD2.....	27
2.4 NIS2	27
2.5 AML	29
3 VÝVOJ A TRENDY	31
3.1 UMĚLÁ INTELIGENCE	32
3.2 ZTA	33
3.3 KVANTOVÁ KRYPTOGRAFIE A KVANTOVÉ POČÍTAČE.....	33
3.4 KRYPTOMĚNY	34
3.4.1 CBDC	35
4 RIZIKA A HROZBY FINANCÍ V KYBERPROSTORU.....	35
4.1 TYPY KYBERNETICKÝCH ÚTOKŮ V OBLASTI FINANCÍ	36
4.1.1 Phishing.....	37
4.1.2 Malware.....	38
4.1.3 Sociální inženýrství	39

4.1.4	Man in the middle.....	39
4.1.5	DDoS útoky.....	39
4.2	KYBERNETICKÉ ÚTOKY A PODVODY NA FINANČNÍ INSTITUCE.....	39
4.2.1	Pád burzy FTX	39
4.2.2	Útok na Bybit	40
4.2.3	DDoS na české banky.....	41
SHRNUTÍ TEORETICKÉ ČÁSTI		41
II PRAKTICKÁ ČÁST		43
5	DOSTUPNÁ BEZPEČNOSTNÍ ŘEŠENÍ.....	44
5.1	CHOVÁNÍ NA INTERNETU	44
5.2	DVOU FAKTOROVÁ AUTENTIZACE	44
5.2.1	Více faktorová autentizace	47
5.3	HESLA	47
5.4	BEZPEČNOSTNÍ PROGRAMOVÉ VYBAVENÍ.....	48
5.5	KRYPTOMĚNOVÉ BEZPEČNOSTNÍ ŘEŠENÍ	49
5.5.1	Seed fráze	51
5.5.2	Online peněženky	51
5.5.3	Software peněženky	51
5.5.4	Hardwarové peněženky	52
5.5.5	Multi-sig peněženka	52
5.5.6	Diverzifikace úložišť	53
5.5.7	Dodatečná zabezpečení kryptoměnových peněženek	53
5.6	SROVNÁNÍ KRYPTOMĚNOVÝCH PENĚŽENEK	54
5.6.1	Trezor Safe 3	56
5.6.2	Ledger Nano S Plus.....	56
5.6.3	Trust Wallet.....	57
5.7	SROVNÁNÍ BROKERŮ	58
5.7.1	EToro.....	60
5.7.2	XTB.....	61
5.7.3	Trading 212	61
6	ANALÝZA HROZEB	62
6.1	PNH ANALÝZA	63
6.1.1	Vyhodnocení analýzy	66
6.2	NIST CYBERSECURITY FRAMEWORK 1.1	66
6.2.1	Sociální inženýrství	68
6.2.2	Krádež identity	68
6.2.3	Krádež přihlašovacích údajů	69
6.2.4	Phishing.....	70
6.2.5	Podvody.....	70
7	BEZPEČNOSTNÍ DOPORUČENÍ.....	72

7.1	BEZPEČNÁ SPRÁVA HARDWAROVÝCH KRYPTOMĚNOVÝCH PENĚŽENEK	73
7.2	BEZPEČNÁ SPRÁVA FINANČNÍCH ÚČTŮ A PREVENCE PROTI PODVODŮM.....	73
7.3	BEZPEČNÉ POUŽÍVÁNÍ INTERNETU	74
7.4	PROČ SE ZABÝVAT BEZPEČNOSTNÍ KYBERNETICKÝCH FINANCÍ A INVESTOVÁNÍM.....	74
SHRNUTÍ PRAKTICKÉ ČÁSTI.....		77
ZHODNOCENÍ PRÁCE.....		78
ZÁVĚR		80
SEZNAM POUŽITÉ LITERATURY.....		81
SEZNAM OBRÁZKŮ		88
SEZNAM TABULEK.....		89
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....		90

ÚVOD

Svět financí se v posledních desetiletích hodně změnil. Jedním z hlavních důvodů je globalizace a digitalizace, která má za úkol zjednodušit a zpříjemnit uživatelům svůj komfort při práci s financemi. S tímto trendem přichází mnoho výhod, jako jsou rychlost a globální dostupnost. Uživatelé mohou spravovat finance kdekoliv ve světě. To znamená posílání plateb, investování do globálních trhů a využívání moderních fintech technologií. S digitalizací ale přichází i velká řada rizik a hrozeb, se kterými se setkávají jednotliví uživatelé i instituce. Kybernetická bezpečnost, je tak klíčovým prvkem pro ochranu finančních aktiv napříč světem.

Ve finančním kybernetickém prostoru již nefiguruje jenom banky, jak tomu bylo před 10 až 20 let zpět. Nyní jsou finance na internetu zastoupeny ve velkém spektru jiných institucí a aktiv. V dnešní době je možné ukládat finance do kryptoměn, investovat virtuálně do zlata, pozemků, nemovitostí, akcií, forexu, komodit a mnoha dalších možností, které přitahují nejen investory, ale i útočníky.

Kybernetické hrozby se ve finančním sektoru vyvíjejí stejně rychle jako nové technologie. Jelikož drtivá většina financí, které na světě i v České republice máme je v digitální podobě. To láká útočníky s vidinou rychlého zbohatnutí využívat a tvořit nové metody k jejich napadení.

Ve světě financí existují dva pohledy na bezpečnost, a to jsou ty viditelné hrozby v podobě útočníků a druhým pohled, kterým je hrozba inflace a poplatků na finance, které v dlouhodobém horizontu mohou ztrácet na své hodnotě. Ve výsledku se tak jedná o velmi podobný problém, jako kdyby nám tyto finance odcizil útočník.

Cílem práce je přiblížit problematiku a jednotlivá rizika pro uživatele na českém trhu, kde na ně čekají hrozby na každém kroku v souvislosti s aktuální a nadcházející digitalizací světa. Ale také si ukázat, jak se k těmto rizikům postavit a jak s nimi pracovat, tak aby se snížila možnost případného incidentu. Dále se práce zaměří na představení aktuálních hrozeb, postupů, regulatorních opatření a ochranných prostředků a strategií, které nám pomohou zabezpečit naše finance.

I TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Definicí kybernetické bezpečnosti je: „*Kybernetická bezpečnost je souhrn metod, procesů, nástrojů a postupů, které chrání počítačové systémy, sítě a data před kybernetickými útoky a neoprávněným přístupem.*“ [1]

Kybernetická bezpečnost je sice úzce spojena s technologiemi, ale její účinnost z velké části závisí na lidském faktoru. Lidská chyba, nedbalost nebo nedostatečné vzdělání může tvořit vyšší míru zranitelnosti. Pro prevenci narušení bezpečnosti informačních systémů je důležité se držet osvědčených postupů a vzdělávat se. [1]

1.1 Bezpečnost

Pro pochopení kybernetické bezpečnosti je důležité si představit co znamená pojem bezpečnost. Pojem bezpečnost představuje stav jistoty, která minimalizuje pocit ohrožení. Bezpečnost je tu již od počátku lidské existence a bezpečnostní odvětví se v čase měnilo a vyvíjelo. Mezi hlavní odvětví ochrany se řadí život a zdraví, majetek a informace. Tyto kategorie spolu úzce souvisí, kdy narušení jednoho odvětví, například úniku důvěrné informace v podobě údajů bankovního účtu může vést k finanční ztrátě, majetku a jiným závažným důsledkům. [2]

Každý jedinec, organizace nebo instituce si musí určit co chránit, proti jaké hrozbě a jakými prostředky. Pro organizace a instituce je základní bezpečnost dána regulacemi, nařízeními a zákony, tak aby se předešlo velkým škodám. [2]

1.2 Informační bezpečnost

Definici informační bezpečnosti chápeme jako „*Zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.*“ [1]

Informace mají hodnotu v závislosti na významu a citlivosti informace. Lze tedy s nimi nakládat podobně jako s penězi, jelikož informace mohou být obchodovány, zničeny nebo zneužity. Třeba informace týkající se chování spotřebitelů a toho co si spotřebitelé kupují, to jsou informace s vysokou hodnotu. Díky těmto informacím lze optimalizovat nabídku, tak aby spotřebitel utratil v daném obchodě více. To vede k navýšení zisků firmem. S digitálním rozvojem se informace staly snadněji přístupné a náchylnější ke kompromitaci. Informační

bezpečnost se stala klíčovým oborem, který se zabývá ochranou dat před neoprávněnou manipulací, přístupem a ztrátou. Odvětví, kde informace mají vysokou hodnotu jsou například bankovníctví, armáda, státní správa, zdravotnictví a podobně. [2]

Moderní informační bezpečnost se zaměřuje na komplexní ochranu informačních systémů, která zahrnuje fyzické, technické, logické a organizační opatření. Bezpečnostní politika se může značně lišit. Od těch nejvíce přísných, kde je vše zakázáno, tak až po zcela otevřený přístup, kde není nic zakázáno. Uprostřed mezi těmito extrémními protiklady se nachází přísná bezpečnost, kterou lze definovat tím co není výslovně povoleno, je zakázáno. Naopak povolná bezpečnost funguje opačně, že co není výslovně zakázáno, je povoleno. Pod povolnou bezpečnost spadají třeba blacklisty (seznamy zakázaných položek), kde mohou být například seznamy zakázaných ip adres, domén a aplikací. V případě přísné bezpečnosti se používají whitelisty (seznamy povolených položek), které mohou obsahovat seznamy ip adresy, kterým byl přístup povolen. [2]

1.3 Význam kybernetické bezpečnosti

Význam kybernetické bezpečnosti spočívá v rychle se transformujícím digitálním světě, kde se změnila návyky organizací i jednotlivců, jakým způsobem nakupují, komunikují a pracují. E-commerce, práce na dálku, cloudová úložiště a digitální data se staly pilíři nynějšího života. [1]

Kromě osobních a obchodních využití je v online prostoru spravována kritická infrastruktura – energetická, vodohospodářská, dopravní, zdravotnická, finanční a mnoho dalších. Ty jsou v ohrožení proti kybernetickým útokům, jelikož v momentě, kdyby nějaká z těchto infrastruktur byla napadena, představovalo by to velké škody. Organizace a spotřebitelé vkládají důvěru v digitální systémy, které používají každý den. [1]

V této rychle vyvíjející se oblasti se neustále zvyšuje složitost nových technologií z důvodu konkurenceschopnosti, vývoje a růstu. Avšak jejich správa a zabezpečení představuje čím dál větší výzvu. Na to navazují i neustále se vyvíjející hrozby. Útočníci přicházejí s čím dál sofistikovanějšími útoky, na zranitelnější organizace díky neustálým potřebám měnit bezpečnostní prvky a politiku s přicházejícími technologiemi. S novými technologiemi se může stát, že bezpečnostní strategie jsou zastaralé a nejsou dostatečně bezpečné pro ochranu systémů. Proto je důležité se zabývat kybernetickou bezpečností a zajištěním spolehlivosti systémů, jelikož na tom závisí osobní bezpečnost, úspory a životy. [1]

1.4 Kybernetická bezpečnost ve finančním sektoru

V bezpečnosti týkající se financí se musí brát v úvahu dva klíčové aspekty. Hodnotový a kybernetický aspekt bezpečnosti, kdy kybernetický aspekt má za úkol chránit před digitálními hrozbami, které vedou k přímým finančním ztrátám a hodnotový aspekt má chránit proti postupné ztrátě hodnoty v podobě inflace, poplatků a podobně.

Poměr financí se liší ve fyzické a virtuální podobě. Na základě průzkumů z roku 2020, kdy na obyvatele spadá 60 153 Kč ve fyzické podobě a ve virtuální podobě to činí necelých 330 000 korun. Tento poměr je 1:5,5 v České republice. Objem virtuálních peněz přesahoval hranici 3,5 bilionu Kč. To jsou jenom peníze uložené ve formě jednodenních vkladů na běžných a spořicíh účtech dle České národní banky. Lze tedy předpokládat, že podíl virtuálních peněz bude ještě vyšší. [4]

Hlavní výhodou financí na internetu je možnost přístupu k finančním prostředkům 24 hodin denně, 365 dní v roce na jakémkoliv místě ve světě. To stejné platí ale i pro potencionální útočníky. [5]

1.5 Význam kybernetické bezpečnosti ve financích

Ve světě financí musí existovat rovnováha mezi kybernetickou bezpečností a hodnotovou ochranou finančních aktiv. Velmi dobře zabezpečená finanční aktiva mohou ztrácet na hodnotě díky inflaci, poplatkům a zároveň nízkému nebo žádnému úročení těchto peněz. V opačném případě, kdy hodnota finančních aktiv narůstají, mohou zároveň představovat vysoké riziko v případě nedostatečného zabezpečení a podvodů. Společnosti musí najít optimální zabezpečení z obou pohledů, aby mohli zůstat konkurenceschopné na trhu.

1.5.1 Ochrana citlivých dat

Hlavním cílem kybernetické bezpečnosti ve financích je ochrana osobních a finančních údajů uživatelů. Banky, fintech společnosti a další instituce pracují s velkým množstvím důvěrných dat. Únik těchto dat může vést ke krádeži identity, neoprávněným transakcím či finančním ztrátám. Bezpečnostní oddělení v těchto firmách se snaží o bezpečné ukládání a šifrování dat s oprávněním jen pro osoby, které s těmito daty musí pracovat. Ochrana citlivých dat je dána právními a regulatorními předpisy. Hraje i klíčovou roli v udržení si důvěry zákazníků v danou instituci. [1]

1.5.2 Prevence finančních ztrát

Útočníci mohou krást peníze přímo z bankovních účtů, manipulovat se záznamy transakcí nebo zneužívat informace o platebních kartách k podvodným nákupům. Tyto skutečnosti mohou vést k pokutám, právním poplatkům a nákladům na odškodnění poškozených klientů. Tím, že instituce implementují kybernetické zabezpečení pomáhají minimalizovat dopad útoků, zvyšovat kredibilitu u zákazníků a vyhýbat se nechtěným nákladům na odškodnění, soudní spory a sankce. [1]

1.6 CIA triáda

Trojimperativ CIA představuje základní tři pilíře kybernetické bezpečnosti confidentiality, integrity a availability neboli důvěrnost, integritu a dostupnost. Jedná se o základní koncept kybernetické bezpečnosti, který se zaměřuje na ochranu dat a informačních systémů. Je využíván k identifikování zranitelností a hledání řešení. Rozdělení důvěrnosti, integrity a dostupnosti do samostatných oblastí pomáhá najít rychlejší a cílenější řešení jednotlivých problémů. V momentě, co organizace splňuje všechny 3 standardy, tak bezpečnost organizace je lépe připravená čelit jednotlivým hrozbám. [6]

1.6.1 Důvěrnost

Důvěrnost lze zajistit tím, že informace jsou sděleny pouze těm, kteří mají oprávnění přístupu k těmto datům dostat. Každá informace má jinou hodnotu a je jinak důležité k těmto informacím přistupovat. V praxi se používají dvě schémata klasifikačních stupňů důvěrnosti. První klasifikační skupina se využívá nejvíce ve státní sféře, kde dělíme informace na přísně tajné, tajné, důvěrné, citlivé a neklasifikované. Pro komerční sféru jsou klasifikační stupně děleny na 4 stupně. [7]

Důvěrné informace jsou klasifikovány nejvyšším stupněm. Zveřejnění těchto informací může mít ničující dopad na společnost. Jedná se o strategické plány, zdrojové kódy, know-how a podobně. Soukromé informace jsou takové informace, které mohou být zneužity a způsobit škody. Mezi ně se řadí například osobní údaje. Citlivé údaje jsou informace o projektech, změnách a vývoji cen. Uniknutí těchto informací může mít na společnost negativní vliv. Veřejné informace jsou veřejně známé informace, které nevyžadují žádnou zvláštní ochranu. Mezi veřejnými informacemi najdeme telefonní čísla, jména a emaily. [7]

Klasifikační stupně se v průběhu času mohou měnit. Například před uvádění produktu na trh jsou informace důvěrné a při uvedení produktu na trh jsou informace o produktu veřejné. [7]

1.6.2 Integrita

Integrita znamená zajištění správnosti, úplnosti a neměnnosti dat. Integritu dat si zachovají v případě, že jsou autentická, přesná a spolehlivá. Nežádoucí modifikaci v informační bezpečnosti nazýváme jako narušení integrity. Porušení integrity dat je obvykle úmyslné, i když může být i v důsledku technického selhání, lidskou chybou nebo náhodou. Odhalení porušení integrity může být složité a trvat dlouhou dobu. Čím déle trvá toto porušení odhalit, tím hůře se opravuje. Samotné zálohy úplně nestačí, protože když nevíme, kdy porušení nastalo, tak je možné, že v zálohách integrita dat již bude porušena. [7]

Ochranu integrity lze zajistit pomocí komplexního zabezpečení hashováním, šifrováním, digitálních certifikátů a podpisů. U webových stránek je možné využívat důvěryhodné certifikační autority jako je třeba CAs, které potvrzují pravost webu. [6]

Ověřit integritu lze pomocí nepopíratelností. To znamená, že určitou akci nelze popřít nebo zpochybnit. Při emailové komunikaci ve firmě zaměstnanec použije digitální podpis, a tak nelze popřít, že email byl skutečně odeslán daným zaměstnancem. [6]

1.6.3 Dostupnost

Zajišťuje, že informace a systémy jsou dostupné oprávněným uživatelům, kdykoliv potřebují. V případě, že data jsou důvěrná a jejich integrita je zachována, nemají žádnou hodnotu, pokud nejsou dostupná zákazníkům a oprávněným uživatelům. To znamená, že systémy, síť, aplikace i hardware musí fungovat správně a po celou dobu v požadovaném čase. [6]

Pokud dojde k výpadku proudu, přírodním katastrofám nebo úmyslným útokům například DoS, tak může nastat narušení dostupnosti, pokud nejsou zavedena opatření pro zajištění dostupnosti. To vede k poškození reputace, snížení ziskovosti a podobně. Pro zajištění integrity organizace používají redundantní síť, servery a aplikace, které se aktivují v případě výpadku primárního systému. Dostupnost se dá zlepšit i pomocí pravidelných aktualizací softwaru a systému, záložních zdrojů napájení, pravidelným auditem hardwaru, zálohováním a plány pro obnovu po havárii. [6]

Pro plánování dostupnosti se používají termíny RTO a RPO. RTO (recovery time objective) určuje, za jak dlouho po výpadku musí být systém funkční. Tedy jak dlouhý výpadek je tolerován. V případě, kdy se RTO rovná nule je infrastruktura systému plně redundantní. RPO (recovery point objective) vyjadřuje, kolik práce a jaké množství dat může být ztraceno vůči poslední záloze, ze které se bude obnova konat. [7]

1.7 Řízení informační bezpečnosti

Funkční metoda podle, které lze v řízení informační bezpečnosti postupovat, je Demingův PDCA cyklus. Ten je založený na 4 základních krocích plánuj, dělej, kontroluj, jednej. Cyklus je vhodný, jelikož zaváděná opatření by měla být pravidelně přezkoumávána, vyhodnocována a z výsledků by měli vznikat reakce a adaptace na vzniklé problémy nebo nedostatky.

Existují normová doporučení pod ISO/IEC 2700x, tyto normy jsou dány ve směrnici Evropské unie a mají za úkol firmám pomoci s implementací bezpečnostních opatření a zavedení jednotlivých funkčních praktik v oblasti kybernetické bezpečnosti. Organizace nemusí splnit všechna doporučená opatření, jelikož každá firma má jiné potřeby a musí zvážit, jestli daná opatření jsou pro ně relevantní nebo ne. [7]

1.7.1 Aktiva

Data a informace v kybernetickém prostoru prochází informačním systémem společnosti. Je důležité se zaměřit na to, jaká informační aktiva prochází tímto systémem a jak na ně může být veden útok. Informační systém se skládá z koncových zařízení, serverů, síťových prvků, zabezpečovacích systémů, lidí, dokumentů, IoT a dalších komponent. Je důležité informační aktiva porovnat a zvážit, kde útok způsobí nejvíce škody a jestli aktiva jsou primární nebo sekundární a na základě toho je zabezpečit. Každému aktivu totiž nelze věnovat stejná pozornost z hlediska času, financí a zdrojů. [7]

1.7.2 Hrozby

Hrozby existují v několika podobách, a to úmyslná nebo neúmyslná událost, která má negativní dopad na integritu, důvěrnost nebo dostupnost aktiv. Informační systémy jsou vystaveny velkému množství hrozeb a většina informačních systémů bývá vystavena stejným hrozbám. I tak je potřeba udělat důraznou analýzu hrozeb a zjistit, jestli se firem netýkají specifické hrozby. Pokud chceme stanovit míru hrozby je důležité vzít v úvahu jednotlivé faktory:

- Četnost výskytu – Z průzkumů, statistik a z vlastní evidence se určuje četnost výskytu dané hrozby, kdy vyšší četnost znamená větší pravděpodobnost hrozby.
- Příležitost – Určuje, jak jednoduché je nějakým způsobem zaútočit. V případě zaměstnanců pracujících s důvěrnými informacemi a nejsou monitorováni, tak je příležitost útoku vyšší než v případě monitorování.
- Motiv – Určuje, proč by člověk chtěl zaútočit. Motivem mohou být třeba finance, frustrace, krize, pomsta, propuštění.
- Schopnost – Set vlastností, které umožní útočníkovi provést zdárně svůj útok.
- Nákladovost – Útoky bývají často motivované financemi a pokud je útok vysoce nákladný a předpokládaná odměna není vyšší než odměna, pravděpodobnost útoku se rapidně sníží.
- Vybavení – Pro jakýkoliv útok je třeba specifického vybavení, které může být obtížné získat nebo je vysoce nákladové. V tomto případě pravděpodobnost klesá v opačném případě, kdy je lehce dostupné a nenákladové pravděpodobnost proveditelnosti útoku roste.
- Čas – Pravděpodobnost roste v případě, kdy stačí krátkodobá přípravy a realizace útoku. V případě, že je příprava časově náročná pravděpodobnost hrozby klesá.
- Atraktivita aktiva – V oblasti financí, jsou aktuálně atraktivní kryptoměny, jelikož jsou trendy, málo regulované a lidé často nejsou dostatečně edukováni o hrozbách a rizicích, které nesou. To z nich dělá vysoce atraktivní aktiva pro útočníky.
- Počet osob – Pravděpodobnost se snižuje s vyšším počtem lidí na provedení útoku. Naopak menší počet tuto pravděpodobnost zvyšuje.

Tabulka 1 Dělení hrozeb

Hrozby	Náhodné	Úmyslné
Externí	Přírodního původu	Hacking
Interní	Lidská a technické selhání	Sabotáž

Zdroj [7]

V případě úmyslných hrozeb se hodnotí složitost proveditelnosti útoku a na základě toho se určuje pravděpodobnost realizace dané hrozby. Úmyslné útoky jsou často prováděny organizovanými skupinami a jsou cílené na lidskou chybu. [7]

1.7.3 Zranitelnost

Zranitelnost představuje slabé místo v bezpečnostním systému nebo jeho částí. To může být zneužito hrozbou k narušení nebo poškození aktiva. Každé aktivum má určitou míru zranitelnosti a je ohroženo různými hrozbami. V informačních systémech jsou vždy přítomna zranitelná místa, které útočník může využít. Slabiny jsou v podobě hardwaru, softwaru, lidských chyb a neznalosti. [7]

1.8 Spotřebitelé v kybernetické bezpečnosti

Kybernetická bezpečnost je důležitá i z pohledu spotřebitele. Častá nevědomost a slabá hesla vedou ke ztrátám financí. Jelikož finanční instituce především v EU jsou silně regulovány a musí plnit bezpečnostní standardy a nařízení. Samotné banky mají na svých stránkách informace a studijní materiály k zvýšení povědomí o možných hrozbách.

Je důležité si chránit svá data v jakékoliv podobě. Hlavně citlivá data, která jsou v digitální podobě. Nejlépe citlivé informace nedávat do digitální podoby, tím se sníží jejich dostupnost. Je třeba se zabývat informační bezpečností jakožto jednotlivce, tak i organizace, protože jejich ztráta dokáže způsobit velké škody. [8]

Proto existují doporučení a kampaně od České bankovní asociace v podobě #nePINdej a ČNB „Desatero spotřebitele“, které mají pozvednout povědomí o rizicích ve finančním sektoru. Důvodem k spuštění kampaně #nePINdej je dlouhodobý růst kybernetických útoků na klienty bank. V první polovině roku 2023 bylo 31 323 kybernetických útoků a z toho nahlášeno na policii 10 219. Vzrůst oproti roku 2022 stejného období byl o 15 %. Škody jsou ve stovkách milionů a průměrně to dělá na klienta 21 522 korun, kdy nejvyšší škodu u jednotlivce činilo přes 15 milionů korun. Tím Česká bankovní asociace spolu s Policií ČR, NÚKIB a dalšími spustili tuto vzdělávací kampaň. [9]

Kampaň #nePINdej je zaměřená na zvýšení povědomí veřejnosti o kybernetických hrozbách a prevenci podvodů v online prostoru. Ke kampani je vytvořený web <https://www.kybertest.cz/>, kde lze najít nejčastější typy podvodů a zároveň tam je test, který si uživatelé mohou vyzkoušet, a tak zvýšit povědomí o svých znalostech týkajících se kyberbezpečnosti. [9]

Do ochrany spotřebitele patří i „Desatero spotřebitele“, které má za účel zvýšit povědomí a ostražitost při spoření, investování a půjčování peněz. [10]

- 1) Nic není zadarmo – Prodejci finančních služeb především usilují o zisk, a i zdarma nabízené služby mohou skrývat náklady, proto je důležité prostudovat podmínky a poplatky, které jednotliví prodejce má. [10]
- 2) Mějte jasno a ověřujte informace – Při vybírání investičních produktů je důležité porovnat nabídku na trhu a konzultovat třeba u nezávislých odborníků. Ověřovat si informace, protože ne všechny finanční produkty spadají pod regulaci ČNB. [10]
- 3) S kým jednáte – Vždy řádně zkontrolujte kvalifikaci a regulaci smluvního partnera a mějte na paměti, že oprávnění v jedné oblasti finančního trhu neznamena automaticky oprávnění v jiných oblastech. [10]
- 4) Váš finanční plán – Mějte finanční rezervy pro mimořádné události, které jsou okamžitě likvidní. Proto není rozumné vše investovat do dlouhodobých produktů, kde jsou případné poplatky za výběr nebo výběr trvá delší dobu. [10]
- 5) Čtete všechno a kontrolujte – Nespoléhejte na ústně sdělené informace a nabídky si nechávejte zaslat písemně a ty pečlivě prostudujte. Nenechte se tlačit do rychlého rozhodnutí a ověřte si prvně všechny odkazy a podmínky před potvrzením. U platebních transakcí raději kontrolujte údaje transakce. [10]
- 6) Nejasné smlouvy – V případě složité dokumentace je na místě větší obezřetnost a pozornost. Hlavně pokud smlouvy obsahují odkazy a formulace „neplatí a nepoužije se“. [10]
- 7) Vysoký výnos – U nabídek, které slibují rychlé zbohatnutí je vysoké riziko podvodu, či ztráty peněz z důvodu vysoké rizikovosti. U složitých produktů mějte na paměti, že bývají riskantnější a vysoké výnosy znamenají často vysoká rizika. [10]
- 8) Investování – Při investování musí být spotřebitel opatrný při vyplňování investičního dotazníku, taktéž je důležité se nenechat zmanipulovat k nepravdivým odpovědím a nepodepisovat nepravdivá prohlášení. Nespoléhat se na tvrzení prodejce a důkladně se informujte o všech poplatcích spojených s investicí, ty vedou k dlouhodobým nižším výnosům. [10]
- 9) Životní pojistka – Životní pojištění kryje proti nepředvídatelným událostem. To není součástí žádného investování a tuto část při zrušení nemůžete dostat. [10]

- 10) Chraňte svá data – Citlivá data nesdělujte cizím osobám v jakékoliv podobě. Nemějte PIN u platební karty nebo kódy a hesla k účtu v bance. Dále dbejte na písemnou dokumentaci, protože ústně poskytnuté údaje se prokazují špatně. [10]

Dílčí závěr

První kapitola se zabývala problematikou bezpečnosti, hodnotou a zabezpečením informací a zároveň přiblížením, jak velký dopad na kybernetické útoky má právě spotřebitel. V úvodu byl osvětlen pojem bezpečnosti a jak se vztahuje na svět kybernetických financí. Dále byl představen význam, proč je důležité řešit bezpečnost financí zvláště v kyberprostoru, kde se pohybuje mnohem více peněz. Následně byly představeny základní koncepty kybernetické bezpečnosti a řízení informační bezpečnosti za pomoci aktuálních standardů a jak velký vliv mají spotřebitelé na bezpečnost svých financí.

2 REGULACE A LEGISLATIVNÍ OPATŘENÍ

Regulace a legislativní opatření v oblasti finanční bezpečnosti by měly sloužit k zajištění stability a důvěryhodnosti finančního sektoru v České republice. Důvěryhodnost a stabilita jsou základními podmínkami pro fungování ekonomiky. Regulace chrání nejen finanční instituce před kybernetickými hrozbami a podvody, ale také zajišťují ochranu spotřebitelů a jejich finančních prostředků. Zároveň by měly podpořit transparentnost finančních operací, které mají za účel pomoc v boji proti praní špinavých peněz a financování terorismu. [11]

2.1 DORA

DORA neboli nařízení o digitální provozní odolnosti je regulace Evropské unie navržená za účelem zvýšení provozní a kybernetické odolnosti. Cílem je posílit bezpečnost finančního sektoru a sjednotit požadavky napříč finančním sektorem. Regulace se vztahuje na banky, pojišťovny, investiční společnosti, poskytovatele platebních služeb, burzy a další subjekty napojené na finanční sektor. Subjekty by měly být odolnější vůči kybernetickým útokům, technickým poruchám a jiným digitálním hrozbám. [12]

Klíčové oblasti DORA se skládají z následujících bodů:

- Řízení ICT rizik – Povinnost zavedení efektivních procesů pro identifikaci, monitorování a řízení digitálních rizik. [13]
- Požadavky na testování odolnosti – Organizace musejí pravidelně testovat své systémy proti kybernetickým hrozbám, včetně pokročilých penetračních testů a simulačních cvičení. [13]
- Hlášení incidentů – Finanční instituce mají povinnost rychle hlásit kybernetické incidenty regulačním orgánům, dle standardizovaných postupů. Pro Česko to je ČNB v případě kybernetických incidentů může být zapojen NÚKIB. [12]
- Dohled nad poskytovateli ICT služeb – DORA zajišťuje, že i externí dodavatelé IT služeb spadají pod regulační dohled. [13]
- Sdílení informací – Podporuje spolupráci mezi finančními subjekty při sdílení informací, které by vedly ke zlepšení kybernetické obrany. [13]

DORA by měla mít také mezinárodní dosah na subjekty, které se nachází mimo EU, ale poskytují služby finančním institucím v EU. Také klade důraz na zvýšení spolupráce mezi regulačními orgány napříč EU a mezinárodní koordinaci se zaměřením na redukci

systémových rizik, které mohou ohrozit finanční systém a trhy EU. Jelikož se digitální prostředí rychle mění, tak byl vytvořen mechanismus, který umožňuje pravidelně kontrolovat a upravovat pravidla, aby odpovídala aktuálním trendům. [13]

Evropské nařízení v České republice bylo přijato pod zákonem č. 31/2025 Sb. účinným od 15.02.2025. Zavedení těchto opatření by mělo minimalizovat dopady kybernetických útoků a přinést stabilitu a vyšší ochranu klientů. [15]

2.2 MiCA

MiCA neboli nařízení o trzích s kryptoaktivy je regulace přijatá v České republice pod stejným zákonem jako DORA, tedy zákon č. 31/2025 Sb. a je účinné od 15.02.2025. MiCA vznikla na základě dosud neregulované oblasti kryptoaktiv, aby poskytla ochranu investorů před riziky jako jsou podvody, manipulace s trhem a podobně. Nařízení reguluje trhy s kryptoaktivy, stanovuje pravidla pro poskytovatele služeb spojených s kryptoaktivy jako jsou směnárny, obchodní platformy, bitcoinové automaty a virtuální peněženky. Cílem je zajistit ochranu klientů a bezpečnost v oblasti kryptoaktiv, také zvýšit důvěru veřejnosti v kryptoinvestice. Snížit volatilitu a spekulace s kryptoaktivy v podobě přísných pravidel pro emitenty. [15][16]

Klíčové aspekty MiCA jsou:

- Působnost – Nařízení se vztahuje na všechna kryptoinvestice, která nejsou pokryta stávajícími finančními regulacemi EU, včetně kryptoměn a stablecoinů. [15]
- Licencování – Zavádí celoevropský licenční režim pro emitenty kryptoaktiv a poskytovatele služeb spojených s kryptoaktivy (CASPs). [14][15]
- Bílá kniha – Vydavatelé kryptoaktiv musí zveřejnit bílou knihu, která obsahuje informace o projektu, rizicích a právech investorů. [16]
- Dělení kryptoaktiv – Elektronické peněžní tokeny (EMT) což představuje stable coinů jako Tether (USDT), tokeny vázané na aktiva (ART), což jsou tokeny vázané na jiná aktiva jako komodity, akcie nebo jiné kryptoměny a ostatní kryptoinvestice což je třeba Bitcoin nebo Ethereum. [15]

CASPs jsou poskytovatelé služeb v oblasti kryptoaktiv. Spadají pod ně burzy, krypto peněženky a poradenství ohledně investic do kryptoměn. Zjednodušeně jakýkoli subjekt,

který poskytuje služby s kryptoměnami veřejnosti na profesionální bázi. V České republice bude vykonávat dohled ČNB. [17]

2.3 PSD2

PSD2 je směrnicí o platebních službách (Payment services directive 2). Účelem je posílit bezpečnost elektronických plateb, ochranu spotřebitelů, posílení konkurence a inovativnímu rozvoji se stejnými podmínkami. Úkolem je zvýšení transparentnosti a bezpečnosti platebních styků. [18]

Hlavní aspekty:

- Zvýšení bezpečnosti – Zavedení dvojité autentizace na straně uživatele např. Pomocí hesla a mobilního zařízení. Výjimkou jsou platby s nízkou hodnotou nebo opakované platby. [18]
- Otevřené bankovníctví – Umožnění sdílení finančních dat mezi bankami a poskytovateli služeb, které provádí platby nebo poskytují přehledy o účtech za předpokladu, že mají souhlas od spotřebitele. [18]
- Ochrana spotřebitele – Posiluje práva spotřebitelů v snížení odpovědnosti za neoprávněné platby z 150 eur na 50 eur a odstranění poplatků při používání kreditních nebo debetních karet spotřebiteli. [18]
- Pojištění odpovědnosti – Platební instituce musí mít sjednané pojištění odpovědnosti za škody vzniklé při výkonu povolání. [18]

Cílem PSD2 bylo zvýšit bezpečnost plateb, posílit ochranu spotřebitelů a otevřít trh novým poskytovatelům platebních služeb. Do legislativy České republiky byla směrnice přivedena 13.1.2018 v zákoně o platebním styku č. 370/2017 Sb. Zákon stanovuje pravidla pro poskytování platebních služeb a definuje práva a povinnosti poskytovatelů těchto služeb. Mezi tyto povinnosti patří například poskytnutí spotřebitelům jasné informace o poplatcích, odpovědnost za neoprávněné platby a ztrátu nebo zneužití platebního nástroje. [19]

2.4 NIS2

Je směrnicí EU 2022/2555 ze dne 14.12.2022 pod názvem NIS2 zabývající se opatřeními pro vyšší úroveň kybernetické bezpečnosti napříč Unií. Tato směrnice rozšiřuje a nahrazuje původní NIS1. [20]

- Rozšíření rozsahu působnosti, kde se směrnice bude vztahovat na širší škálu subjektů a odvětví. Jedná se o podniky s klíčovou infrastrukturou, které jsou na obrázku 1. [20]
- Zavádí přísnější požadavky na řízení rizik. Subjekty, na které se směrnice vztahuje musí zavést opatření pro řízení kybernetických rizik, posouzení rizik a bezpečnostní politiku a postupy pro reakci na útoky. [20]
- Hlášení incidentů v momentě, co se nastane útok organizace má za povinnost nahlásit útok do 24 hodin. Incidenty v České republice se budou hlásit prostřednictvím portálu NÚKIB. [20]
- Vyšší sankce na organizace, které nedodrží pravidla v rámci NIS2 a dodává pravomoc auditů a kontrol. [20]
- Harmonizace pravidel má za úkol sjednotit kybernetické bezpečnostní standardy napříč EU. [20]

NIS2 rozlišuje služby na základní a významné. To se v českém právním řádu projeví v podobně povinností vyššího a nižšího režimu. Rozdíl je v pravidlech hlášení, dohledu i bezpečnostních opatření. V České republice by měla směrnice NIS2 implementována pod zákonem o kybernetické bezpečnosti v polovině roku 2025. [21]



Obrázek 1 Odvětví NIS2 [22]

Směrnice byla přijata, aby posílila bezpečnost členských států vzhledem k růstu kybernetických hrozeb. Předchozí směrnice NIS1 již neodpovídala dnešním technologickým standardům. Proto NIS2 rozšiřuje okruh regulovaných odvětví, zpřísňuje bezpečnostní standardy a zlepšuje koordinace mezi členskými státy EU. Cílem NIS2 je posílit a dosáhnout vysoké společné kybernetické bezpečnosti napříč Evropskou unií, chránit občany a minimalizovat dopad kybernetických útoků na společnost. [23]

2.5 AML

V celém znění anti-money laundering je v české legislativě popsáno v zákoně č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Tento zákon prošel řadou novelizací, které odráží vývoj v této oblasti. Převádí do českého práva mezinárodní standardy a směrnice Evropské unie. Zákon tvoří komplexní systém opatření, které slouží k prevenci proti zneužívání finančního systému k nezákonným aktivitám. Hlavní zaměření zákona je na prevenci proti praní špinavých peněz, financování terorismu a financování zbraní hromadného ničení. [24]

AML zákon zabraňuje praní špinavých peněz tím, že požaduje po finančních institucích a určitých podnikatelích opatření, které mají zamezit legalizaci nelegálně získaných finančních aktiv z trestné činnosti. Vybrané organizace a podnikatelé musí ověřovat identitu svých klientů při navazování obchodních vztahů. Jedním z klíčových opatření je zamezení anonymních účtů, což vede k tomu, že každá finanční operace je spojena s určitou osobou. Banky i instituce mají právo požádat o doložení původu finančních prostředků, tak aby se eliminovala možnost nekontrolovaných toků peněz. [24]

Podezřelé transakce a činnost musí instituce hlásit na Finanční analytický úřad. Jedná se o samostatný úřad, který je podřízen ministerstvu financí. Stará se o přijímání a analýzu podezřelých obchodů, dohlížení na plnění AML zákona, koordinování mezinárodních sankcí spojených s AML zákonem a vyhodnocování rizik v oblasti praní peněz. [24]

Tabulka 2 Statistický přehled činnosti FAÚ za roky 2020 až 2023

	2020	2021	2022	2023
Oznámené podezřelé obchody	4860	5693	6145	7114
Podaná trestná oznámení	426	512	911	995
Zajištěné prostředky (miliard Kč)	3,9	2	2,6	3,8

Zdroj [25]

Mezi právnické a fyzické osoby, kterých se týká AML zákon se řadí banky, investiční společnosti, pojišťovny, makléři, směnárny, brokeri, burzy, kasina, investiční poradci, obchodníci s drahými kovy, osoby přijímající platby v hotovosti nad 250 000 Kč a mnoho dalších. Mezi administrativní povinnosti, které musí být plněny od momentu začátku podnikání se řadí: [24]

- Identifikace klienta – Organizace musí ověřit totožnost klienta pomocí platného dokladu při transakcích nad 1000 EUR. [24]
- Kontrola klienta – Organizace musí průběžně provádět kontroly, zejména pokud přesáhne transakce hodnotu 15 000 EUR, je politicky exponovaná osoba nebo pokud je obchod podezřelý. Kontrola zahrnuje ověření účelu a povahy obchodu, majitele firmy a zdroj financí. U rizikovějších klientů nutnost původu majetku. Při menším riziku lze použít čestné prohlášení. [24]
- Neuskutečnění obchodu a nahlášení podezření – Obchod nelze uskutečnit v momentě odmítnutí ověření identity nebo pochybnosti o pravosti údajů. Finanční transakce musí být neprodleně nahlášeny na FAÚ pomocí online formuláře. [24]
- Systémová opatření – Určení osoby pro dohled nad AML a kontaktní osoby s FAÚ, pravidelná roční školení zaměstnanců na AML. Zavedení systému zásad a rizik, které se týkají převážně online prostředí. [24]

Ověření identity online lze přes bankovní identitu, eObačnaky. Některé organizace požadují ofocení občanského průkazu, pasu nebo řidičského průkazu. [24]

Dílčí závěr

V kapitole jsou představeny jednotlivé legislativní opatření, které mají za úkol vytvořit stabilní a bezpečný finanční kyberprostor. Bylo zmíněno několik významných nařízení, které institucím a organizacím nařizují, jak postupovat v oblasti bezpečnosti, tak aby organizace byly odolnější a zůstali v souladu s legislativou.

3 VÝVOJ A TRENDY

Vývoj a trendy v oblasti financí se posouvá kupředu enormní rychlostí. S novými technologiemi v podobě placení mobilními telefony, chytrými hodinkami, rozvoj kryptoměn nebo okamžité bankovní převody jsou důležitými inovacemi v posledních letech a s nimi přichází i velká rizika.

Finanční služby především v Evropě čelí mnoha regulacím, které mají za úkol připravit tento sektor na prevenci a vypořádávání se s kybernetickými hrozbami. Vytváří se nové metody a vyvíjí se nové technologie, které k tomu mají dopomoc. Příkladem je využití umělé inteligence, které pomáhá k detekci hrozeb, ale zároveň je využívána na vytváření kybernetických hrozeb. [26]

3.1 Umělá inteligence

Využití AI v kybernetické bezpečnosti se rozvíjí v oblasti obranných a útočných strategií. Strojové učení se umožňuje adaptovat na nové útoky rychleji a rozpoznávat anomálie. Na druhé straně je využíváno k tvorbě sofistikovaných útoků pomocí deepfake, phishingu a podobně. [26]

Využití AI k posílení bezpečnosti. Zdokonalují se systémy na analýzu v reálném čase obrovského množství dat a snaží se najít vzorce a anomálie, které mohou představovat potenciální kybernetické útoky. Umožňuje analýzu a skenování zranitelností logů. [27]

Taktéž dokáže behaviorální analýzu, kde modely vytváří profily aplikací a zpracovává velké objemy dat o zařízeních a uživateli. Generativní AI vytváří realistické simulace útoků, které umožňují testování obranných mechanismů. Taktéž dokáže vypomoci v detekci phishingu a spamu, které detekuje analýzou emailů. Tedy využití AI v kybernetické bezpečnosti je velmi užitečné a nákladově výhodné, díky kontinuálnímu učení a adaptaci v reálném čase. [27]

AI se využívá i pro útočné účely. Hlavní oblastí je zde využití pro phishingové emaily a deepfake technologie, které se používají v sociálním inženýrství. Ty nejen kvůli generativní AI dokážou vypadat přesvědčivě a manipulativně, ale taktéž se rychle šíří díky vysoké škálovatelnosti a automatizaci. [28]

Jak již bylo zmíněno u využití AI k obraně, tak adaptivně učící se AI se taktéž dokáže v reálném čase učit a vyhýbat se detekci a identifikovat zranitelnosti. Existují i modely jako je CaaS (Crime-as-a-Service) neboli „Zločin jako služba“. Tento model umožňuje méně

zkušeným útočníkům jednoduchý přístup k automatizovaným sadám pro realizaci kybernetických útoků. [28]

V poslední řadě využití AI v managementu investování a investičních modelů. AI se začíná využívat napříč investičním spektrem. Dokáže automatizovat obchody na základě analýzy dat, která by člověku trvala déle. Je osvobozeno od emocí, které na lidi u investování dopadají, a to vede ke špatným úsudkům. Dokáže predikovat na základě analýzy a matematických modelů trendy a vývoj. I přes tyto výhody, které AI přináší jsou tu rizika. AI ještě není neomylná a může se stát, že zpracovává špatná data, vygeneruje chybné výsledky a nemusí replikovat lidskou intuici, kdy třeba geopolitické vztahy mohou ovlivnit jednotlivé investiční příležitosti, které AI nemusí brát v potaz. [29]

3.2 ZTA

ZTA (Zero Trust Architecture) funguje na principu „nikdy nedůvěřuj a vždy prověřuj“. Model se zaměřuje na kontinuální ověřování přístupu. Každý uživatel v organizaci nebo mimo organizaci je neustále kontrolován. Zabezpečuje ochranu dat a systému prostřednictvím neustálého autentizování. Každý přístup k zdrojům uvnitř sítě je ověřován, uživatelé mají přístup pouze ke zdrojům, co nutně potřebují pro vykonávání své práce. Zároveň zahrnuje dvoufaktorovou nebo multifaktorovou autentizaci, která dodává další vrstvu zabezpečení. Síť je rozdělena na malé segmenty, které mají za účel zamezit šíření hrozeb v případě útoku. ZTA představuje komplexnější ochranu a omezuje šíření útoků. Taktéž pomáhá organizacím plnit požadavky na ochranu dat a bezpečnost. [30]

3.3 Kvantová kryptografie a kvantové počítače

Kvantové počítače slouží jako velký „strašák“ aktuálního kryptografického zabezpečení napříč sektory, především pro finanční sektor. Útočníci již zachytávají šifrovanou komunikaci, s vidinou příchodu kvantových počítačů, kde za jejich pomoci by mohli zpětně dešifrovat data. Primárně jsou ohrožena data s dlouhodobou citlivostí jako jsou státní tajemství, osobní údaje a podobně. [31]

NIST, což je americký Národní institut pro standardy a technologie standardizoval post-quantové šifrovací standardy v podobě CRYSTALS-Kyber (pro výměnu klíčů) a tři algoritmy pro digitální podpisy, kterými jsou CRYSTALS-Dilithium, SPHINCS+ a FALCON. Tyto kvantové algoritmy budou fungovat stejně jako digitální podpisy. Tyto

podpisy mají nahradit tradiční digitální podpisy RSA a ECC. Zároveň NÚKIB v roce 2023 vydal doporučení o kombinování těchto šifrování s osvědčenou kryptografií. [32][33]

Z hlediska časových horizontů podle zprávy Global Risk Institute se v krátkodobém horizontu, který představuje 5 až 10 let se očekává zdokonalení kvantových počítačů, ale bez ohrožení aktuální kryptografie. Ve střednědobém horizontu se očekává možné narušení bezpečnostních standardů a prolomení asymetrických algoritmů. V posledním dlouhodobém horizontu nad 15 let se očekává širší dostupnost kvantových počítačů, což představuje hrozbu pro kryptografické systémy bez post-quantového šifrování. [31]

3.4 Kryptoměny

Kryptoměny představují novou formu digitálního platidla, které využívá šifrovací metody k zajištění bezpečnosti transakcí a kontrole emisí nových jednotek. Základem je technologie blockchain nazývaná jako ledger. Ta představuje databázi v spojení s financemi to je velká účetní kniha. Dalším důležitým prvkem je decentralizace této sítě, kde není žádná centrální autorita, která by mohla transakci zrušit, pozastavit a podobně. Tento decentralizovaný systém slouží k transparentnímu a bezpečnému zaznamenávání všech provedených transakcí. [34]

Svět kryptoměn v čele s Bitcoinem si vytvořil pozici ve finančním ekosystému. Aktuálně s tržní kapitalizací 3 biliony dolarů z toho Bitcoin představuje 60 % tržní kapitálace kryptoměn, tedy necelých 1,8 bilionu dolarů. V porovnání s největšími společnostmi na světě by se umístil na 6. místě po společnostech Apple, Microsoft, NVIDIA, Amazon a Alphabet ke dni 6.3.2025. Kryptoměny již nejsou vnímány jako nástroj pro geeky na hraní. Však i americký prezident Donald Trump si spustil svoji kryptoměnu Trump coin. [47][48]

Důvodů, proč jsou kryptoměny populární a převážně tedy Bitcoin je mnoho. Kryptoměnová 16letá historie, kde investoři dokázali rychle a jednoduše zbohatnout a dělat vysoké násobky zhodnocení, tak přitahují nové investory. Ti doufají, že se bude historie opakovat jako u bitcoinu a na nových altcoinech se často spálí. Kryptoměny už jsou v povědomí širší veřejnosti. Kryptoměny po světě již prošli nějakou legitimizací, když jsou uvedeny do české legislativy, v Americe vznikla Bitcoinová rezerva, evropská centrální banka plánuje spustit digitální euro a vznikli ETF fondy na Bitcoin a Ethereum.

Kryptoměny jako peníze budoucnosti především Bitcoin, to je přesvědčení nemála lidí. Všechny měny potřebují způsob kontroly nabídky a prosazování opatření proti podvodům.

U běžných fiat měn jsou v roli kontrolora centrální státní banky, které kontrolují oběh a tisknutí nových peněz a jejich padělání. To pro padělatele není nepřekročitelná překážka, a tak jsou tyto opatření k ochraně doprovázena zákony. U Bitcoinu nic takového není. Zde se úpravy řeší napříč komunitou vývojářů, těžařů, provozovatelů uzlů a uživatelů. Není tedy možné, aby jedinec nějakým způsobem změnil kód. Dále u Bitcoinu je známí finální počet jednotek, které budou existovat a to 21 miliónů. U centrálních bank tuto informaci neznáme, jelikož se neustále tisknou nové peníze. [36]

Kryptoměnový trh se potýká i s řadou problémů, které ohrožují jeho kredibilitu a stabilitu. Je to stále poměrně nová technologie a stále vysoce volatilní. Dalším problémem je škálovatelnost, kdy na Bitcoinové síti je možné provést 7 transakcí za vteřinu pro porovnání platební systém Visa jich provádí 1 700 s možností provést až 24 000 transakcí za sekundu. I když toto je již v řešení v podobě Lightning networku. K stabilitě také nepomáhají hackerské útoky na burzy a rozsáhlé podvody napříč kryptoměnovým spektrem, které podkopávají kredibilitu. To jsou závažnější problémy, které také brání k širší adopci kryptoměn a potenciálu se stát globálním finančním nástrojem. [35]

3.4.1 CBDC

Digitální peníze centrálních bank představuje CBDC. Jedná se o novou formu peněz, která existuje pouze v elektronické podobě. Je to digitální verze fiat měn. Rozdíl mezi CBDC a kryptoměnami je v tom, že CBDC je vydávána centrální bankou a regulována. O tuto technologii se zajímá evropská centrální banka. Ta spustila projekt na tvorbu digitálního Eura v listopadu 2023. Jako pozitivní dopady uvádí větší kontrolu nad osobními údaji a zabezpečením a zvýšení anonymity v platebním procesu. Na druhou stranu existují i obavy z důvodu velké koncentrace dat v rukou centrálních bank, což by z centrálních bank činilo atraktivní cíle pro kybernetické útoky. Dále nedostatek bezpečnosti by se mohl projevit v nedůvěře uživatelů. [37]

Dílčí závěr

V této kapitole byly představeny nejvýznamnější trendy ve vývoji a jejich kladné, tak záporné dopady a jakým způsobem ovlivní finanční bezpečnost kyberprostoru. Nadále byly představeny kryptoměny, které jsou stále poměrně novou technologií a byly přiblíženy jejich vlastnosti a nová technologie CBDC, která by mohla změnit aktuální peněžní systém.

4 RIZIKA A HROZBY FINANČÍ V KYBERPROSTORU

Počty kybernetických útoků stoupají alespoň na základě informací z České bankovní asociace. V roce 2023 bylo zaznamenáno 69 685 podvodů s průměrnou škodou 19 357 korun a celkovou škodou 1,35 miliardy korun. V roce 2024 počet útoků byl 87 407 a průměrná škoda byla 15 952 korun s celkovou škodou 1,39 miliardy korun. Nárůst útoků na klienty bank meziročně vzrostl o 20 %, avšak průměrná ztracená částka je o 17,5 % nižší. V porovnání s rokem 2014, kde jsou odhadovány škody v desítkách až stovkách milionů, tak po deseti letech se pohybujeme v jednotkách miliard. [7][38]

Hrozby kybernetických útoků jsou ale i v kryptoměnovém odvětví. V Česku se podle kryptosměnárny Bit.plus a Anycoin obchoduje s objemem kolem 10 miliard korun za rok 2024. Anycoin uvedl, že má v současnosti přes 100 tisíc uživatelů. V Česku se kryptoměnová komunita zvedá, ať už je to prostřednictvím influencerů, firem nebo legislativou. [39]

Co se týče útoků na kryptoměny, tak Coinbase přední světová kryptoměnová burza, tak se předpokládá, že její klienti ztratili kolem 300 milionů dolarů za rok 2024. [40] Zároveň dne 21.02.2025 došlo k útoku na kryptoměnovou burzu Bybit. Dle generálního ředitele se jedná o největší útok v historii kryptoměn. Bylo odcizeno necelých 1 a půl miliardy dolarů z toho 1,12 miliardy dolarů v druhé největší kryptoměně podle tržní kapitalizace Ethereum a zbytek ukradených prostředků tvořily deriváty jako třeba stETH. [41]

Pro policii a orgány zabývající se trestním řízením v kyberprostoru je největší překážkou anonymita. Dnes už není složité skrýt IP adresu pod VPN a počítač se bude tvářit, že je na druhé straně světa. Existují i další pokročilejší metody jako třeba proxy servery. To vše zvyšuje nákladnost a problémovost se dohledat původu útočníka. [42]

4.1 Typy kybernetických útoků v oblasti financí

Stoupající trend kybernetických útoků představuje stále větší hrozbu pro finanční sektor. S útoky se setkávají organizace, instituce i jednotlivci, kteří čelí rizikům spojených s krádeží dat, omezení provozu nebo neoprávněnými transakcemi. Útoky mohou mít devastující dopad na organizace, klienty ale i ekonomickou stabilitu. Je tedy důležité být obeznámen s jednotlivými typy kybernetických hrozeb, aby se jim dalo předcházet.

Zpráva o stavu kybernetické bezpečnosti od NÚKIBU evidovala celkem 262 kybernetických bezpečnostních incidentů v roce 2023 což je oproti roku 2022 skoro 80 %

nárůst incidentů. Mezi nejčastější útoky řadí DDoS útoky, které zaznamenali státy po celé Evropě. Významných incidentů, kterých bylo 43 ze 74 meziročně ubylo o třetinu, ale ty méně významné se více než ztrojnásobily z 69 na 217. [43]

Co se týká samotného finančního sektoru, kde byl prováděn anonymní průzkum pomocí dotazníkového šetření pro 423 subjektů, kterým bylo položeno 63 otázek, ze kterých vycházejí následující údaje. S útoky pomocí podvodných emailů, což je lákání na finanční obnosy, CEO podvody nebo vydírání, se setkala 100 % respondentů. S phishingovými útoky, které se snaží získat citlivé údaje se setkala 95 % respondentů a s DDoS nebo DoS útoky se se setkala 86 % respondentů. Ve všech těchto incidentech se jednalo o meziroční nárůst ve smyslu setkání se s útoky. [43]

V dokumentu se taktéž nachází statistika Phishingových útoků, kde za rok 2023 se stalo 19592 útoků s meziročním nárůstem 6 %. Avšak když se tyto útoky porovnají s počtem útoků před 10 lety, tak je více jak šestinásobně vyšší tento počet útoků, jelikož v roce 2013 je zaevidovaných pouze 3108 útoků. [43]

4.1.1 Phishing

Je typ útoku, kde se útočník snaží získat důvěrná data oběti nebo spustit na zařízení škodlivý kód. Nejčastější útoky jsou pomocí podvodných emailů a na sociálních sítích. Účelem těchto útoků je získat informace o platebních kartách, údajů k účtům u finančních institucí a podobně. Existuje více typů phishingu se stejným cílem získat citlivá data od oběti. [44]

- Email phishing – Nejrozsáhlejší a nejznámější druh phishingového útoku je pomocí emailu, který je adresován specifickým osobám nebo organizacím na velké množství cílů. [44]
- Spear phishing – Je cíleným útokem na jednotlivce nebo skupiny, o které si předem získá všechny dostupné informace a následně vytvoří phishingovou zprávu přesně na míru. [44]
- Whaling – Je taktéž cíleně mířený útok jako spear phishing se zaměřením na vrcholové manažery a majitele firem. [44]
- CEO fraud – Je opakem whalingu, kdy zpráva se tváří, jako by pocházela od vysoce postavených manažerů a cílí na ostatní zaměstnance v podniku. [44]
- Page hijacking – Typ phishingového útoku, kdy uživatel je nevědomě směrován na podvodný web, který je duplikátem již existujícího webu. Nebo

kompromitují webové stránky, aby uživatele přesměrovali na škodlivé stránky. [44]

- Catfishing – Útočník vytvoří falešnou identitu zejména na sociálních sítích za účelem kompromitování oběti, získání financí a podobně. [44]
- Smishing – Útočníci zasílají podvodné zprávy na mobilní telefony. Ve zprávách se nachází odkazy nebo obsahují telefonní čísla, či emaily na které má oběť kontaktovat organizaci za kterou se útočník vydává. [44]
- Vishing – Podvodná technika při, které se využívá telefonních hovorů s falešným zobrazením skutečného telefonního čísla skutečné organizace. Útočník se falešně vydává za banku, úřad a podobně. Útočník následně využívá sociální inženýrství nebo zastrašovací taktiky k vylákání platby za vymyšlený dluh dané organizaci. Vishing taktéž může zahrnovat předem namluvené hlasové zprávy, které oběti lákají k zavolání zpět a oběti jsou naváděny k zadání svých osobních údajů nebo údajů o účtech a podobně. [45]

4.1.2 Malware

Malware se skládá ze dvou slov malicious neboli škodlivý a software. Obecně se dá říct, že za malware lze označit všechny kód a software, který byl vytvořen se škodlivým úmyslem. Existuje mnoho typů malwaru, ale pro tuto práci jsou primárně důležité jsou ransomware, keylogger, cryptojacking a trojské koně. To jsou nejčastější typy malwaru v oblasti financí.

- Ransomware – Škodlivý software, který šifruje nebo odebere přístup k datům oběti. Následně tento útok doprovází vyhrožování, kde útočník vyžaduje výkupné, aby znovu zpřístupnil data oběti. Výkupné se nedoporučuje platit, jelikož v praxi po zaplacení data obvykle nedostanete nebo se stanete opakovaným terčem. [46]
- Keylogger – Program označovaný i jako spyware zaznamenávající stisknuté klávesy na klávesnici a následně je posílá útočníkovi. Používá se pro získání přístupů k heslům, citlivým informacím a osobním údajům. [46]
- Trojský kůň – Maskuje se jako legitimní software, který si uživatel stáhne nebo nainstaluje. Program umožňuje útočníkům získat přístup do systému. [46]

- Cryptojacking – Útočník pomocí malwaru, který oběť stáhne nebo na webu otevře, zneužívá cizí výpočetní techniku k neoprávněnému těžení kryptoměn. [46]

4.1.3 Sociální inženýrství

Pomocí sociálního inženýrství útočníci používají různé netechnické formy útoku, nejčastěji vydáváním se za někoho jiného, než ve skutečnosti jsou. Pomocí těchto netechnických technik dokáže útočník zmanipulovat uživatele k ignorování bezpečnosti a snaží se zmanipulovat oběti k předání citlivých informací. [46]

Na těchto útocích se snaží vydávat za nějakou autoritu, známé instituce nebo podporu. U obětí se snaží vyvolat emoce často to bývá strach a stud pomocí lživých informací a arguje k rychlému jednání. Využívají spoofing, různé metody phishingu, scareware a sextorzi. [46]

4.1.4 Man in the middle

MITM neboli prostředník je kybernetický útok, při kterém útočník vstoupí nepozorovaně do komunikace mezi 2 stranami. Útoky MITM představují vážnou hrozbu pro důvěrnost a integritu dat, hlavně v oblasti financí. Příkladem mohou být transakce, které útočník modifikuje a přesměruje na své konto nebo peněženku, aniž by původní 2 strany měly vědomí o narušení, dřív, než je pozdě. Útoky se neomezují jen na finanční transakce, ale i na odposlech nebo manipulaci jakékoli komunikace. [46]

4.1.5 DDoS útoky

Distributed Denial of Service je útok, který se snaží narušit nebo přerušit síť nebo nějakou online službu tím, že ji přetíží velkým počtem falešných a nevyžádaných požadavků, dokud služba není vyřazena z provozu. Mohou také působit jako kamufláž pro další závažnější aktivity, které mohou způsobit větší škodu. [46]

4.2 Kybernetické útoky a podvody na finanční instituce

Dějiny se učí z důvodu neopakování stejných chyb a poučení se ze situací, které se již staly, a to by mělo pomoci lidem vytvořit obezřetnost pro budoucí situace, kde by se mohli nachytat. Právě na základě útoků, které nastaly se vytvářejí nová opatření a regulace proto, aby se znovu neopakovaly. Nejčastější útoky jsou phishingové, ale tyto útoky se velice liší v podobě hovorů, sms, emailů a podobně.

4.2.1 Pád burzy FTX

FTX Trading Ltd. byla čtvrtou největší kryptoměnovou burzou podle objemů obchodu v roce 2022. Dětila se na FTX což byla burza zaměřená na mezinárodní trh se širokou škálou produktů a nebyla určena pro americké uživatele. Pro ty byla burza FTX.US, která byla více regulována a měla menší nabídku produktů. Společnost FTX měla i svůj vlastní token FTT, který bylo možné nakupovat. Zakladatelem společnosti byl Sam Bankman-Fried, který také založil obchodní společnost Alameda Research. [49]

Dne 02.09.2022 vyšla zpráva na CoinDesk o problematice rozvaze společnosti Alameda. Největší aktivum zde bylo FTT v miliardách dolarů. Ředitel Changpeng Zhao konkurenční burzy Binance, což je aktuálně druhá největší kryptoměnová burza, oznámil prodej podílu v FTT, kvůli informacím, které vyplávaly na povrch. Po tomto oznámení začala hodnota FTT klesat a vznikly obavy, že FTX nemá dostatek likvidity na pokrytí transakcí, již 6. listopadu na burze byly výběry v hodnotě 6 miliard dolarů. Tyto zprávy přišly v době medvědího trhu, a způsobily to propad ostatních kryptoměn. Tato skutečnost také ovlivnila i další kryptoměnové burzy díky obavám zákazníků o své finance na jiných burzách. Na stole byla i možnost, že Binance koupí neamerickou část FTX, ale z prodeje sešlo díky špatnému nakládání s finančními prostředky a údajnému vyšetřování. [49]

FTX podala 11.11.2022 žádost o ochranu před bankrotem pro FTX, FTX.US a Alamedu. Výběry z burzy byly dočasně zmrazené. Téhož dne v noci došlo k útoku na FTX a FTX.US, kde bylo odcizeno přes 400 milionů dolarů z kryptoměnových peněženek pomocí SIM swap podvodu. FTX vydalo oznámení o tom, že byli hacknuti a uživatelé si mají odstranit aplikace a nechodit na web. Díky tomu byly aktiva přesunuta do cold storage neboli offline peněženky. Při krachu společnosti byla nahlášena ztráta 8 miliard dolarů z prostředků zákazníků. [49][50]

Téměř všechny finance, které byly klientům odcizeny budou dle současného CEO FTX navraceny v hodnotě původních vkladů, navíc s dodatečnými procenty, něco kolem 119 %. tato částka se pohybuje okolo 16,5 miliardy dolarů. Reakce bývalých zákazníků je na tento výsledek smíšená i přes to, že se jim investované peníze vrátí. Aktuální hodnota Bitcoinu se od té doby ztrojnásobila. [51]

4.2.2 Útok na Bybit

Kryptoměnová burza byla napadena 21.02.2025 největším hackem kryptoměnové burzy doposud. Bylo odcizeno přes 400 tisíc Ethera, které v té době mělo hodnotu 1,5 miliardy

dolarů. Útok byl proveden během rutinního převodu z cold wallet na hot wallet, kdy útočníci využili zranitelnost při schvalování transakce. [52]

Útok proběhl tak, že útočníci získali přístup k třetí straně, která poskytovala bezpečné rozhraní pro multi-signature transakce. Útočníci vložili do rozhraní škodlivý kód, který umožňuje měnit transakční údaje v reálném čase. Ty v momentě převodu útočníci změnili na jinou cílovou adresu a kryptoměny se odeslaly k útočníkům. [52]

Tento hack je připisován severokorejské skupině Lazarus Group. Burza Bybit po útoku hned ujistila klienty, že ostatní peněženky jsou v bezpečí a jsou solventní, takže se historie opakovat nebude. [52]

4.2.3 DDoS na české banky

Koncem srpna a počátkem září české banky zaznamenaly DDoS útoky, které byly motivovány politickým postojem, aby instituce přestaly podporovat Ukrajinu. Útoky probíhaly od 30. srpna až po 1. září roku 2023 a postihlo to přední české banky jako ČSOB, Komerční banka, Air Bank, Fio banka, Česká spořitelna, Raiffeisenbank, Moneta Money Bank a ČNB. Těmto problémům se nevyhnul ani web Pražské burzy. [53]

Za těmito útoky stojí ruská hackerská skupina NoName057(16). Útoky způsobily dočasné výpadky nebo zpomalení jednotlivých služeb. Finanční prostředky zůstaly nedotčeny. Banky na obnově a prevenci spolupracují s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). [53]

Dílčí závěr

Poslední kapitola přiblížila konkrétní typy kybernetických útoků, se kterými se nejčastěji v online prostoru mohou uživatelé setkat a následně byly popsány jednotlivé útoky na velké finanční instituce, které způsobily velké finanční škody nebo významně ovlivnily uživatele v podobě nedostupnosti bankovních služeb.

SHRNUTÍ TEORETICKÉ ČÁSTI

V teoretické části byla představena bezpečnost, jaký má význam a proč se jí zabývat. Dále v práci je uvedeno propojení kybernetické bezpečnosti s financemi a její důležitost na základě uvedených dat. Došlo k představení základního zabezpečovacího konceptu a představení řízení informační bezpečnosti. V poslední části první kapitoly je uvedena spojitost mezi bezpečností a uživatelem a také, jak se snaží významné orgány, starající se o bezpečnost a finance edukovat spotřebitele.

Následně jsou uvedeny jednotlivé legislativní opatření a jejich obecné představení s podmínkami, jejich účelem a smyslem, jaký tato opatření mají. Všechny tyto opatření by měly vzbudit důvěru spotřebitelů, stabilitu ekonomiky a bezpečnost. Dále jsou představeny trendy a vývoj v oblasti kybernetické bezpečnosti související s financemi a jejich aktuální nebo možné dopady, které na tuto oblast mohou mít.

V závěru jsou vyjmenovány jednotlivé typy kybernetických útoků, uvedená statistika v oblasti České republiky spojená s kybernetickými incidenty, a nakonec byly představeny výraznější útoky na finanční instituce, které se staly v posledních letech.

II PRAKTICKÁ ČÁST

5 DOSTUPNÁ BEZPEČNOSTNÍ ŘEŠENÍ

Způsobů, jak se dají zabezpečit vlastní finanční aktiva v kyberprostoru je mnoho. Od opatrného chování na internetu, silných hesel až po využívání bezpečnostních řešení poskytovatelů služeb. Nejlepší kombinací bezpečnosti jsou úplně všechny.

Když se na internetu chováme zodpovědně a neprocházíme stránkami, které jednak nejsou zabezpečené a zároveň se na nich nachází velké množství reklam nebo výhodných nabídek, jedná se s největší pravděpodobností o scam stránky. To platí nejenom pro webové stránky ale i pro sociální sítě a emailové schránky. Zde se nachází mnoho podvodných odkazů, které se snaží získat informace nebo obsahují nějaký vir s účelem škodit.

Pokud se chováme na internetu zodpovědně, tak se šance hrozby snižuje, avšak neeliminuje. Proto je dobré používat bezpečnostní řešení, která jsou uživatelům dostupná. Pod tím si lze představit silná a odlišná hesla, používání password manageru, VPN, antivirů a podobně. Toto jsou preventivní opatření, která slouží k odepření neoprávněného přístupu a pomáhají s odhalením škodlivých stránek a chrání tak zařízení před hrozbami.

Jelikož se zabýváme financemi, tak finanční organizace mají svá vlastní opatření, které zákazníkům nabízí nebo přikazuje používat. Nejčastěji se jedná o dvoufaktorové nebo multifaktorové zabezpečení. Tyto opatření znovu zvyšují bezpečnost před neoprávněným vniknutím.

Ale ani v případě, že používáme všechny možné druhy opatření a chováme se zodpovědně na internetu, neexistuje a nelze zaručit nulové riziko. Vždy existuje nějaká míra rizika ať už v podobě vnější nebo vnitřní hrozby, která nelze kompletně eliminovat. I přes tuto skutečnost je důležité se bezpečností zabývat a řešit. Je třeba se snažit riziko snížit na minimum tak, aby úspory byly co nejvíce zabezpečené, jelikož v opačném případě by to mohlo mít velký negativní dopad na naše životy.

5.1 Chování na internetu

Chování na internetu je klíčovým prvkem, který hodně ovlivní míru rizika ztrát, napadení a podobně. Je to také esenciální prvek, který zaručuje prevenci proti výše zmíněným hrozbám. Pokud se budeme chovat zodpovědně, tak se snižuje šance na to, abychom byli napadeni. Stejně jako v reálném životě, kdy se snažíme vyhnout nebezpečným situacím, které představují nějakou hrozbu, tak stejně to funguje i na internetu.

Základem je nesdílet více než je potřeba. To platí pro sociální sítě, registrace do soutěží, aplikací, ve hrách a podobně. Každá informace, která se dostane do online prostoru, je skoro nemožné ji vzít zpět. Každý uživatel zanechává svoji digitální stopu. To jsou všechny informace, které na internetu po sobě zanecháváme příspěvky, komentáře, fotky, účty a historii. Zároveň zejména na sociálních sítích je prostor pro sdílení osobních informací, aniž bychom si uvědomovali riziko tohoto sdílení. Pokud například máme slabá hesla, která jsou tvořena na základě osobních informací jako jsou jména mazlíčku, datumy narození a další, tak pokud budeme sdílet jméno našeho mazlíčka může to pomoci útočníkům získat jednodušeji přístup k účtům.

Dalším důležitým bodem je pohybovat se v „bezpečné části internetu“. To znamená pohybovat se na ověřených stránkách, neotvírat zbytečně odkazy, pod kterými nevíme, co se nachází to hlavně na emailech, forách, aplikacích a sociálních sítích. Právě pod těmito odkazy se nachází největší hrozba útoků a podvodů. Často se ale skrývá hrozba i pod oficiálními obchody s aplikacemi na mobilních zařízení v podobě Google Play nebo App Store. To, že si aplikaci stáhneme od oficiálního zdroje neznamená, že samotná aplikace je bezpečná. Proto i zde je třeba být obezřetný.

V online prostoru se objevuje velké množství podvodů v různých podobách. Když jdeme do kamenného obchodu vidíme a víme co si kupujeme. Na internetu to tak ale nefunguje. Všichni se určitě setkali s nabídkami, které jsou až moc dobré, aby byly pravdivé. Nabídky v podobě levných produktů, vysoce výnosných investic, věcí zadarmo a mnoho dalších. Proto je důležité používat kritické myšlení a ověřovat si informace. Ověřit si stránku nebo firmu, která nabízí tyto produkty. Pokud existují další obchody se stejným produktem podívat se na cenu i na ostatních obchodech, podívat se na recenze.

Uživatelé by také měli řešit na jakou síť se přihlašují. Pokud nejsme doma v privátní síti a jsme někde venku bez dat a chceme využít veřejnou Wi-Fi, tak je třeba být opatrný, jelikož pro přístup mohou tyto Wi-Fi chtít osobní informace nebo jsou sledovány. Proto na veřejných Wi-Fi sítích není dobré se přihlašovat na bankovní účty a podobně.

Pokud zjistíme, že jsme byli napadeni je dobré řešit situaci okamžitě. Pokud byl narušen nějaký účet je dobré změnit heslo na jiné unikátní heslo. Dále pokud to služba umožňuje odhlásit se ze všech zařízení, tak aby útočníkovi nezůstal účet přihlášený. V případě nemožnosti se dostat na daný účet kontaktovat podporu dané služby. Ta může navrátit přístup a zablokovat neoprávněnou aktivitu. V případě finančních podvodů, krádeží identity

a jiných trestných činů se obrátit na policii a nahlásit útok i na CSIRT.CZ, což je národní bezpečnostní tým, který se zabývá kybernetickými incidenty v ČR.

5.2 Dvou faktorová autentizace

2FA (Two-factor authentication) je bezpečnostní opatření, které přidává další vrstvu ochrany při přihlašování. Proces vyžaduje ověření v podobě dvou faktorů ověření. Ty zvyšují pravděpodobnost správného ověření, že uživatel je skutečně ten, za koho se vydává. Jako nevýhodu lze považovat delší čas na přihlášení nebo integrace s ostatními zařízeními nebo aplikacemi na kterých je uživatel závislý v době přihlášení. Výpadky nebo poškození by mohly ovlivnit možnost se přihlásit. [54]

Nejčastější faktory, dle kterých lze ověřit identitu osoby jsou faktory znalosti, vlastnictví, polohy a času. Faktorem znalosti ověřuje danou informaci, kterou uživatel zná. To je například heslo, PIN, kód a podobně. Faktor vlastnictví představuje předmět nebo jakékoliv vlastnictví v podobě ID karet, mobilních zařízení nebo autentizačních aplikací, které generují kódy pomocí, kterých se následně dá ověřit. Faktor polohy je dán na základě místa odkud se uživatel snaží připojit. Organizace může omezit přihlašování na určitá zařízení na specifických místech v závislosti na tom, odkud se zaměstnanci přihlašují. Faktor času omezuje ověření na určitou dobu, konkrétní čas, kdy se uživatel může přihlásit. Pokusy mimo tento čas budou například zablokovány. [54]

Mezi běžné metody 2FA metody patří SMS, notifikace, autentizační aplikace, hardwarové tokeny a mobilní zařízení. Hardwarové tokeny generují časově omezené kódy. Hardwarové tokeny mohou být taktéž USB zařízení, která připojíme k počítači a kód se automaticky přenesa a ověří nás. Výhodou je vysoká úroveň zabezpečení v síti. Náchylné na odcizení nebo ztrátu. SMS a hovory dostávají jednorázový kód v podobě SMS nebo hovoru. Toto byla oblíbená metoda přihlašování se do bank a finančních institucí. Výhodou je široká dostupnost a jednoduchá implementace a nevýhodou je možnost odposlouchávání. Od této metody se přestupuje na jiné. Push notifikace je modernější forma SMS, kdy dostáváme na registrovaném zařízení notifikaci s kódem. Je to uživatelsky přívětivá metoda, avšak nese riziko v kompromitaci nejčastěji mobilního zařízení. Mobilní zařízení umožňují několik metod v podobě autentifikačních opatření, biometrických údajů, GPS nebo push notifikací. Výhodou je více faktorů ověření, ale nevýhodou hrozba ztráty nebo kompromitace. [54]

2FA se využívá již běžně napříč kyberprostorem k přihlášení se do emailu, bank, sociálních sítí a podobně. Všechno, co obsahuje důvěrné a osobní informace. Je to klíčový prvek v dnešní bezpečnosti na internetu. [54]

5.2.1 Více faktorová autentizace

MTA (Multi-factor authentication) je bezpečnostní opatření, které vyžaduje od uživatelů poskytnutí dvou nebo více ověřovacích faktorů pro ověření přístupu k dané službě. To způsobuje vícevrstvou ochranu proti neoprávněnému vniknutí a ztěžuje útočníkům jednoduché prolomení. [55]

MTA funguje podobně jako 2FA, avšak uživatelé navíc přidávají další metodu ověření. MTA je využívána hlavně v kritických infrastrukturách, jako je například zdravotnictví, finance, bezpečnost, vládní organizace a podobně. 2FA je stále mezi uživateli a službami, které organizace nabízejí častější, ale do budoucna si myslím, že MTA začne převažovat. [55]

MTA poskytuje zvýšenou ochranu oproti 2FA. Umožňuje bezpečný a poměrně snadný přístup k práci na dálku a dodává více vrstev k prolomení. Co se týče rizik a nevýhod, může to být právě finančně nákladnější implementace tohoto zabezpečení. Ztráta nebo odcizení tokenů nebo telefonů představuje poměrně vysoké riziko a taktéž může být časově náročnější pro uživatele, a tak snížit efektivitu práce. [55]

Proto, aby MFA nebylo časově náročné pro zaměstnance a nesnižovalo by efektivitu práce je možné provést jednotné přihlášení, kdy u prvotního přihlášení se využije MTA. Poté už jednotné přihlášení autorizuje přístup ke všem potřebným aplikacím, ke kterým má uživatel oprávnění. [55]

5.3 Hesla

Hesla jsou stavebním kamenem kybernetické bezpečnosti. Hesla chrání osobní údaje před neoprávněným přístupem a jsou často prvním cílem útočníků. Hesla máme pro internetové bankovníctví, email, sociální sítě a mnoho dalších aplikací, zkrátka všude, kde je třeba se přihlásit. Útočníci mají různé techniky, například útok hrubou silou a slovníkový útok, při kterém zkoušejí hesla z uniklých databází nebo běžně používaných hesel. Proto je důležité se zajímat, zda je heslo silné, nebo naopak slabé.

Pod slabým heslem si lze představit „qwerty“, „heslo123“ a podobně. Pro silné heslo se doporučuje použít alespoň 12 znaků složených z velkých a malých písmen, číslic a

speciálních znaků. Čím delší heslo je, tím je obtížnější na prolomení. Dále by takové heslo nemělo být odvoditelné ze známých údajů o uživateli, jelikož by nemělo být uhodnutelné na základě sdílených informací na sociálních sítích. Pod tím si lze představit jména mazlíčka, oblíbené filmy a další. Hesla by neměla být skládána z posloupnosti znaků jako je „123456“ a další podobné posloupnosti. Pro tvorbu takových hesel lze využít generátory náhodných hesel, které vytvoří náhodné heslo „HdiQ5TzM<?3!“. Tato náhodně vygenerovaná hesla jsou obtížnější na zapamatování. Také je užitečné používat různá hesla a nemít jedno pro všechny účty. Pro zapamatování to ale může být velice složité, a proto lze používat správce hesel nebo heslové fráze. [56]

Frázová hesla jsou uživatelsky přívětivý způsob, jak tvořit silná a snadno zapamatovatelná hesla. Místo náhodných kombinací písmen, znaků a čísel se použije spojení slov nebo nějaká věta, která má pro nás význam a zároveň je těžce uhodnutelná pro ostatní. Příkladem frázového hesla může být „Vý!etpře5Kr4ter“, pokud je věta nebo fráze delší, než je maximální dovolený počet znaků, je dobré využít počátečních písmen a vytvořit kombinaci „Šjp!pvknH225“, což představuje větu „Šli jsme přes lávové pole v kráteru na Havaji 2025“.

5.4 Bezpečnostní programové vybavení

Na výše zmíněné bezpečnostní opatření není potřeba žádného programového vybavení, ale pro vyšší bezpečnost lze doplnit tyto bezpečnostní prvky o sadu programového vybavení, které pomůže s prevencí a identifikací potenciálních hrozeb. Jedná se o VPN, antivirové programy a správce hesel. Všechny tyto programy slouží k zvýšení kvality bezpečnosti uživatelů.

Antivirus je program nebo sada programů, která plní činnost k ochraně elektronických zařízení před potencionálními kybernetickými hrozbami. Programy dokážou předcházet, detekovat a odstranit či zablokovat potencionální hrozby dříve, než způsobí reálné škody. Antiviry běží na pozadí zařízení a provádějí kontrolu systému, souborů a webových stránek. V případě hrozby upozorní uživatele nebo zablokuje přístup na danou stránku v reálném čase. To je umožněno jejich komplexností a strojovému učení, kvůli kterému mohou zachytit dosud neznámé hrozby. Součástí antivirových programů bývá firewall, správce hesel, ochrana online bankovníctví a další funkce. To zajišťuje větší ochranu zařízení včetně identity a dat uživatele. Antivirové programy ESET, Avast, Bitdefender a mnoho dalších mají jak placené, tak neplacené verze. Placené verze logicky poskytují větší ochranu než ty

neplacené a je na uvážení, zda je potřeba vyšší ochrana s tím, že uživatel si musí odpovědět na tuto otázku sám. [57]

Virtuální privátní síť (VPN) vytváří šifrované spojení mezi uživatelem a internetem. Tím chrání přenášená data před neoprávněným přístupem, odposlechem a sledováním. Slouží k ochraně dat a anonymitě uživatele na internetu. Hlavní výhodou je maskování skutečné IP adresy za jinou IP adresu zabezpečeného serveru. VPN poskytuje bezpečné připojení na veřejných Wi-Fi sítích, které jsou často méně zabezpečené. Dále umožňují zaměnit geografickou lokaci k omezenému obsahu nebo vzdálenému firemnímu připojení. Některé VPN vytváří prostor pro bezpečné online placení a zabraňují potenciálním kybernetickým hrozbám na škodlivých webových stránkách. Nevýhodou VPN je pomalejší internetové připojení. VPN programů existuje velké množství například NordVPN, ProtonVPN a Surfshark. [58]

Správce hesel, jak již z názvu vypovídá je aplikace pro ukládání a správě přihlašovacích údajů, které se používají k přístupu do různých online účtů. Umožňují mít unikátní hesla na každý účet a automaticky vyplňují přihlašovací údaje. Hesla jsou šifrována a přístup k nim je chráněn jedním heslem. Uživatelům si stačí pamatovat jedno heslo, zatímco jsou všechny přihlašovací údaje ve větším bezpečí. Správci hesel nabízejí komfort, ale hlavně bezpečnost. Tím, že uživatelé nemusí používat stejná a slabá hesla se snižuje riziko zneužití účtů. Většina správců hesel nabízí generování silných hesel, takže uživatelé nemusí vymýšlet vlastní hesla a ty vygenerované jsou bezpečnější. [59]

Dnes většina správců hesel lze stáhnout na mobilní zařízení i přidat jako rozšíření do internetového prohlížeče. To zvyšuje pohodlné používání k přihlašování kdekoli a odkudkoli. Existuje několik správců hesel jako ESET Password Manager, Bitwarden, Keeper a 1Password umožňují multiplatformní synchronizaci mezi různými zařízeními. [59]

5.5 Kryptoměnové bezpečnostní řešení

Bezpečnost kryptoměn se odlišuje od normální bezpečnosti financí v kyberprostoru. Kryptoměny jsou digitální aktiva založená na blockchainové technologii. Bezpečnostní architektura kryptoměn kombinuje kryptografii, decentralizovanost a neměnnost záznamů. To dělá kryptoměny z technologického hlediska velmi bezpečné aktivum, ale rizika spojená s kryptoměnami jsou zaměřena na uživatelské chyby. V kapitole se primárně zaměřím na Bitcoin, jelikož to je hlavní kryptoměnové aktivum, které přesahuje přes 60 % kryptoměnového trhu.

Existuje hned několik možností, jak vlastnit kryptoměny. První možnost je kryptoměny nevlastnit, ale investovat do nich pomocí ETF. V tomto případě držitelé neřeší samotnou bezpečnost jeho kryptoměn, tu přenechává na instituci, která ETF spravuje. Aktuálně kryptoměny, které mohou být zakoupeny skrze ETF jsou Bitcoin a Ethereum. Podobnost tohoto nepřímého držení kryptoměn můžeme najít u brokerů, kteří neumožňují kryptoměny vybrat. To znamená, že pokud Bitcoin tímto způsobem koupíme, tak ho fakticky nevlastníme, ale vlastníme pouze nástroj odrážející jeho cenu.

Další možností držení kryptoměn je na burzách. Burzy umožňují nakupovat širokou škálu kryptoměn, které mají v nabídce. Nabídka se může lišit na každé burze. Nakoupit kryptoměny lze na dvou základních typech burz, a to centralizované a decentralizované.

V případě centralizované burzy, tak jsou spravovány jednou autoritou a vyžadují KYC (Know your customer). KYC slouží pro ověření totožnosti kupujícího v podobě nahrání občanky nebo jiných dokumentů, které ověří totožnost. To zvyšuje ochranu před praním špinavých peněz. Centralizované burzy jako Binance, Coinbase, Anycoin jsou běžnějším typem burz, kde většina investorů nakupuje. Je dobré využívat centralizované burzy v případě, kdy chcete krypto prodat, tak můžete dokázat vlastnictví kryptoměn a tím se vyhnout problémům spojených s AML zákonem. V případě dlouhodobého držení je lepší krypto přesunout z burzy na osobně vlastněnou peněženku, jelikož burza z výše uvedených útoků není nejbezpečnější forma na držení kryptoměn.

Druhým způsobem je nakupovat decentralizovaně pomocí burz, automatů nebo P2P platform. U decentralizovaného nakupování nemusíte uvádět identitu a nikdo ji nepožaduje. To zvyšuje anonymitu vlastnictví Bitcoinu a dalších držení kryptoměn, jelikož není přímý záznam na blockchainu, který by spojil transakci s daným držitelem, pokud předtím nepoužil adresu, na kterou mu byl Bitcoin poslán. Decentralizované obchodování nefunguje stejně jako centralizované, kdy burza kryptoměny drží, ale zde držitel má plnou kontrolu a zodpovědnost za své kryptoměny, které drží na své peněžence. Decentralizované burzy fungují za pomoci smart kontraktů, tedy program, který běží na blockchainu a provádí automatické akce, pokud jsou splněny dané podmínky. Není zde tedy potřeba obchodní partner. P2P platformy fungují na přímém nákupu mezi 2 stranami. V případě, že je poptávka někdo musí udělat nabídku. Příklad krypto za Kč nebo krypto za krypto na základě domluvy. Hlavním rozdílem mezi centralizovaným obchodováním a decentralizovaným obchodováním je anonymita a zodpovědnost.

Držet kryptoměny jinak než ve vlastním vlastnictví, zvyšuje enormně míru rizika. Taktéž držet kryptoměny jinak, znamená nemít nad nimi kontrolu. Proto existují různé typy kryptoměnových peněženek, které umožňují držet kryptoměny mimo burzy. Pro představení budou v práci jen ty nejznámější a nejpoužívanější. Uchovávat kryptoměny na vlastní peněženke znamená vlastnit privátní klíče a tím pádem mít plnou kontrolu. Vlastní držení zvyšuje bezpečnost, soukromí a nedotknutelnost. Naopak držet kryptoměny na burze představuje hrozbu ztráty v případě hacku, zmrazení účtu nebo krachu. [62]

5.5.1 Seed fráze

Při zařizování kryptoměnových peněženek je vygenerován seed, ten je složen z 12-24 náhodných anglických slov. Seed umožňuje obnovit přístup v případě ztráty, poškození zařízení nebo při instalaci softwaru na další zařízení. Seed je nejdůležitější věcí, která je třeba řádně chránit. Vlastník seedu má totiž plnou kontrolu nad kryptoměnami v dané peněženke. Pokud to jde je lepší nepřevádět seed do digitální podoby a vždy ho uchovat ve fyzické podobě. V případě, že někdo získá seed, tak má přístup a kontrolu nad všemi kryptoměnovými adresami a klíči, které se na peněženke nacházejí, a to mu umožňuje volný přesun kryptoměn. To je nebezpečné z důvodu nemožnosti rušit takovéto nechtěné transakce jako to lze udělat třeba v bankách.

5.5.2 Online peněženky

Online peněženky jsou přístupné přes webové prohlížeče. Jsou také nazývané „hot“ peněženkou, která slouží k rychlým převodům a na každodenní transakce vzhledem k jednoduchému přístupu a manipulaci. Peněženka umožňuje uživatelům přijímat, posílat a spravovat kryptoměny. Peněženky jsou neustále připojené k internetu, což je dělá přístupné odkudkoliv a kdekoliv. Bezpečnost online peněženek je jednou z nejrizikovějších. Online peněženky mají uložené klíče na serverech poskytovatele služeb, což značí riziko v případě napadnutí. Neustálé připojení k internetu není jenom výhodou, ale i bezpečnostním rizikem vzhledem k riziku kybernetického útoku. Takové peněženky se primárně používají na platformách burzy jako Coinbase, Binance a Anycoin. Co se týče bezpečnostní opatření z pohledu uživatele, tak může nastavit pouze silné heslo a 2FA nebo MFA ověřování, pokud to poskytovatel umožňuje. Jedná se tedy o jednu z nejrizikovějších možností, jak uchovávat dlouhodobě kryptoměny.

5.5.3 Software peněženky

Softwarové peněženky jsou aplikace, které lze nainstalovat na počítač či mobilní zařízení. Privátní klíče jsou uchovávány na zařízení, kde je program nainstalován. To ze softwarových peněženek dělá bezpečnější peněženky než online peněženky. Softwarovou peněženku lze využívat kdekoliv, kde uživatel má přístup ke svému zařízení. Taktéž jako online peněženky podporují širokou škálu kryptoměn. Bezpečnostní opatření z pohledu uživatele jsou podobné jako u online peněženek. Proti neoprávněnému vniknutí slouží hesla a několikafaktorové ověření. U mobilních zařízení to mohou být i biometrické prvky jako rozpoznání obličeje nebo otisky prstu. Dalším rozdílem jsou aktualizace, které by měly odstranit předešlé mezery v bezpečnosti. Bezpečnostní riziko pro tento typ peněženek představuje napadení systému zařízení v podobě malwaru nebo viru. Příkladem softwarových peněženek jsou Trust Wallet a Exodus.

5.5.4 Hardwarové peněženky

Hardwarové peněženky představují fyzická zařízení většinou o velikosti lehce většího USB flash disku. Tyto peněženky uchovávají privátní klíče offline a při připojení se k počítači nebo jinému zařízení, tak tyto klíče neopouští peněženku a zůstávají chráněné. I v případě, že zařízení je napadené malwarem, tak klíče nejsou v nebezpečí. Podporují také bezpečnost podepisování transakcí, kdy se na obrazovce peněženky zobrazuje adresa, na kterou jsou kryptoměny posílány. Podepisování je také doplněno potvrzením skrze PIN kód nebo tlačítka na peněžence. Seed se zobrazí pouze jednou, kdy se na zařízení zakládá účet, poté už stejný seed není možné získat a zobrazit. Výhodou hardwarových peněženek je zvýšená bezpečnost oproti softwarové a online peněžence. Plná kontrola na prostředky a nemožnost kohokoli zablokovat nebo zmrazit prostředky na peněžence. Zároveň zařízení je malé a lehce přenosné. Avšak i hardwarové peněženky nesou rizika. Jedním z nich je ztráta nebo krádež, ale pokud osoba, která zařízení získá nezná PIN, popřípadě ještě passphrase, tak se do zařízení stejně nedostane. Větší riziko představuje poničení zařízení a spolu s tím ztráty seedu pro obnovení. Největší riziko pro hardwarové peněženky tedy představuje odpovědnost uživatele a jak se zařízením a seedem nakládá. Je ideální volbou pro dlouhodobé držení kryptoměn a zejména vyšších částek. Hardwarové peněženky jsou považovány za jeden z nejbezpečnějších způsobů uchovávání kryptoměn. Mezi výrobce hardwarových peněženek se řadí Ledger a Trezor, který je zároveň českou společností.

5.5.5 Multi-sig peněženka

Tím nejbezpečnějším typem peněženek je multi-signiaure zkráceně multi-sig peněženka. Ta pro potvrzení provedení transakce požaduje více než jeden podpis. Oproti všem výše zmíněným, kde vždy stačí jeden podpis. Zároveň si u multi-sig peněženky nastavíme, kolik klíčů bude existovat a kolik z nich bude potřeba pro provedení transakce. Například stanoví se 3 privátní klíče, a z nich si lze nastavit ještě kolik jich bude potřeba pro provedení transakce. Můžou to být 2 nebo 3 klíče. Obvykle se klíče rozdělují mezi více lidí nebo na více míst, tak aby se zvýšila bezpečnost. V případě kompromitace jednoho klíče nehrozí nebezpečí neoprávněného přístupu nebo potvrzení transakce. Využívají se hlavně ve firmách, kde jsou využívány v představenstvech, aby jedna osoba neměla plnou kontrolu. Dále pro dědické účely nebo i pro jednotlivce, kteří chtějí zvýšit bezpečnost svých kryptoměn. Jejich výhodou je vyšší bezpečnost a redundance pro možnost obnovy. Nevýhodou je složitější nastavení a neshody mezi držiteli klíčů, zároveň ne všechny peněženky a platformy podporují multi-sig peněženky.

5.5.6 Diverzifikace úložišť

Efektivní správa kryptoměn často bude požadovat více než jeden typ úložišť. Už jen při nákupu kryptoměn a jakékoliv další manipulaci a přesunu kryptoměn na vlastní peněženku je využití dvou peněženek. Diverzifikace je důležitá na základě potřeby uživatele. Pokud uživatel chce kryptoměny dlouhodobě držet a nemá v plánu s nimi nějak manipulovat a podobně, tak je dobré použít takzvané „cold wallet“, to jsou peněženky, kde neděláme velké množství operací a necháváme kryptoměny dlouhodobě ležet, příkladem třeba hardwarové peněženky. Tedy nejsou vhodné pro každodenní transakce. Pro ty jsou určeny „hot wallets“, ke kterým je snadný přístup a jednoduchá manipulace. To jsou třeba online peněženky nebo softwarové peněženky. Pokud uživatel však chce dlouhodobě držet kryptoměny a zároveň jimi třeba i platit, je vhodné využívat více typů peněženek, jelikož platit s hardwarovou peněženkou v kavárně není úplně optimální a taktéž držet dlouhodobě kryptoměny na peněžence připojené k internetu, zvyšuje riziko prolomení takového účtu nebo ztráty kryptoměn.

5.5.7 Dodatečná zabezpečení kryptoměnových peněženek

Peněženky může chránit PIN. Tento PIN funguje pouze na tom zařízení, kde ho nastavíme., podobně jako mobilní zařízení, které je chráněno PINem. Ten funguje pouze na tom daném mobilním zařízení a pokud vezmeme SIM kartu a vložíme ji do jiného mobilního zařízení,

tak toto zařízení nebude požadovat ten stejný PIN, který byl nastaven na předešlém zařízení, pouze PIN SIM karty. V případě, že máme hardware peněženku číslo 1, kde se nastavil PIN a tato peněženka se poničila, tak v případě obnovení seedu na peněžence číslo 2 tento PIN již nebude. PIN slouží jako ochrana před fyzickým odcizením a je to první vrstva ochrany. [63]

Další dodatečnou vrstvu ochrany tvoří passphrase neboli přístupová fráze. Je to v podstatě obyčejné heslo, ale i zde je doporučeno se řídit zásadami správného hesla a primárně použít frázové heslo. Jelikož věty se lépe pamatují a jsou několikanásobně složitější na prolomení. Passphrase slouží jako doplňkové slovo k seedu. V případě, že někdo zjistí váš seed, tak bez znalosti passphrase na peněžence nenajde nic. Výhodou je, že passphrase se nikde nezapisuje ani neukládá v zařízení, takže je nemožné ji, jakkoliv zjistit, aniž bychom to sami vyrazili. Taktéž může být použita pro rodinné účely, kde každý člen rodiny bude sdílet jeden hardware se svou vlastní přístupovou frází. Riziko používání přístupové fráze je úschova této fráze, jelikož v případě, že zapomeneme toto heslo, frází, větu, tak se již ke svým kryptoměnovým prostředkům nedostaneme. Výhodou oproti seedu při úschově je to, že nelze na první pohled poznat, že se jedná o heslo ke kryptoměnové peněžence, takže je dobré to neuchovávat vedle seedu. [63]

Dodatečná zabezpečení na online a softwarových peněženkách jsou různé. Můžou tam být výše zmíněné možnosti nebo mohou bezpečnostní řešení být doplněny o multifaktorovou autentizaci.

5.6 Srovnání kryptoměnových peněženek

Porovnání známých kryptoměnových peněženek pro snazší rozhodování při výběru kryptoměnové peněženky. Jsou zde uvedeny 2 hardwarové peněženky od Trezoru a Ledgeru, v podobné cenové kategorii pro smysluplnější porovnání, a poté softwarová peněženka Trust Wallet pro kontrast, jak si softwarové peněženky vedou proti hardwarovým.

Tabulka 3 Porovnání kryptoměnových peněženek

Parametr	Trezor Safe 3	Ledger Nano S Plus	Trust Wallet
Cena	1899 Kč	2049 Kč	-
Typ peněženky	Hardware	Hardware	Software
Secure element čip	EAL6+	EAL6+	Ne
Zdrojový kód	Open-source	Uzavřený	Uzavřený
Passphrase	Ano	Ano	Ne
PIN	Ano	Ano	Ano
Fyzické potvrzení	Na zařízení	Na zařízení	Ne
Biometrie	Ne	Ne	Ano
Seed fráze	12/20/24 slov	12/24 slov	12/24 slov
Pokročilá záloha Shamir	Ano	Ne	Ne
Ochrana privátních klíčů	Na zařízení	Na zařízení	Na zařízení uživatele
Staking	Ano	Ano	Ano
NFT podpora	Přes třetí strany	Ano	Ano
Platforma	Trezor Suit, web	Ledger Live, web	Mobilní aplikace nebo rozšíření
Podpora kryptoměn	1000+	500+	10 000 000+
Možnost nákupu	Ne	Ano	Ano
Připojeno k internetu	Ne	Ne	Ano

Zdroj [65][66][67]

5.6.1 Trezor Safe 3

Trezor Safe 3 je třetí verzi hardwarových peněženek vyráběných českou firmou Trezor. Tato peněženka má otevřený zdrojový kód, což představuje větší transparentnost. Obsahuje bezpečnostní certifikaci čipů EAL6+. Podporuje pokročilé bezpečnostní funkce, jako jsou passphrase, shamir backup a privátní klíče jsou šifrovány na zařízení a peněženka nemá přístup k internetu. V případě připojení do počítače, trezor nepředává informace o privátních klíčích do počítače. Každé potvrzení transakce se musí potvrdit přímo na zařízení, kde je kryptoměnová adresa pro kontrolu. Je ideálním řešením pro bitcoinové fanoušky a dlouhodobé držitele. Rozhraní je přehledné a lze nastavit možnost sledování kryptoměn na peněžence v aplikaci Trezor Suite, aniž by se musela připojit peněženka. Nevýhodou může být staking a podpora NFT, která je možná přes třetí strany, což nemusí vyhovovat každému. [65]



Obrázek 2 Trezor Safe 3 [65]

5.6.2 Ledger Nano S Plus

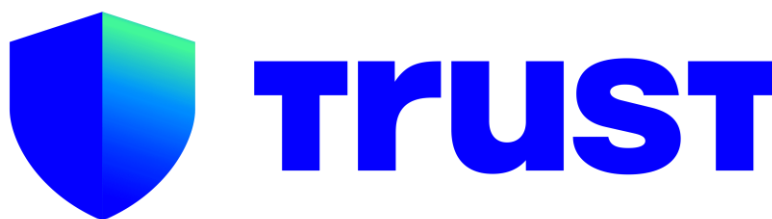
Ledger Nano S Plus je hardwarová peněženka vyráběná americkou společností Ledger. Jedná se o nejlevnější model prodáváný touto společností. Taktéž, jak u Trezoru, má bezpečnostní certifikaci čipů EAL6+. Zařízení podporuje v aplikaci Ledger Live přes 500 kryptoměn, ale přes třetí strany 5000+ kryptoměn. Dále přímo v aplikaci podporuje staking a NFT. Je tedy vhodné pro fanoušky Ethereum a NFTs. Bezpečnostní prvky jsou stejné jako u Trezoru až na možnost Shamir backupu. To pro kryptoměnové experty a skeptiky dnešní společnosti může představovat nevýhodu. Zdrojový kód je uzavřený, tedy až na aplikaci, která je open-source. Bezpečnost kódu je tedy přijímána na základě důvěry ve společnost. [66]



Obrázek 3 Ledger Nano S Plus [66]

5.6.3 Trust Wallet

Trust Wallet je softwarová peněženka převážně dělaná na mobilní zařízení a jako rozšíření do prohlížečů. Výhodou je to, že peněženka je zcela bezplatná, a tak pro začátečníky může být ideální, a zároveň podporuje miliony tokenů. Lze zde nakupovat přímo v aplikaci jednotlivé kryptoměny. Bezpečnostní opatření jsou výrazně horší v porovnání s hardwarovými peněženkami. Nelze zde nastavit passphrase, seed je při nastavování peněženky v digitální formě a klíče jsou ukládány na mobilním zařízení. Nenabízí ani fyzické potvrzení transakcí, tedy může být náchylná na man-in-the-middle útoky. Peněženka je spíše vhodná pro menší částky a běžné používání nikoli pro úschovu většího množství kryptoměn jako tomu je u předešlých dvou peněženek. [67]



Obrázek 4 Trust Wallet [67]

5.7 Srovnání brokerů

Porovnání brokerů je klíčovým krokem každého, kdo chce investovat. Je důležité se zaměřit na nabídku aktiv, bezpečnostní prvky, poplatky, kvalitu platformy, regulace a dostupnost. Dnes existuje velká řada brokerů a všichni přináší různé služby. Srovnání tří nejvíce promovanych brokerů na české půdě. V práci se zaměříme na eToro, Trading 212 a XTB.

Tabulka 4 Srovnání brokerů

Parametr	eToro	XTB	Trading 212
Akcie	Ano	Ano	Ano
ETF	Ano	Ano	Ano
Forex	Ano	Ano	Ano
Komodity	Ano	Ano	Ano
Kryptoměny	Ano	Ano	Ano
Poplatek za vklad	Ne	Ano	Ano
Poplatek za výběr	Ano	Do 3000 Kč	Ne
Poplatek za neaktivitu	Ano	Ano	Ne
Webová platforma	Ano	Ano	Ano
Mobilní aplikace	Ano	Ano	Ano
Copy trading	Ano	Ne	Ne
Demo účet	Ano	Ano	Ano
Výukové materiály	Ano	Ano	Ano
Minimální vklad	50 USD	Ne	1 EUR
Regulace	CySEC	ČNB	CySEC
Počet instrumentů	6 000	7 900	10 000
MFA/2FA	Ano	Ano	Ano
Veřejně obchodovány	Ano	Ano	Ne
Privátní pojistka	Ano	Ne	Ne
Frakční akcie	Ano	Ano	Ano

Zdroj [68][69][70]

5.7.1 EToro

Na základě odpovědí jsou si vyjmenovaní brokeri velice podobní. EToro je brokerem regulovaným Kyperskou komisí pro cenné papíry, která může působit po celé EU. Peníze klientů jsou drženy na oddělených účtech a broker tyto prostředky nemůže použít na provozní účely nebo investice. V případě insolvence brokera každý uživatel má nárok na vrácení 20 000 EUR celkových prostředků v EU, které měl nenakoupené i nakoupené. Nakoupené aktiva se drží u custodiana, což jsou subjekty, které drží akcie nebo jiná aktiva. Existuje zde i pojistka do výše 1 milionu EUR pro každého klienta a kryje hotovost, ETF, akcie, CFD držené na eToro v případě insolvence, podvodu nebo krádeže instrumentů. Tato pojistka má celkový limit 25 milionů EUR pro všechny klienty dohromady. Tato pojistka platí pro všechny klienty automaticky, nehledě na to, jakou mají úroveň. EToro má odměňovací systém za investované prostředky na jejich platformě v podobě úrovní. Tyto úrovně poskytují benefity pro uživatele, kteří mají více zainvestováno. Jako bezpečnostní opatření je možné mít aktivované 2FA ověření a přidat věrohodné zařízení, které se musí každý měsíc znovu potvrdit 2FA. [68]

Nabízí širokou škálu investičních instrumentů a typů investic. Poskytuje českou zákaznickou podporu a problémy z vlastní zkušenosti se řeší rychle. Umožňuje vytvořit si demo účet, kde se neobchoduje s reálnými penězi. Jako jediný z porovnávaných brokerů umožňuje copytrading nebo možnost sledovat dalších uživatelů. Přes copytrading mohou investoři investovat skrze jiného uživatele na platformě a pokaždé když daný investor udělá obchod, vám se automaticky provede taky. Obchody se provádí procentuálně z dostupných prostředků. [68]

Poplatky jsou na eToru v případě neaktivity na účtu delší jak 1 rok 10 USD měsíčně z volných prostředků. Proto, aby tento poplatek nebyl účtován, stačí se přihlásit jednou ročně nebo nemít ve volných prostředcích 10 USD. Dále jsou poplatky za otevření a zavření pozice 1 nebo 2 dolary. Tento poplatek se liší na základě burzy. Výběrový poplatek na USD účtech je 5 USD a minimální částka pro výběr je 30 USD. Pro Eura nebo GBP poplatky ani minimální částka není. [68]

Platforma ze všech uvedených brokerů je nejvíce uživatelsky přívětivá a vhodná pro začátečníky. Umožňuje tvorbu přehledného watchlistu a správu portfolia a nabízí instrumenty pro analýzu jednotlivých společností. Mezi slabé stránky patří lehce vyšší rozdíl mezi nákupní a prodejní cenou kryptoměn. Poplatky pro účty vedené v dolarech. A minimální vklad je 50 USD pro Českou republiku. [68]

5.7.2 XTB

Platforma XTB je regulovaná ČNB, což oproti ostatním uvedeným brokerům zvyšuje kredibilitu převážně pro české uživatele. Společnost je také veřejně obchodovaná na polské burze a lze zjistit její finanční stav a tím zvýšit důvěryhodnost. Peníze klientů jsou drženy znovu na oddělených účtech a broker s těmito penězi nemůže nakládat dle vlastního uvážení. V případě insolvence mají uživatelé právo na 20 000 EUR celkových prostředků napříč účty, pokud by došlo k selhání ochrany vlastních aktiv. Existuje možnost si zapnout dvoufázové ověření a přidat věrohodné zařízení. [69]

Je možné si založit několik měnových účtů, jako například český, dolarový, eurový. Broker nabízí širší škálu obchodovaných instrumentů než eToro. Dále XTB se snaží tvořit vzdělávací materiály a analýzy společností, které jsou veřejně dostupné. Jako jediný broker nabízí tituly na české burze. Nabízejí možnost tvorby vlastního watchlistu. Slabou stránkou XTB je jejich ne úplně uživatelsky přívětivá platforma a může být obtížnější pro začátečníky. [69]

Co se týče poplatků, jsou zde poplatky za vklad ve všech měnách pomocí platební karty, PayU a PayPal. Tyto poplatky jsou aktuálně maximálně do 1 % vkladu a liší se dle měn, které vkládáme. Lze vložit prostředky i přes bankovní účet, a to bez poplatku. Poplatek za výběr je zde 350 Kč do hodnoty výběru 3 000 Kč, poté jsou výběry zdarma. Poplatky jsou i za neaktivitu na účtu, které jsou účtovány měsíčně v podobě 10 EUR. Proto, aby účet byl aktivní, se musí otevřít nebo zavřít jedna pozice ročně anebo vložit prostředky během posledních 90 dnů. Poplatek za neaktivitu bere pouze z volně dostupných prostředků a existuje zde ochrana proti zápornému zůstatku, takže se poplatek nevybírám, pokud nejsou na účtu volné prostředky. [69]

5.7.3 Trading 212

Trading 212 je regulován stejně jako eToro Kyperskou komisí pro cenné papíry. Peníze klientů, jako v předešlých případech, jsou drženy na účtech custodianů. Akcie jsou drženy u třetí strany Bank of New York Mellon a Interactive brokers, což je zároveň i další broker. V případě insolvence jsou znovu kryti uživatelé do 20 000 EUR celkových prostředků v případě, že by došlo k selhání ochrany vlastních aktiv. Je zde možnost dvoufázového ověření a dodatečné zaslání informací v případě připojení z nového zařízení anebo při pohybech na účtu. [70]

Trading nabízí ještě širší škálu investičních instrumentů a rozděluje investiční a CFD účty zvlášť. Umožňuje vklad, výběr a obchodování v několika měnách a při koupi daného aktiva se přepočítává změna kurzu měn a dopad změny kurzu v reálném čase na otevřené pozice. Umožňuje tvořit watchlisty a tvořit si vlastní investiční „koláč“, kde si lze vybrat vlastní akciové tituly, ETF nebo další investiční nástroje a rozdělit procenta jednotlivých titulů, které vložíme do takzvaného „koláče“ a umožňuje uživatelům automaticky investovat do vlastního „ETF“. Dále je možnost obchodování 24/5, neboli 5 dní v týdnu amerických akcií. Trading také tvoří vzdělávací materiály. Uživatelská přívětivost platformy je z osobního pohledu lehce lepší než u XTB a o něco horší než u eTora. Sice Trading nemá podporu na řešení problémů v českém jazyce, tak alespoň rozhraní platformy je v českém jazyce. [70]

Na Trading je minimální vklad, výběr a nákup či prodej 1 EUR na investiční účet a vklad 10 EUR na CFD účet. Peníze lze převádět mezi jednotlivými účty bez poplatků. Nemá poplatky za otevření nebo zavření obchodů. Poplatek za vklad na investičním účtu je na platební karty 0,7 % až po vložených 60 000 Kč, které jsou osvobozeny od tohoto poplatku. Vklad bankovním převodem je zdarma a může trvat až dva dny. Poplatek za neaktivitu na účtu neexistuje. [70]

Dílčí závěr

Kapitola obsahuje dostupná bezpečnostní opatření a řešení. Jedná se o technické a netechnické opatření. Jednotlivá opatření mají přiblížit možnosti, jak opatření využívat, a k čemu jsou užitečné. Dále kapitola obsahuje srovnání kryptoměnových peněženek a významných brokerů dostupných, které má přiblížit dostupné produkty na českém trhu s detailním popisem funkcí a zabezpečení.

6 ANALÝZA HROZEB

Pro analýzu hrozeb jsem vybral PNH analýzu, která bude sloužit k určení největších hrozeb proti kterým budou potřeba dále tvořit dodatečné bezpečnostní opatření, které budou provedeny v modelu NIST Cybersecurity Framework (CSF), který slouží k identifikaci a následnému cyklu přidávání bezpečnostních opatření, které mají za úkol zvýšit bezpečnost.

6.1 PNH analýza

PNH analýza je tvořena, tak aby dodala výsledky, které budou odrážet největší nástrahy a nejvíce zásadní hrozby se kterými se uživatelé běžně setkávají a proti kterým je důležité přidat dodatečná bezpečnostní opatření nebo jiné způsoby, jak snížit riziko těchto hrozeb, aby se minimalizoval jejich dopad.

Jsou vytvořeny 3 tabulky pravděpodobnost, následek a odhalitelnost. Každá z těchto tabulek má 5 hodnotících bodů, kdy 1 je nejméně závažný a 5 nejvíce závažný. Tabulka rizik je tvořena na základě násobení přiřazených čísel v každé tabulce a čím vyšší číslo vyšlo, tím závažnější hrozba je.

Tabulka 5 PNH analýza – pravděpodobnost

P – pravděpodobnost vzniku rizika	
1	Hrozba se vyskytuje zcela výjimečně, jednou za 5–10 let
2	Hrozba se vyskytuje neobvykle, jednou za 2–3 roky
3	Hrozba se vyskytuje ročně
4	Hrozba se vyskytuje pravidelně několikrát do roka
5	Hrozba se vyskytuje denně

Tabulka 6 PNH analýza – následky

N – Následek	
1	Bez finanční ztráty nebo minimální dopad
2	Malá finanční ztráta neovlivňující život (ztráta do 5 tisíc)
3	Znatelná finanční ztráta nebo ztráta přístupu k účtu (do 50 tisíc)
4	Významná finanční ztráta nebo ztráta identity (50 tisíc plus)
5	Extrémní finanční ztráta s trvalými následky (stovky tisíc)

Tabulka 7 PNH analýza – Odhalitelnost

H – Odhalitelnost rizika	
1	Riziko odhalitelné během jeho spáchání, automaticky odhalitelné
2	Riziko lze odhalit pomocí běžných nástrojů
3	Riziko vyžaduje určitou pozornost na odhalení
4	Riziko je velmi obtížně odhalitelné
5	Riziko je nemožné identifikovat před útokem

Tabulka 8 PNH analýza – tabulka rizik

R	Výsledná rizika	Přijatelnost rizika
1-3	Bezvýznamné riziko	Přijatelné
4-15	Méně významné riziko	Tolerované
16-40	Mírné riziko	Podmínečně přijatelné
41-99	Významné riziko	Nepřijatelné
100-125	Nežádoucí riziko	Nepřijatelné

Tabulka 9 PNH analýza

Hrozba	Pravděpodobnost	Následek	Odhalitelnost	Míra rizika
DDoS útoky	3	1	1	3
Falešné investiční nabídky	5	3	3	45
Krádeže přihlašovacích údajů	4	4	4	64
Ransomware	3	4	3	36
Phishing a spear phishing	5	3	3	45
Fake apps a podvodné weby	5	3	3	45
Krádež identity	3	5	5	75
Únik dat	2	4	4	32
Keylogger	4	4	2	32
Malware	4	4	2	32
Sociální inženýrství	5	4	5	100
SIM swapping	3	4	3	36
Zneužití cloudových úložišť	3	4	3	36
Zneužití zranitelností zařízení	3	3	4	36
Deepfake podvody	5	3	3	45
Cryptojacking	4	1	3	12
Zneužití veřejných Wi-Fi	4	3	3	36

6.1.1 Vyhodnocení analýzy

Přiřazené hodnoty k jednotlivým hodnotícím prvkům jsou na základě dat získaných při tvorbě této práce a na základě expertního odhadu. Jednotlivá kritéria jsou posuzována obecně. Například podvody, phishing a podobné hrozby, tak je u nich uvedena pravděpodobnost maximální, jelikož se s touto hrozbou uživatelé setkávají denně napříč internetem. Co se týče následku, tak jsou případy, kdy ztráty jsou zanedbatelné a jsou i případy, kde ztráty jsou enormní až život měnící. Je tedy uveden následek 3, který dle dostupných dat z podvodů na klienty bank činí za rok 2024 15 952 Kč. Tato částka nepředstavuje nijak významnou finanční ztrátu, která by změnila život, ale je určitě znatelná. Odhalitelnost těchto podvodů záleží na sofistikovanosti. Ve většině případů lze tyto podvody odhalit zvýšenou pozorností a základní znalostí, tedy znovu hodnota 3. Na základě tohoto vysvětlení jsou hodnoceny jednotlivé hrozby.

Z analýzy vyšlo, že hrozba DDoS útoku je přijatelná z pohledu uživatele, jelikož obecně na jednotlivé uživatele DDoS útoky převážně nejsou. Pro útočníka to nedává finančně smysl, a zároveň DDoS útok na finanční instituci, kde má uživatel spravované finance, nepředstavuje finanční ztrátu, ale špatnou zkušenost. Avšak i zde se může stát, že díky DDoS útoku neproběhne nějaká transakce, která by mohla vést k potencionálním škodám. Ale z analýzy vyplývá, že není potřeba zvýšené ochrany proti DDoS útokům.

V další kategorii, kde riziko je tolerované je znovu jenom jedna položka a to cryptojacking. Cryptojacking nepředstavuje žádnou přímou finanční ztrátu například z bankovního účtu, ale může zvýšit cenu placenou za elektřinu, tedy nějaká finanční ztráta se na to váže, a zároveň zpomaluje zařízení, na kterém útočník těží. Cryptojacking útoky by měly vzrůst o 20 % meziročně. Je to díky tomu, že tyto útoky mohou být dlouhodobější zdroje příjmu pro útočníky v případě, že malware na těžbu nebude detekován. Detekovat cryptojacking malware dokážou antivirové programy, nebo lze zjistit zpomalením zařízení a přehříváním, taktéž zvýšenou zátěží procesoru a grafické karty. [60]

Kategorie podmíněčně přijatelného rizika je většina analyzovaných hrozeb. Do této kategorie spadají hrozby typu únik dat, malware, ransomware, SIM swapping, zneužití zranitelnosti cloudu, zařízení a veřejných Wi-Fi sítí. V případě zneužití zranitelnosti cloudu, zařízení, Wi-Fi sítí a úniku dat z institucí uživatelé podmíněčně přijímají riziko spojené s využíváním těchto zařízení a ukládáním dat na nich, které mohou vést k finančním ztrátám nebo ztrátě účtů a podobně. Zvýšení bezpečnosti u těchto hrozeb je diverzifikace institucí (banky, burzy, brokeri), dále minimální digitální stopa citlivých údajů (hesla a osobní citlivé

údaje). U zbylých hrozeb riziko uživatel podmíněčně nepřijímá, ale většinou se jedná o hrozby, které nejsou tak časté nebo jsou jednodušeji detekovatelné pomocí antivirů a podobně.

V posledních dvou kategoriích jsou rizika nepřijatelná a je důležité se vůči nim bránit vícero bezpečnostními prvky. Jsou zde převážně hrozby s velkým dopadem a vysokou pravděpodobností setkání se s danými hrozbami. Spadají pod ně phishingové útoky, krádeže přihlašovacích údajů a identit, podvodné weby, aplikace a investiční nabídky. To jsou hrozby, proti kterým je potřeba využívat výše zmíněné bezpečnostní opatření a zodpovědné chování se na internetu, tak aby se minimalizovala expozice vůči těmto útokům a podvodům.

Nejvíce zásadní hrozbou z analýzy vyšlo sociální inženýrství. To jako jediné vyšlo jako nežádoucí riziko vzhledem k nemožné ochraně skrze bezpečnostní aplikace jako antivirus a podobně, dále nedodržováním tvorby správných hesel a jejich uchovávání, enormnímu sdílení osobních informací na sociálních sítích a využíváním AI pro uvěřitelnější dojem. Je to z důvodu, že pro samotné sociální inženýrství nejsou potřeba nadstandardní technologické dovednosti k získání informací, co útočník potřebuje. Zároveň sociální inženýrství je úzce spojeno s ostatními kybernetickými útoky, jako je phishing, ransomware, krádež identity, získání přihlašovacích údajů a vydírání.

6.2 NIST Cybersecurity Framework 1.1

Je model, který má za úkol zlepšit ochranu kritické infrastruktury před kybernetickými útoky. Je navržen převážně pro organizace, ale lze využít i pro jednotlivce pro zabezpečení svých aktiv. Skládá se z pěti hlavních částí. Těmi jsou identifikace, ochrana, detekce, reakce a obnova. V tomto pořadí probíhá nekonečný cyklus vylepšování ochrany vůči kybernetickým útokům. Poskytuje jednotný přístup k řešení kybernetické bezpečnosti. Je využíván po celém světě. NIST je organizace pro kybernetickou bezpečnost v USA, která tento model vytvořila. [61]



Obrázek 5 CSF 1.1 [61]

Všechny hrozby, u kterých vyšlo riziko nepřijatelné, jsou ve většině případů podvody zaměřující se na informace o uživateli nebo jeho přihlašovací údaje, díky kterým získá útočník kontrolu nad důležitými účty s financemi. Případně se snaží získat důvěru uživatelů za účelem zisku financí nebo osobních údajů.

6.2.1 Sociální inženýrství

Vyšlo jako nejzávažnější hrozba s největším rizikem. Sociální inženýrství může být propojeno s dalšími hrozbami jako jsou podvody, phishing, smishing a podobně.

- Identifikace – Uvědomění, kde útočník může získat informace ze sociálních sítí, fór, emailů, telefonů.
- Ochrana – Používat technická zabezpečení jako MFA a správná hesla nebo správce hesel, důkladně kontrolovat emaily a stránky, kde se přihlašujeme. Neposkytovat citlivé osobní informace po telefonu nebo emailu, omezit sdílení osobních informací na sociálních sítích.

- Detekce – Útok lze poznat, že útočník tlačí na čas a vyžaduje okamžitou platbu, či vydání informací. Útočník požaduje informace o citlivých údajích, jako platební karty, hesla, rodné číslo a podobně, přehnaně dobré nabídky.
- Reakce – V momentě podezření útoku je dobré změnit hesla v případě pocitu napadení. Vždy ověřovat informace, pokud se jedná o emaily nebo podvodné telefonáty, kontrolovat hlavičku emailu, volat zpět instituci, která volala. Označit adresu jako spam nebo ji blokovat. Nahlásit útok příslušné instituci.
- Obnova – Poučení se z předešlých incidentů, doplnění dostupných možných bezpečnostních opatření například silnější hesla, aktivní antivirový program, MFA autentizaci a být obezřetnější při komunikaci s neznámými lidmi přes internet.

6.2.2 Krádež identity

Krádež identity je druhou nejrizikovější hrozbou na základě analýzy, kvůli velkému možnému dopadu. Zároveň umožňuje pachateli vytvářet falešné účty, žádat o půjčky na cizí jméno nebo jinak zneužívat identitu oběti.

- Identifikace – Znovu jako u sociálního inženýrství určit, kde jsou citlivé údaje uloženy, a kdo k nim má přístup. Řádná úschova fyzických dokumentů a prošlé dokumenty skartovat.
- Ochrana – Používání silných hesel a znovu mít aktivované 2FA/MFA u všech účtů, kde to jde. Neodpovídat a neklikat na přílohy v podvodných emailech. Nesdílet osobní informace na sociálních sítích. Využívání VPN při přístupu na veřejné Wi-Fi sítě.
- Detekce – Monitorovat všechny účty, hlavně tam, kde se mohou ztratit finance. K detekci mohou sloužit emaily upozorňující o změně hesel nebo pokusu o přihlášení. Dále při 2FA sms s kódy k ověření.
- Reakce – V případě podezřelé transakce okamžitě zablokovat účet či kartu, nahlásit incident bance a změnit hesla. Nahlášení incidentu na příslušné orgány, tedy policii.
- Obnova – Obměna aktuálních hesel, zrušení podvodných účtů kontaktováním příslušných poskytovatelů služeb. Provést kontrolu zabezpečovacích prvků na stávajících účtech a případně je posílit.

6.2.3 Krádež přihlašovacích údajů

Krádež přihlašovacích údajů, registrací nebo přihlášením se na podvodných stránkách může vést k neoprávněnému přístupu útočníka na email, kde dokáže způsobit velké škody.

- **Identifikace** – Určení kritických účtů a identifikace možných útoků, které mohou způsobit krádež přihlašovacích údajů (phishing, keylogger, úniky dat společností nebo ze zařízení). Tvorba následných ochranných opatření na tyto útoky.
- **Ochrana** – Technická opatření jako aktivní antivirus pro detekci malwaru, aktivovaná MFA, neuchovávat přístupné přihlašovací informace v digitální podobě a bezpečně uchovávat ve fyzické podobě, pokud je to nutné. Ověřování URL adresy, zdali je zabezpečená doména „https//“. Používání silného hesla. Nemít stejná hesla na důležitých účtech.
- **Detekce** – Nastavení notifikací na email o pokusech přihlášení nebo o nových přihlášení na účet. Pravidelná kontrola účtů.
- **Reakce** – Pokud existuje možnost odhlásit účet ze všech zařízení na kterých je účet přihlášen. Nahlásit útok poskytovateli služeb a v případě finančních ztrát obeznámit policii. V případě nemožnosti se přihlásit na účet okamžitě kontaktovat poskytovatele služby.
- **Obnova** – Kontaktovat příslušnou instituci se žádostí obnovy hesla a následné změny hesla. Přidat dvoufázové ověření. Aktivní antivirus pro detekci malwaru, jako je například keylogger. Provést kontrolu zařízení pro případné možné keyloggery a jiný malware.

6.2.4 Phishing

Nejrozsáhlejší forma kybernetických útoků, hlavně v podobě emailu, kde denně „vyhráváme“ miliony od princů z Afriky nebo dědíme velké peněžní částky z bohatých rodin v zahraničí.

- **Identifikace** – Hrozba hrozí převážně přes emaily, sociální sítě, mobilní zařízení a falešné webové stránky.
- **Ochrana** – Používání blokátorů reklam k filtraci vyskakovacích oken a reklam se škodlivými odkazy. Aktivní antispamové filtry na emailu. Mít aktivní 2FA/MFA.

Kontrola nevyžádaných emailů, hovorů a sms s poskytovatelem služeb a zároveň kontrola hlavičky emailu či telefonního čísla.

- Detekce – Emaily požadují odpovědi s osobními informacemi. Přílohy mají koncovky „.exe“ a odkazy přesměrovávají na nezabezpečené weby.
- Reakce – V případě rozkliknutí nebo zadání údajů, okamžitě odhlásit účet ze všech zařízení. Změna hesla. Aktivovat vícefaktorovou autentifikaci, pokud není. Informovat organizaci a poskytovatele služeb, že se jedná o phishing.
- Obnova – Požádání o obnovu hesla u poskytovatele služeb. Kontrola emailu pro nastavená pravidla, kde mohou být nastavená pravidla o přesměrování zpráv nebo o mazání zpráv. V případě finanční instituce kontrola účtu a neoprávněné transakce nahlásit.

6.2.5 Podvody

Podvody jsou oblíbené praktiky útočníků z důvodu rychlého a jednoduchého zbohatnutí. Ve falešných nabídkách jsou 90 % slevy na produkty. Velmi výhodné investiční nabídky s vysokou a rychlou návratností. Tlak na uživatele s časově omezenou nabídkou do 15 minut nebo posledních 5 uživatelů pro, které je tato výhodná nabídka.

- Identifikace – Nejčastější pokusy o podvody jsou u online nákupů za zvýhodněné ceny, vysoce výnosné investiční nabídky a na sociálních sítích žádosti o peníze. Podvodné e-shopy, falešné technické podpory a investiční nabídky.
- Ochrana – Provádět nákupy na ověřených e-shopech a podívat se na recenze obchodu, i když i ty mohou být falešné. Ověření identity lidí na sociálních sítích, zdali to jsou vážně ti lidé, za které se vydávají. Používání blokátorů reklam k zamezení vyskakování podvodných reklam. U investičních nabídek si zjistit více o společnosti a nabízeném produktu.
- Detekce – V případě dobře znějících nabídek, třeba návratnost investic 50 % ročně a časových limitací na výrobky je třeba upozornit. Vyhledat si společnosti, zda o ni neexistují články nebo komunikace na fórech o tom, že je podvodná stejně jako s mobilním číslem, kdy stačí zadat číslo do vyhledávače a číslo bude označeno lidmi jako podvodné.

- Reakce – V případě napálení se je dobré kontaktovat banku a požádat o zrušení a vrácení platby. Při investičních podvodech obeznámit i policii. Nahlásit podvody na platformách, kde k nim došlo, aby se nenapálilo více lidí a společnosti je stáhly dolů.
- Obnova – Poučení se z incidentu a začít ověřovat weby, společnosti a nabídky před zasláním peněz. Nastavení limitů pro online platby, pro minimalizaci finančních ztrát. Vyhledání právních rad.

Dílčí závěr

Kapitola se zabývá analýzou rizik hrozeb pro zjištění největších hrozeb v kyberprostoru. Analýza byla provedena z pohledu koncového uživatele, tedy určuje největší hrozby, se kterými se uživatel může setkat. Potom je v práci uveden cyklický model QSF 1.1. Model slouží ke zvýšení kybernetické bezpečnosti před hlavními hrozbami, které vyšly z analýzy rizik.

7 BEZPEČNOSTNÍ DOPORUČENÍ

Dodatečná a výsledná doporučení na základě zpracované diplomové práce, obsahující klíčové aspekty bezpečnosti financí v kyberprostoru. Zahrnují preventivní opatření a zásady správného chování. Tato doporučení jsou především pro běžné uživatele, kteří se chtějí zvýšit bezpečnost digitálních financí a snížit své stopy na internetu.

7.1 Bezpečná správa hardwarových kryptoměnových peněženek

Při pořízení peněženky zkontrolovat, zda je pečeť proti manipulaci „stříbrná nálepka“ na produktech od Trezoru nedotčená, a vždy nakupovat HW peněženky z oficiálních obchodů. Pro bezpečnostní uchování hardwarových peněženek je vhodné ji skladovat na bezpečném místě. Může se jednat o trezor, skříň na zámek nebo pouze obyčejnou skříň, kde by měl přístup pouze vlastník. Zároveň by peněženka měla být uchována tak, aby nebyla na očích při pouhém otevření. Vhodné je ji uložit někde, kde ji nepoškodí voda nebo oheň, pokud existuje taková možnost.

Seed v každém případě vždy uchovávat pouze ve fyzické podobě a nikdy digitálně. Dvě možnosti, jak zapsat seed, a to na papír, kde se opíšou slova seedu ručně. Není od věci mít 2 až 3 papírové kopie seedu na více místech. V případě katastrofy nebo mimořádné situace existují další kopie a my tak nepřijdeme o všechny kryptoměny. Znovu tyto kopie je třeba bezpečně uložit. Důležité je neskladovat seed hned vedle hardwarové peněženky. Zvyšuje to bezpečnost před lidmi, kteří neví, o co se jedná, anebo pokud najde někdo trezor, tak nemá přístup k seedu a peněženka je zabezpečená PINem. Pokud máme doma trezor, je lepší tam vložit seed a prioritizovat ho před hardwarovou peněženkou. Další možností zapsání seedu je na kovové destičky, které výrobci hardwarových peněženek vyrábí a slouží jako kvalitnější úschova před vodou a požárem. Další vhodné opatření je využít pečeť proti manipulaci a tím zalepit uložené seedy, abychom věděli, zdali s nimi nebylo manipulováno. Tyto pečete dostává uživatel při zakoupení kovových záloh.

Passphrase je znovu dobré uchovávat mimo místa úschovy trezoru a seedu. Passphrase má velkou výhodu při úschově, pokud ji neoznačíme na papíře nebo v kterékoliv podobě, že se jedná o passphrase. Je pro útočníka složité zjistit, že se jedná o passphrase. Proto se nedoporučuje passphrase jakýmkoliv způsobem označovat jako heslo nebo podobně. Je vhodné ji uschovat na méně viditelné místo a nikomu neříkat, že se jedná o passphrase. Zde není taková potřeba ochrany jako v případě seedu, který by měl být zabezpečen nejvíce.

7.2 Bezpečná správa finančních účtů a prevence proti podvodům

Bezpečná správa financí v kyberprostoru se skládá z technických a netechnických opatření, které jsou ve většině případů volně dostupné. Klíčovým opatřením je ověřovat správnost webů, na které se přihlašujeme. To lze zjistit pomocí ověření URL odkazu tak, že tam nebudou překlepy anebo podobné znaky. Dále lze ověřit přes adresní řádek, který obsahuje „https://“, či ikonu zámku, také pomocí platného certifikátu webu. Pro správu finančních údajů určitě nemít oblíbené poznámkové bloky s přihlašovacími údaji snadno dostupné na ploše bez zabezpečení zařízení a už vůbec ne pokud je zařízení sdílené. Pro správu účtů používat správce hesel s velmi silným heslem, které si budeme pamatovat nebo ho mít napsané ve fyzické formě někde mimo zařízení, bezpečně uchované.

Při investování dávat pozor, zda investice a slibované výsledky nejsou až moc dobré. V případě, že se bude zdát, že tomu tak bude, tak ve většině případů se jedná o podvod. Dávat si pozor na nově spuštěné kryptoměny, které jsou hodně promovány na sociálních sítích, a je úplně jedno kým. Obecně je dobré být obezřetný při investicích do kryptoměn. Často se u nově spuštěných kryptoměn jedná o „pump and dump“ scam, kde „insideři“ nakoupí před začátkem promování dané mince a po vypromování mince vlivnými influencery na sociálních sítích, tak dojde k rapidnímu nárustu ceny. Poté insideři prodají své pozice a cena mince spadne dolů a lidé, kteří vstupovali s pozicemi později, přijdou o značné procentuální částky pozice.

Vždy používat všechny možné prostředky k ochraně. Silná hesla a neopakující se hesla na více účtech. Využívat dvoufaktorové nebo vícefaktorové ověření na účtech, i přesto, že to může být v některých případech nepříjemné. Při připojování se na veřejných Wi-Fi sítích používat VPN a nepřipojovat se na bankovní a jiné podobné účty. K tomu je dobré využívat mobilních dat nebo bezpečnou domácí síť. Aktivovaný antivirový program, který dopomáhá s detekcí škodlivých programů a hlídá bezpečnost zařízení v případě nepozornosti otevírání emailových příloh nebo kliknutím na vyskakovací okna. Ta lze omezit přes ad blockery a zároveň tyto blokátory reklam chrání před podvodnými reklamami.

7.3 Bezpečné používání internetu

Základní informace k správnému používání internetu jsou již výše zmíněny. Ale škála hrozeb, se kterou se uživatel může setkat, je široká. Cílem je minimalizovat riziko zneužití osobních a finančních údajů. To zahrnuje vyhýbání se nedůvěryhodným webovým stránkám, zvláště pokud stránky požadují registrace a osobní data. Pokud není potřeba, nepřipojovat se

zbytečně na veřejné Wi-Fi sítě, a když už, tak s VPN. Aktualizovat software, operační systémy a podobně pro předejití napadení zastaralých systémů. Aktualizace bývají většinou opravy chyb nebo bezpečnostní opatření na nalezené hrozby.

Zaměření se na omezení sdílení informací na sociálních sítích. Velké sdílení osobních informací může vést k cíleným útokům skrze vydírání, krádeže identity nebo účtů. I sdílení polohy může vést k fyzickému vloupání do domu. Takže čím méně o sobě dáme vědět, tím více v bezpečí budeme. Snažit se být odolný na naléhání urgentních nabídek a proti přesvědčování k odeslání osobních informací. Zálohujte si data, která jsou pro vás důležitá, příkladem mohou být třeba fotky na externí zařízení nebo do cloudu. Proti hrozbám jako je ransomware nebo proti poškození disků na zařízení. Bezpečné používání internetu nestojí jenom na technických opatření, ale na zdravých návycích a prevenci.

7.4 Proč se zabývat bezpečnostní kybernetických financí a investováním

Zabývat se kybernetickou bezpečností financí je důležité hned z několika důvodů. Jedním z důvodů je velká převaha digitálních peněz oproti těm fyzickým v poměru 1:5,5, jak je uvedeno výše. Skutečný poměr ale bude ještě vyšší pro digitální finance. Velká část populace v České republice má úspory v digitální podobě. Sofistikovanost útoků stále roste a jsou čím dál efektivnější, i když regulatorní podmínky pro instituce a bezpečnostní podmínky, kterými se musí organizace řídit, se taktéž zpřísňují. Ale většinou to je právě lidská chyba, která je tou fatální. Proto je dobré se zabývat a zajímat o aktuální dění v oblasti kybernetické bezpečnosti, a ještě o to víc, když využíváme služby poskytované online související s penězi.

V případě otázky, zda není lepší vybrat všechny peníze z kyberprostoru a uložit je někam do trezoru, tak na to neexistuje správná odpověď. Každý hodnotí riziko jinak a koneckonců výsledné rozhodnutí stojí právě na každém z nás. Ale důvod, proč se zabývat investičními nástroji, a je jedno, ať už to jsou nástroje online nebo fyzické investice, tak je prostý. Je to inflace, která se v průměru v České republice pohybuje za posledních 10 let na 4,36 % a za posledních 20 let na 3,33 %. [71]

Tabulka 10 Inflace za posledních 10 let

Rok	Počáteční hodnota 1 000 Kč
2015	997,01 Kč
2016	990,08 Kč
2017	965,93 Kč
2018	946,06 Kč
2019	920,29 Kč
2020	891,76 Kč
2021	859,11 Kč
2022	746,40 Kč
2023	674,26 Kč
2024	657,81 Kč

Český statistický úřad [71]

$$1000 / (1 + \frac{\text{inflace}}{100})$$

Tabulka ukazuje hodnotu tisícikorunové bankovky v roce 2015 a jakou hodnotu by měla ta stejná bankovka z roku 2015 na konci roku 2024 při započítání inflace, tedy 657,81 Kč. To činí 34,2 % což je ztráta hodnoty lehce přes jednu třetinu počáteční hodnoty. Takže v případě nic nedělání s touto bankovkou za posledních 10 let bychom přišli o 1/3 hodnoty, bez jakéhokoliv útoku nebo krádeže. V případě 20 let je to necelých 50% ztráty počáteční hodnoty. To si myslím, že je pádný argument na to, proč se zabývat jakoukoliv formou investic a jejím zabezpečením, ať už je to v kyberprostoru nebo ne. Avšak je důležité mít na paměti, že investice přináší riziko, a je vždy nutné zvážit, zda jsme ochotni to riziko podstoupit.

Dílčí závěr

V poslední kapitole jsou praktická doporučení, jakým způsobem uchovávat hardwarové peněženky a náležitosti kolem. Dále praktická opatření k používání internetu, aby bylo co nejvíce bezpečné. Opatření se zaměřují primárně na prevenci, jak už proti kybernetickým útokům a finančním podvodům. Na závěr kapitoly jsou uvedeny důvody, proč se zabývat kybernetickou bezpečností a investováním.

SHRNUTÍ PRAKTICKÉ ČÁSTI

Praktická část představuje bezpečnostní opatření rozdělená na technická a netechnická. Zmíněná opatření jsou čtenářům přiblížena jako konkrétní možnosti zabezpečení s praktickým využitím pro zvýšení jejich ochrany jak finančních prostředků, tak i ochrany zařízení a účtů v kyberprostoru. V návaznosti na představené bezpečnostní opatření jsou rozebrány a porovnány kryptoměnové peněženky a významní brokeri působící na českém trhu. V tomto srovnání se nachází detailnější popis konkrétních produktů a služeb.

Následně se v práci nachází analýza rizik pro jednotlivé uživatele. Jejím cílem je identifikovat nejzásadnější hrozby, které mají velký dopad, a zároveň jsou velmi pravděpodobné. Vyhodnocení PNH analýzy má přispět k povědomí čtenářů o možných hrozbách a jak se proti nim obecně preventivně chránit. Na základě této analýzy je model QSF proveden rozbor nejvíce rizikových hrozeb, kde jsou konkrétní indicie, jak hrozbu poznat, jak se bránit. Tento model slouží ke zvýšení úrovně kybernetické bezpečnosti.

V poslední kapitole jsou uvedena dodatečná doporučení o tom, jak uchovávat kryptoměnové peněženky a související věci k tomu. Přehled praktických opatření při používání internetu a sociálních sítí. Opatření jsou zaměřena především na prevenci proti kybernetickým útokům a finančním podvodům. Na závěr jsou uvedeny důvody, proč se zabývat kybernetickou bezpečností a případným investováním.

ZHODNOCENÍ PRÁCE

Diplomová práce se z úvodu zaměřila na vysvětlení pojmů bezpečnosti a její důležitosti, hlavně při ochraně financí v kyberprostoru. V práci bylo zjištěno, že kybernetické útoky jsou na vzestupu, ale překvapivě škody se v průměru snižují na základě dostupných informací. To může naznačovat dvě věci. To může znamenat, že regulatorní opatření a investice organizací do kybernetické bezpečnosti jsou efektivnější. Ze snižování průměrné škody můžeme vyvodit, že je lepší reakceschopnost vůči jednotlivým útokům a tím se snižuje škoda. Avšak případů přibývá a jedná se převážně o podvodné útoky na koncové uživatele, jelikož jsou nejzranitelnější. To nahrává argumentu, že uživatelé nemají dostatečné povědomí v dané problematice.

Praktická část nevychází pouze z popisu možných opatření, ale vychází i z vlastního ověřování informací a analýz. Zaměřil jsem se na sběr dat o konkrétních produktech, službách, statistikách a zjišťování mezer v povědomí uživatelů o kybernetické bezpečnosti. Na tomto základu jsou z vyhodnocených dat tvořeny výstupy na míru a konkrétní doporučení pro řízení a snižování rizik v kyberprostoru.

V práci se povedlo nastínit jednotlivé typy útoků a jednotlivé případy útoků, ze kterých se lze poučit. Zároveň se povedlo rozebrat správné chování na internetu, které je doplněno o to, jak nastavit správné heslo, multifaktorovou autentizaci a využívat další programy ke zvýšení preventivní bezpečnosti. U kryptoměn jsou rozebrány hlavně úložiště, jelikož ty bývají právě nejčastějším kamenem úrazu při hrozbách spojených s kryptoměnami.

Naopak práce by šla rozšířit o případové studie jednotlivých hrozeb a doplnit praktickou část o pohledy ze strany organizací. Dále vytvořit materiál vhodný k propagaci kybernetické bezpečnosti. I přesto, že tyto materiály již existují, stejně nejsou dostatečně viditelné, aby to minimálně snížilo meziroční vzrůst počtu útoků, který stále rapidně stoupá.

ZÁVĚR

Digitální proměna světa, především hlavně světa financí a bezpečnosti přináší velké pohodlí, ale i velké nástrahy. Ještě před 20 lety informace v této práci nebyli mnohdy ani na světě. Jak práce ukázala, tak svět v online prostředí se nesmírně posunul a stále se posouvá. Bezpečností na internetu se již nezabývají pouze velké organizace a technologické firmy, ale i my, koncoví uživatelé využívající služeb těchto gigantů.

V práci je představen pojem bezpečnost a její historie, taktéž jsou zde uvedeny vývojové trendy, které nás v blízké době mohou čekat. No a pokud se například dočkáme kvantových počítačů, tak kybernetická bezpečnost bude znovu pozměněná. Součástí práce je přehled hrozeb a skutečných útoků, které přiblíží rizika a jejich dopady na finance uživatelů. Teoretická část slouží k přiblížení tématu, vysvětlení jednotlivých hrozeb a pochopení problematiky kybernetické bezpečnosti.

V praktické části jsou rozvedeny dostupná bezpečnostní opatření pro uživatele, které mohou využívat pro zvýšení prevence proti kybernetickým hrozbám. Bezpečnost je především zaměřena na finanční část, tedy kryptoměny, banky, účty, brokery a všechno, kde hrozí riziko ztráty finančních prostředků nebo identity. Práce v praktické části se zejména zaměřuje na to, jak s riziky nakládat a pracovat tak, aby se minimalizovaly incidenty. Srovnány jsou i některé dostupné řešení na trhu, které uživatel může využívat.

Z analýzy rizik hrozeb vyplynulo, že největší hrozbu představují útoky podvodného typu, jelikož to jsou útoky, které preventivně bezpečnostní programové vybavení nezastaví, nebo velmi zřídka. Ty nejvíc rizikové hrozby jsou detailněji rozebrány s radami a pomůckami, jak se chránit.

Konečným výstupem práce jsou bezpečnostní doporučení o přístupu k bezpečnosti, a hlavně chování se na internetu za využití výše zmíněných opatření. Kybernetická bezpečnost nelze jednorázově provést, ale musí se konstantně monitorovat změny, trendy a těm se přizpůsobovat tak, abychom byli v co největším klidu a bezpečí.

SEZNAM POUŽITÉ LITERATURY

- [1] Kyberbezpečnost, 2025. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity>. [cit. 2025-03-20].
- [2] JAŠEK, Roman a MALANÍK, David, 2013. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 9788074543128. Dostupné také z: <http://hdl.handle.net/10563/25821>.
- [3] Kyberbezpečnost financí v online prostoru. Online. Darktrace. Dostupné z: <https://darktrace.com/cyber-ai-glossary/cybersecurity-for-financial-services>. [cit. 2025-03-03].
- [4] Poměr peněz, 2020. Online. Seznamzpravy. 28.02.2020. Dostupné z: <https://www.seznamzpravy.cz/clanek/na-kazdeho-cecha-pripada-60-tisic-fyzickych-a-330-tisic-virtualnich-korun-89504>. [cit. 2025-03-03].
- [5] PŘÁDKA, Michal a KALA, Jan. Elektronické bankovníctví: rady a tipy. Praxe manažera. Praha: Computer Press, 2000. ISBN 8072263285
- [6] CIA triáda, c2025. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/cia-triad>. [cit. 2025-03-19].
- [7] ŠULC, Vladimír, 2018. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 9788073807375.
- [8] KORYČANSKÁ, Martina. Informační technologie v bankovníctví. Vedoucí Zelinka, Stanislav. Zlín: Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav elektroniky a měření, 2020. Dostupné také z: <http://hdl.handle.net/10563/47908>.
- [9] #nePINdej. Online. Nukib.gov. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/2002-ceska-bankovni-asociace-opet-spousti-kampan-nepindej-nove-do-ni-zapojila-i-umelou-inteligenci/>. [cit. 2025-03-05].
- [10] Desatero spotřebitele. Online. Cnb. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/desatero-spotrebitele/>. [cit. 2025-03-05].
- [11] Regulace a legislativa. Online. Cnb. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/regulace-a-dohled-nad-platebnimi-institucemi-a-institucemi-elektronickych-penez/>. [cit. 2025-03-03].

- [12] DORA. Online. Cnb. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/dora-digitalni-provozni-odolnost-financniho-trhu/>. [cit. 2025-03-03].
- [13] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2554 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, 2022. Online. In: Eur-lex.europa. Dostupné z: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>. [cit. 2025-03-21].
- [14] *MiCA*. Online. Cnb. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/novinky/pusobnost-cnb_podle_narizeni_o_trzich_kryptoaktiv_mica/. [cit. 2025-03-03].
- [15] Zákon č. 31/2025 Sb. Zákon o implementaci předpisů Evropské unie v oblasti digitalizace finančního trhu (zákon o digitalizaci finančního trhu), 2025. Online. In: Zakonyprolidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2025-31>. [cit. 2025-03-21].
- [16] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937, 2023. Online. In: Eur-lex.europa. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32023R1114>. [cit. 2025-03-21].
- [17] CASPs. Online. Kryptoregulace. Dostupné z: <https://www.kryptoregulace.cz/poskytovatele-sluzeb-souvisejicich-s-kryptoaktivy-casps/>. [cit. 2025-03-04].
- [18] Směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu, 2015. Online. In: Eur-lex.europa. Dostupné z: <https://eur-lex.europa.eu/CS/legal-content/summary/revised-rules-for-payment-services-in-the-eu.html?fromSummary=24>. [cit. 2025-03-21].
- [19] Zákon č. 370/2017 Sb., o platebním styku, 2017. Online. In: E-sbirka. Dostupné z: <https://www.e-sbirka.cz/sb/2017/370/2025-02-15>. [cit. 2025-03-21].
- [20] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU)

- 2016/1148 (směrnice NIS 2), 2022. Online. Eur-lex.europa.eu. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32022L2555>. [cit. 2025-03-21].
- [21] NIS2. Online. Nukib. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>. [cit. 2025-03-04].
- [22] Odvětví NIS2, c2025. Online. In: Nukib. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2025/03/11/nis-srovnani_uid_67d085d72f1ad.svg. [cit. 2025-03-21].
- [23] NIS2, c2025. Online. In: Nukib. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-smernici-nis2>. [cit. 2025-03-21].
- [24] AML zákon, c2024. Online. Bankid. Dostupné z: <https://bankid.cz/aml/aml-zakon/#co-je-aml-zakon>. [cit. 2025-03-26].
- [25] Výroční zpráva Finančního analytického úřadu 2023, 2024. Online. Fau.gov.cz. Dostupné z: <https://fau.gov.cz/files/4053-vyrocní-zprava-financniho-analytickeho-uradu-za-rok-2023.pdf>. [cit. 2025-03-26].
- [26] 2025. Online. Sentinelone. Dostupné z: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/>. [cit. 2025-03-04].
- [27] Využití AI k ochraně v kyberprostoru. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity>. [cit. 2025-03-04].
- [28] Využití AI k útokům v kyberprostoru. Online. O2cybernews. Dostupné z: <https://o2cybernews.cz/clanky/co-ocekavat-od-roku-2025-odpovidaji-odbornici-z-o2>. [cit. 2025-03-04].
- [29] AI v investování, 2023. Online. Financialregulationcourses. Dostupné z: <https://www.financialregulationcourses.com/the-role-of-ai-in-investment-banking-and-management-practices>. [cit. 2025-03-04].
- [30] ZTA, 2025. Online. CrowdStrike. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/zero-trust-architecture/>. [cit. 2025-03-04].

- [31] Kvantové počítače, 2024. Online. Qubits. Dostupné z: <https://qubits.cz/clanky/blizi-se-quantova-boure-revoluce-ktera-prepise-pravidla-digitalniho-sveta/>. [cit. 2025-03-05].
- [32] Kvantová kryptografie, 2025. Online. Digicert. Dostupné z: <https://www.digicert.com/blog/nist-pqc-standards-are-here>. [cit. 2025-03-04].
- [33] Útoky s využitím kvantového počítače. Online. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>. [cit. 2025-03-05].
- [34] MACHEK, Vojtěch, 2025. Kryptoměny. Online. Finex. Dostupné z: <https://finex.cz/rubrika/kryptomeny/>. [cit. 2025-03-20].
- [35] GEORGE, Emily, 2024. Kryptoměny. Online. Gate. Dostupné z: <https://www.gate.io/learn/articles/predicting-the-next-five-years-of-cryptocurrency-2024-2029-innovations-regulations-and-market-predictions/3267>. [cit. 2025-03-20].
- [36] NARAYANAN, Arvind; BONNEAU, Joseph; EDWARD, Felten; MILLER, Andrew a GOLDFEDER, Steven. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, [2016]. ISBN 978-0-691-17169-2.
- [37] LEUCCI, Stefano, 2025. CBDC. Online. Edps. Dostupné z: https://www.edps.europa.eu/press-publications/publications/techsonar/central-bank-digital-currency_en. [cit. 2025-03-27].
- [38] Kybernetické útoky na banky. Online. Ct24.ceskatelevize. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/domaci/kyberutoky-na-klienty-bank-loni-vzrostly-o-ctvrtinu-357557>. [cit. 2025-03-05].
- [39] Kybernetické útoky na kryptoměny. Online. Czechcrunch. Dostupné z: <https://cc.cz/jedni-tvrdi-ze-se-v-cesku-obchodovaly-kryptomeny-za-4-miliardy-nesmysl-je-to-vic-kontruje-konkurent/>. [cit. 2025-03-05].
- [40] Kybernetické útoky na kryptoměny. Online. Yahoo finance. Dostupné z: <https://finance.yahoo.com/news/coinbase-users-losing-300m-social-151909141.html>. [cit. 2025-03-05].
- [41] Útok na Bybit. Online. Forbes. Dostupné z: <https://forbes.cz/burza-bybit-celila-hackerskemu-utoku-odcizeno-bylo-temer-15-miliardy-dolaru-v-tokenech/>. [cit. 2025-03-05].

- [42] GLENNY, Misha. Temný trh: kyberzloději, kyberpolicisté a vy. Zip. Praha: Argo, 2013. ISBN 9788073635220.
- [43] Zpráva o stavu kybernetické bezpečnosti 2023, 2024. Online. Nukib.gov.cz. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf. [cit. 2025-03-26].
- [44] Phishing. Online. Eset. Dostupné z: <https://www.eset.com/cz/phishing/>. [cit. 2025-03-05].
- [45] Phishing, c2025. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/phishing>. [cit. 2025-03-26].
- [46] Kybernetické hrozby. Online. Eset. Dostupné z: <https://www.eset.com/cz/slovník/>. [cit. 2025-03-06].
- [47] Kryptoměny. Online. Coinmarketcap. Dostupné z: <https://coinmarketcap.com/>. [cit. 2025-03-06].
- [48] Společnosti. Online. Companiesmarketcap. Dostupné z: <https://companiesmarketcap.com/>. [cit. 2025-03-06].
- [49] RAMIREZ, Dalia, 2024. FTX pád. Online. Nerdwallet. Dostupné z: <https://www.nerdwallet.com/article/investing/ftx-crash>. [cit. 2025-03-10].
- [50] Útok, 2024. Online. Cointelegraph. Dostupné z: <https://cointelegraph.com/news/crypto-exchange-ftx-400m-hack-sim-swap-attack>. [cit. 2025-03-10].
- [51] FTX vrácení peněz, 2024. Online. Bbc. Dostupné z: <https://www.bbc.com/news/articles/c0qz3dg21vqo>. [cit. 2025-03-10].
- [52] PEAK, BRADLEY. Bybit útok. Online. Cointelegraph. Dostupné z: <https://cointelegraph.com/learn/articles/how-the-bybit-hack-happened>. [cit. 2025-03-14].
- [53] DDoS útok. Online. Byznys. Dostupné z: <https://byznys.hn.cz/c1-67239210-kyberutoky-pokracuji-treti-den-hackeri-tentokrat-napadli-web-cnb>. [cit. 2025-03-14].
- [54] 2FA. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/two-factor-authentication>. [cit. 2025-04-03].

- [55] MTA. Online. Fortinet. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication>. [cit. 2025-04-03].
- [56] Hesla, c1992–2025. Online. Eset. Dostupné z: <https://www.eset.com/cz/generator-hesel/#c5832972>. [cit. 2025-04-08].
- [57] Antivirus, c1992 – 2025. Online. Eset. Dostupné z: <https://www.eset.com/cz/antivirus-software/>. [cit. 2025-04-15].
- [58] VPN, c1992 – 2025. Online. Eset. Dostupné z: <https://www.eset.com/cz/vpn/>. [cit. 2025-04-15].
- [59] Správce hesel, c1992 – 2025. Online. Eset. Dostupné z: <https://www.eset.com/cz/spravce-hesel-pojem/>. [cit. 2025-04-15].
- [60] FERGUSON, RANDY. Cryptojacking. Online. Cloudtweaks. 2024. Dostupné z: <https://cloudtweaks.com/2024/10/how-recognize-prevent-cryptojacking-2025-expert/>. [cit. 2025-05-04].
- [61] NIST CSF 1.0. Online. Nist. 2014. Dostupné z: <https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10>. [cit. 2025-05-04].
- [62] NOVÁK, Michal. Lightning network: platby budoucnosti. [Praha]: Braiins Systems, 2023. ISBN 978-80-908709-4-9.
- [63] Passphrase a PIN. Online. Anycoin. 2024. Dostupné z: <https://www.anycoin.cz/blog/blog-passphrase>. [cit. 2025-05-07].
- [64] CSF 1.1. Online. In: Nist. 2018. Dostupné z: <https://www.nist.gov/sites/default/files/styles/social/public/images/2018/04/16/framework-01.png?itok=qpEb9OMg>. [cit. 2025-05-07].
- [65] Trezor safe 3. Online. Trezor.io. Dostupné z: <https://trezor.io/trezor-safe-3>. [cit. 2025-05-07].
- [66] Ledger Nano S Plus, c2025. Online. Ledger. Dostupné z: <https://shop.ledger.com/pages/ledger-nano-s-plus>. [cit. 2025-05-07].
- [67] DOLEŽAL, Martin, 2024. Trust wallet. Online. Finex. Dostupné z: <https://finex.cz/recenze/trust-wallet/>. [cit. 2025-05-07].

- [68] EToro, c2006-2025. Online. Etoro. Dostupné z: <https://help.etoro.com/s?language=cs>. [cit. 2025-05-07].
- [69] XTB, c2025. Online. Xtb. Dostupné z: <https://www.xtb.com/cz/help-center/platby-a-poplatky>. [cit. 2025-05-07].
- [70] Trading212, c2006-2025. Online. Trading212. Dostupné z: <https://www.trading212.com/cs/terms/invest>. [cit. 2025-05-07].
- [71] Inflace ČR. Online. CSU. 2025. Dostupné z: <https://csu.gov.cz/prumerna-rocni-mira-inflace-v-letech-1998-2023>. [cit. 2025-05-08].

SEZNAM OBRÁZKŮ

Obrázek 1 Odvětví NIS2 [22]	28
Obrázek 2 Trezor Safe 3 [64].....	56
Obrázek 3 Ledger Nano S Plus [65]	57
Obrázek 4 Trust Wallet [66]	57
Obrázek 5 CSF 1.1 [61]	68

SEZNAM TABULEK

Tabulka 1 Dělení hrozeb.....	20
Tabulka 2 Statistický přehled činnosti FAÚ za roky 2020 až 2023	30
Tabulka 3 Porovnání kryptoměnových peněženek	55
Tabulka 4 Srovnání brokerů	59
Tabulka 5 PNH analýza – pravděpodobnost.....	63
Tabulka 6 PNH analýza – následky	64
Tabulka 7 PNH analýza – Odhalitelnost.....	64
Tabulka 8 PNH analýza – tabulka rizik	64
Tabulka 9 PNH analýza	65
Tabulka 10 Inflace za posledních 10 let	76

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ETF – Exchange traded fund

KYC – Know your customer

AML – Anti money laundering

2FA – Two factor authentication

MFA – Multi-Factor authentication

P2P – Peer to peer

ZTA – Zero trust architecture

PNH – Pravděpodobnost, Následek, Odhalitelnost

QSF – Cybersecurity Framework

FAÚ – Finanční analytický úřad

NIST – National Institute of Standards and Technology

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

ČNB – Česká národní banka

CFD – Contract for Difference

VPN – Virtual Private Network

Wi-Fi – Wireless Fidelity

NFT – Non-Fungible Token

HW – Hardware

SMS – Short Message Service

NIS – Network and Information Security

DORA – Digital Operational Resilience Act

PSD2 – Payment Services Directive 2

MiCA – Markets in Crypto-Assets Regulation

DDoS – Distributed Denial of Service

DoS – Denial of Service

CBDC – Central Bank Digital Currency

IoT – Internet of things

CA – Certifikační autorita

IP – Internet protocol

CIA – Confidentiality, Integrity, Availability

RTO – Recovery time objective

RPO – Recovery point objective

Kč – Koruna česká

USD – United States Dollar

CySEC – Cyprus Securities and Exchange Commission

CaaS – Crime as a Service

EAL – Evaluation Assurance Level