Krádež majetku jako specifický způsob narušení bezpečnosti

Bc. Vojtěch Galda

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Vojtěch Galda**
Osobní číslo:	**A17252**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Krádež majetku jako specifický způsob narušení bezpečnosti**
Téma anglicky:	**The Theft of Property as a Specific Way of Breaching Security**

Zásady pro vypracování:

1. **Specifikujte druhy bezpečnosti, v nichž krádež majetku představuje významné narušení bezpečnosti.**
2. **Analyzujte krádež majetku jako formu narušení bezpečnosti. Zaměřte se na právní a sociální stránku problému.**
3. **Analyzujte procesní stránku krádeže majetku. Popište způsob krádeže fyzickou cestou a logickou cestou. Vytvořte model krádeže majetku.**
4. **S využitím modelu krádeže analyzujte konkrétní příklady krádeže majetku, realizované fyzickou a logickou cestou. Zaměřte se na popis bezpečnostního prostředí a zranitelností, které byly při krádeži využity.**
5. **Specifikujte rozdíly mezi krádeží fyzickou cestou a logickou cestou. Zaměřte se na klíčové momenty, které by mohly zvrátit úspěšnost krádeže majetku.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HULVA, Tomáš. Ochrana majetku. Praha: Linde, 2008. ISBN 978-80-7201-712-6.**
2. **LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7.**
3. **PROCHÁZKOVÁ, Dana. Ochrana osob a majetku. V Praze: České vysoké učení technické, 2011. ISBN 978-80-01-04843-6.**
4. **HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.**
5. **HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.**
6. **Šulc, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-737-5.**
7. **POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. Právní problémy kybernetické bezpečnosti. Brno: Masarykova univerzita, 2016. ISBN 978-80-210-8426-1.**
8. **KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Vydání první. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.**

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21.5.2019

VOJTĚCH GALDA, v.r.
.....
podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá problematikou majetkové trestné činnosti, konkrétně krádeží majetku. V teoretické části jsou popsány druhy bezpečnosti, ve kterých může mít krádež závažný dopad na společnost. Rozebírá se zde bezpečnostní prostředí fyzické a kybernetické krádeže, sociální i právní aspekty a skutková podstata krádeže. Dále následují jednotlivá vývojová stádia a klasifikace způsobů páchání krádeží. Pro ilustraci byl vytvořen obecný model krádeže ukazující jednotlivé kroky pachatele. Dále je tento model využit v praktické části práce, což pomáhá při určování klíčových momentů a zjednodušuje tak celkovou analýzu. Hlavním cílem praktické části je analýza vybraných zločinů, popis bezpečnostního prostředí, ve kterém se krádež odehrála, a zranitelností, kterých pachatel využil. Na základě získaných poznatků jsou navržena adekvátní bezpečnostní opatření. V poslední části jsou uvedeny různé motivy pachatelů a specifikovány rozdíly mezi fyzickou a kybernetickou krádeží se zaměřením na klíčové momenty a aktiva, která delikventy zajímají.

Klíčová slova: krádež, bezpečnostní prostředí, bezpečnost, fyzická bezpečnost, kybernetická bezpečnost, kyberprostor.

ABSTRACT

This thesis concerns the problematics of criminal activity, specifically thefts of property. The theroretical part describes the types of security in which a theft might have a major impact on society. It is discussing the issue of the security environment of physical and cybernetic theft, its social and legal aspects and its factual substantiantion. This part also describes the particular stages of theft development and classifies different ways of committing the crime. An universal model was created to demonstrate individual steps followed by the perpetrator. It is used in the practical part of this theses to identify key moments and simplify the analysis. The main goal of the practical part is to analyze chosen thefts, describe the security environment that the theft was commited in and vulnerabilities that the offender took advantage of. Based on the acquired knowledge there are suggested adequate protective steps. In the last part are listed diverse perpetrators‘ motives. There are also specified differences between physical and cybernetic thefts with a focus on key moments during the processes and assets which are in the interest of delinquents.

Keywords: theft, security environment, security, physical security, cybernetic security, cyberspace

Tímto způsobem bych chtěl poděkovat panu doc. Ing. Luďkovi Lukášovi, CSc. za jeho vedení a pomoc při tvorbě této diplomové práce.

Rád bych také poděkoval všem kamarádům, rodině a přítelkyni za podporu při studiu a psaní této diplomové práce.

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

OBSAH

ÚVOD

Dnešní společnost soustavně zatěžuje problematika krádeží. Lidé se již od nepaměti snaží chránit svůj majetek. Poslední dobou se však velmi dynamicky mění povaha trestných činů a velmi často se tak stává, že lidé podceňují možnost, že zrovna oni nebo jejich firma by mohli být cílem pachatelů. To má za následek nedostatečné zabezpečení objektů, firemních sítí, používání zastaralých bezpečnostních prvků a mnoho dalších nedostatků, kterých poté zloději využívají ve svůj prospěch. Není to však pouze nedbalost, ale také nevědomost, která pachatelům ulehčuje uskutečňovat jejich plány. Lidé často nemají povědomí o hrozbách, kterým vystavují svůj majetek v důsledku jejich chování. Firmy sice mívají zpracovány zásady a pravidla pro zacházení zaměstnanců s jejich majetkem, ať už se jedná o vybavení nebo citlivá data. Ovšem tyto směrnice bývají často neaktuální a seznámení zaměstnanců s těmito informacemi nebo kontrolování dodržování stanovených pravidel bývá často zanedbáváno či dokonce zcela opomenuto. Dalším problémem, který je nutno zmínit, je ten, že trestné činnosti se nedopouštějí pouze lidé zvenčí, ale v poslední době roste trend, kdy zlodějem nebo spolupachatelem bývají samotní zaměstnanci. Čímž se dostáváme k problematice řízení přístupu, která se v poslední době jeví jako jeden z nejvýznamnějších, ale zároveň nejvíce zanedbávaných prvků bezpečnosti ve firmách. Firmy nerealizují dostatečná opatření k zabezpečení svého majetku, jako jsou například důležité firemní informace (know-how, osobní údaje, strategické plány). Ty jsou poté zaměstnanci vynášeny a prodávány konkurenčním firmám nebo zájemcům třetích stran.

V kapitolách teoretické části jsou vysvětleny jednotlivé druhy bezpečnosti, kterých se krádež nejčastěji dotýká, co si pod jednotlivými oblastmi představit, jaké prvky do nich spadají a co mají za úkol chránit. Poté se práce zaměřuje na bezpečnostní prostředí fyzické a kybernetické krádeže, skutkovou podstatu a sociální a právní aspekty. Jsou zde také zmíněny faktory ovlivňující objektivní a subjektivní stránku trestné činnosti. V další pasáži teoretické části je popsán samotný proces krádeže, vývojová stádia, co ještě není trestné a co už naopak je, podle jakých kritérií lze krádež klasifikovat a jaké jsou nejčastější způsoby její realizace. Posledním bodem je obecný model krádeže, který má pomoci zmapovat činnosti zloděje při krádeži a pomoci tak v praktické části s analýzou zločinů.

Praktická část využívá poznatky z teoretické části, především pak vytvořený model, který se využívá jako pomocník při analýze vybraných zločinů. Samotná analýza se zabývá popisem jednotlivých krádeží, jejich bezpečnostního prostředí, zranitelností, pachatelových činností

a návrhem vhodných opatření k předcházení podobným incidentům. Znalosti získané analýzou se následně využívají v poslední části práce, kterou jsou rozdíly mezi fyzickou a kybernetickou krádeží a klíčové momenty, které mohly změnit průběh krádeže.

I. TEORETICKÁ ČÁST

1 DRUHY BEZPEČNOSTI, VE KTERÝCH KRÁDEŽ PŘEDSTAVUJE VÝZNAMNÉ RIZIKO

Bezpečnost a ochrana majetku představuje pro lidstvo jednu ze zásadních otázek již od nepaměti. Postupem času vzniklo mnoho druhů bezpečnosti, z nichž každý se zabývá jinou oblastí našeho života: fyzická bezpečnost, kybernetická bezpečnost, bezpečnost práce, bezpečnost provozu, mezinárodní bezpečnost a mnoho dalších. Následující kapitola se zabývá především těmi druhy bezpečnosti, kde je jednou z hlavních hrozeb krádež. Jedná se o oblasti, ve kterých může mít tento trestný čin závažný dopad na společnost.

1.1 Fyzická bezpečnost

Pokud se na tento pojem budeme dívat jako na soubor opatření, tak se zabývá ochranou majetku včetně fyzických nosičů, na kterých jsou zaznamenány utajované informace. Tvoří ji systém opatření, která mají za úkol zabránit nebo ztížit neoprávněné osobě přístup k chráněnému majetku. Jedná se o ochranu pomocí stavebních prvků, mechanických zábranných systémů, elektronických systémů, režimových opatření a fyzické ostrahy. [1, 2, 3]

Oblasti zájmu nalezneme v normě ČSN EN ISO/IEC 27001 (369797), lze je rozdělit do dvou kategorií.

Do první kategorie lze zařadit fyzickou bezpečnost budovy, místnosti nebo sídla. Jedná se především o následující oblasti:

- zabezpečení objektu či místnosti (stavební prvky),
- mechanické zábranné systémy,
- elektronická požární signalizace,
- poplachový, zabezpečovací a tísňový systém,
- kontrola vstupu do zabezpečených oblastí,
- řízení pohybu osob a materiálu,
- oddělení a ochrana zařízení na zpracování informací,
- ochrana před přírodními katastrofami a před katastrofami způsobenými lidskou činností. [1, 3]

Druhá kategorie se zabývá především zařízeními na zpracování informací. V tomto případě jde hlavně o tyto oblasti:

- Zajištění dodávek energií a služeb potřebných k provozu (elektřina, telekomunikační rozvody),
- Správné umístění těchto zařízení,
- Bezpečnost a údržba mimo organizaci (zaměstnanci nosí pracovní notebooky domů, servis zařízení mimo organizaci),
- Bezpečná likvidace nosičů (počítače, paměťová média, dokumenty). [1, 2]

Zabezpečení těchto oblastí je zajištěno systémem fyzické bezpečnosti, který je obvykle tvořen:

- **režimovými opatřeními** (jejich úkolem je stanovit pravidla a oprávnění osob ve střeženém prostoru, způsob pohybu a nakládání s materiálem apod.),
- **technickými prostředky** (mechanické zábranné systémy, tísňové systémy, kamerové systémy, systémy kontroly vstupu, elektrická požární signalizace, poplachové zabezpečovací systémy),
- **fyzickou ostrahou** (osoby, které zajišťují ochranu aktiv v souladu s režimovými opatřeními, většinou se jedná o hlídače, strážné nebo policisty). [3]

Z hlediska prostoru se systém fyzické bezpečnosti dělí následovně:

- perimetrická ochrana,
- plášťová ochrana,
- prostorová ochrana,
- předmětová ochrana.

Cílem všech ochranných opatření v rámci fyzické bezpečnosti je pachatele:

- odradit nebo odstrašit,
- zabránit vniknutí,
- zpozdit (prodloužit dobu potřebnou k vniknutí do chráněného prostoru),
- identifikovat,
- zadržet a předat policii. [3]

Aby byla aktiva co nejlépe chráněna, je důležité správné určení rozsahu zabezpečení a k tomu je třeba stanovit aktiva, jenž je potřeba ochránit. Aktivy mohou být: šperky, peníze, starožitnosti, umělecká díla, nosiče utajovaných informací, cenné papíry, ale také aktiva typu duševního vlastnictví nebo zbraně, drogy, nebezpečné chemické látky apod. Chráněná aktiva

nemusí představovat pouze majetek s vysokou finanční hodnotou. Může jimi být také majetek, který představuje vysoké riziko při jeho zneužití. [1, 4]

Dále je potřeba stanovit míru bezpečnosti. Ta vyjadřuje vztah hrozeb a rizik oproti opatřením, kterých bylo využito k jejich minimalizaci. K určení míry bezpečnosti se využívá bezpečnostní posouzení, které nám pomůže určit rozsah zabezpečení a doporučený stupeň bezpečnosti, jenž je potřeba dodržet při ochraně aktiv. K docílení požadovaného stavu bezpečí se využívá systém fyzické bezpečnosti, což je soubor opatření, který nám pomáhá chránit referenční objekt před případnými narušiteli. [4, 5]

Krádež v oblasti fyzické bezpečnosti tedy představuje odcizení jakéhokoliv aktiva z výše zmiňovaných. Nezáleží na tom, jestli má velkou finanční hodnotu i přesto může být velmi důležité kvůli rizikům plynoucím z jeho zneužití (nebezpečné látky, jed, utajované informace). Nejčastější způsob, jak dochází k fyzické krádeži, je vloupáním.

1.2 Ekonomická bezpečnost

Ekonomická bezpečnost je: „*Stav, ve kterém ekonomika objektu, jehož bezpečnost má být zajištěna, není ohrožena hrozbami, které výrazně snižují nebo by mohly snížit její výkonnost potřebnou k zajištění obranných i dalších bezpečnostních kapacit, sociálního smíru a konkurenceschopnosti objektu i jeho jednotlivých složek, to je především jednotlivých podnikatelských subjektů na vnitřních i vnějších trzích.“* [6, s.5]

Ekonomická bezpečnost je spjata se všemi ostatními oblastmi bezpečnosti, vztahuje se jak k vnitřní, tak poslední dobou čím dál více taky k vnější bezpečnosti. Na problematiku ekonomické bezpečnosti lze nahlížet ze dvou pohledů. Ze strany státu, kde se jedná především o státní podniky, státní organizace a o stát jako celek. Druhým je soukromý sektor, ve kterém jde o firmy, družstva, živnostníky a podniky (v podstatě se jedná o makroekonomický a mikroekonomický přístup). Mezi nejdůležitější vlastnosti v obou případech, pak patří:

- hospodářský růst,
- konkurenceschopnost,
- měnová stabilita,
- surovinová dostatečnost,
- vývoj a aplikace nových technologií (sledování nových trendů),
- nízká nezaměstnanost,

- chránění obyvatel před bídou,
- schopnost efektivní obrany a zajištění bezpečnosti. [6, 7]

Ekonomická bezpečnost státu je přímo zahrnuta v bezpečnostní strategii České republiky. Podle této strategie se jedná především o vhodné ekonomické a právní prostředí v kombinaci s makroekonomickou stabilitou. Také je v ní uvedeno, jakým způsobem chce Česká republika dosáhnout udržitelného rozvoje a hospodářského růstu, který úzce souvisí s ekonomickou bezpečností. [8]

Pokud se zaměříme na mikroekonomický směr budou nás zajímat především hmotné a nehmotné zdroje podniku, které lze označit za chráněná aktiva.

Hmotné zdroje představují hlavně budovy, pozemky, výrobní zařízení, dopravní prostředky, nářadí, zásoby apod. Rozlišujeme zdroje dlouhodobé a krátkodobé. Za dlouhodobé je považován majetek, který slouží k aktivnímu využívání, protože dochází k jeho stárnutí a opotřebení. Je charakteristický vyšší pořizovací cenou. Krátkodobé zdroje jsou převážně zásoby materiálu. V tomto případě by se neměl skladovat moc dlouho a měl by být nakupován pouze v nezbytně potřebném množství. Proto je potřeba dobře organizovat práci, pracovní postupy a mít zpracovaný plán řízení zásob. [7]

Podíváme-li se na zdroje nehmotné, tak do těch spadají zejména: informace, patenty, lidské zdroje, know-how, licence, pověst a image. Z nichž nejdůležitější pro ekonomickou bezpečnost jsou informace a lidské zdroje. [7]

V případě ekonomické bezpečnosti lze za krádež považovat zcizení hmotných či nehmotných zdrojů podniku. V případě hmotných by šlo například o dopravní prostředky, stroje, nebo třeba zásoby. Pokud by se jednalo o nehmotné zdroje jsou to především patenty, know-how, důležité informace apod.

1.3 Administrativní bezpečnost

Dříve se této problematice říkalo ochrana utajovaných skutečností. Lze ji chápat jako ochranu hmotných nosičů (dokumenty, flashdisky, harddisky), které nesou klíčové informace, jejichž odcizení by organizaci způsobilo újmu. Je to v podstatě soubor opatření chránící utajované (či jinak citlivé) informace při jejich tvorbě, zpracování, příjmu, odesílání, přenášení, ukládání, likvidaci, archivaci nebo jiných činnostech při kterých se s nimi jakkoli manipuluje. Jde o zabezpečení prostor a soubor režimových opatření, které mají za úkol zabránit neoprávněným osobám ve fyzickému přístupu k nosičům informací. [3, 6, 7]

Zavedení administrativní bezpečnosti v organizace je nutné, pokud dochází ke splnění následujících skutečností:

- Informace je pro organizaci důležitá:
  - její prozrazení by přineslo vážnou újmu,
  - je důležitá pro splnění cílů a pro fungování organizace.
- Informace je zaznamenána na fyzickém nosiči (flashdisk, papír, harddisk apod.).
- S tímto nosičem se dále manipuluje. [7]

Základní prostředky administrativní bezpečnosti jsou:

- jednací protokol (evidence utajovaných dokumentů),
- pomocný jednací protokol (záznamy o pohybu),
- doručovací kniha (záznamy o předání),
- zápůjční kniha (záznamy o zapůjčení),
- manipulační kniha (záznamy o vytváření, předávání a převzetí),
- sběrný arch (rozšíření jednacího protokolu – více dokumentů k jedné věci),
- kontrolní list (evidence osob seznámených s obsahem dokumentu). [7, 8, 9]

1.3.1 Funkce administrativní bezpečnosti

Ochranná

Určuje oprávněné osoby a jejich pravomoci při nakládání s utajovanými informacemi a zamezuje přístupu neoprávněných osob k těmto informacím. [7, 9]

Identifikační

Má za úkol rozpoznat, označit a zaevidovat informace, které spadají do administrativní bezpečnosti. [7, 9]

Lokalizační

Zajišťuje uchování dat o pohybu dokumentů a osobách, které k nim měly přístup. Případně i o druhu manipulace dané osoby s utajovanou informací. Tato funkce je stěžejní při vyzrazení informace. Určuje totiž osoby, které by mohly být za zneužití informace odpovědny. [7, 9]

V administrativní bezpečnosti lze za krádež považovat odcizení nosiče na kterém je utajovaná informace.

1.4 Informační bezpečnost

Pokud mluvíme o bezpečnosti informací jedná se především o zajištění jejich důvěrnosti (utajení informací). Nesmíme ovšem zapomínat ani na zbylé dvě související oblasti, a to udržení integrity (správnost a kompletnost informací) a zachování dostupnosti (zajištění přístupu k informacím). [9]

Důvěrnost

Informace jsou dostupné pouze pro oprávněné osoby. V praxi se jedná především o kontrolu přístupu, tedy o určení pravomocí a odpovědnosti podle pracovního zařazení a náplně práce daného zaměstnance. Většina organizací v tomto ohledu využívá klasifikační informační schémata, tato schémata rozdělují informace do různých stupňů utajení, a to od veřejně dostupných přes důvěrné, až po přísně tajné. Nejčastěji se v organizacích setkáme s rozdělením do tří skupin:

- chráněné informace (Protected, Restricted),
- interní informace (Internal use),
- veřejné informace (Public). [9]

Integrita

Jedná se o zajištění správnosti, úplnosti, důvěryhodnosti obsahu informací a ověření jejich zdrojů. V praxi to znamená přesné stanovení pravidel a pravomocí pro úpravu dat. V případě, že dojde k porušení integrity, je tato situace označována jako nežádoucí modifikace. [9]

Dostupnost

Tato část bezpečnosti informací zajišťuje, že informace jsou dostupné v momentě jejich potřeby, ale pouze pro kompetentní osoby. V případě, že data nejsou k dispozici v okamžiku jejich potřeby, označujeme tento případ jako nedostupnost, popřípadě nežádoucí zničení. [9]

1.4.1 Opatření k ochraně informací

Ochranu je nutné řešit komplexně a je třeba dbát na vyvážení jednotlivých oblastí zabezpečení systému. Největší a nejčastější chybou je zaměření se na jeden prvek a na úkor toho opomenutí jiného. K dobré ochraně informací je dobré se zaměřit na následující bezpečnostní opatření. [7, 9, 10]

- Režimová bezpečnost:
  - vhodné podmínky pro provoz informačního systému,
  - oprávnění osob pro vstup na pracoviště a práci s konkrétními daty,
  - opatrnost při nakládání se vstupními a výstupními informacemi.
- Bezpečnost technických prostředků a programového vybavení:
  - ochrana před poškozením, neoprávněnou manipulací či odcizením,
  - zajištění pravidelné aktualizace HW a SW prostředků,
  - nastavení oprávnění pro tyto úkony – pouze pověření pracovníci (administrátoři), běžný uživatel na to nemá oprávnění.
- Bezpečnost dat:
  - zabezpečit data proti neoprávněné manipulaci,
  - stanovení pravidel pro nakládání s uloženými daty, ať již v pracovní stanici nebo na přenosném médiu (externí disky, flashdisky, DVD),
  - zajistit upravené podmínky v případě opravy nebo likvidaci zařízení obsahujících utajované informace.
- Bezpečnost komunikačních cest:
  - zajistit rozvody a přenosové cesty proti zcizení, odposlechu a jinému zneužití,
  - věnovat pozornost náhlým úpravám nebo poškozením,
  - zajistit dohled při montážích nových zařízení,
  - veškeré eventuality hlásit nadřízeným.
- Fyzická bezpečnost:
  - ochrana objektu před narušením bezpečnosti s využitím mechanických zabraných systémů a elektronických prostředků,
  - objekt se chrání před krádeží, poškozením a neoprávněným vniknutím.
- Personální bezpečnost:
  - pečlivý výběr zaměstnanců vzhledem k vykonávané práci,
  - poučení a proškolení o dodržování bezpečnostních opatřeních a pravidlech při manipulaci s informacemi,
  - kontrola dodržování těchto opatření. [9, 10]

V informační bezpečnosti lze za krádež považovat odcizení dat z informačního systému.

1.5 Kybernetická bezpečnost

Je to souhrn opatření, která mají za úkol zajistit klíčové služby a informace před zneužitím. Kybernetická bezpečnost je odvětví výpočetní techniky úzce související s informační bezpečností. Jejím cílem je ochrana informací (jako aktiv, majetku) před krádeží, zneužitím, přírodní katastrofou nebo korupcí. Tato problematika je prosazována v oblasti výpočetní techniky a sítí. Při ochraně aktiv je nutné, aby veškeré prostředky zůstaly nadále přístupné pro uživatele. Primárním účelem využívaných prostředků je zabránit nežádoucí manipulaci s výpočetní technikou. Opět se zde jedná o zajištění důvěrnosti, dostupnosti, integrity, a navíc zamezení ovládaní zařízení neoprávněnou osobou. [11]

Kybernetická bezpečnost se zabývá zabezpečením **kybernetického prostoru**. Tento prostor je v podstatě prostor, který vznikl díky počítačům. Kybernetický prostor není pouze internet, je to svět tvořený počítači: notebooky, stolní počítače, mobilní telefony, tablety, herní konzole, servery, TV, přehrávače, hračky, domácí spotřebiče, průmyslová a zdravotnická zařízení, řídící systémy (ve výrobě, dopravě, telekomunikacích), stroje (výrobní i nevýrobní) a veškeré jejich periferie (tiskárny, skenery, …). Nesmíme opomenout, že zde patří také přenosové prostředí – aktivní a pasivní síťové prvky (routery, switche, datové rozvaděče, ...). Podle zákona o kybernetické bezpečnosti se pod kybernetickým prostorem rozumí: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [12]

Existuje více způsobů, jak nahlížet na kybernetickou bezpečnost. Z hlediska krádeže majetku se lze zaměřit na následující oblasti, které považuje Policie ČR za nejvýznamnější:

- **Podvodné jednání** – nejčastější jednání pachatele. Většinou jde o oklamání uživatele za účelem získání finančních prostředků prostřednictvím falešných e-shopů, inzerátů (bazary, aukce), sbírek, podvodné emaily a phishing (získání údajů k internetovému bankovnictví, platebním portálům). [12, 13]
- **Hacking –** neoprávněný přístup k datům, počítačovým systémům, zařízením a jejich následné zneužití. Nejčastěji se setkáme s krádeží údajů oběti, ale spadá zde také: šíření škodlivých kódů, získání citlivých informací, backdoor, napadení účtů na sociálních sítích, emailových účtů, internetového bankovnictví, DDoS, ransomware (zašifrování dat a následné vydírání), sniffing (odposlech komunikace). [12, 13]
- **Násilné projevy a hate crime –** v tomto případě jde především o vydírání pomocí kterého se pachatel snaží získat majetek oběti. [12, 13]

- **Blagging –** sociální inženýrství. Zmanipulování lidí za účelem vlastního prospěchu. Útočník se vydává za ředitele, právníka, účetní, aby působili co nejvíce věrohodně. Následně kontaktují konkrétního zaměstnance, kterého se snaží pomocí fiktivního příkazu zmanipulovat k provedení určité činnosti. [12, 13]
- **Podvodné e-shopy** – nákup u neověřeného e-shopu a následná platba předem. Pachatelé využívají následně brigádníky, kteří za ně zadávají inzeráty a přeposílají platby od obětí. Sami většinou neví, že se dopouští trestného činu legalizace výnosů z trestné činnosti. [12, 13]
- **Trestné činy v oblasti autorských práv** – sdílení filmů, hudby a softwaru v rozporu s autorskými právy. [12, 13]

Základními funkcemi kybernetické bezpečnosti jsou:

- **identifikace a organizace** (hodnocení důležitosti aktiv),
- **schopnost reagovat na bezpečnostní incident** (ohlášení, klasifikace, opatření k odvrácení nebo zmírnění incidentu a sběr dat o incidentu pro jeho následnou analýzu),
- **ochrana aktiv** (bezpečnostní dokumentace a postupy při narušení bezpečnosti).

1.5.1 Kybernetická bezpečnost ve firmách

Protože právě firmy jsou častým terčem hackerských útoků, je důležité zde zmínit, jaké kroky mohou podniknout k zabezpečení kybernetické bezpečnosti. Jedná se především o následující:

- určení zranitelných míst (strategické plány, osobní údaje, duševní vlastnictví, know-how),
- zabezpečit ochranu počítačů a zařízení v síti (pravidelné aktualizace, antivirová ochrana, firewall pod.),
- ochrana citlivých dat (šifrování, zálohování, ochrana hesel),
- nastavení oprávnění pro jednotlivé zaměstnance (jednotlivci by měli mít přístup pouze k tomu co potřebují k práci),
- školení zaměstnanců v oblasti kybernetické bezpečnosti (zavedená pravidla, postupy). [11]

1.5.2 Opatření kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti uvádí následující opatření:

- *„Organizační:*
  - *systém řízení bezpečnosti informací,*
  - *řízení rizik,*
  - *bezpečnostní politika,*
  - *organizační bezpečnost,*
  - *stanovení bezpečnostních požadavků pro dodavatele,*
  - *řízení aktiv,*
  - *bezpečnost lidských zdrojů,*
  - *řízení provozu a komunikací významného informačního systému,*
  - *řízení přístupu osob k významnému informačnímu systému,*
  - *vývoj a údržba významných informačních systémů,*
  - *zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,*
  - *řízení kontinuity činností a*
  - *kontrola a audit významných informačních systémů.*
- *Technické:*
  - *fyzická bezpečnost,*
  - *nástroj pro ochranu integrity komunikačních sítí,*
  - *nástroj pro ověřování identity uživatelů,*
  - *nástroj pro řízení přístupových oprávnění,*
  - *nástroj pro ochranu před škodlivým kódem,*
  - *nástroj pro zaznamenávání činnosti významných informačních systémů, jejich uživatelů a administrátorů,*
  - *nástroj pro detekci kybernetických bezpečnostních událostí,*
  - *nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,*
  - *aplikační bezpečnost,*
  - *kryptografické prostředky,*
  - *nástroj pro zajišťování úrovně dostupnosti informací,*
  - *bezpečnost průmyslových a řídících systémů.“* [12]

Za krádež v kyberprostoru se považuje odcizení chráněných aktiv, v tomto případě se bude jednat o nehmotná aktiva. Jde tedy především o: data, informace, porušení autorských práv (nelegální šíření filmů, hudbu, programů), oklamání či zmanipulování lidí za účelem finančního prospěchu (sociální inženýrství, podvodné e-shopy, bazary, aukce), krádež identity (zcizení emailové schránky, účtu na sociální síti) apod.

1.5.3 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Ústřední správní orgán v oblasti kybernetické bezpečnosti, komunikačních systémů, ochrany utajovaných informací, kryptografie a družicového systému Galileo. Jeho činnosti se řídí zákonem o kybernetické bezpečnosti a s ním souvisejícími zákony. Jedná se například o: koordinaci při narušení bezpečnosti ve výše zmíněných oblastech, ukládá správní testy, zajišťuje prevenci (vzdělání, metody), kontrola příslušných oblastí. Ředitel se musí pravidelně účastnit jednání Bezpečnostní rady státu a Výboru po kybernetickou bezpečnost. [2]

Mimo jiné má taky NÚKIB za úkol zajišťovat následující činnosti v oblasti kryptografické ochrany:

- certifikace kryptografických pracovišť a zařízení (vyhláška 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací),
- koordinace výzkumu a vývoje,
- řízení kryptografické ochrany.

K zajištění těchto činností má NÚKIB specializované oddělení: Oddělení certifikace kryptografických prostředků a pracovišť, Oddělení šifrované služby a Oddělení kryptologie a vývoje kryptografických prostředků. [2]

2 KRÁDEŽ MAJETKU JAKO FORMA NARUŠENÍ BEZPEČNOSTI

2.1 Charakteristika bezpečnostního prostředí

Bezpečnostní prostředí je charakterizováno všemi subjekty (státy, mezinárodní organizace, firmy, domácnosti), které mohou mít vliv na bezpečnost v daném prostoru a jejich aktivitami či vzájemnými vazbami. V podstatě se jedná o prostor, kde může docházet k ohrožování aktiv či chráněného zájmu. Jak je bezpečnostní prostředí rozsáhlé, je dáno pozicí a vlivem daného subjektu v systému mezinárodních, národních a ostatních vztahů (bezpečnostní prostředí EU, bezpečnostní prostředí ČR, bezpečnostní prostředí určité organizace). [14]

2.1.1 Bezpečnostní prostředí kybernetické krádeže (kyberprostor)

Kyberprostor je technicky vzato: *„celosvětová distribuovaná počítačová síť složená z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem“.* [11]

Kyberprostor je *„virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.“* [15]

Za **základní znaky kyberprostoru** lze považovat následující:

- globálnost,
- otevřenost,
- decentralizovanost,
- interaktivnost,
- bohatost na informace,
- ovlivňování uživatelů. [15]

Kyberprostor lze rozdělit několika způsoby, podle toho, z jakého pohledu se na něj budeme dívat. Můžeme jej například rozdělit podle jeho vrstev, ze kterých se skládá nebo podle dostupnosti dat pro uživatele.

Pokud se zaměříme na jeho jednotlivé **vrstvy kyberprostoru** lze jej rozdělit následovně:

- fyzická vrstva,
- logická vrstva,
- sociální vrstva. [15]

Fyzická vrstva zahrnuje fyzické síťové komponenty (routery, switche, servery apod.) a jejich přesné umístění ve fyzickém světě. [15]

Logická vrstva se skládá z logických síťových komponentů. Pod tím si lze představit propojení mezi jednotlivými síťovými uzly prostřednictvím komunikačních protokolů (tedy logickou komunikační cestu ve virtuálním světě přes fyzické síťové komponenty). [15]

Sociální vrstva je tvořena z tzv. „kyberosobností" a osobností. To představuje identifikaci osoby v síti (IP adresa, e-mail apod.). Osobnost poté představuje konkrétní reálnou osobu připojenou k síti. Jedna osobnost může využívat více „kyberosobností" a naopak. [15]

Podle **dostupnosti a dohledatelnosti dat pro běžné uživatele** lze kyberprostor rozdělit do následujících tří oblastí:

- Surface Web (cca 4%),
- Deep Web (cca 90%),
- Dark Web (cca 6%).

Naneštěstí používání tohoto rozdělení způsobilo, že laická veřejnost si myslí, že platí toto pravidlo: kyberprostor = internet = web. To, ale není ani zdaleka pravda, protože kyberprostor nezahrnuje jen webové stránky, ale všechny počítačové systémy, služby, uživatele a data, která se v tomto prostředí pohybují. [15]

Surface Web (Visible Web, Indexed Web) je viditelná část kyberprostoru, kde se běžný uživatel pohybuje. Jedná se o část, která je dostupná většině uživatelů za pomocí standardních prostředků (webový prohlížeč). Obsahuje služby jako Facebook, Google, Seznam, Youtube, e-shopy, osobní webové stránky, blogy apod. Má jasně danou strukturu a spravuje je ICANN (Internet Corporation for Assigned Names and Numbers). Tato nezisková organizace například spravuje IP adresy, doménová jména a dohlíží na regionální organizace, které mají na starost registrace na jednotlivých kontinentech. [11, 16]

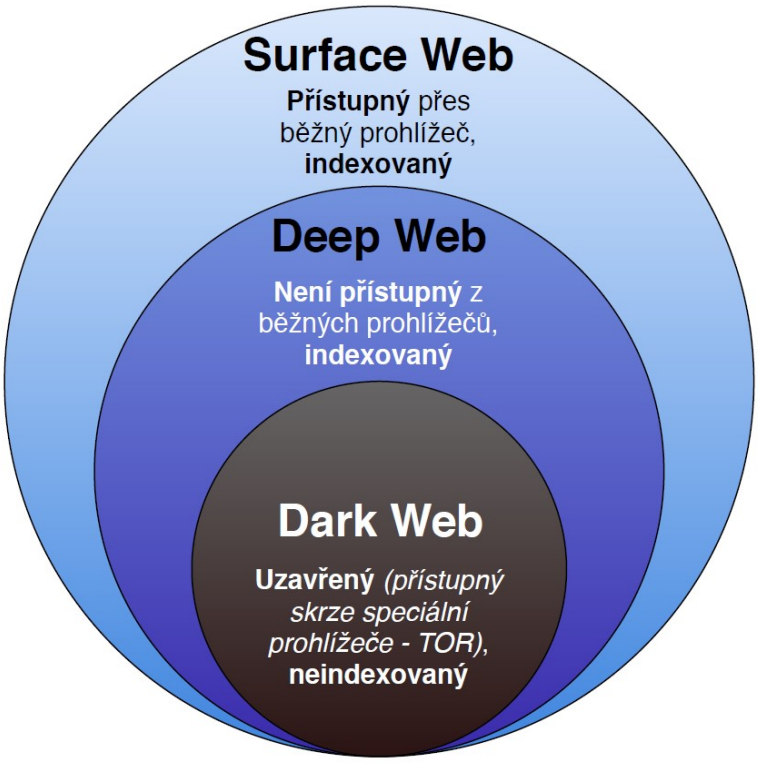
Deep Web cca obsahuje většinu obsahu, který je pro běžného uživatele přímo nedostupný, jedná se především o následující:

- zdravotní záznamy,
- akademické informace,
- finanční záznamy,
- legální dokumenty,
- vícejazyčné databáze,

- vládní zdroje,
- vědecké zprávy,
- informace o úpisech a předplatném,
- specifické zprávy organizací,
- konkurenční webové stránky. [11, 16]

Dark Web je většinou lidí považován za hrozbu, kde lze sehnat drogy, zbraně, dětskou pornografii aj. Zbytkem uživatelů je nazýván „internetem pod Internetem, jehož základní ideou je neregulované a necenzurované prostředí“. Do Dark Webu spadají především následující zákoutí internetu:

- TORem šifrované stránky,
- obchod s drogami,
- soukromá komunikace,
- ilegální informace,
- politické protesty. [11, 16]



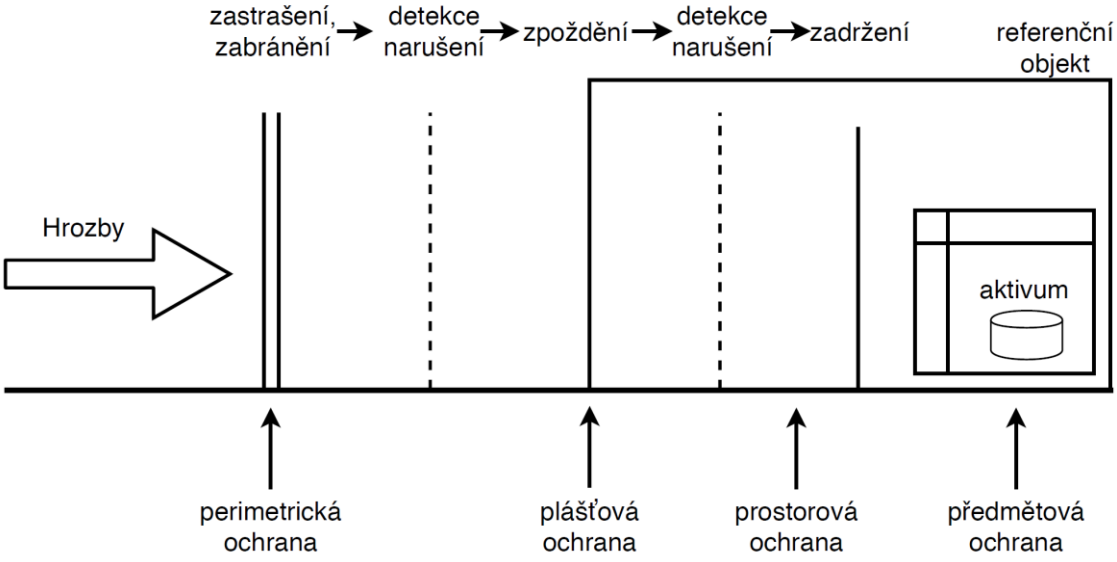
Obrázek 1 – Schéma kyberprostoru [11]

2.1.2 Bezpečnostní prostředí fyzické krádeže

Bezpečnostním prostředím fyzické krádeže se v našem případě rozumí především objekt, ve kterém se nachází chráněná aktiva a jeho přilehlé okolí. K ochraně těchto aktiv slouží tzv. systém fyzické bezpečnosti, který musí případný pachatel překonat.

2.1.2.1 Systém fyzické bezpečnosti

Jedná se o soubor opatření, které primárně slouží k zdržení pachatele nebo ztížení jeho přístupu k chráněným aktivům nebo alespoň k jeho odrazení či zastrašení.



Obrázek 2 – Systém fyzické bezpečnosti [4]

Opatření lze rozdělit podle chráněné oblasti (prostorově) následovně:

Perimetrická (obvodová) ochrana

Jejím cílem je vnější ochrana objektu a pozemku, na kterém se nachází. K tomu se využívají vnější mechanické zábranné systémy (plot, zeď, brány, závory) a detektory narušení. Na detektory jsou kladeny vyšší požadavky z hlediska jejich odolnosti vůči klimatickým podmínkám a planým poplachům. Zpravidla mívají delší dosah a užší detekční charakteristiku. Tyto detektory dělíme následovně:

- **Pasivní** – plotová tenzometrická čidla, vibrační detektory, seismická čidla, mikrofonní kabely, infračervené termovizní detektory, perimetrická pasivní infračervená

čidla, vláknově optické systémy, diferenciální tlakové čidla, čidla magnetických anomálií, systémy střežící drátěnou osnovu. [5]

- **Aktivní** – infračervené bariéry a závory, štěrbinové kabely, laserové závory, kapacitní čidla, reflexní detektory dynamických změn elektrického pole, aktivní infračervená čidla, kombinované (duální) detektory a bariéry, dvojité mikrovlnné detektory a čidla, laserové radiolokátory. [5]

Plášťová ochrana

Zabývá se zabezpečením objektu proti vniknutí narušitele. Její prvky mají za úkol zabránit nebo detekovat narušení vstupu do budovy (okna, dveře, vrata). Mezi základní mechanické zábranné systémy patří stavební prvky budov a otvorové výplně jako jsou okna, dveře, vrata. Ty lze doplnit o další prvky ať už se jedná o pasivní či aktivní prvky jsou to: fólie na okna, bezpečnostní vložky, magnetické kontakty, senzory tříštění skla, tlakové detektory, drátové senzory, vibrační detektory apod. V neposlední řadě do této kategorie spadají taky turnikety a branky v obchodech. [4]

Prostorová ochrana

Jde o ochranu vymezeného prostoru buď uvnitř nebo vně budovy. Většinou je realizována pomocí detektorů pohybu. Opět se zde prvky dělí na aktivní a pasivní. Hojně se také využívá jejich vhodná kombinace (duální detektory).

- **Pasivní** – pasivní infračervené detektory (PIR).
- **Aktivní** – mikrovlnné detektor (MW), ultrazvukové detektory. [4, 5]

Předmětová ochrana

Předmětová ochrana má ochránit cennosti (finanční hotovost, šperky, smlouvy) před odcizením. K tomu se využívají nejrůznější prostředky – trezory, schránky, kontejnery. Pokud se zaměříme na detektory bude se jednat především o závěsové, otřesové, polohové a kapacitní. Ty mají za úkol detekovat neoprávněnou manipulaci s daným předmětem (sundání obrazu ze zdi, vynesení schránky z místnosti). [4, 5]

Pokud se na systém fyzické bezpečnosti bude dívat, jako na celek, pak bude tvořen následujícími oblastmi:

Režimová opatření

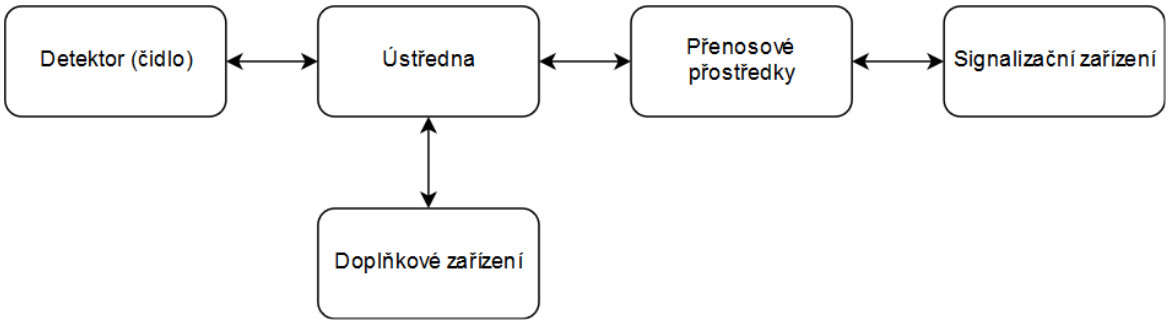
Mají za úkol stanovit pravidla, zásady a oprávnění pro pohyb osob po objektu, provádění bezpečnostních kontrol, nakládání s důležitými bezpečnostními prvky apod. [4]

Fyzická ostraha

Osoby, které zajišťují ochranu majetku v souladu s režimovými opatřeními. Mají za úkol zamezit krádeži aktiv, odhalit a zadržet pachatele apod. Většinou se jedná o hlídací službu, strážné nebo policii. [4]

Technické prostředky

Jsou to prostředky, které mají podpořit činnosti fyzické ostrahy a realizaci režimových opatření. Jejich úkolem je například odhalení pachatele, identifikace narušení, ztížit přístup k aktivům apod. Do těchto prostředků spadají především poplachové zabezpečovací a tísňové systémy (PZTS). Jejich hlavní funkcí je reakce na narušení způsobené pachatelem. Pokud dojde k narušení, tak PZTS akusticky či dálkově vyšle signál o detekované změně. [4, 5]



Obrázek 3 – zabezpečovací řetězec [5]

Na obrázku výše můžeme vidět strukturu tohoto systému. Skládá se z následujících prvků:

- **Detektor** – reaguje na fyzikální změny tykající se narušení detekčního pole prvku.
- **Ústředna** – zpracovává a vyhodnocuje signály z čidel. Zabezpečuje ovládání celého systému a nastavení jednotlivých pravidel.
- **Přenosové prostředky** – zajišťují přenos veškerých informací mezi ústřednou a jednotlivými prvky systému.

- **Signalizační zařízení** – převádí zachycené informace na akustický, optický či jiný vhodný signál.
- **Doplňková zařízení** – slouží k provádění speciálních funkcí systému nebo zjednodušují jeho ovládání. [5]

Všechny výše zmiňované druhy ochrany je dobré doplnit o vhodný kamerový systém. Ten by měl sloužit k zobrazování a archivaci záběrů ze zastřežené oblasti. Slouží k vyhodnocení poplachu obsluhou a snížení počtu planých poplachů. Skládá se z kamer, zobrazovacích zařízení (monitory), záznamového média (harddisky) a software pro ovládání. Lze jej doplnit i mikrofony a reproduktory.

2.2 Právní a sociální aspekty krádeže

Obecně lze říci, že krádež je neoprávněné přisvojení si cizí věci. Ve všech zemích se na tento čin nahlíží jako na trestný čin. Existují ovšem výjimky, kdy může být přisvojení si cizí věci tolerováno. Jedná se především o situace v určitých obdobích nebo za určitých společenských okolností (válečná kořist, konfiskace majetku).

Zákon č. 40/2009 Sb., trestní zákoník nám krádež definuje následovně:

„Krádež

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a

a) způsobí tak na cizím majetku škodu nikoliv nepatrnou,

b) čin spáchá vloupáním,

c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,

d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo

e) čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Kdo si přisvojí cizí věc tím, že se jí zmocní, a byl za takový čin v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody na šest měsíců až tři léta.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo 2 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

c) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.“ [17]

2.2.1 Typy krádeží

Krádeže prosté

Pro tento typ krádeží je typická jednoduchost provedení. Pachatel většinou odcizí snadno přístupnou věc a nepřekonává při tom žádné velké překážky. Výsledek vyšetřování je většinou závislý na zajištění svědků.

Krádeže vloupáním

V tomto případě se jedná o složitou většinou i promyšlenou krádež, kdy je pachatel nucen překonat s použitím lsti, síly nebo nástrojů jistící překážku, aby tak mohl vniknout do uzavřeného prostoru.

Krádeže motorových vozidel

Jedná se o jeden z nejrozšířenějších druhů krádeží. Pachatel jedná s úmyslem si vozidlo ponechat nebo jej zpeněžit. Často jsou takto ukradená vozidla demontována na náhradní díly nebo s využitím padělaných dokladů legalizována k dalšímu provozu.

Krádeže v bytech

Tento typ krádeže by se dal považovat za krádež vloupáním, není tomu tak. Pachatel je totiž do bytu vpuštěn samotným majitel bez použití síly. Většinou za klamavým účelem – prodej, nákup, opravář, elektrikář atd. Pachatel poté využije nepozornosti majitele k odcizení nejrůznějších předmětů.

Kapesní krádeže

I když se jedná o krádeže prosté, kvůli specifickým schopnostem, kterými pachatelé disponují (zručnost, postřeh, odvaha) jsou řazeny do zvláštní kategorie. Provedení bývá většinou dvojího typu, buď nekrytou rukou nebo krytou (částí oděvu, nebo jiným předmětem – novinami).

Předstírané krádeže

Většinou se jedná o fingování krádeže za účelem vyplacení pojistky nebo uhrazení dluhu. Obvykle pachatel předstírá krádež vloupáním. Poslední dobou se fingují také například krádeže motorových vozidel, kdy jej majitel prodá v zahraničí a následně nahlásí jeho odcizení, aby získal peníze od pojišťovny.

2.2.2 Protiprávnost

U krádeže se jedná o pojmový znak, znamená to, že čin je v rozporu s právní normou. Může se jednat o normu trestního, občanského, správního nebo jiného práva. Nemusí se nutně jednat o právo trestní. Protiprávní činy totiž mohou být i přestupkem nebo správním deliktem. V případě krádeže musí být čin společensky škodlivý. V případě drobné krádeže, tak může být čin posuzován jako přestupek. [18, 19]

Pokud jsou přítomny okolnosti vylučující protiprávnost činu (krajní nouze, nutná obrana apod.), nelze čin posuzovat jako trestný, protože není protiprávní. Posouzení takových činů je ovšem vysoce individuální a podléhá přísné kontrole. [18, 19]

2.2.3 Hranice škody

Na základě toho, jak velkou škodu způsobí pachatel, se posuzuje, zda se jedná o trestný čin či nikoli. Výše nepatrné škody je do 5000 Kč, do této hranice se jedná pouze o přestupek. Ovšem jestli byl čin spáchán vloupáním, pak výše škody nehraje roli. V takovém případě se vždy jedná o trestný čin. Výše škody pouze pomáhá určit výši trestu.

Rozdělení výše škody podle trestního zákoníku je následující:

- Nikoliv nepatrná/malá: 5 000 – 24 999 Kč
- Nikoliv malá: 25 000 – 49 999 Kč
- Větší: 50 000 – 499 999 Kč
- Značná: 500 000 Kč – 4 999 999 Kč
- Velkého rozsahu: 5 000 000 Kč a více [17]

2.2.4 Právní předpisy

Problematika krádeže majetku je velmi rozsáhlá, proto existuje legislativa, která tuto oblast upravuje. Nejzásadnějším právním předpisem v České republice je především **zákon č. 40/2009 Sb., trestní zákoník**. Jde o základní právní ustanovení pro hmotné trestní právo. Popisuje, které chování je trestné a jak se za něj bude pachatel trestat. Pokud se na krádež podíváme z pohledu informačních technologií, je důležité zmínit **zákon č. 181/2014 Sb., o kybernetické bezpečnosti** a **zákon č. 412/2005 Sb., o ochraně utajovaných informací**. Zákon o kybernetické bezpečnosti stanovuje základní práva a povinnosti osob a pravomoci orgánů v této oblasti. Zabývá se předpisy Evropské unie a zajištěním bezpečnosti sítí a informačních systémů a stanovuje úroveň bezpečnostních opatření v oblasti kybernetické bezpečnosti. Nezabývá se ovšem ochranou utajovaných informací, to má na starost zákon o ochraně utajovaných informací. Ten stanovuje která informace má být utajovaná, podmínky jejího utajení a opatření k ochraně utajovaných informací. V neposlední řadě také vymezuje činnosti státní správy. [19]

Tabulka níže nám uvádí zásadní zákony a vyhlášky z pohledu krádeže majetku, ať už fyzickou nebo kybernetickou cestou.

Tabulka 1 – Důležité právní předpisy související s krádeží majetku [autor]

Označení zdroje	Název předpisu
Zákon č. 40/2009 Sb.	Trestní zákoník
Zákon č. 141/1961Sb.	O trestním řízení soudním (trestní řád)
Zákon č. 181/2014 Sb.	O kybernetické bezpečnosti a o změně souvisejících zákonů
Zákon č. 412/2005 Sb.	O ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
Zákon č. 89/2012 Sb.	Občanský zákoník
Zákon č. 250/2016 Sb.	O odpovědnosti za přestupky a řízení o nich
Zákon č. 480/2004 Sb.	O některých službách informační společnosti a o změně některých zákonů
Zákon č. 127/2005 Sb.	O elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
Směrnice Evropského parlamentu a Rady 2000/31/ES	O některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)
Zákon č. 251/2016 Sb.	O některých přestupcích

2.3 Skutková podstata krádeže

Objektem krádeže je vlastnictví nebo držení majetku (majetek je v něčí moci – vlastníka, věřitele, nájemce nebo i jiného zloděje).

Subjektem může být zpravidla kdokoli, až na výjimky, kdy se jedná o speciální subjekt (voják při výkonu služby). Jedná se o osobu dopouštějící se trestného činu krádeže.

Pachatelem může být pouze fyzická osoba, která je v době krádeže příčetná, již dovršila patnáctý rok věku. Pokud jde o mladistvého, měl by být rozumově a mravně vyspělý/á. V případě, že pachatel nedovršil patnáct let, není trestně odpovědný, ale soud nařídí nápravná opatření k nápravě pachatele. [17]

2.3.1 Objektivní stránka

Popisuje trestný čin, jak se jeví navenek. Obligatorní (povinné) znaky objektivní stránky jsou jednání, následek a kauzální spojitost mezi nimi. V případě krádeže je tedy objektivní stránkou to, že si pachatel přisvojí cizí věc a současně splní jednu z těchto podmínek:

- čin provede vloupáním,
- způsobí škodu (nikoli nepatrnou),
- přisvojí si věc, kterou má někdo jiný u sebe (popřípadě na sobě),
- čin uskuteční na území, kde je prováděna evakuace,
- bezprostředně po uskutečnění činu si věc pokusí uchovat výhružkou nebo násilím.

Předmětem krádeže je vždy věc cizí. Pachatel se nikdy nemůže dopustit krádeže na své vlastní věci. A to ani v případě, že ji odejme např. nájemci, zástavnímu věřiteli nebo jinému oprávněnému držiteli. Věcí cizí se rozumí vždy věc, která zcela nebo částečně náleží jiné osobě než pachateli (i věc ve spoluvlastnictví – výjimkou je společný majetek manželů). [17, 18]

Podíváme-li se na obligatorní znaky blíže, tak **jednání** je projev pachatelovy vůle, jednak samotná vůle pachatele (vnitřní složka) a její projevy navenek (vnější složka). Pro naplnění trestněprávního jednání musí být splněny obě tyto složky. Za **následek** trestného činu je považováno porušení, či ohrožení hodnot, které jsou objektem trestného činu. V případě krádeže jde tedy o porušení vlastnictví či držení věci. Poslední složkou objektivní stránky je **příčinná souvislost**. Je to nutný předpoklad pro vznik odpovědnosti za trestný čin. V podstatě jde o to, že bez určité příčiny (např. protiprávního jednání) by nenastal daný škodlivý jev nebo by nastal jiným způsobem. [17, 18, 20]

Objektivní faktory jsou:

- předmět útoku,
- společenské podmínky,
- místo činu a podmínky na něm,
- vztah mezi pachatelem a předmětem útoku, obětí a místem činu,
- existence spolupachatelů,
- čas spáchání trestného činu,
- dostupnost a charakter použitých nástrojů, zbraní, dopravních prostředků a ostatních pomůcek. [21]

Předmět útoku podstatně ovlivňuje způsob, jakým je krádež provedena. Na základě toho, o jakou věc se jedná, si pachatel vybírá prostředky. V případě, že se jedná o vloupání, je důležitý druh překážky. Od toho se poté odvíjí výběr nástroje, doba trvání útoku a míra použitého násilí. [21]

Společenské podmínky mají sice podstatně menší vliv, ale rozhodně ne zanedbatelný. Pokud vezmeme v potaz makrosociální podmínky jako jsou: společenské zvyklosti, tradice, vysoký výskyt kriminality, organizovaný zločin apod. Pachatel poté může mít sklony k násilnější trestné činnosti, což se u krádeží může projevit vyšším zastoupením střelných či jiných zbraní, pohrůžkami bezprostředním násilím apod. Ovšem tyto souvislosti jsou obtížně prokazatelné. Naopak je tomu u mikrosociálních faktorů. Zde se jedná především o vliv společenství, ve kterém se pachatel pohybuje: vězeňské prostředí, zločinecké party, gangy a jiné uskupení. [21]

Místo činu a podmínky na něm mají dopad na způsob páchání krádeže. Pachatel na základě vlastností místa činu (přístupnost, druh stavby, vzdálenost, frekventovanost pohybu osob, dopravní sítě, hustota osídlení) volí přístupovou trasu, způsob překonání překážek, intenzitu použitého násilí, délku pobytu na místě, vhodný čas pro realizaci, trasu odchodu apod. [21]

Vztah mezi pachatelem a předmětem útoku, obětí a místem činu hraje velkou roli v informovanosti pachatele. Pokud má pachatel blízký vztah k oběti, místu činu nebo k samotnému předmětu útoku, je pak zpravidla mnohem lépe informován o podmínkách, za kterých je pro něj co nejsnazší krádež uskutečnit. Pokud má třeba blízký vztah k oběti, může mu to například usnadnit vnik do objektu. Zde je třeba si uvědomit, že pachatel mohl potřebné informace získat i z doslechu nebo předchozího pozorování místa činu. Takový pachatel jde tzv. najisto. Ví, co se na daném místě nachází za cennosti, zná bezpečnostní opatření a ví, jak se co nesnadněji dostat dovnitř i ven. V tomto případě si oběť nemusí hned všimnout, že byla okradena. V případě, že pachatel nemá potřebné informace, ani blízký vztah k některé z uvedených oblastí, projeví se to na jeho zvolené cestě i samotném postupu. Zvolí špatnou přístupovou či únikovou cestu, vynaloží zbytečnou námahu, prodlouží se čas strávený na místě činu, dělá zbytečný nepořádek (hledá cennosti, peníze). Může se stát, že ty nejcennější věci ani nenajde. Takto „naslepo“ provedeného činu si oběť zpravidla ihned všimne (rozbité okno, rozházené věci). [21]

Existence spolupachatelů (pomocníků, překupníků, organizátorů) a jejich počet ovlivňuje způsob provedení. Pro pachatele může být spolupráce výhodná, protože si můžou práci

rozdělit a tím usnadnit spáchání činu. Ovšem čím více lidí je zapojeno, tím je vyšší riziko odhalení. Hrají zde roli i jiné okolnosti, jako je například vyrušení pachatele při činu, možnost odprodeje ukradených předmětů a jiné. [21]

Čas spáchání trestného činu souvisí s podmínkami na místě činu: frekvence pohybu osob, způsob střežení, přítomnost osob v objektu, meteorologické podmínky aj. Pachatel se snaží zvolit dobu, která je pro něj nejvýhodnější (nízký pohyb lidí, střídání služeb, dobrá viditelnost). Většinou zde hraje roli roční období, den v týdnu a denní doba. V případě, že si pachatel nemůže vybrat čas, snaží se alespoň přizpůsobit způsob provedení. [21]

Charakter použitých prostředků záleží především na možnostech pachatele si dané nástroje, zbraně nebo dopravní prostředky obstarat. Pokud je některý předmět využit, stává se determinujícím faktorem vůči ostatním komponentům při způsobu provedení. [21]

2.3.2 Subjektivní stránka

Subjektivní stránka je vnitřní vztah pachatele k jeho jednání a vzniklým následkům. Spočívá v úmyslném zavinění činu a musí zahrnovat celou podstatu objektivní stránky, včetně přisvojení si cizí věci. I příprava k takovému činu je trestná. O krádež se jedná i v případě, že pachatel nemá v úmyslu věc užívat, ale po jejím odcizení ji zničí nebo daruje. Obligatorním znakem je zavinění, úmyslné nebo z nedbalosti (v případě krádeže se jedná výhradně o úmysl). Aby vznikla trestní odpovědnost pachatele, je zavinění nutným předpokladem, protože trestní zákoník nepřipouští objektivní odpovědnost. Vedlejšími znaky subjektivní stránky jsou pohnutka (motiv) a účel (cíl). [17, 18]

Subjektivní faktory jsou:

- věk pachatele,
- pohlaví pachatele,
- psychické vlastnosti:
    - rozumové schopnosti,
    - charakterové vlastnosti,
    - psychické poruchy,
    - psychomotorické schopnosti,
    - temperament
- somatické vlastnosti. [21]

Věk pachatele se špatně určuje podle způsobu provedení činu. Hraje roli spíše odlišení mladých delikventů (cca do 20. let) od dospělých. A to proto, že v jednotlivých fázích lidského života se daný jedinec vyznačuje specifickou úrovní psychických a somatických vlastností. Většinou v případě starších pachatelů jsou činy více sofistikované a rafinované oproti mladším. Ti dost často využívají spolupachatele a při páchání trestných činů používají neadekvátní násilí (vandalismus). Protože si činy většinou míň promýšlejí, liší se věci, které kradou. Jedná se spíše o předměty určené k zábavě, kde neberou v potaz jejich tržní hodnotu. Trestnou činnost zpravidla páchají blíže svého místa bydliště. [21]

Pohlaví pachatele je důležitým faktorem, který ovlivňuje způsob páchání krádeží. A to z důvodu odlišných psychických i somatických vlastností obou pohlaví. Z průzkumů vyplývá, že ženy zřídka kdy krádež předem plánují, spíše využívají momentální příležitosti. Proto jsou činy žen zpravidla méně promyšlené než činy mužů. Naopak muži zase více využívají spolupachatelství a vyšší míru agresivity a násilí. [21]

Psychické vlastnosti – nejzásadnější vliv na způsob páchání krádeží má následujících šest skupin psychických vlastností:

- **Rozumové (intelektuální) schopnosti** mají zásadní vliv především u složitých trestných činů. V případě krádeží se jedná o důkladně promyšlené krádeže, například krádež identity, utajovaných informací, krádeže aut, vloupání. Nadprůměrná inteligence je předpokládaná v případě kybernetické kriminality, jako je hacking, softwarové pirátství, podvodné e-shopy apod. Naproti tomu u primitivních trestných činů není nutným předpokladem. [21]
- **Charakterové vlastnosti** mohou být často příčinou, proč se pachatel rozhodl k trestné činnosti. Jedná se například o chamtivost, krutost, závist, nepřátelskost, sobeckost. Často se, ale pachatel v dané situaci přetvařuje, hraje někoho, kým ve skutečnosti není, aby oklamal oběť a vzbudil v ní strach a nejistotu. [21]
- **Psychické poruchy** se projevují ve způsobu provedení krádeže. Ovšem jejich vliv se špatně určuje, jelikož trestný čin sám o sobě je patologickým jevem. U některých obzvláště závažných poruch se může jednat o specifické jednání pachatele. Psychotici si můžou počínat neopatrně, bezcílně a jakoby bez rozmyslu. U schizofrenie se může jednat o nadměrnou brutalitu a násilí, které nedávají smysl. Naopak je tomu u dočasného ovlivnění psychického stavu alkoholem nebo drogami, tyto případy mají svá specifika, kterými se odlišují. [21]

- **Psychomotorické schopnosti** se výrazně projevují ve stopách, díky čemuž lze snáze určit skupinovou příslušnost pachatele podle způsobu provedení krádeže. Dají se dobře popsat, a lze určit míru jejich zvládání (stupeň koordinace, zručnosti, orientace v prostoru, rychlosti, obratnosti). To umožňuje rozdělit pachatele do skupin podle typu a stupně ovládání těchto dovedností. Při samotné krádeži se poté projevují především v lokomoci pachatele (schopnost překonat určitou překážku – vyšplhat na balkon, přelézt plot) a při manuálních úkonech (otevření zámku, vypáčení dveří, odpojení bezpečnostního systému). [21]
- **Temperament** ovlivňuje reakci pachatele na různé podněty při páchání trestného činu. Z těch se poté dá vyvodit pachatelova impulzivnost, vytrvalost, důkladnost, vznětlivost, klidnost apod.

Somatické vlastnosti, tedy tělesné dispozice pachatele (svalová a kosterní stavba) nám určují pachatelovy hranice. Dále mírou možného násilí, volbu přístupové cesty, použité nástroje, přizvání spolupachatele, předmět krádeže a další. [21]

3 PROCES KRÁDEŽE MAJETKU

Krádež je v podstatě zmocnění se cizí věci s úmyslem nakládat s ní jako s vlastní. Skutková podstata krádeže je stejná jak u trestného činu, tak u přestupku, liší se pouze nebezpečnost činu pro společnost. Rozdíl mezi přestupkem a trestným činem je hranice způsobené škody, která je do 5 000 Kč (nepatrná) u přestupku. Pokud je hranice škody vyšší, už se jedná o trestný čin.

3.1 Vývojová stádia krádeže

Netrestněprávní stádia:

- **Pojetí myšlenky** – pachatel přemýšlí nad spácháním trestného činu (ukradení aktiva), je to obligatorní (nutné) stádium, bez kterého by nemohla být krádež realizována. Ovšem bez dalšího jednání nemá trestněprávní následky. Pro společnost tato myšlenka nepředstavuje reálné nebezpečí, protože není jisté, zda bude tato myšlenka realizována. [19, 20]
- **Projevení navenek** – pachatel dá okolí vědět o svém úmyslu (vychloubá se před kamarády co má za nápad). Jedná se o fakultativní (nepovinné) stádium. Pachatel před provedením činu musí pojmout myšlenku o jeho spáchání, ale nemusí o ní dát vědět svému okolí. Ani takovéto jednání nemá trestněprávní následky, pokud se na to díváme z pohledu krádeže majetku. Ovšem je potřeba zvážit, zda se nejedná o verbální trestný čin, kdy vyjádření hrozby může naplnit skutkovou podstatu. Tedy jestli při projevení úmyslu spáchat např. krádež nedojde k naplnění skutkové podstaty jiného trestného činu. [19, 20]

Trestněprávní stádia trestného činu:

- **Příprava** – vytváření podmínek pro spáchání trestného činu (spolčování se, shánění prostředků, pomáhání, navádění apod.). Jde o první trestněprávní stadium. Ovšem pouze u obzvláště závažných zločinů. V trestním právu obecně příprava trestná není, trestnost musí být vymezena ve zvláštní části zákona u příslušného trestného činu. Trestní zákoník ustanovuje zvlášť závažný zločin následovně: "*§ 14 (3) zvlášť závažnými zločiny jsou ty úmyslné trestné činy, na něž trestní zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně deset let.*" [17] V případě krádeže se tedy musí jednat o přípravu k vyšší formě kvalifikovaného jednání s horní trestní sazbou

nejméně deset let a trestnost přípravy musí být stanovena v příslušné skutkové podstatě. [17, 19]

- **Pokus** – pachatel odstraňuje poslední překážky (vniká na pozemek, vylamuje zámek, rozbíjí okno) bránící mu v krádeži a směřuje k dokonání trestného činu. Pokus je vždy trestný, ukládá se stejný trest jako za dokonaný trestný čin. Zákon ustanovuje pokus následovně: *„Jednání, které bezprostředně směřuje k dokonání trestného činu a jehož se pachatel dopustil v úmyslu trestný čin spáchat, je pokusem trestného činu, jestliže k dokonání trestného činu nedošlo.“* [17] Při posuzování pokusu je nutné dbát také na pachatelův záměr a jeho představu o předmětu, který byl cílem jeho krádeže.
    - Do druhé části pokusu, kdy pachatel uskutečňuje jednání k dokonání krádeže patří následující kritéria:
        - Časová určenost (spojitost mezi jednáním a následkem – lze očekávat dokonání krádeže)
        - Místní určenost (pachatel je připraven na místě činu)
        - Odstraňování překážek, které brání v dokonání krádeže (pachatel rozbíjí okno, čeká na vhodný okamžik, vylamuje zámek, rozesílá škodlivý software, prolamuje zabezpečení serveru, čeká na připojení uživatele k síti)
        - Použití prostředků, nástrojů k uskutečnění krádeže (použití již opatřených nástrojů – vypáčení dveří, použití paklíče, rozbití okna kladivem, prolomení šifrovacího algoritmu, aktivace škodlivého softwaru, využití získaných přihlašovacích údajů)
        - Působení na hmotný cíl (předmět krádeže – příprava předmětu k odcizení –finanční hotovost, šperky, osobní údaje, firemní data) [17, 19, 20]
- **Dokonání** – jde o naplnění všech znaků skutkové podstaty krádeže uvedených v zákoně. Jde o společensky neškodlivější stádium trestného činu. Musí se ovšem odlišovat dokončení od ukončení trestného činu, protože k **ukončení** trestného činu může dojít ještě před jeho dokončením (např. zadržení pachatele policii či ochrankou při pokusu o krádež). [17, 19, 20]

3.2 Typologie krádeží

Klasifikace způsobů páchání krádeží se provádí podle následujících kritérií:

- složitost způsobu provedení,
- fakt, zda byly použity nástroje,
- stupeň připravenosti,
- zda je páchána vnitřními nebo vnějšími pachateli,
- objekt zaměření pachatele nebo předmět zájmu. [21]

Složitost (kvalifikovanost) způsobu provedení:

- krádeže prosté (jednoduché),
- krádeže složité (kvalifikované).

Krádeže prosté jsou takové, k jejichž provedení není většinou potřeba násilí k překonání překážek. Co se způsobu provedení týče, bývá jednoduchý. Ve většině případů nevyžaduje přípravu a využití nástrojů nebo pomůcek k jeho zdárnému provedení. Jedná se především o krádeže snadno dostupných předmětů, jako jsou například jízdní kola, odložená zavazadla, oblečení apod. Takové krádeže bývají často náhodné. Kdy pachatel například uvidí nezamčené kolo ve stojanu, odložené zavazadlo v čekárně, neuzamčené vozidlo na parkovišti apod. Významným faktem u těchto krádeží je, že pachatelé zanechávají minimum stop a jejich provedení nevyžaduje zručnost nebo schopnost plánování. Vyšetřování je potom vedeno na základě odcizených věcí nebo výpovědi případných svědků (popis pachatele). [21]

Krádeže složité vyžadují určitou přípravu a je pro ně typické, že jsou složitější než krádeže prosté. Předměty zájmu bývají zabezpečeny proti odcizení a pachatel je nucen tuto ochranu překonat. Proto je pro složité krádeže charakteristické plánování, zajištění nástrojů, prostředků a vykonání určitých úkonů bez kterých, by pachatel nebyl schopen překážky překonat. Často se jedná o krádeže vloupáním, krádeže motorových vozidel, krádeže dat, osobních údajů apod. [21]

Fakt, zda byl použit nástroj:

- bez nástroje,
- s nástrojem.

Bez nástroje se většinou páchají u věcí, které jsou pro pachatele snadno dostupné. Bývají to krádeže prosté a krádeže prováděné vnitřními pachateli. [21]

S nástrojem se převážně páchají krádeže vloupáním, kdy bývá použití nástroje nutnou podmínkou k realizaci krádeže. Ve většině případů se setkáváme s nástroji sériové výroby, případně zvláště upravenými. Pouze v ojedinělých případech se můžeme setkat se speciálně vyrobenými nástroji, sloužícími výhradně k provedení krádeže. [21]

Pokud pachatel využije při krádeži nějaký nástroj, tak to zpravidla usnadňuje pátrání na základě metod kriminalistické identifikace pro zjištění využitého nástroje. [21]

Stupeň připravenosti:

- připravené,
- nepřipravené.

Připravené krádeže se vyznačují tím, že pachatelé před její realizací provádějí činnosti jako typování objektů, opatřování nástrojů, dopravních prostředků, sestavování plánu, kontaktování překupníků, hledání úkrytu, sledování osob či objektů apod. Občas se při této činnosti pachatelé snaží navázat kontakt s obyvateli objektu, aby zjistili potřebné informace. Jedná se většinou o tyto informace: místo uložení cenných věcí, vhodná doba k provedení krádeže, způsob zabezpečení objektu, možné přístupové cesty apod. [21]

Nepřipravené krádeže se od připravených odlišují tím, že pachatel krádež realizuje bez předchozího plánování. Většinou využívá vhodné příležitosti a krádež provádí okamžitě po pojetí myšlenky a rozhodnutí krádež spáchat. Za nepřipravené se považují i krádeže, kdy se pachatel v daném prostoru pohybuje po delší čas s úmyslem spáchat krádež. Čeká však na vhodný okamžik k jejímu provedení. [21]

Okolnost, jestli je krádež páchána vnitřními nebo vnějšími pachateli:

- vnitřními pachateli,
- vnějšími pachateli,
- kombinované spolupachatelství (vnitřní + vnější).

Vnitřní pachatelé se od vnějších odlišují tím, že mají k předmětu zájmu přístup. Pro tyto krádeže bývá charakteristické jejich následné utajování, čímž se pachatel zpravidla dopouští další trestné činnosti, většinou podvodu. Například skladník odcizí ze skladu materiál, aby krádež utajil, zfalšuje doklady. Tím docílí toho, že krádež zůstane určitou dobu latentní, ale

dopustí se tím kromě krádeže, také další trestné činnosti. Takto páchané krádeže bývají často odhaleny až s odstupem několika měsíců nebo i let. [21]

Vnějším pachatelem může být prakticky kdokoliv. Pachatel nemá předchozí vztah s předmětem zájmu. V tomto případě takřka nedochází k snaze krádež utajit. Její odhalení totiž nevrhá podezření na konkrétní osobu, pachatel tak spoléhá na to, že nebude odhalen. Proto bývají většinou rychle odhaleny a oznámeny. Můžeme se ale setkat se snahou dočasně krádež utajit (zahlazení stop po vniknutí do skladu). Důvod tohoto jednání je prostý, pachatel si tím snaží zajistit možnost opakovaného vniknutí do objektu. [21]

Kombinované spolupachatelství se vyznačuje tím, že zločin je spáchaný za spolupráce vnitřního pachatele s vnějším. Vnitřní pachatel má většinou za úkol poskytnout informace o předmětu zájmu, jeho zabezpečení a připravit jej k odcizení vnějším pachatelem. Občas se u krádeží organizovaných většími gangy stává, že někteří členové nevědí, že se jedná o trestnou činnost. Tito pachatelé jsou označování jako tzv. bílí koně. [21]

Podle objektu zaměření a předmětu zájmu:

Objekt zaměření nám krádeže rozděluje na kapesní, bytové, v restauracích, kinech, krádeže motorových vozidel, věcí z aut, vloupání do domů, chat apod.

Předmět zájmu rozčleňuje krádeže podle toho, co chce pachatel odcizit, o co má největší zájem: peníze, starožitnosti, elektronika, alkohol, potraviny, auta, kola apod.

Takové rozdělení má smysl pouze, pokud se krádeže a způsob jejich provedení vyznačují specifickými rysy nebo pokud jde o recidivisty (osoby opakovaně páchající stejnou TČ), kteří se zaměřují na podobné objekty nebo předměty zájmu. [21]

3.3 Metody realizace krádeže

3.3.1 Příklady používaných metod fyzickou cestou

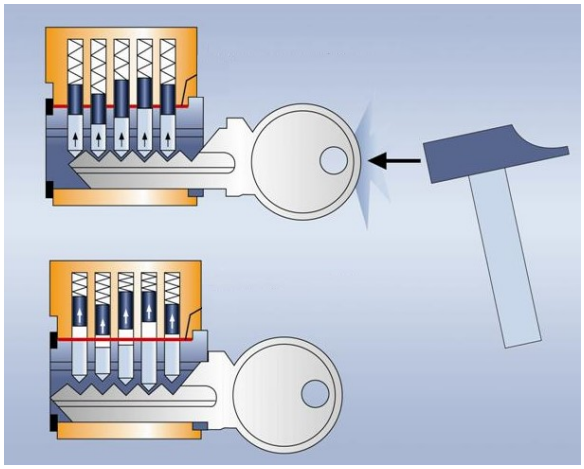
Vloupání

- Hrubá síla
- Paklíč
- Bumping (tzv. SG metoda – speciální vyklepávací klíč)
- Lockpicking (Odemykací pistole Lock Pick Gun nebo taky snap gun)
- Matení za pomoci převleků (stěhováci, opraváři, řemeslníci)
- Vloupání během spánku

Hrubá síla je jedním z nejčastěji využívaných způsobů. Není třeba používat sofistikované nástroje. Lidé často nemají dostatečně zabezpečená okna, z toho důvodu téměř 3/4 pachatelů považuje toto místo za nejsnazší cestu do objektu při vloupání. Pachatelů stačí jednoduše vybít prosklenou tabuli a kličkou si okno otevřít nebo pomocí šroubováku odemknout obvodové kování. Dále zloději často využívají páčidlo, kladivo, sekeru, krumpáč apod. [22]

Paklíč byl běžnou pomůckou zlodějů, v dnešní době už se ale moc nevyužívá, protože pro zloděje je snazší koupit si na internetu sofistikovanější a snáze použitelné nástroje (speciální odemykací pistole).

Bumping se využívá u starších typů cylindrických vložek, kdy pachatel zasune speciální klíč (polotovar vybroušený na krajní pozici stavítek). Poté následuje předem nacvičený úder do klíče, pomocí kterého se pachatel snaží seřadit stavítka ve vložce do roviny a tím odjistit zámek. Předpokladem k úspěšnému využití této metody je nižší bezpečnostní třída zámku. [23]



Obrázek 4 – Bumping [24]

Nejúčinnější ochranou proti bumpingu je používání zámků s vyšší bezpečnostní třídou vložek 3 a 4. Ty jsou proti této metodě chráněny. [23]

Lockpicking neboli vyháčkování, je nedestruktivní metoda překonání zámků pomocí manipulace se zámkovou vložkou na základě znalostí, jak zámek funguje. Tento způsob využívá toho, že při správném tlaku na napínák se po umístění stavítek do odblokované polohy, v této pozici stavítka zaseknou, což po odblokování všech stavítek a odjištění pojistky umožní zámek otevřít. [25, 26]

Je více metod, kterých se při vyháčkování využívá. Především se jedná o tyto:

- **Picking** – pomocí napínáku se zlehka tlačí na bubínek ve směru otevírání zámku, to zajistí, že po zatlačení stavítka planžetou, se stavítko zasekne o okraj shearline. To umožní postupně zaseknou všechny stavítka a tím otevřít zámek. [25, 26]
- **Raking** – podobný princip jako u pickingu, ale používá se jiná planžeta, kterou se přejíždí po stavítkách, které se tímto způsobem snažíme zaseknout o okraj shearline. [25, 26]
- **Lock Pick Gun (snap gun)** – jedná se o pružinový nástroj, který se podobá pistoli s háčkem připevněným na přední straně. Jehla se zasune do zámku a umístí pod všechny stavítka. Pro napnutí a otáčení zámku je použit samostatný nástroj, na který se zlehka tlačí. Poté se spoušť pistole pustí což způsobí, že stavítka poskočí do svých komor. Pokud všechny stavítka zároveň přeskočí nad smykovou linii, zámek lze otevřít. [25, 26]

  Elektrické a vibrační snap guny pracují na podobném principu, ale místo úderu, oscilují jehlou tam a zpět, což způsobuje vibrace. Nástroj se snaží docílit toho, aby stavítka skákala nad smykovou linií. [25, 26]

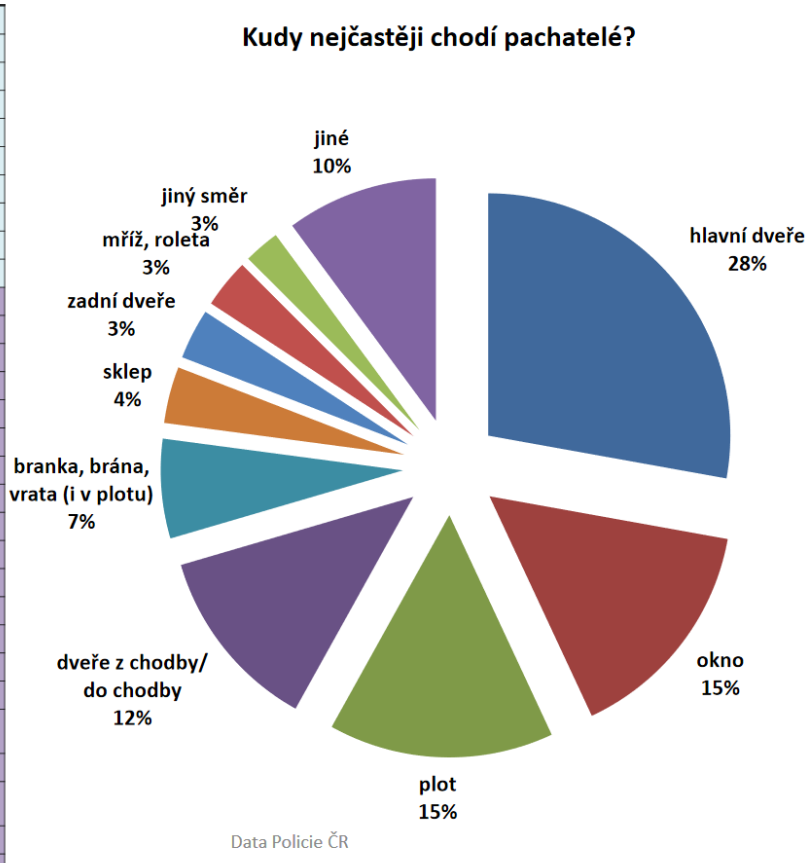
Obrázek 5 – Lock Pick Gun [27]

Matení za pomoci převleků je v poslední době také čím dál více využívanou technikou zlodějů. V ohrožení jsou především senioři. Pachatel nebo pachatelé se vydávají například za stěhováky, opraváře nebo třeba za plynaře či topenáře. Pomocí těchto převleků se snaží

oklamat oběť a získat si tak jejich důvěru. Když se jim to povede, oběť je sama pustí do bytu či domu, kde je často nechá „pracovat“ bez dozoru. Takoví pachatelé se většinou zaměřují na drobnou elektroniku, peněženky, šperky a další cennosti.

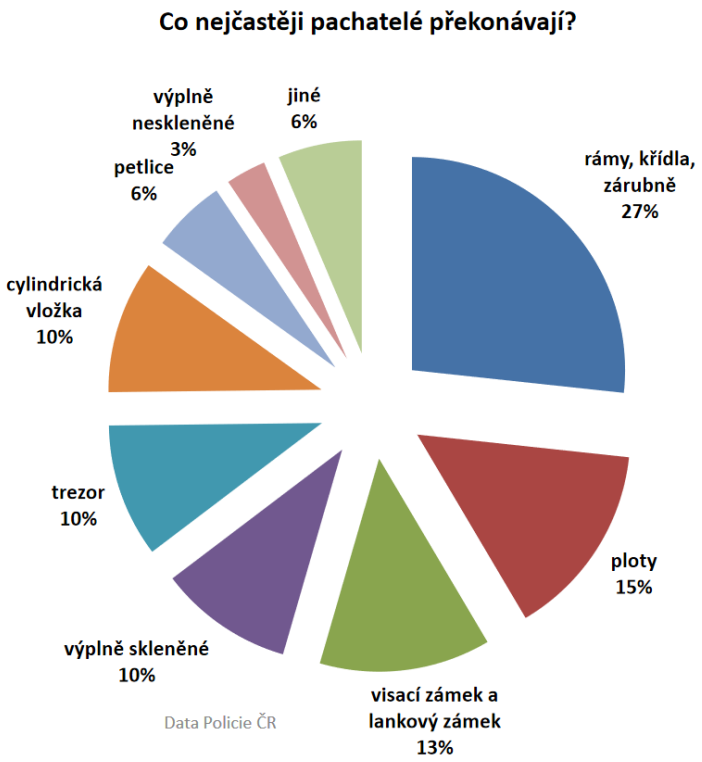
Vloupání během spánku je způsob, který preferuje více než 1/3 zlodějů. Takto vykradené domácnosti bývají opakovaně terčem zlodějů, kdy po prvním vloupání následuje několika týdenní až měsíční pauza. Při dalším pak většinou odcizí nově nakoupené věci. Může se ale jednat i o zloděje, kteří se spokojí s malým finančním obnosem, který pak použijí pro soukromé účely. Opět jsou zde rizikovou skupinou senioři. [22]

hlavní dveře	29031
okno	15881
plot	15679
dveře z chodby/ do chodby	12924
branka, brána, vrata (i v plotu)	6918
sklep	3933
zadní dveře	3505
mříž, roleta	3408
jiný směr	2493
páčí víka, dvířka, skříně	1990
stěna, podlaha, strop	1296
dveře z balkonu/na balkon	1233
okenice	1015
garáží	784
výloha	764
střecha, půda	713
trezor	564
balkonem, lodžií	522
terasou	437
prodejní, výdejní okénko	281
větračka, ventilátor	219
po bleskosvodu, okapu, římse	162
veranda	151
po přístavku	146
světlík, šachta větrací, výtahová šachta	115
lešení	69
poklopem v podlaze, ve stropě	56
kanál, kanalizace, kolektor	23
vzduchotechnikou	13



Obrázek 6 – Nejčastější přístupové cesty zlodějů [28]

rámy, křídla, zárubně	30373
ploty	16832
visací zámek a lankový zámek	14771
výplně skleněné	11591
trezor	11534
cylindrická vložka	11501
petlice	6440
výplně neskleněné	3467
mříže, rolety	2986
stěny, podlahy, stropy	1389
zadlabací zámek	925
sklep	859
závěsy	578
střecha, půda	505



Obrázek 7 – Nejčastější překážky, které pachatelé překonávají [28]

3.3.2 Příklady používaných metod kybernetických krádeží

Podvodné jednání

- Podvodné inzeráty
- Falešné e-shopy
- Phishing
- Sociální inženýrství
- Porušování autorského práva
- Krádež identity

Podvodné inzeráty jsou v poslední době čím dál více oblíbenou technikou zlodějů. Rozmáhají se především podvodné nabídky pronájmů bytů. Kdy lákají na nízký nájem například v centru města. Obvyklými praktikami jsou ale také nabídky na bazarových serverech, aukčních portálech apod. Předmětem prodeje jsou především ojeté automobily, použitá elektronika a mnoho dalšího. Většinou jdou takové inzeráty odhalit tím způsobem, že člověk trvá na osobním předání dané věci. [29, 30]

Falešné e-shopy zneužívají důvěřivosti zákazníků. Jde o webové stránky, které se tváří jako obchod, doopravdy je ovšem jejich jediným cílem získat peníze od zákazníků. Takové stránky vypadají jako spolehlivý e-shop se širokou nabídkou zboží. Požadují však platbu předem, po zaplacení ovšem zákazník nic neobdrží. Při platbě na dobírku mu pak přijde například cihla, balíček vycpaný novinami apod. Nápovědou jak takový e-shop odhalit může být podezřele nízká cena za kvalitní zboží. [29]

Phishing je podvodná technika, jejímž cílem je získat citlivé údaje (heslo, přihlašovací údaje do internetového bankovnictví, číslo kreditní karty apod.) pomocí elektronické komunikace. Útočník předstírá, že je ze známé populární společnosti (sociální sítě, aukčního webu, banky, zdravotní pojišťovny, platebního portálu, úřadu) nebo, že je jejich administrátorem. Tím si získá důvěru oběti, která mu poté sdělí důvěrné informace. [29]

Sociálním inženýrstvím se označuje technika využívající manipulace s lidmi za účelem získání nějaké konkrétní informace. Většinou se útočník s obětí nedostávají do osobního kontaktu. Útoky bývají směřovány na zaměstnance firem, kdy se útočník snaží získat utajované informace nebo přístup do informačního systému. [29]

Krádež identity bývá důsledkem předchozího podvodného jednání, kdy útočník získá citlivá data o oběti, za kterou se následně vydává. Nejčastěji k tomu dochází za účelem získání finančních prostředků.

Napadení škodlivým softwarem (malware)

- Keylloger
- Ransomware

Keylloger pomocí škodlivého software zaznamenává klávesy, které uživatel stisknul. Tyto záznamy následně odesílá jeho tvůrci, který tímto způsobem může získat přihlašovací údaje k nejrůznějším službám. Jedná se především o počítačový software, ale výjimkou nejsou ani případy hardwarových keyllogerů. [29]

Ransomware je druh škodlivého programu, který zablokuje přístup k počítači nebo zašifruje data a následně požaduje po oběti odškodné za jejich znovu zpřístupnění. Existují jednodušší formy, které pouze zablokují operační systém a složitější, ty většinou zašifrují data na pevném disku. [29]

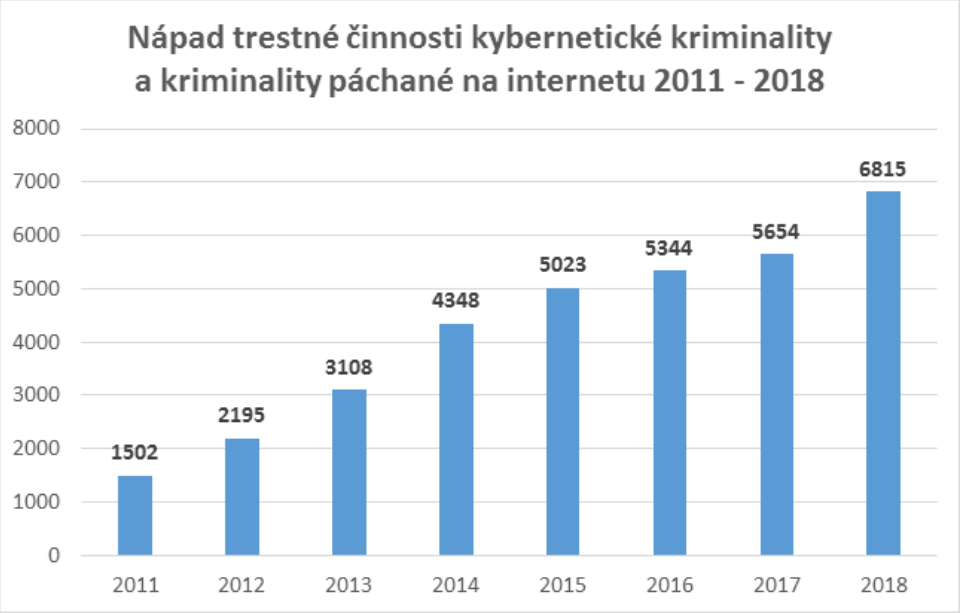
Kybernetické útoky

- Hacking
- Cracking
- Pharming

Hacking představuje využívání nestandartních funkcí programů či systému a jejich nekomentovaných funkcí k využití jejich běžně nepřístupných možností. Při tomto postupu se často zasahuje do struktury kódu, k čemuž je potřeba odborná znalost fungování těchto souborů. Hacking je v podstatě průnik do systému nestandartní přístupovou cestou nebo prolomení jeho ochrany. [29, 30]

Cracking se využívá k odstranění ochranných prvků software (většinou jde o zabezpečení před kopírováním, prodloužení trial verze apod.). K tomu se využívá technika disassemblování, což je v podstatě získání zdrojového kódu z již zkompilovaných souborů. To následně pomůže crackerovi v úpravě souborů a tím prolomení ochrany programu. [29]

Pharming je opět technika sloužící k získání citlivých informací od oběti. Obvykle se získávají přístupové údaje k chráněným aktivům. V tomto případě se jedná o napadení DNS a následné přepsání IP adresy, což má za následek přesměrování oběti na falešné stránky po zadání URL adresy do prohlížeče. Stránky mají totožný vzhled jako originál, proto je velmi těžké rozeznat rozdíl. [29, 30]

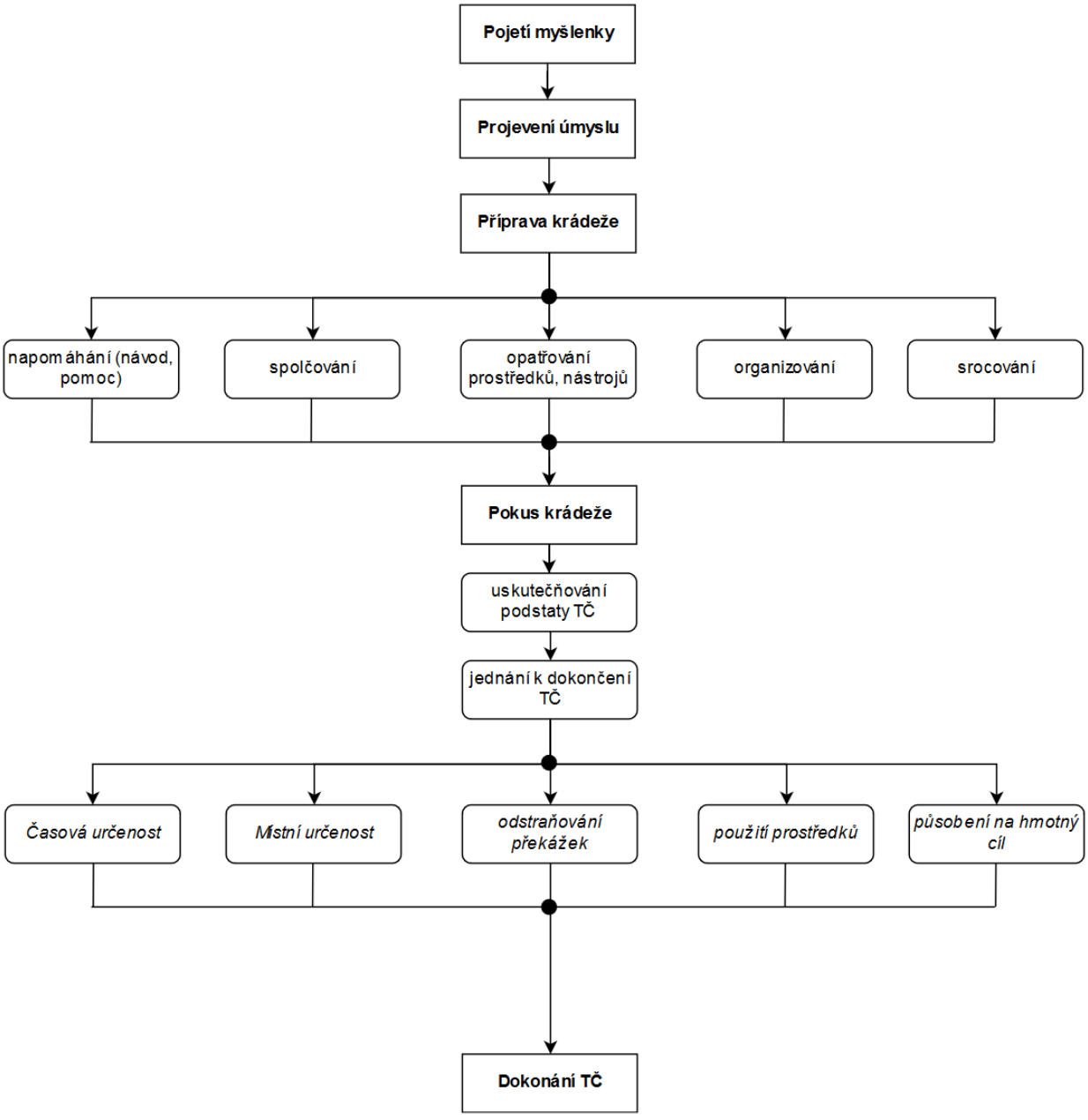


Obrázek 8 - Kybernetická kriminalita 2011 – 2018 [30]

3.4 Model krádeže majetku

Následující model popisuje posloupnost jednotlivých fází, které jsou typické pro uskutečňování úmyslu pachatele spáchat krádež. Jedná se o obecný model, který zahrnuje vývojová stádia krádeže popsaná v předcházející podkapitole. Zohledňuje i rozdíl mezi dokonanou krádeží a jejím ukončením.

Tučným textem v hranatých obdélnících jsou hlavní stádia krádeže. V obdélnících s oblými hranami, pak jejich podkategorie a kurzívou ve stejných obdélnících jednotlivé činnosti.



Obrázek 9 – Model krádeže majetku [autor]

Pojetí myšlenky je v podstatě první stádium, které předchází samotné přípravě a realizaci krádeže. Pachatele nejdříve musí napadnout, že chce něco ukrást. Toto stádium není trestněprávní, ale je nutné k realizaci krádeže.

Projevení úmyslu znamená, že pachatel navenek projeví svůj úmysl něco ukrást (chlubí se před kamarády). Jedná se o nepovinné stádium, které se může vyskytovat pouze v některých případech. Taktéž jako pojetí myšlenky, je i toto stádium netrestněprávní.

Příprava ke krádeži již je trestněprávním stádiem a spočívá zejména ve vytváření vhodných podmínek k uskutečnění krádeže. Jedná se například o přípravu plánu, shánění spolupachatelů, opatřování nástrojů apod.

Pokus krádeže představuje samotnou realizaci činu a využití příprav. Pachatel tedy překonává překážky, které mu brání v odcizení aktiv (vykopává dveře, rozbíjí okno, přihlašuje se na server pomocí získaného hesla). Více k tomuto stádiu je napsáno v kapitole 3 (viz. kapitola 3.1).

Dokonání TČ je naplnění všech znaků skutkové podstaty. Například pachatel opustil objekt s předmětem zájmu v tašce nebo zkopíroval ukradená data na svůj soukromý harddisk. V tomto případě je nutné si uvědomit, že může dojít i k ukončení TČ, což není to stejné jako dokonání. Ukončení může nastat v kterékoliv fázi krádeže, ať již z osobních důvodů pachatele nebo kvůli jeho zadržení na místě činu.

II. PRAKTICKÁ ČÁST

4 ANALÝZA VYBRANÝCH ZLOČINŮ

V následující kapitole je provedena analýza vybraných krádeží majetku. Jedná se o krádeže provedené fyzickou cestou nebo pomocí útoku přes kyberprostor. Z důvodu ochrany bezpečnosti zainteresovaných stran není možno zveřejnit podrobné informace o daných subjektech. Proto kvůli anonymizaci byla některá data pozměněna a mohou se tak mírně odlišovat od skutečnosti. Žádná z úprav však nemá zásadní vliv na podstatu či způsob provedení trestného činu.

4.1 Krádež firemních dat

Jednalo se o únik uživatelských dat z e-shopu firmy. Útočník byl tzv. outsider (člověk zvenku, který ve firmě nepracuje), kterému se podařilo získat data o téměř 357 000 uživatelských účtech. Šlo především o e-mailové adresy, telefonní čísla, hesla, jména, adresy, a dokonce i čísla platebních karet. [29, 30]

Pachatel využil zastaralého zabezpečení, kdy hesla k účtům byla uložená jako plaintext, tedy v čitelné podobě. Což znamená že při přihlašování či registraci uživatele nedocházelo k šifrování ani hashování těchto dat. Útočník tak mohl tyto údaje odposlouchávat a ukládat do svého zařízení (tzv. Man-in-the-middle). [29, 30]

Dalším problémem byly více než rok zastaralé aktualizace systému řízení báze dat (konkrétně MySQL) kvůli kterým nebyla funkčnost systému korektní. Proto bylo možno v průběhu několika dní provést až několik set databázových dotazů, aniž by si toho firma všimla. [29, 30]

Krádež dat byla odhalena až 2 týdny poté co se odehrála. A to tak, že několik dotčených zákazníků si stěžovalo na to, že je oslovují konkurenční firmy a vše nasvědčuje tomu, že mají k dispozici důvěrné informace, které měly zůstat pouze mezi nimi a firmou, která o data přišla. [29, 30]

Konečný dopad škod lze jen těžko vyčíslit, pokud někteří uživatelé používají stejné přihlašovací údaje i u jiných služeb (el. bankovnictví, e-mail, sociální sítě), mohly být v důsledku tohoto narušení poškozeny i tyto účty. [29, 30]

4.1.1 Bezpečnostní prostředí a využité zranitelnosti

Z dostupných informací je zřejmé, že firma nevyužívala žádné pokročilejší hardwarové prvky zabezpečení (HW klíče, HW firewally apod.). Šifrování dat při přihlašování uživatelů (před odesláním do databáze, kde musí být ověřeny) bylo buď naprosto opomenuto nebo byl použit snadno prolomitelný algoritmus. Další velkou chybou bylo to, že jednotlivé podsítě jejich podnikové sítě byly připojeny do vnějšího internetu a filtrace komunikace probíhala pouze pomocí základních SW firewallů, takže případný útočník se mohl snadno dostat do jejich intranetu. Pokud se zaměříme na software, tak zde bylo největším pochybením používání neaktuální a zastaralé verze, která měla známé bezpečnostní chyby. Společnost ani nevyužívala žádný monitorovací nebo analytický software, který by mohl rozpoznat nežádoucí chování uživatelů. Jak už bylo řečeno, jednou z největších chyb byla absence šifrování dat ať už při jejich šíření po síti, nebo při jejich uchovávání. Z pohledu zaměstnanců došlo k pochybení v podobě používání triviálních a snadno prolomitelných hesel. To je ale i chyba administrátora, který by měl nastavit minimální doporučené parametry pro hesla. Ve firemní síti se dokonce nacházela data k osobním profilům a službám zaměstnanců, které pachateli pomohly identifikovat jednotlivé zaměstnance a jejich pozici v systému. [29, 30]

Prvky bezpečnostního prostředí:

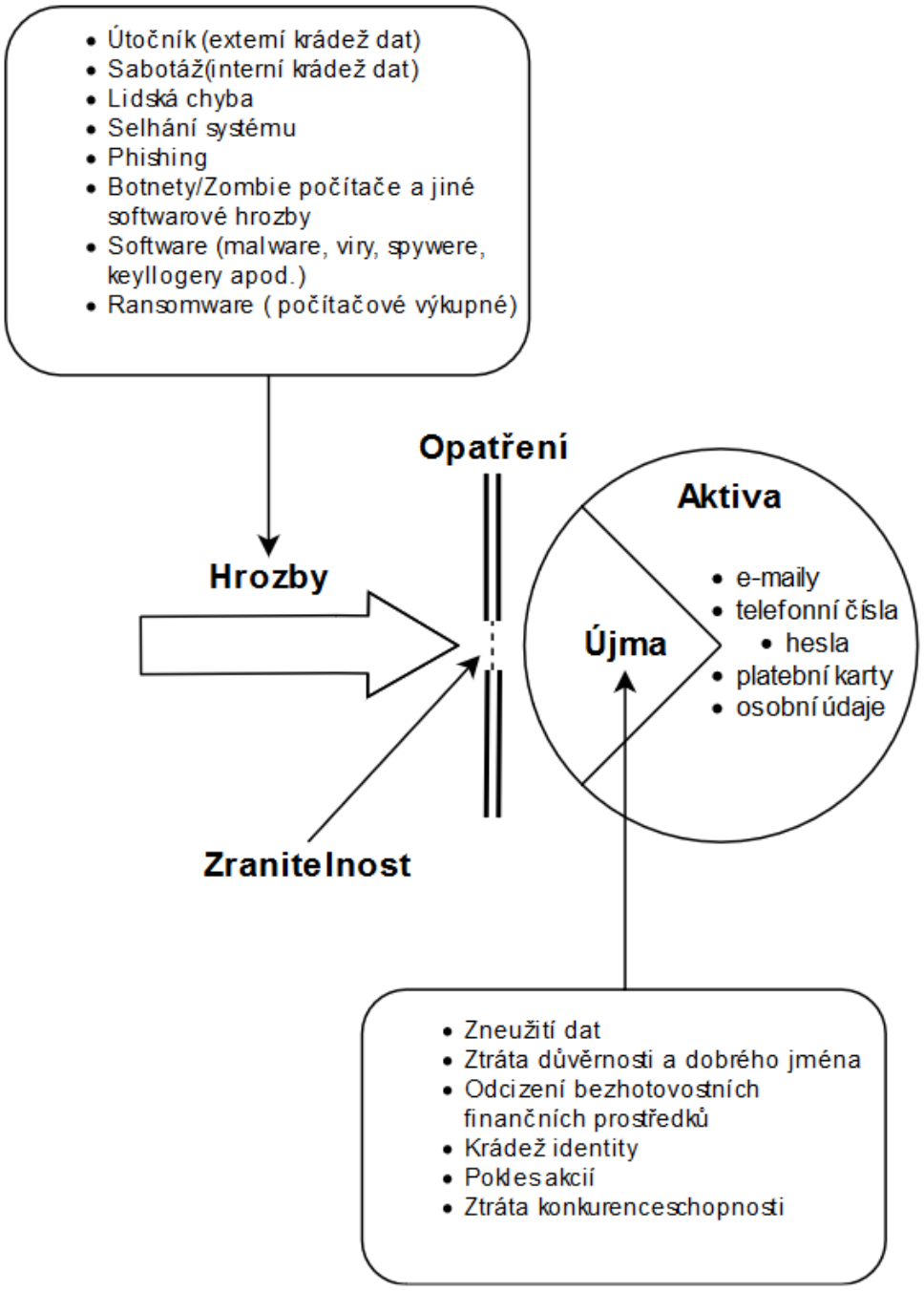
- webový server,
- databáze,
- síť poskytovatele internetu,
- datová úložiště firmy,
- vnitřní podniková síť,
- uživatelé,
- zaměstnanci,
- správci zařízení a služeb.

Využité prostředky/metody:

- Man-in-the-middle (sniffing)
- SQL injection (databázové dotazy)
- Exploitace

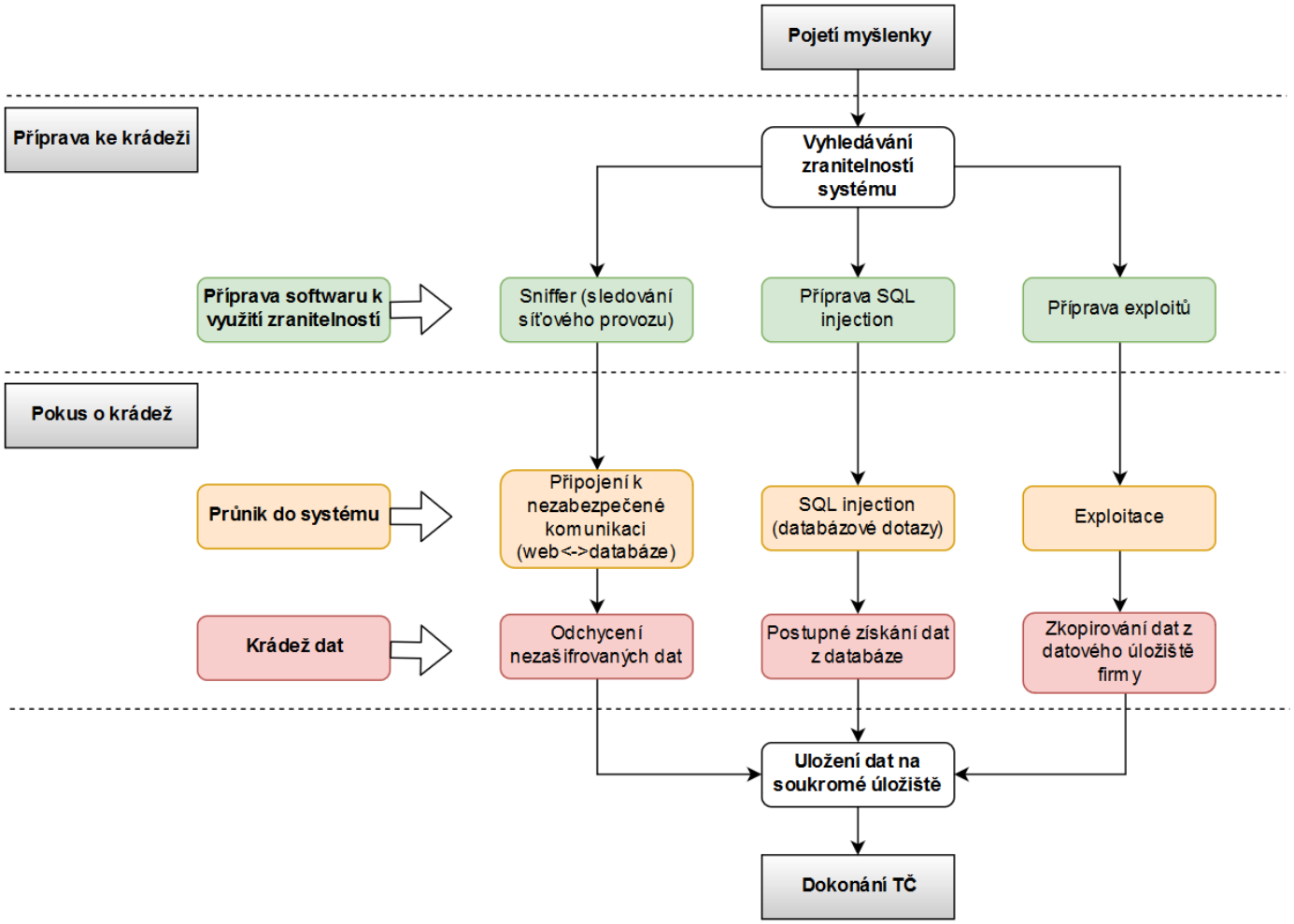
4.1.2 Bezpečnostní model

Na obrázku níže je znázorněn obecný bezpečnostní model zaměřený na e-shop dotčené firmy. Neznázorňuje pouze případ krádeže, který je popisován výše, ale zahrnuje i potenciální hrozby, které mohou firmu ohrozit v případě nepřijetí nápravných opatření.



Obrázek 10 – Bezpečnostní model (krádež firemních dat) [autor]

4.1.3 Model krádeže



Obrázek 11 – Krádež firemních dat [autor]

4.1.4 Návrh opatření

Návrh a provedení bezpečnostních opatření je klíčový pro budoucí ochranu před vlivem bezpečnostních hrozeb na referenční objekt (firmu). Narušení bezpečnosti se také stalo varováním pro ostatní organizace, aby zlepšily svou kybernetickou bezpečnost a politiku v oblasti nakládání s citlivými daty.

Preventivní opatření:

- Používání HW klíčů pro přístup, administraci a konfiguraci klíčových prvků systému.
- Použití HW firewallů pro filtrování komunikace v podnikové síti a na webu.
- Oddělení jednotlivých sítí – intranet od vnějších sítí.
- Definovat parametry hesel, vynucovat jejich dodržování a stanovit jejich platnost.
- Používání VPN a šifrování dat (https s certifikátem SSL/TLS ideálně SSL EV).
- Šifrování dat v datových úložištích firmy a databázích (minimálně SHA-2 hash).
- Pravidelné aktualizace softwaru a obnova hardwaru.
- Zavedení systému managementu bezpečnosti informací podle normy ČSN ISO/IEC 27001.
- Pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti.
- Provádění pravidelných penetračních testů.
- Využití vícefaktorové autentizace (MFA – Multi-Factor Authenticcation) – ověření identity uživatele na základě toho: co zná, co má, co je a jeho kontext.
    - Faktory, které musí uživatel znát jsou například: uživatelské jméno, heslo, PIN, obrázek důvěryhodnosti apod.
    - Faktory, které musí mít: jednorázové heslo, token, šifrovací klíč atd.
    - Faktory, jenž charakterizují uživatele: biometrie, specifické chování uživatele v systému.
    - Kontextové faktory: IP adresa, poloha, čas přihlášení, zařízení, ze kterého se uživatel připojuje.
- Monitoring povozu na síti – poskytuje detailní statistiky o síťové komunikaci, některý software dokonce dokáže tyto data analyzovat, a rozpoznat tak nežádoucí chování v síti.

- Virtualizace a monitoring jednotlivých zařízení – pomáhá odhalit napadené zařízení a díky virtualizaci je následně izolovat od zbytku sítě (využívá většinou behaviorální analýzy).
- Antivirový štít s heuristickou analýzou programů.
- Převedení odpovědnosti na subjekt třetí strany (pojištění).

Represivní opatření:

- Včasné přiznání chyby a informování uživatelů.
- Změna hesel uživatelů u všech využívaných služeb.
- Rychlá detekce narušení a identifikace místa vzniku.
- Izolace nebo úplná odstávka narušené části systému nebo zařízení.
- Zřízení 24 h podpory pro dotčené uživatele a řešení akutních problémů.
- Restart služeb a změna administrátorských hesel a jmen.
- Neprodleně provést veřejné prohlášení a přijmout odpovědnost za vzniklou škodu.

4.2 Krádež finanční hotovosti

Všichni spolupachatelé se po předcházející dohodě sešli okolo 22:00 na parkovišti před obchodním domem Billa za účelem spáchání trestného činu krádeže vloupáním. Odtud se následně přesunuli dvěma vozidly do sousední obce, kde měli vytipovaný objekt. S sebou měli veškeré potřebné vybavení, které potřebovali k realizaci jejich plánu. Po příjezdu k místu činu rozdal hlavní organizátor krádeže svým kolegům vysílačky. Dva z nich se vydali na předem dohodnutá místa hlídat provoz vozidel. Zbývající dva vyložili z auta žebřík a odnesli jej k objektu. Jeden z nich zůstal poblíž objektu, kde dával pozor. Hlavní pachatel poté odešel k prvnímu předem vytipovanému rozvaděči, kde pomocí páčidla odstranil plechové dvířka a nejspíš s použitím kleští a šroubováku přerušil telekomunikační kabely a účastnické přípojky. Poté se přesunul k druhému vytipovanému rozvaděči, kde stejným způsobem přerušil telekomunikační kabely. [31]

Následně se vrátil k objektu firmy, kde pomocí doneseného žebříku vylezl do prvního patra a páčidlem vypáčil okno do prostoru kuchyňky. Tady přišla na řadu rozbrušovačka, kterou použil k vyřezání uzamykacího mechanismu plechové skříně, kde byly dvě příruční pokladny, které následně vypáčil. Z těchto pokladen tak odcizil hotovost ve výši 11 252 €, 15 125 Kč a 203 400 HUF. Pak opustil objekt přivolal hlídajícího spolupachatele, pomocí vysílaček vyrozuměl zbývající dva. V autě měl připravené SPZ (státní poznávací značky)

s jinými evidenčními čísly motorových vozidel. Ty vyměnil za stávající SPZ a všichni opustili místo činu pomocí již zmíněných vozidel. [31]

Celková způsobená škoda

- **Ukradení hotovosti:** 11 252 €, 15 125 Kč a 203 400 HUF, dohromady **320 720 Kč**.
- **Poškození objektu firmy:** 21 291 Kč a 15 767 Kč, dohromady **37 063 Kč**.
- **Poškození rozvaděčů telekomunikační firmy**: **18 720 Kč**. [31]

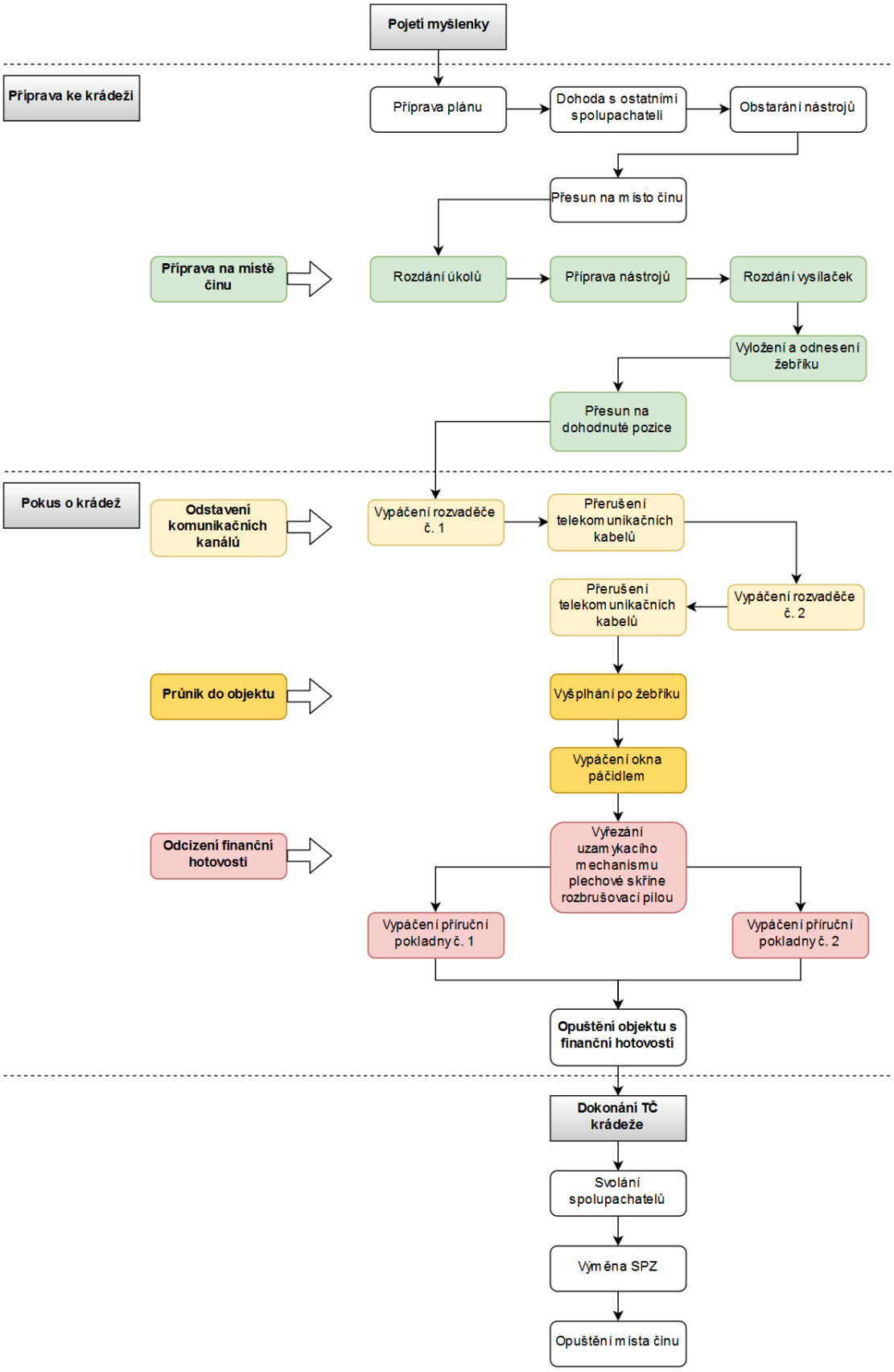
4.2.1 Bezpečnostní prostředí a využité zranitelnosti

Ze způsobu provedení je zřejmé, že pachatelé museli mít informace od některého ze zaměstnanců firmy, který jim poskytl informace o tom, kde se nachází finanční hotovost a ve kterých dnech ji tam bývá nejvíce. To byla zřejmě největší motivace ke spáchání činu. Co se zabezpečení objektu týče, tak zde byla zásadní chyba v nezabezpečených oknech u místnosti, ve které se nacházela plechová skříň s penězi. Na okně zcela chyběla mříž či jiný bezpečnostní prvek. Pachatelé také museli mít znalost zabezpečovacího systému objektu, který rovněž nebyl dostačující. Absence GSM modulu pro odeslání poplašné zprávy jinou cestou, než přes běžný komunikační kanál zapříčinila, že zlodějům stačilo přerušit rozvaděče na ulici k odstřižení PZTS od vnějšího okolí. Další chybou byla absence perimetrické ochrany objektu. Stačil by kamerový systém z vnější strany. Podíváme-li se na zabezpečení samotné místnosti, tak kromě chybějících mříží zde nejspíš také chyběly prvky PZTS, které by detekovaly narušení a spustily alespoň sirénu. Co se týče rozvaděčů, zde byly staré visací zámky, se kterými si hlavní pachatel bez problému poradil. Rozvaděče byly na sloupech veřejného osvětlení blízko u země, čímž se pachateli usnadnil přístup. [31]

4.2.2 Využité prostředky

- Auta – BMW a Seat
- Hliníkový vysouvací žebřík
- Vysílačky 3 ks
- Kleště
- Páčidlo
- Rozbrušovací pila
- Diamantové kotouče 4 ks
- Šroubovák
- SPZ 4 ks

4.2.3 Model krádeže



Obrázek 12 – Krádež finanční hotovosti [autor]

4.2.4 Návrh opatření

Firma

- Instalace okenních mříží, alespoň na budovy, které tvoří okraj areálu.
- Pořízení magnetického kontaktu do okna. Toto je nejméně nákladné řešení, které cenově vyjde v řádu stokorun.
- Pořízení trezoru zabudovaného do zdi, místo plechové skříně. Trezor by měl splňovat alespoň 1. bezpečnostní třídu, v ideálním případě 2. bezpečnostní třídu. Pořízení takové trezoru se pohybuje okolo 15 000 Kč – 20 000 Kč.
- Pořízení ústředny s GSM modulem (cena se pohybuje okolo 10 000 Kč) + montáž.
- Vybavení místnosti, kde se nachází finanční hotovost kombinovaným detektorem (detektor pohybu – PIR + detektor tříštění skla). Tato položka se pohybuje okolo 1 000 Kč – 2 000 Kč.
- Instalace kamerového systému CCTV v místnosti s uloženou finanční hotovostí a jako obvodovou ochranu, pro sledování dění okolo objektu.
- Uschování finanční hotovosti na hůře přístupném místě – v jiné místnosti v objektu, ideálně bez oken.
- Instalace seismického detektoru do plechové skříně. Zajistí detekci narušení, při řezání zámku.
- Pořízení senzoru hluku do místnosti s trezorem. Pokud je místnost zajištěna bude na základě intenzity a frekvence hluku detekovat narušení.
- Pojištění proti odcizení – to ovšem vyžaduje koupi trezoru alespoň 1. bezpečnostní třídy.
- Instalace kapsle s barvou, která exploduje po násilném otevření příruční pokladny.
- Fyzická ostraha objektu – v případě detekce narušení provádí obhlídku místa.
- Zvážit, jestli se firma nedokáže obejít bez velké finanční hotovosti.

Poskytovatel telefonních služeb

- Instalace magnetických kontaktů na rozvodné skříně.
- Tamper kontakt, pro zjištění sabotáže komunikačních kanálů.

4.3 Krádež měděných forem

Po předchozí dohodě pachatel A oslovil pachatele B, aby pro něj ukradl měděné formy ze skladu firmy, ve které pracoval. Pachatel B tedy neváhal a v nočních hodinách, když měl zrovna směnu, překonal nejspíše pomocí bumping metody čtyři bezpečnostní visací zámky a vnikl do skladu, kde pomocí nákladního vozidla odcizil nejméně 42 forem o celkové hmotnosti 5 300 Kg. Formy byly uskladněny v kontejneru na korbě nákladního vozidla. Výjezd z areálu firmy mu po předchozí domluvě zajistil pachatel C, pracovník bezpečnostní služby, který pracoval na vrátnici. Provedl fiktivní kontrolu a nechal pachatele B projet přes bránu. Poté se pachatel B telefonicky spojil s pachatelem A, že krádež zrealizoval a ukradenou bednu plnou forem složil na dohodnutém místě (na odstavné ploše u benzínové pumpy). Svým jednáním způsobili firmě škodu za 22 832 € (586 859 Kč). [32]

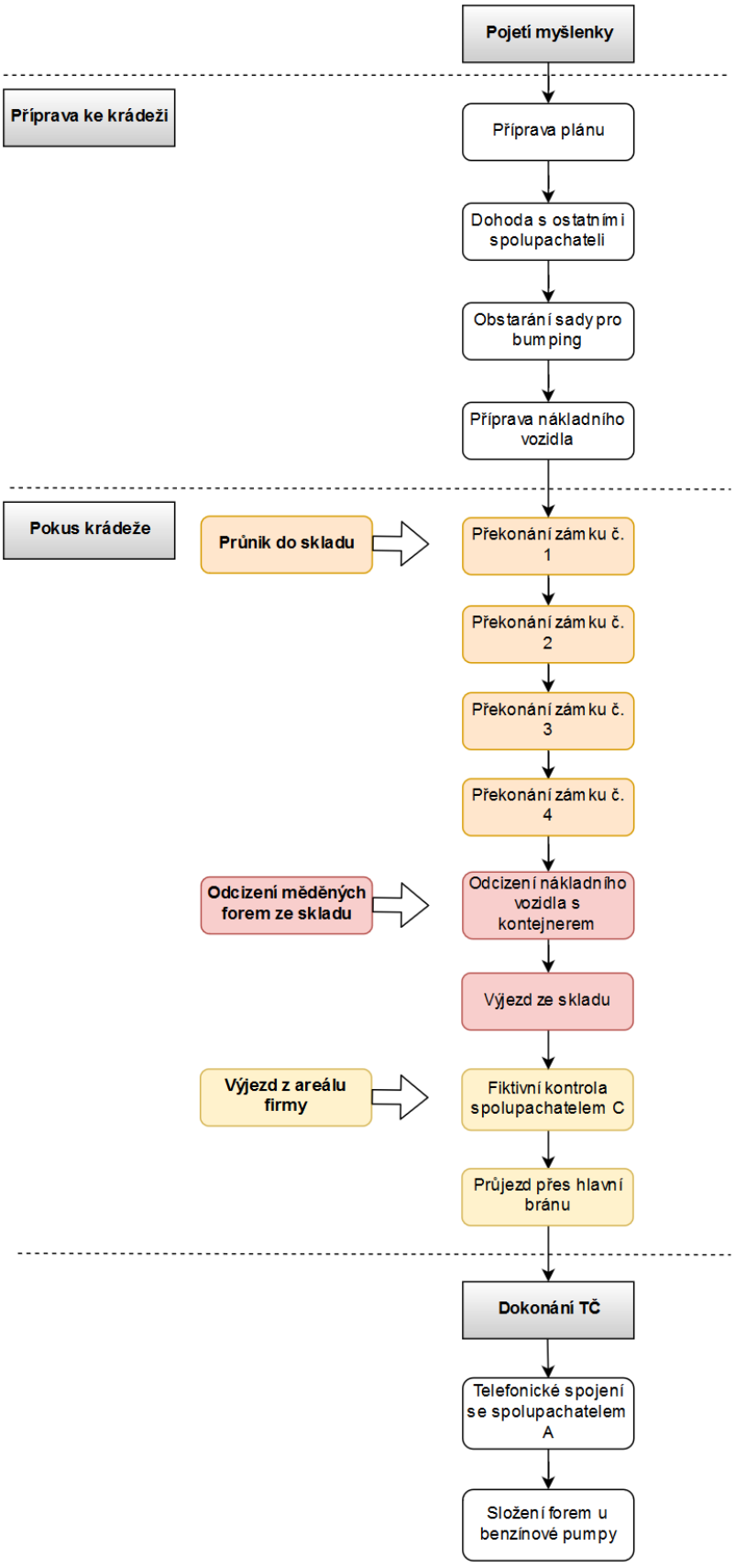
4.3.1 Bezpečnostní prostředí

V tomto případě byl největší problém v důvěře zaměstnavatele špatným lidem. Především tedy pracovníkovi bezpečnostní služby. Těmto problémům se do jisté míry dalo předejít prověrkou před samotným zaměstnáním daného pracovníka. Ovšem ani to nebývá často dostačující. Dalo se ale předejít odcizení samotných forem ze skladu, kde byly použity staré visací zámky, které šly překonat pomocí jednoduché bumping metody. Taktéž absence prvků zabezpečovacího systému ve skladu (kamer, čidel pohybu, magnetických kontaktů) dopomohla k snadnému průběhu krádeže. Další chybou bylo ponechání odemčeného nákladního vozidla ve skladu. Auto rovněž postrádalo jakýkoliv GPS systém pro sledování jeho trasy. Pachatel tedy mohl s autem odjet a přijet, aniž by si toho všimnul kdokoliv jiný než strážný u brány. [32]

4.3.2 Využité prostředky

- Dohoda
- Nákladní vozidlo
- Sada pro bumping

4.3.3 Model krádeže



Obrázek 13 – Krádež měděných forem [autor]

4.3.4 Návrh opatření

- Vstupní prověrka zaměstnanců.
- Školení zaměstnanců v oblasti bezpečnostní politiky společnosti a kontrola jejího dodržování.
- Instalace poplachového zabezpečovacího systému do skladových prostor. Kompletní systém vyjde na cca 30 000 Kč, záleží na velkosti zabezpečovaných prostor.
- Instalace infračervené závory u vstupních vrat do skladu a její napojení na ústřednu.
- Namontování GPS modulu do nákladních aut a instalace GPS dozoru pro vozový park firmy. Cena se pohybuje okolo 2 500 Kč za GPS modul + cca 200 Kč měsíční poplatek za sledování v ČR. Tento systém umožňuje vést GPS knihu jízd, takže lze snadno zjistit kdo, kdy a kam jel. Další výhodou je možnost plánování jízd a sledování, jestli vozidlo neopustilo areál v jinou než stanovenou dobu.
- Kontejner lze rovněž vybavit GPS modulem, pro jeho sledování.
- Nejsnazší opatření, které může firma realizovat je výměna starých zámků za nové, které budou splňovat alespoň 3. bezpečnostní třídu. To znamená, že tyto zámky jsou odolné proti bumpingu, vyhmatávání apod. Také jsou uznávány pojišťovnami. Cena jednoho takového zámku je 700 Kč a více.
- Další možností je fyzická ostraha, kdy prověření bezpečnostní pracovníci budou kontrolovat vnitřní i vnější prostory areálu, popřípadě je lze dovybavit cvičeným psem.
- Jednou z dalších možností je opatření kontejneru bezpečnostním prvkem a instalace brány pro detekci opuštění skladových prostor. Pro tyto účely se hojně využívají RF (radiofrekvenční) systémy, RFID systémy nebo také elektromagnetické systémy.
    - Pro účely zabezpečení skladu by byl nejvhodnější RFID systém s aktivním tagem. Takže funkčnost detekce by nezávisela na funkčnosti detekční brány. Další výhodou je možnost zápisu až 2 MB dat do tagu a možnost využít jej i pro jiné účely (například v logistice – po načtení tagu, lze zjistit podrobnosti o obsahu kontejneru, druhu zboží apod.).

4.4 Krádež duševního vlastnictví

Pachatelem je bývalý zaměstnanec strojírenské firmy, který využil získané důvěry, znalostí a starých přihlašovacích údajů k proniknutí do systému společnosti. Další z věcí, kterou při krádeži využil byla IP autorizace. Administrátor totiž nevymazal pachatelovy IP adresy, které byly autorizované k přístupu do poštovního serveru firmy. Dále se mu povedlo získat přístup do interního systému sdílení dokumentů. Díky získanému přístupu poté během zhruba dvou následujících let odcizil více než 100 PDF dokumentů obsahujících návrhy projektů, digitálně zpracovaná technická schémata, marketingové plány, struktury firemních poplatků a interní dokumenty. Celkově byla škoda ohodnocena na více než 500 000 USD (11 478 376 Kč). Jednalo se o úmyslný neoprávněný přístup k počítačové síti konkurenční společnost. [33]

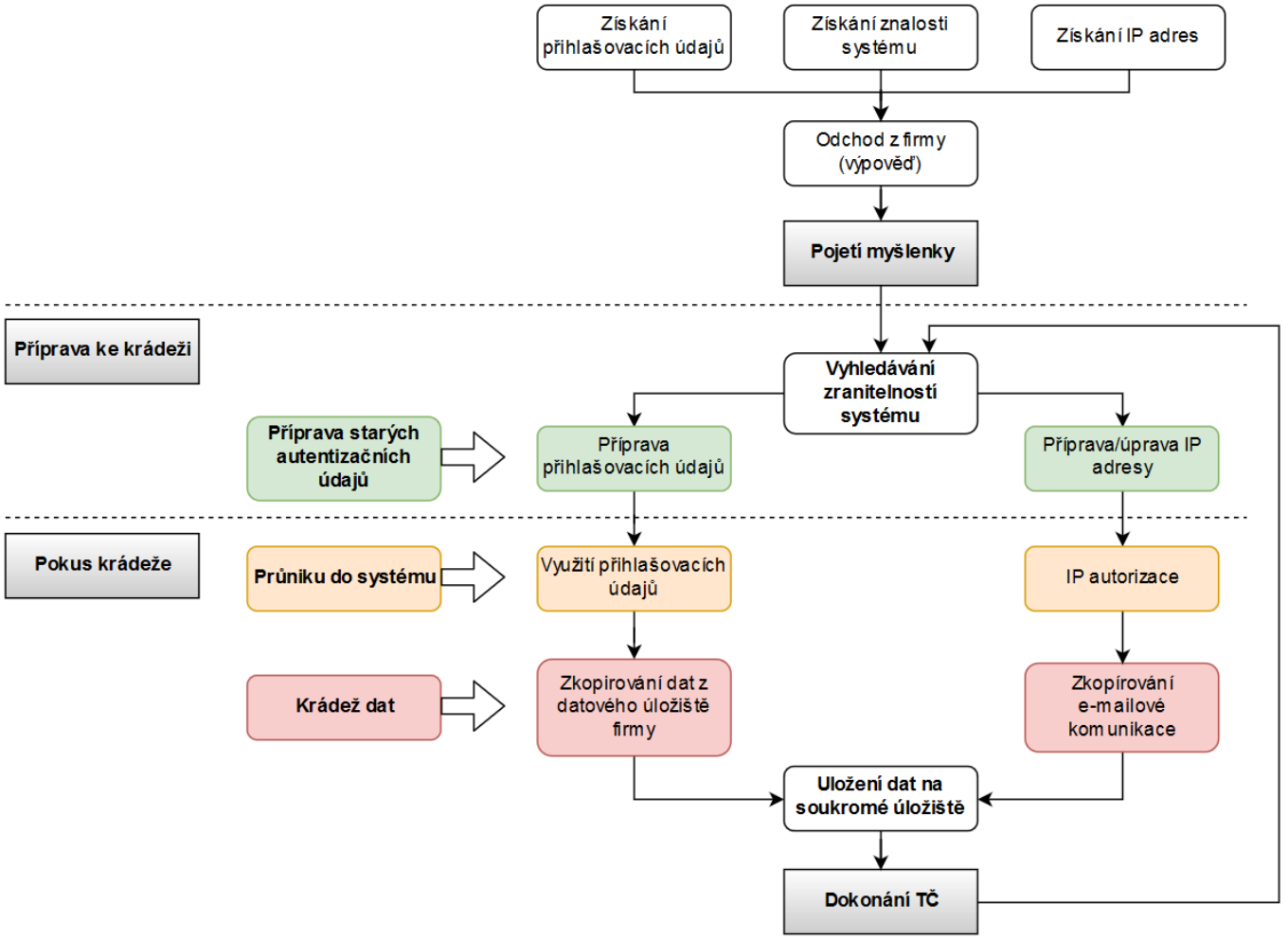
4.4.1 Bezpečnostní prostředí

V tomto případě bylo největší chybou to, že zaměstnavatel nevymazal účet zaměstnance po jeho propuštění. Také nebyly odstraněny jeho IP z autorizační databáze e-mailového serveru firmy. Tyto chyby a pachatelova znalost systému dopomohly k snadnému průniku do firemní sítě a následnému odcizení důležitých souborů. Nejhorší bylo, že pachatel se opakovaně v průběhu dvou let připojoval k této síti, aniž by jeho aktivita byla detekována. Z toho lze usuzovat, že dohled správce nebo používaný software byly zcela nedostačující. Co se poštovního serveru týče, zde byl problém v ukládání e-mailové komunikace všech zaměstnanců, ovšem před uložením nedocházelo k zašifrování. Stejně tak používaný firewall byl zastaralý a jeho poslední aktualizace více než rok stará. Soubory v datovém úložišti firmy rovněž nebyly šifrovány z důvodu rychlejšího přístupu ostatními zaměstnanci. [33]

4.4.2 Využité prostředky

- Staré přihlašovací údaje
- IP autorizace
- Znalost systému
- Důvěra firmy

4.4.3 Model krádeže



Obrázek 14 – Krádež duševního vlastnictví [autor]

4.4.4 Návrh opatření

- Důslednější bezpečnostní politika v oblasti kybernetické bezpečnosti a kontrola dodržování stanovených pravidel.
- Vymazání přihlašovacích údajů bývalých zaměstnanců a kontrola, zda byly po odchodu zaměstnance vymazány jeho přístupové údaje.
- Oddělit firemní síť od internetu.
- Použít nástroj pro sledování provozu na síti a kontrolu vzdálených připojení k síti.
- Šifrování e-mailové komunikace – VPN, https s certifikátem SSL/TLS ideálně SSL EV.
- Šifrování posílaných souborů (minimálně SHA-2 hash).
- Šifrování dat v datových úložištích firmy (minimálně SHA-2 hash).
- Pořízení nového HW i SW firewallu a provádět pravidelné aktualizace softwaru a obnovu hardwaru.
- Používání hardwarových klíčů pro připojení do datového úložiště firmy a jeho administraci.

5 ROZDÍLY MEZI KRÁDEŽÍ FYZICKOU A KYBERNETICKOU CESTOU

5.1 Osobnost pachatele

Kybernetická krádež

Většinou se jedná o vysoce kvalifikované osoby, které dobře rozumí dané problematice. Mívají přístup k informační a komunikační technice nebo disponují vlastní. Jejich metody na zakrývání stop a jejich činností bývají sofistikované a komplikované. Tyto osoby mají často vysoké rozumové schopnosti. Bývají to studenti vysokých škol, programátoři apod. Touto činností se relativně dobře uživí a díky prostředí ve kterém se vyskytují mají dostatečné technické i praktické zkušenosti. Ve studentském prostředí je i dostatečný zájem o jejich služby. Podle statistik Policie České republiky jsou dalšími pachateli v této oblasti podnikatelé, kteří prodávají či nakupují výpočetní techniku a při tom porušují autorská práva. Motivací u kybernetických krádeží nemusí být finanční obohacení, často jde o odhalení informací o nekalých praktikách osob nebo firem. Nebo to pachatel dělá jen pro zábavu nebo proto, že to prostě umí. [37]

V poslední době roste trend, kdy se pachatelé sjednocují do zločineckých gangů. Do páchání kybernetické kriminality se zapojují mladí lidé. Přesněji řečeno šéfové těchto gangů si kupují mladé hackery. Ti pak pod jejich vedením páchají zločiny. Díky nízkému věku nebývají trestně odpovědní, což komplikuje řešení takovýchto případů. Hackery se často stávají osoby s nízkým sociálním postavením, které nemají moc přátel, nejsou uznávány svým okolím, bývají konfliktní kvůli svému rozdílnému postavení v reálném světě oproti tomu virtuálnímu. Po ukončení školy a s rostoucím věkem hackera přicházejí existenční problémy, mění se životní priority apod. To bývají důvody k ukončení hackerství a změně životního stylu. [37]

Hackeři bývají přesvědčeni o své nepolapitelnosti a nedostižitelnosti, to se jim občas stane osudným. Pokud se ale podíváme na možnosti počítačových expertů, policie nebo administrátorů sítí jaké mají možnosti na jejich identifikaci. Nemůžeme se pak divit, že se tak cítí, jejich možnosti jsou totiž značně omezené a nedostačující. Ovšem hodně záleží na odborných znalost, kterými hacker disponuje.

Fyzická krádež

V tomto případě se často jedná o běžné lidi, kteří nedisponují výjimečnými rozumovými schopnostmi. V mnoha případech tomu bývá právě naopak. Stopy se nesnaží skrývat, spoléhají na to, že je malá pravděpodobnost jejich identifikace. Jejich metodami bývá často pouze hrubá síla nebo nástroje běžně využívané (šroubovák, kladivo, páčidlo). Často se jedná o lidi ze sociálně slabších poměrů nebo lidi v ekonomické tísni. U fyzických krádeží je motivací ve většině případů vlastní obohacení.

Pachatelé fyzických krádeží dále mohou být rozlišování na příležitostné a recidivující. Příležitostní pachatelé jednají na základě momentálního nápadu, impulzu. Při bližším pohledu lze vypozorovat, že podnětem bývá frustrace, emoční napětí apod. Naopak u recidivistů jde o zajištění jejich potřeb nebo je to jejich životní styl. Většinou se nebojí potrestání, proto své činy opakují.

Psychicky nemocní lidé se také stávají pachateli krádeží. Může se jednat o nejrůznější psychické poruchy, které podněcují pachatele k trestné činnosti. Jednou z nich je tzv. kleptomanie. V tomto případě je ale potřeba si dávat velký pozor při odlišování kleptomana od zloděje, protože pouze asi 1 % ze všech zlodějů jsou kleptomani.

5.2 Předmět krádeže

Níže jsou uvedeny předměty zájmu, na které se pachatelé nejčastěji zaměřují, jak v oblasti kyberprostoru, tak při fyzických krádežích.

Kybernetická krádež:

- know-how,
- data (firemní, osobní),
- duševní vlastnictví,
- finanční zdroje (kryptoměny, bezhotovostní finanční prostředky),
- identita (krádež přístupových údajů k nejrůznějším službám – sociální sítě, internetové bankovnictví, e-mail),
- informace (často se jedná o osobní údaje z databází firem),
- patenty,
- licence.

Fyzická krádež:

- finanční hotovost,
- elektronika,
- starožitnosti,
- potraviny (jídlo, alkohol),
- kola,
- motorová vozidla (auta, motorky),
- nářadí,
- materiál (z firemních skladových prostor, ze zahrad, chat),
- umělecké předměty,
- šperky,
- oblečení.

5.3 Využité prostředky

V této části jsou uvedeny příklady prostředků, které pachatelé nejčastěji využívají při realizaci krádeží kybernetickou nebo fyzickou cestou.

Kybernetická krádež:

- Man-in-the-middle (sniffing)
- SQL injection (databázové dotazy)
- Exploitace (využití zranitelností systému)
- Získané přihlašovací údaje
- IP autorizace
- Znalost systému
- Důvěra oběti
- Backdoor (zadní vrátka)
- Škodlivý software (keylloger, ransomware)

Fyzická krádež:

- Hrubá síla
- Kladivo
- Sekera
- Automobil

- Žebřík
- Vysílačky
- Kleště
- Páčidlo
- Rozbrušovací pila
- Šroubovák
- Dohoda
- Bumping
- Paklíč
- Lockpicking
- Převlek
- Pilka na železo

Tabulka 2 – Tabulka rozdílů mezi krádeží fyzickou a kybernetickou [38]

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	Riziko fyzického poranění	Bez rizika poranění
Zisk	cca 50 000 - 120 000 Kč	1 200 000 - 12 000 000 Kč
Pravděpodobnost dopadení	40 - 60 %	méně než 10 %
Pravděpodobnost odsouzení	více než 90 %	cca 5 %
Trest	5 - 6 let	2 - 4 roky

5.4 Klíčové momenty, které by mohly zvrátit průběh krádeže

V této podkapitole jsou uvedeny hlavní klíčové momenty pro každou z analyzovaných krádeží, které by v případě vhodných opatření mohly pomoci zmařit činnosti pachatele. Vždy je uveden klíčový moment, případně jeho jednotlivé činnosti a v závorce za ním opatření, které by mohlo pomoci snížit riziko jeho využití.

5.4.1 Krádež firemních dat (kybernetická krádež)

- Hledání zranitelností (opatření – bezpečnostní záplaty, aktualizace)
- Průnik do systému
    - Nezabezpečená komunikace (opatření – šifrovaná komunikace)
    - SQL injection (opatření – kontrola aktivit pomocí specializovaného SW nebo administrátorem)
    - Exploitace (opatření – pravidelná aktualizace SW i HW ochrany)
- Krádež dat
    - Odchycení nezašifrované komunikace (opatření – šifrovat veškerou komunikaci)
    - Získání dat z databáze (opatření – monitoring provozu na síti, šifrovat data)
    - Zkopírování dat z datového úložiště firmy (opatření – MFA – vícefaktorová autorizace, šifrovat data)

5.4.2 Krádež finanční hotovosti (fyzická krádež)

- Příprava na místě činu
    - Vyložení a přenesení žebříku (opatření – kamerový systém v okolí objektu a kontrola ochrankou)
- Odstavení komunikačních kanálů
    - Vypáčení rozvaděčů (opatření – magnetický kontakt pro detekci)
    - Přerušení komunikačních kabelů (opatření – tamper ochrana – vyvolá poplach po narušení komunikace)
- Průnik do objektu
    - Vypáčení okna (opatření – čidlo pohybu nebo magnetický kontakt)
- Odcizení finanční hotovosti
    - Vyřezání uzamykacího mechanismu plechové skříně (opatření – seismický detektor)
    - Vypáčení příručních pokladen (opatření – prasknutí kapsle s barvou – znehodnocení bankovek a označení pachatele)
- Opuštění objektu

5.4.3 Krádež měděných forem (fyzická krádež)

- Příprava ke krádeži
    - Příprava nákladního vozidla (opatření – zaznamenání podivného chování fyzickou ostrahou)
- Průnik do skladu
    - Překonání čtyřech zámků (opatření – pořízení lepších zámků s 3. bezpečnostní třídou a kamerového systému)
- Odcizení měděných forem ze skladu (opatření – detekční brána u vjezdu do skladu – detekce opuštění skladu s naloženým kontejnerem, který je vybaven bezpečnostním prvkem RF, RFID apod.)
- Výjezd z areálu firmy (opatření – použití jiných bezpečnostní opatření než jen fyzické ostrahy, například GPS sledovací modul v nákladním vozidle)

5.4.4 Krádež duševního vlastnictví (kybernetická krádež)

- Odchod z firmy (opatření – smazání přihlašovacích údajů a IP adres po odchodu zaměstnance z firmy)
- Pokus krádeže
    - Využití starých přihlašovacích údajů (opatření – detekce administrátorem nebo autorizačním softwarem)
    - Využití starých IP adres (opatření – detekce administrátorem nebo autorizačním softwarem)
- Krádež dat (opatření – šifrovat veškerou komunikaci a firemní data)

ZÁVĚR

Tato práce se zabývala fyzickou a kybernetickou krádeží. Oba tyto typy krádeží mají podobné fáze, kterými musí pachatel projít, aby dosáhl dokonání trestného činu (pojetí myšlenky, příprava, pokus, dokonání). Mají ovšem naprosto odlišné prostředí, ve kterém se odehrávají, pachatelé tudíž využívají i rozdílných prostředků a dovedností při jejich realizaci. Úkolem práce tedy bylo rozebrat bezpečnostní prostředí (popsat klíčové prvky) a znázornit jednotlivé kroky pachatelů pomocí grafického modelu, aby se zjednodušila analýza vybraných zločinů a určení klíčových momentů. Na základě takto určených klíčových momentů se poté navrhovala opatření pro odvrácení budoucích potenciálních hrozeb (pachatelů) a určovaly rozdíly mezi fyzickou a kybernetickou krádeží. Hlavní rozdíly byly nalezeny především v osobnostech pachatelů, jejich předmětu zájmu a využívaných prostředcích.

Úvodní kapitola práce se věnuje jednotlivým druhům bezpečnosti, ve kterých se odehrává majetková trestná činnost. Jakým způsob v nich funguje systém bezpečnosti a co se v dané oblasti ochraňuje.

Další kapitola se zaměřuje na bezpečnostní prostředí fyzické a kybernetické krádeže. Čím se tyto prostředí vyznačují, co do nich spadá a jakou hrají roli v oblasti krádeže majetku. Následně se práce zabývá sociálními a právními aspekty krádeže. Jak chápat krádež z pohledu zákona, jaké jsou nejdůležitější zákony související s krádeží majetku a v neposlední řadě také její skutková podstata. Jsou zde popsány objektivní a subjektivní stránky a následně jejich faktory.

Poslední kapitola teoretické části pojednává o vývojových stádiích krádeží, kdy je pachatelovo jednání beztrestné a kdy už naopak překročil hranice zákona. Popisuje se zde typologie krádeží, tedy podle jakých kritérií lze krádeže rozdělit. V závěru kapitoly jsou uvedeny příklady metod realizace krádeží, metody používané při krádeži fyzickou cestou a kybernetickou. Úplný závěr teoretické části tvoří model krádeže majetku, který má pomoci lépe pochopit danou problematiku. Také je následně využit v praktické části při analýze zločinů.

Praktická část práce má za úkol analyzovat vybrané zločiny. Jedná se o krádeže provedené jak fyzickou cestou, tak také v kybernetickém prostoru. Je zde podrobně popsán průběh samotné krádeže a následně bezpečnostní prostředí a zranitelnosti, kterých pachatel využil k odcizení majetku. Všechny zločiny se týkají krádeží ve firmách, a to z toho důvodu, že v poslední se s touto problematikou setkáváme čím dál častěji. Na konci každé analýzy jsou uvedeny návrhy na opatření a doporučení pro zlepšení zabezpečení referenčních objektů.

Poslední kapitola této práce uvádí rozdíly mezi krádeží fyzickou a kybernetickou. Zaměřuje se především na osobnost pachatel a klíčové momenty jednotlivých krádeží spolu s vhodnými opatřeními. Také je zde uvedena stručná tabulka rozdílů, kde se porovnává loupežné přepadení a kybernetický útok.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN EN ISO/IEC 27001. I*nformační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Ženeva: Mezinárodní elektrotechnická komise, 2014. 28 p.

[2] *Národní bezpečnostní úřad* [online]. Praha: Národní bezpečnostní úřad [cit. 15. 02. 2019]. Dostupné z: https://www.nbu.cz/cs/

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.

[4] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III.* 1. vyd. Zlín: VeRBuM, 2013. 456 s. ISBN 9788087500354.

[5] HALOUZKA, Kamil. *Fyzická bezpečnost: Perimetrické zabezpečovací systémy* [online]. In: Operační program Vzdělávání pro konkurenceschopnost, s. 55 [cit. 01. 03. 2019]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18075/mod_resource/content/2/10_Perimetrick%C3%A9%20zabezpe%C4%8Dovac%C3%AD%20syst%C3%A9my.pdf

[6] *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu* [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 25. 02. 2019]. Dostupné z: http://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

[7] MAREŠ, Miroslav. Ekonomická bezpečnost. In Petr Zeman. Česká bezpečnostní terminologie. Výklad základních pojmů. 1. vyd. Brno: Masarykova univerzita v Brně, ÚSS VA v Brně, 2002. s. 28-31, 4 s. Sborníky 11. ISBN 80-210-3037-2.

[8] LUKÁŠ, Luděk. *Teorie bezpečnosti I.* 1. Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.

[9] *Bezpečnostní strategie České republiky*. 2015. Praha: Ministerstvo zahraničních věcí České republiky, 2015. ISBN 978-80-7441-005-5.

[10] ČSN EN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Ženeva: ISO/IEC JTC 1 Informační technologie, subkomise SC 27 IT Bezpečnostní techniky, 2013. 73 p.

[11] KOLOUCH, Jan. *Cybercrime*. 1. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[12] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 1. 3. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p2-1-a

[13] Jednotlivé druhy kyberkriminality - Policie České republiky. *Policie České republiky* [online]. © 2019 Policie ČR, [cit. 01. 03. 2019]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[14] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

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

[16] Surface Web, Deep Web, Dark Web -- What's the Difference?. *CambiaResearch* [online]. 2016 [cit. 10. 03. 2019]. Dostupné z: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

[17] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 12. 3. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[18] CHMELÍK, Jan, František NOVOTNÝ a Simona STOČESOVÁ. *Trestní právo hmotné: obecná část*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-583-8.

[19] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 6. aktualizované a doplněné vydání. Praha: Leges, 2017. Student (Leges). ISBN 978-80-7502-236-3.

[20] Vývojová stadia trestné činnosti. *IUS-wiki* [online]. 2016 [cit. 15. 03. 2019]. Dostupné z: http://www.ius-wiki.eu/trestni-pravo/pfuk/trest/zkouska/otazka-a-17

[21] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.

[22] Nejčastější nástroje a metody zlodějů. Víte, jak vás vykradou?. *Frýdecko-Místecko.cz* [online]. [cit. 01. 05. 2019]. Dostupné z: http://www.nasefrydeckomistecko.cz/zpravy-31/nejcastejsi-nastroje-a-metody-zlodeju-vite-jak-vas-vykradou

[23] Co je bumping. *Jakov* [online]. Praha: Zámečnictví JAKOV A-Z [cit. 2019-05-08]. Dostupné z: http://www.jakov.cz/co-je-bumping

[24] *Wikimedia* [online]. [cit. 01. 05. 2019]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/1/19/Tecnica_Bumping_%28Small%29.jpg

[25] *Lockpickers.cz* [online]. Praha, 2018 [cit. 01. 05. 2019]. Dostupné z: http://www.lockpickers.cz

[26] *Lockpicking Forensics* [online]. Praha, 2017. Dostupné také z: http://www.lockpickingforensics.com

[27] *Selfdefenseproducts: Scorpion Lock Pick Gun* [online]. [cit. 02. 05. 2019]. Dostupné z: https://cdn10.bigcommerce.com/s-pecmny2vd/products/2231/images/4504/e1392c13-dbf6-47d8-8231-8424a58c61f5__23135.1483033855.1280.1280.jpg?c=2

[28] *„Kudy a přes co" se dostávají pachatelé krádeží vloupáním do objektů* [online]. In: . Praha: MV ČR, 2014 [cit. 05. 05. 2019]. Dostupné z: http://www.obeccervenyujezd.cz/assets/File.ashx?id_org=2115&id_dokumenty=1776

[29] MCQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. ISBN 978-0-313-33974-5.

[30] HOLT, Thomas J., Adam M. BOSSLER a Kathryn C. SEIGFRIED-SPELLAR. *Cybercrime and digital forensics: an introduction*. London: Routledge, 2015. ISBN 978-1-138-02130-3.

[31] *Policie České Republiky* [online]. Policie ČR, ©2019 [cit. 02. 05. 2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[32] CLANCY, Thomas K. *Cyber crime and digital evidence: materials and cases*. Third edition. Durham, NC: Carolina Academic Press, [2019]. ISBN 9781531009618.

[33] Publikace – Bezpečnostní incidenty. *Národní centrum kybernetické bezpečnosti* [online]. Brno, 2016 [cit. 28. 04. 2019]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/publikace/2512-bezpecnostni-incidenty-prosinec-2016/

[34] Rozhodnutie. *Ministerstvo spravodlivosti SR* [online]. 2017 [cit. 29. 04. 2019]. Dostupné z: https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/1398ab1d-22af-4788-94eb-7beb47440901%3A4e2ad125-9cb6-46c9-bbc4-0a8509959d9a

[35] Rozhodnutie. *Ministerstvo spravodlivosti SR* [online]. 2017 [cit. 30. 04. 2019]. Dostupné z: https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/4173719d-a4a3-4c5d-9cbc-c9bd7d7b6372%3A3bdc23c4-1330-40b5-9aea-aff138feb4be

[36] LORD, Nate. "Insider" IP Theft Suit Ends in Prison Time, Hefty Fines. *Digital Guardian* [online]. 2017 [cit. 03. 05. 2019]. Dostupné z: https://digitalguardian.com/blog/insider-ip-theft-suit-ends-prison-time-hefty-fines

[37] POŽÁR, Josef. Kybernetická kriminalita v organizaci. Praha: Policejní akademie České republiky, 2014.

[38] POŽÁR, Josef. *Některé aspekty kybernetické kriminality* [online]. Praha: Policejní akademie české republiky, 2011 [cit. 04. 05. 2019]. Dostupné z: https://www.cybersecurity.cz/data/Pozar.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
HW	Hardware
SW	Software
PIR	Pasivní infračervené detektory
MW	Mikrovlnné detektory
TČ	Trestný čin/trestná činnost
SPZ	Státní poznávací značka
PZTS	Poplachový zabezpečovací a tísňový systém
CCTV	Closed Circuit Television (uzavřený televizní okruh)
PIR	Pasivní infračervené čidlo
RF	Radiofrekvenční
RFID	Rádio Frekvenční Identifikace

SEZNAM OBRÁZKŮ

SEZNAM TABULEK