Bezpečnost informací veřejných i soukromých subjektů

Radomír Malík

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Radomír Malík**
Osobní číslo:	**L18289**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnost informací veřejných i soukromých subjektů**

Zásady pro vypracování

1. Zpracujte rešerši současného stavu oblasti bezpečnosti informací.
2. Seznamte se se závaznými i doporučujícími normami veřejných subjektů v oblasti bezpečnosti informací.
3. Seznamte se se závaznými i doporučujícími normami soukromých subjektů v oblasti bezpečnosti informací.
4. Proveďte komparaci závazných a doporučujících norem veřejných a soukromých subjektů v oblasti bezpečnosti informací.

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

Seznam doporučené literatury:

1. BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4307-3.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
3. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉPRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 12. května 2021

Jméno a příjmení studenta: Radomír Malík

…….
Podpis studenta

ABSTRAKT

Tato práce se věnuje bezpečnosti informací veřejných i soukromých subjektů. V úvodu teoretické části představuje obraz současné situace v oblasti bezpečnosti informací současné digitální společnosti. V další části je zobrazen přehled normalizačních institucí dle oboru působnosti, na který navazuje přehled závazných a doporučených norem regulujících bezpečnost informací veřejných a soukromých subjektů. Praktická část zahajuje komparací vybraných oblastí, které jsou regulovány jak závaznými tak doporučenými normami. Za účelem zvýšení bezpečnosti informací a orientace v kyberprostoru pokračuje několika vybranými technikami na uživatelské úrovni, které zahrnují práci s programy jako Recuva nebo VeraCrypt.

Klíčová slova: bezpečnost informací, informace, informační a komunikační technologie, soukromé subjekty, veřejné subjekty

ABSTRACT

This work deals with the security of information of public and private entities. The introduction to the theoretical part presents a picture of the current situation in the field of information security of today's digital society. The next part shows an overview of standardization institutions by field of activity, which is followed by an overview of binding and recommended standards governing the security of information of public and private entities. The practical part begins with a comparison of selected areas, which are regulated by both binding and recommended standards. In order to increase information security and orientation in cyberspace, it continues with several selected techniques at the user level, which include working with programs such as Recuva or VeraCrypt.

Keywords: information security, information, information and communication technologies, private entities, public entities

Poděkování

Tímto bych chtěl poděkovat svému nejbližšímu okolí a to konkrétně své manželce a dětem za trpělivost, kterou měli a stále mají od začátku mého studia a rovněž za to, že mi vytváří prostředí a podmínky pro práci na školních projektech, i když to mnohdy znamená odloučení otce od rodiny. Dále můj dík patří vedoucímu bakalářské práce Ing. Petru Svobodovi Ph.D. za odborné rady, lidský přístup a pomoc s nasměrováním při tvorbě této bakalářské práce.

„Nebojím se člověka, který trénoval 10 000 kopů, ale bojím se člověka, který trénoval jeden kop 10 000krát.“

Bruce Lee

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

V Uherském Hradišti Radomír Malík

OBSAH

ÚVOD

Bezpečnost informací je v současné moderní a digitální společnosti klíčovou a neustále aktuální disciplínou. Tato oblast je v současné době jednou z nejvíce proměnlivých a to z mnoha důvodů. Mezi příklady by se dal zařadit rychlý a neustálý vývoj v oblasti informačních a komunikačních technologií, navyšování počtu organizací využívajících počítačové systémy a moderní komunikační prostředky a s tím spojené navyšování informací potažmo informačních aktiv, které jsou prostřednictvím těchto moderních technologií ukládány a spravovány. S nárůstem množství informací spravovaných informačními technologiemi roste i hrozba jejich zneužití prostřednictvím kybernetické kriminality. Informace v dnešní době mohou mít velmi vysokou hodnotu srovnatelnou s jinými cennými komoditami a proto je jejich ochrana stejně důležitá.

Hlavním cílem této bakalářské práce je sumarizace problematiky týkající se bezpečnosti informací veřejných a soukromých subjektů v České republice. Tento primární cíl bude naplňován pomocí dílčích cílů, jimiž jsou zamyšlení se nad rozdělením subjektů a škálou doporučených postupů v oblasti bezpečnosti informací v prostředí České republiky.

Dalším dílčím cílem je samotná identifikace závazných a doporučujících dokumentů, které regulují oblast bezpečnosti informací jak veřejných tak soukromých subjektů. Na tento přehled identifikovaných dokumentů navazuje další dílčí cíl, který zahrnuje provedení komparace doporučení ve zvolených oblastech vybraného závazného a doporučeného dokumentu – normy, jenž slouží pro lepší pochopení diference mezi závaznými a doporučenými dokumenty – normami.

Posledním dílčím cílem je specifikování vybraných praktických doporučení a popis vybraných funkcionalit na uživatelské úrovni, jenž zahrnuje vybrané volně dostupné programy.

V úvodu této práce byla využita metoda analýzy, která analyzuje současný stav problematiky bezpečnosti informací v České republice. Následuje syntéza získaných poznatků. Při analyzování obsahu jednotlivých norem bylo využito metod dedukce a indukce, kdy byl na základě zjištěných poznatků krátce uveden jejich význam ve vztahu k bezpečnosti informací. Další využitou metodou pak byla komparace, která je zaměřená na porovnání jednotlivých oblastí ze strany prováděcího předpisu zákona o kybernetické bezpečnosti a normy z řady ISMS.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ NÁZVOSLOVÍ A POJMY

V této kapitole jsou autorem představeny specifické oblasti a samotné pojmy, jejichž vysvětlení a specifikace má zásadní význam pro pochopení celkového obsahu této práce.

1.1 Bezpečnost informací

V současné době není rozvoj digitální společnosti založen přímo na hospodářském rozvoji, ale především na rozvoji IT, do čehož lze zahrnout stále větší množství nově připojených uživatelů internetu či jejich připojení k samotným aplikacím jako takovým. V neposlední řadě hraje velmi významnou roli samotný zisk informací a dat od uživatelů. Změny zmíněné v souvislosti s vývojem IT probíhají ve více rovinách a to jak v ekonomické tak v sociální a jsou jednou z příčin kyberkriminality. Samotné využívání informačních a komunikačních technologií má i temnou stránku. V tomto případě se jedná o obrovský a dynamický nárůst nového druhu trestné činnosti, kterou lze souhrnně označit jako kyberkriminalitu a která může vést k ohrožení a porušování zájmů společnosti. Lze zpozorovat v celosvětovém měřítku snahu, která je schopna reagovat na tento dynamický fenomén současnosti a to jak z právní stránky, tak z bezpečnostní úrovně, přičemž jde o společný cíl v podobě přijetí adekvátních opatření (Kolouch, 2016).

Když lidé používají informační systémy, dochází k chybám. Bez ohledu na příčinu mohou i neškodné chyby způsobit rozsáhlé škody. Například jednoduchá chyba klávesnice může způsobit celosvětové výpadky internetu (Whitman, Mattord, ©2012).
Lidé představují klíčový prvek jakékoliv bezpečnosti a to i v případě kybernetické bezpečnosti, kdy se jejich role ještě umocňuje a typicky jsou to právě lidé, kdo je oním nejslabším prvkem a současně nejčastějším cílem útočníků (Kolouch, et al., 2019).

Mnoho IT odborníků věří, že pokud síť obsahuje jakýkoli druh citlivých informací, všichni uživatelé musí být pravidelně certifikováni v základech kybernetické bezpečnosti. Myšlenkou je certifikace veškerého personálu od juniorského personálu až po vedení (Singer, Friedman, 2014).

Informační bezpečnost má za úkol zajistit odpovídající ochranu všech údajů a informací organizace ve všech formách. Jedna ze součástí celkového informačního systému organizace je bezpečnost automatizovaného informačního systému, neméně důležitou částí

je i část neautomatizovaná, která představuje písemné dokumenty, rukou psané poznámky, telefonické hovory, obchodní jednání, faxové zprávy, poštovní zásilky apod. Hlavním a základním krokem v rámci budování informační bezpečnosti organizace je provedení klasifikace informací, která definuje potřebnost, důležitost a stupeň ochrany jednotlivých informací. S informacemi bude následně nakládáno takovým způsobem, který odpovídá jejich klasifikaci (Smejkal, Rais, 2006).

Rozšiřování technologií a pohlížení na informace jako na zboží mění jejich roli na zdroj, který je svým významem rovnocenný tradičním ekonomickým zdrojů, kterými jsou například půda, práce či kapitál (Smejkal, Rais, 2013).

Mezi klíčový princip jádra informační bezpečnosti lze zařadit tzv. triádu "**CIA**". Tento nástroj pomáhá odborníkům na informační bezpečnost přemýšlet o tom, jak nejlépe chránit organizační data.

Význam zkratky CIA

- **C**onfidentiality (důvěrnost) Má co do činění s tím, zda jsou informace utajovány nebo soukromé. Měly by být použity mechanismy, jako je šifrování, které zneplatní data, pokud k nim bude přistupováno neoprávněným způsobem.
- **I**ntegrity (integrita) Souvisí to s tím, zda jsou informace udržovány přesné. Informace by neměly být upravovány neoprávněným způsobem a měla by být zavedena ochranná opatření umožňující zjistitelné a včasné neoprávněné změny.
- **A**vailability (dostupnost) Souvisí to se zajištěním dostupnosti informací, když jsou potřeba. Této kontroly lze dosáhnout implementací nástrojů od zálohování baterie v datovém centru po síť distribuce obsahu v cloudu (Death, 2017, s. 13).

Význam informační bezpečnosti

Protože se počítačové systémy nyní staly nedílnou součástí každodenního fungování podniků, organizací, vlád a jednotlivců, naučili jsme se vkládat do těchto systémů obrovskou důvěru. Díky tomu jsme do nich umístili neuvěřitelně důležité a cenné informace. Historie ukazuje, že hodnotné věci budou pro zločince vždy terčem. Počítačová kriminalita se nijak neliší (Death, 2017).

Dobrá úroveň a kvalita informační bezpečnosti jsou důležité jak z hlediska ochrany práv a zájmů občanů, subjektů komerční i nekomerční sféry, tak i z hlediska ochrany zájmů státu a zabezpečení jeho funkcí orgány veřejné správy a jejího obrazu na veřejnosti.

Nedostatečně zajištěná informační bezpečnost může ohrozit bezpečnost a hospodářské zájmy státu, privátního sektoru i občanů a oslabit důvěryhodnost jednotlivých subjektů. Vzniklé škody a ztráty informací mohou vyvolat další práci a náklady, které by nevznikly v případě dostatečné preventivní ochrany těchto informací (NSIB ČR, 2005).

Implementace informační bezpečnosti

Implementace informační bezpečnosti v organizaci musí někde začít a nemůže k ní dojít přes noc. Zabezpečení informačních prostředků je ve skutečnosti přírůstkový proces, který vyžaduje koordinaci, čas a trpělivost. Zabezpečení informací může začínat jako základní efekt, ve kterém správci systémů pomáhají zlepšovat zabezpečení svých systémů. To se často označuje jako přístup „zdola nahoru“. Klíčovou výhodou přístupu zdola nahoru je technická odbornost jednotlivých správců. Tito administrátoři mají každodenní práci s informačními systémy a mají hluboké znalosti, které mohou výrazně zlepšit vývoj informačního bezpečnostního systému. Znají a chápou hrozby pro jejich systémy a mechanismy potřebné k jejich úspěšné ochraně. I při nejlepším plánování a implementaci je nemožné dosáhnout dokonalé bezpečnosti informací. Zdůrazněme, že potřeba vyváženosti bezpečnosti a přístupu je klíčová. Informační bezpečnost nemůže být absolutní: je to proces, nikoli cíl. Je možné zpřístupnit systém komukoli, kdekoli a kdykoli jakýmkoli způsobem. Takový neomezený přístup však představuje nebezpečí pro bezpečnost informací. Naproti tomu zcela bezpečný informační systém by nikomu neumožňoval přístup. Aby bylo možné dosáhnout rovnováhy, to znamená provozovat informační systém, který uspokojí uživatele i bezpečnostního profesionála, úroveň zabezpečení musí umožňovat rezonanční přístup a přitom chránit před hrozbami (Whitman, Mattord, ©2012).

Při rozhodování ohledně zajištění bezpečnosti informací je nutné vzít do úvahy následující:

- Vzájemné propojování různých odvětví života pomocí informačních technologií.
- Rozmach informačních technologií, vzhledem k faktu, že stále více informací je předáváno v digitální formě a většina důležitých dat je ukládána v informačních systémech a v případě výpadku by byla narušena akceschopnost infrastruktur (Luděk a kol., 2013).

1.2 Informační společnost

Data a informace představují v současné době obrovský politický a ekonomický potenciál. Informace a jejich obsah mohou mít mnohdy vliv na rozhodnutí o samotném bytí či nebytí jednotlivců nebo dokonce i firem, ale co je zásadní, ve své podstatě jsou schopny ovlivnit celosvětový vývoj. Nutno podotknout, že narůstající závislost na ICT a narůstající množství dat o nás, které tyto technologie budou sbírat, nás činí zranitelnějšími. Případná rezignace na využívání ICT by pro dotčeného jedince či organizaci znamenala izolaci od zbytku společnosti a v řadě případů by mohla vést až k nemožnosti fungování ve společnosti, která tyto technologie využívá, případně jejich využívání vyžaduje. Proto je tedy téměř nemožné, chceme-li v současné společnosti žít a využívat její výhody, abychom se oprostili od využívání ICT (Kolouch, et al., 2019).

Informační společnost by se také dala popsat jako společnost schopná využívat a využívající informační a komunikační technologie. Základním znakem je neustálá výměna znalostí a informací a práce s nimi za předpokladu schopnosti jim rozumět. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity (Jirásek, Novák, Požár, 2015).

Informace jsou dnes co do významu jedním z klíčových zdrojů úspěchu podniku (či jakéhokoliv subjektu) a dnes je řadíme mezi základní zdroje stejně jako zaměstnance či hmotný majetek (Smejkal, Rais, 2006).

V budované informační společnosti se zvyšuje význam přímého elektronického přístupu k informacím a službám, poskytovaným jak subjekty veřejné správy, tak informačními systémy subjektů komerční i nekomerční sféry. Z hlediska ochrany informací je důležitý bezpečný bezporuchový provoz informačních a komunikačních systémů, stejně jako i správnost, spolehlivost, dostupnost, integrita, důvěrnost a aktuálnost informací, které se v nich vyskytují (NSIB ČR, 2005).

Jednou z nepřízní digitální informační společnosti, která zahrnuje spíše sociální oblast je samotná závislost na ICT. Tato závislost nese název „netolismus“ a vede k nadměrnému užívání ICT (videohry, mobily, sociální sítě, televize), přičemž se po odepření mohou objevit i abstinenční příznaky jako neklid, nervozita, případně pokles pracovních výsledků a zhoršení rodinných vztahů (Fukárková, 2019).

1.3 eGovernment

Jedna z definic uvádí, že eGovernment je využívání informačních technologií veřejnými institucemi za účelem zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi s cílem zvyšování efektivity vnitřního fungování a poskytování dostupných, rychlých a kvalitních informačních služeb. Do eGovernmentu je zapotřebí zahrnout také legislativní prostředí, které umožňuje výměnu informací mezi občany, orgány veřejné zprávy a komerčními subjekty ve všech možných komunikačních směrech.

Činnosti eGovernmentu v České republice:

- Informační systém veřejné správy, open source.
- Elektronická komunikace.
- Ochrana osobních údajů, implementace biometrických údajů.
- Elektronický podpis, elektronická značka.
- Elektronické správní řízení, elektronické podání, e-podatelny.
- Dlouhodobé uchovávání elektronických dokumentů.
- Konverze dokumentů.
- Registry veřejné správy.
- Bezpečnost a ochrana utajovaných informací.
- Elektronické veřejné zakázky (Lindovský a kol., 2008).

1.4 Globalizace a její vliv na informační systémy

Globalizace může z jedné strany přinášet příležitosti k dalšímu růstu, zároveň však i hrozbu v podobě neudržitelnosti vhodných podmínek pro život na Zemi. Tato širší tematika je plně relevantní s veškerými IS, protože nelze opomenout, že samotná oblast ICT je v současnosti závislá na široké škále klíčových prvků, které jsou mimo jiné využívány např. v bateriích notebooků či mobilních telefonů, přičemž nutno říci, že zásoby těchto prvků na Zemi nejsou nekonečné. Závislost veškerých ICT na elektrické energii se může v budoucnu potýkat s problémem vzhledem k faktu, že v budoucnosti může dojít k vyčerpání fosilních paliv a nutnosti hledání alternativního zdroje energie (Basl, Blažíček, 2012).

1.5 Zákon a politika v oblasti informačních technologií

V rámci organizace pomáhají odborníci na zabezpečení informací udržovat bezpečnost při budování a prosazování zásad. Tyto zásady a pokyny, které popisují přijatelné a nepřijatelné chování zaměstnanců na pracovišti, fungují jako organizační zákony, doplněné o sankce, soudní praktiky a sankce vyžadující dodržování předpisů. Protože tyto zásady fungují jako zákony, musí být vytvořeny a prováděny se stejnou péčí, aby bylo zajištěno, že jsou úplné, vhodné a spravedlivě aplikovatelné na všechny pracovníky. Rozdíl mezi politikou a zákonem však spočívá v tom, že neznalost politiky je přijatelnou obranou. Aby se politika stala vymahatelnou, musí splňovat následujících pět kritérií.

- **Šíření (distribuce)** Organizace musí být schopna prokázat, že příslušná politika byla snadno k dispozici pro kontrolu zaměstnancem. Mezi běžné techniky šíření patří tištěná kopie a elektronická distribuce.
- **Revize (čtení)** Organizace musí být schopna prokázat, že šířila dokument ve srozumitelné formě včetně verzí pro negramotné, neanglické čtení a zaměstnance se sníženou schopností čtení. Mezi běžné techniky patří záznamy zásad v angličtině a alternativních jazycích.
- **Pochopení (porozumění)** Organizace musí být schopna prokázat, že zaměstnanec porozuměl požadavkům a obsahu politiky. Mezi běžné techniky patří kvízy a další hodnocení.
- **Shoda (dohoda)** Organizace musí být schopna prokázat, že zaměstnanec souhlasil s dodržováním zásad prostřednictvím jednání nebo potvrzení. Mezi běžné techniky patří přihlašovací banner, který vyžaduje konkrétní akci (kliknutí myší nebo stisknutí klávesy) k potvrzení souhlasu, nebo ojedinělý dokument jasně označující, že zaměstnanec tyto zásady přečetl, porozuměl jim a souhlasil s nimi.
- **Jednotné vymáhání** Organizace musí být schopna prokázat, že zásady byly prosazovány jednotně, bez ohledu na status nebo přiřazení zaměstnance.

Pouze tehdy, jsou-li splněny všechny tyto podmínky, může organizace potrestat zaměstnance, kteří zásady porušují, aniž by se obávali legální odplaty (Whitman, Mattord, ©2012, s. 89-90).

1.6 Úniky informací

Tato práce se zabývá především bezpečností potažmo ochranou informací, ovšem tato část se vydá krátce opačným směrem a zaměří se na úniky informací. Mějme totiž na paměti, že kromě nežádoucího úniku informací může existovat i únik žádoucí, který je řízený a máme jej pod kontrolou a který nám může přinést i určitý užitek.

Obecně lze rozdělit jednotlivé tipy úniků následovně:

- Cílený a načasovaný únik vybraných informací do médií, který je naaranžován tak, aby vypadal jako náhodný a nechtěný v rámci legální zpravodajské hry. Tento specifický „modus operandi“ se využívá pouze v důležitých případech.
- Vybrané informace jsou diskrétně a draze poskytnuty kriminálním klientům nebo subjektům zpravodajského zájmu (aniž by byly zveřejňovány). Jedná se zde o nebezpečný kriminální delikt, který bývá obvykle dále využit k vydírání nebo jiným druhům trestné činnosti.
- Vybrané informace jsou cíleně a za úplatu poskytovány médiím ve vhodném čase s cílem ovlivnění privátních, hospodářských či bezpečnostních zájmů. I v tomto případě se může jednat o kriminální delikt. Typickým příkladem takového úniku je „pouštění“ informací o prognóze určitého odvětví, nebo o skutečnostech, které se týkají konkrétního podnikatelského subjektu, například akciové společnosti za účelem změny ceny akcií.
- Různé informace unikají nahodile a neúmyslně z důvodu indiskrece a nesprávné manipulace. Náhodný příjemce či nálezce je následně poskytne tisku. Tento jsme schopni omezit, nikoliv jej však zcela eliminovat, protože svou důležitou roli tu hraje lidský faktor.
- Vybrané informace o vnitřní situaci v určitých orgánech státu jsou zveřejněny spontánně a zdarma, přičemž načasování zde nehraje roli. Cílem tohoto úniku je vyvolání reakce politického vedení státu. Tokové jednání může být v některých případech postižitelné z hlediska OUI jako porušení zákonem uložené mlčenlivosti (Smejkal, Rais, 2013).

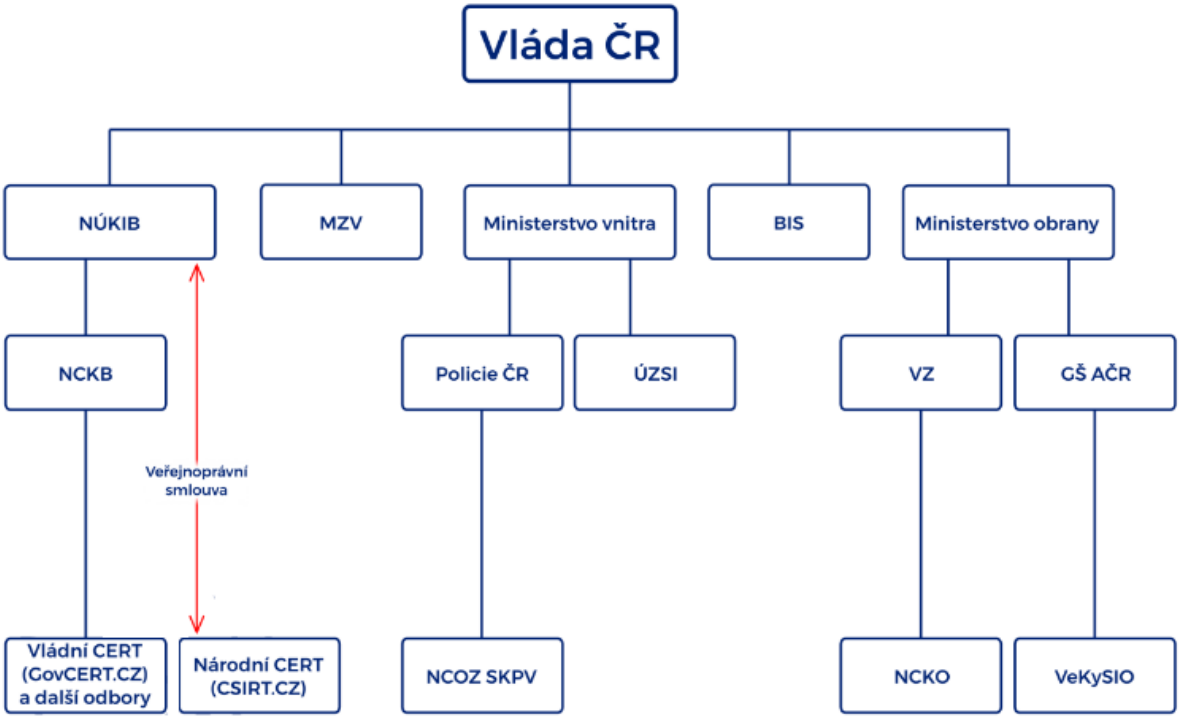
1.7 Národní strategie kybernetické bezpečnosti na období let 2021 až 2025

V této nové koncepci jsou hlavními cílovými skupinami strategie kybernetické bezpečnosti bezpečnostní složky státu a další subjekty veřejné správy. Přesto že tyto subjekty jsou primární oblastí této strategie, tento dokument podporuje a informuje i ostatní částí české společnosti v tom, aby lépe porozuměli krokům, které podniká stát v případě, kdy je nucen čelit kybernetickým hrozbám a rizikům.

Mezi hlavní vize koncepce patří například myšlenka sebevědomého chování v kyberprostoru. V duchu této vize se strategie zabývá myšlenkou společného přístupu ke kybernetické bezpečnosti, což zahrnuje koordinaci množství státních i nestátních subjektů za účelem posílení schopnosti čelit i těm nejzávažnějším výzvám, myšlenkou bezpečné infrastruktury, která se zaměřuje na kontinuální navyšování odolnosti strategické informační infrastruktury, myšlenkou účinné strategické komunikace, myšlenkou sebevědomé reakce která se opírá o využití kolektivní obrany NATO počítající s využitím působení aliančních partnerů v kyberprostoru a myšlenkou zaměřenou na budoucí výzvy počítající s budoucími kybernetickými hrozbami.

Druhá hlavní vize je zaměřená na silná a spolehlivá spojenectví především posílením efektivní mezinárodní spolupráce. Účinná mezinárodní spolupráce v KB vyžaduje propojení jak civilní a vojenské sféry tak rovněž státní, soukromé a akademické sféry. V rámci této vize jde také o prohlubování a tvorbu aktivních spojenectví, participaci na tvorbě mezinárodního právního rámce a prohlubování schopností a expertízy prostřednictvím cvičení KB.

Třetí vizí této koncepce je vytvoření tzv. „odolné společnosti 4.0“, což lze definovat jako stav, kdy celá společnost využívá výhod moderních technologií takovým způsobem, že jsou minimalizována kybernetická rizika. Předpokladem toho je posílení digitální hygieny, která uživatelům představuje soubor zásad, postupů a návyků umožňující bezpečný pohyb ve virtuálním prostředí. Pozornost je zde věnována také zabezpečení digitální společnosti a veřejné správy, vzdělávání a osvětě zaměřené na široké spektrum cílových skupin a rozšiřování expertní základny výchovou a udržováním kvalifikované pracovní síly v oblasti KB (Řehka, 2020).



Obr. 1 Instituce, které se podílejí na zajišťování kybernetické bezpečnosti (Řehka, 2020)

Instituce zmíněné na snímku výše nepředstavují výčet veškerých subjektů, které tvoří systém zajišťování kybernetické bezpečnosti ČR. S kybernetickou bezpečností je úzce spjata i problematika digitální ekonomiky či rozvoje telekomunikačního trhu, což znamená, že významnou roli zde hraje i Ministerstvo průmyslu a obchodu, potažmo Českého telekomunikačního úřadu. Dalšími důležitými subjekty jsou např. MŠMT, jehož role ve vzdělávání nových generací občanů je neopominutelná pro řádné fungování systému zajišťování KB (Řehka, 2020).

1.8 Pojmový aparát z oblasti bezpečnosti informací

Pojmy níže zmíněné nezahrnují všechny tzv. termíny, na které lze v této oblasti narazit, ale autor zvolil několik dle něj klíčových pojmů, které považuje za nutné představit čtenáři této práce pro lepší orientaci. Zvláštní pozornost je věnováno pojmu „informace“, který je představen z různých úhlů pohledu.

Aktivum *(Asset)* „*Aktiva jsou všechny hmotné i nehmotné statky, vše co má pro majitele informačního systému jistou hodnotu. Za nejcennější aktiva se považují peníze, majetek a především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou škodu“* (Požár, 2005).

Autorizace (*Authorization*) „*Udělení práv, které zahrnuje udělení přístupu na základě přístupových práv. Proces udělení práv subjektu pro vykonávání určených aktivit v informačním systému“* (Jirásek, Novák, Požár, 2015).

Bezpečnost *(Security)* „*Pod pojmem bezpečnost chápeme vlastnost nějakého objektu nebo subjektu (informačního systému či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám“* (Požár, 2005).

Bezpečnost dat (*Data security*) „*Počítačová bezpečnost aplikovaná na data. Zahrnuje například řízení přístupů, definování politik a procesů a zajištění integrity dat“* (Jirásek, Novák, Požár, 2015).

Bezpečnostní hrozba (*Information security threat*) „*Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb“* (Jirásek, Novák, Požár, 2015).

Bezpečnost informací / informačních systémů (*Information security INFOSEC*) „*Uplatnění obecných bezpečnostních opatření a postupů sloužících k ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, a dalších vlastností jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření a k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení“* (Jirásek, Novák, Požár, 2015).

Bezpečnostní politika informačního systému (*IS Security policy*) „*Celkový záměr vedení a směr řízení bezpečnosti informačního systému se stanovením kritérií pro hodnocení rizik“* (Jirásek, Novák, Požár, 2015).

Bezpečnostní standardy (*Security standards*) „*Soubor doporučení a obecných principů pro vymezení, udržování a zlepšování bezpečnosti informací v organizaci“* (Jirásek, Novák, Požár, 2015).

Citlivá data (*Sensitive data*) „*Chráněná data mající pro chod organizace zásadní význam. Jejich vyzrazením, zneužitím, neautorizovanou změnou nebo nedostupností by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání“* (Jirásek, Novák, Požár, 2015).

Citlivá informace (*Sensitive information*) „*Informace, která na základě rozhodnutí příslušné autority musí být chráněna, protože její zpřístupnění, modifikace, zničení, nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu, škodu“* (Jirásek, Novák, Požár, 2015).

Důvěrnost (*Confidentiality*) „*Pojem důvěrnost definuje skutečnost, že k informacím, datům a ICT je umožněn přístup pouze těm subjektům, které jsou k tomu autorizovány“* (Kolouch, et al., 2019).

Hrozba *(Threat)* „*Hrozba je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. zaměstnanec, hacker apod.)“* (Požár, 2005).

Incident bezpečnosti informací „*Jednotlivá nežádoucí nebo neočekávaná událost bezpečnosti informací nebo série nežádoucích nebo neočekávaných událostí bezpečností informací, které mohou s významnou pravděpodobnosti vyvolat kompromitování operací souvisících s činností organizace a ohrožení bezpečnosti informací“* (Jirásek, Novák, Požár, 2015).

Informační systém *(IS)* *„Je to soubor prvků, které jsou spojeny vzájemnými vztahy a vazbami. Prvky informačního systému tvoří místa transformace dat a informací jako hardware, lidé, programy apod. Vazby jsou tvořeny především vzájemným působením mezi prvky“* (Požár, 2005).

Integrita (*Integrity*) „*Vlastnost přesnosti a úplnosti“* (Jirásek, Novák, Požár, 2015).

Kybernetická bezpečnost (*Cyber security*) „*Stejně jako u předchozího pojmu je i tento možno vyjádřit pomocí různých definic, přičemž jejich znění v zásadě směřuje ke stejnému závěru (zdroj vlastní). Jednou z možných definic je tvrzení, že kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem“* (Kolouch, et al., 2019).

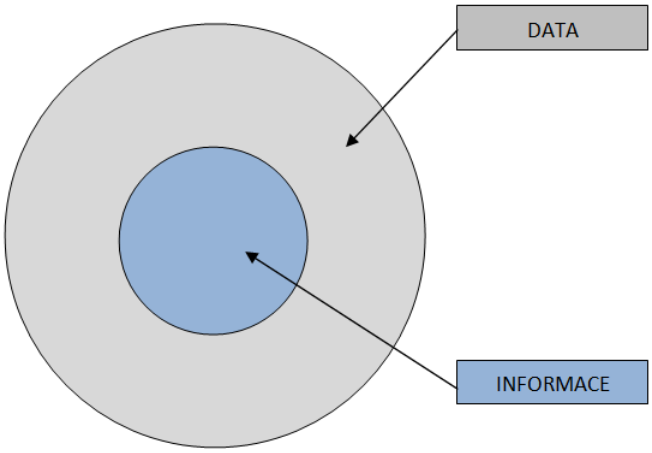
Kybernetická kriminalita (*Cyber crime*) „*Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá zjeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti“* (Kolouch, et al., 2019).

Kyberprostor (*Cyberspace*) *„Je náročné definovat pojem kyberprostor tak, aby bylo možné pochopit komplexnost tohoto prostředí. Jedna z možných definic kyberprostoru uvádí, že kyberprostor je fiktivní prostředí, ve kterém dochází ke komunikaci prostřednictvím počítačových sítí. Také lze použít tvrzení, že 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“* (Kolouch, et al., 2019).

Riziko (*Risk)* *„Je to pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva“* (Požár, 2005).

Pojetí informace a způsoby jejího chápání a definování

Pojem informace patří v současné vědě k nejobecnější kategorii. Na základě toho, v jakém vědním oboru nebo v jaké oblasti lidské činnosti informace používáme, pro ně můžeme aplikovat specifické přístupy, či je můžeme chápat nebo definovat různými způsoby. Samotný pojem informace se v praxi často zaměňuje či slučuje s pojmem data. Jsou to však různé pojmy, které je třeba odlišit a je vhodné pokusit se vymezit jejich vztah. Data jsou většinou chápána jako statická fakta, která jsou časově nezávislá, kdežto informace odrážejí stav reality v určitém okamžiku, a proto je nelze měnit. Můžeme pouze získávat nová data o realitě v jiném časovém okamžiku. Smyslem zpracování dat je tedy vytvoření informace, která představuje význam přisouzený datům. Můžeme tedy říci, že na data zle pohlížet jako na objektivní reprezentanty objektů, událostí či pojmů, ale informace naopak jsou subjektivní a existují jen ve vztahu k příjemci-uživateli. Data jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány a jsou základním materiálem pro informace. „*Informace jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Můžeme tedy říci, že každá informace je tedy údajem neboli datem, ale jakákoli uložená data se nemusejí nutně stát informací“*, tou se stanou totiž až v okamžiku, kdy příjemci přinesou něco nového (Požár 2005, Kolouch 2016)



Obr. 2 Vztah data a informace (Požár, 2005)

TLP Protocol– „*Slouží ke snadnému určení míry důvěrnosti informací a možnosti jejich dalšího sdílení. Informace se za tímto účelem označí příznakem, který stanoví podmínky jejího použití*“ (NUKIB, 2020).

Informace mohou mít tyto příznaky:

TLP: WHITE – „*Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena*“. (NUKIB, 2020).

TLP: GREEN – „*Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace*“ (NUKIB, 2020).

TLP:AMBER – „*Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit*“ (NUKIB, 2020).

TLP:RED – „*Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité, informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace*“ (NUKIB, 2020).

2 NORMLIZAČNÍ INSTITUCE

Normalizační instituce se kromě ostatních standardizačních činností zabývají i standardizací bezpečnosti IT na různých úrovních. Spravujeme li informace prostřednictvím IT je nutné pro samotné zabezpečení informací zabezpečit IT jako takové. Na úvod této kapitoly nejprve vysvětlíme rozdíl mezi pojmy **norma** a **standard**.

Norma nedoporučení pro daný standard nebo řešení (v ICT se jedná o směrnici či předpis vydávané různými konsorcii uživatelů a výrobků IT, v podstatě se jedná o doporučení využitelných standardů za účelem realizování požadovaného kompatibilního řešení).
Standard je dokumentovaná úmluva obsahující technické specifikace nebo jiná podobná přesně stanovená kritéria důsledně používaná jako pravidla, směrnice, respektive jako definice charakteristických vlastností zabezpečujících, že materiály, výrobky, procesy, služby apod. jsou takové, jaké se zamýšlelo (Ondrák, Sedlák, Mazálek, 2013).

2.1 Národní, světové normalizační instituce

ISO-International Organization for Standardization
Jeho posláním je podporování rozvoje standardizačních a s tím spojených aktivit ve světě se zaměřením na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře vědeckých, technických a ekonomických aktivit.

IEC – International Electrotechnical Comission
Je to celosvětová organizace, jejímž úkolem je připravovat a vydávat mezinárodní normy z oblasti elektrotechnických, elektronických a jim příbuzných odvětví jako např. (elektřina, magnetismus, multimédia, telekomunikace apod.).

ITU – International Telecommunications Union
Je mezinárodní organizací spadající do hierarchie OSN. V minulosti již normalizační aktivity ITU podpořily růst nových technologií jako např. mobilní technologie a nyní v dnešní době obracejí svůj zájem na stavební prvky objevující se v globální informační infrastruktuře potažmo k tvorbě vyspělých multimediálních systémů využívajících slučování hlasových, datových, zvukových a video signálů (Ondrák, Sedlák, Mazálek, 2013).

2.2 Evropské normalizační instituce

CEN – Comité Européen Normalisation

Posláním této instituce je podpora dobrovolné harmonizace technických norem v Evropě. Díky harmonizaci dochází ke zmenšení obchodní překážky, podpoře bezpečnosti, umožnění vzájemné funkčnosti výrobků, systémů a služeb a podpoře běžného technického porozumění.

CEN/ISSS – *CEN* Information Society Standardization Systém

Hraje klíčovou roli v rámci CEN z hlediska standardizace bezpečnosti IT. Jejím cílem je poskytování úplné a ucelené řady standardizačně orientovaných služeb a produktů účastníkům trhu za účelem dosažení úspěchů informační společnosti v Evropě.

CENELEC – Comité Européen de Normalisation Eléstrotechnique

Organizace CENELEC založila sektor ICT, kam přesunula normalizační aktivity, které souvisejí s oblastí informačních a komunikačních technologií. Vznikla tedy úzká spolupráci mezi tímto novým sektorem a organizacemi CEN a ETSI.

ETSI – European Telecommunications Standards Institute

Posláním této neziskové organizace je tvorba telekomunikačních norem cílených především na evropský region (Ondrák, Sedlák, Mazálek, 2013).

2.3 Národní instituce

Oblast normalizace v oblasti informačních technologií v rámci jednotlivých států obvykle zajišťují národní normalizační organizace. Tyto organizace jsou vesměs členskými organizacemi ISO a/nebo IEC. Vydávají vlastní národní normy.

BSI (U. K.), British Standard Institute

Tato britská norma je vytvářena náležitě kvalifikovanými a zkušenými lidmi. Tento tým odborníků schvaluje detaily, které formují nové britské normy. Po vydání návrhu normy běží 60 denní lhůta, během které může kdokoli, kdo má zájem komentovat obsah návrhu. Po posouzení všech komentářů dojde k tomu, že je návrh publikován jako nová britská norma (Ondrák, Sedlák, Mazálek, 2013).

ANSI (U. S. A.), American National Standards Institute
ANSI nefunguje jako přímý vývojář amerických národních norem, ale ustanovením konsensu mezi kvalifikovanými skupinami tento vývoj umožňuje.

DIN (Německo), Deutsches Institut für Normung
DIN nabízí možnost veřejné diskuse, ve které se mohou setkat a diskutovat představitelé průmyslu, spotřebitelských organizací, vědy, vlád, zkrátka všechny subjekty, které se zajímají o standardizaci za účelem definic a specifických normalizačních požadavků a výsledek zaznamenat jako německé normy.

ČSNI, Český normalizační institut
Byl zřízen jako státní příspěvková organizace a v současnosti patří mezi organizace podřízené Ministerstvu průmyslu a obchodu. ČSNI má statut národní normalizační organizace, která zastupuje národní zájmy v mezinárodních a evropských normalizačních organizacích. ČSNI je rovněž členem mezinárodních normalizačních organizací ISO a IEC, evropských normalizačních organizací CEN a CENELEC a zastává také funkci národní normalizační organizace v evropském normalizačním institutu pro telekomunikace ETSI.
ČSN, česká technická norma, vzniká dvojím způsobem:

- Přejímáním evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN IEC, ČSN ISO, ČSN ETS atd.).
- Tvorbou původních ČSN, které vyplývají z národních potřeb a z hledisek zachování funkčnosti fondu ČSN (Ondrák, Sedlák, Mazálek, 2013).

2.4 Evropské normalizační organizace zabývající se bezpečností IT

ECMA European Computer Manufacturers Association
Působí v Evropě jako nadnárodní standardizační asociace výrobců hardware a software a IT služeb. Jejím účelem je standardizační činnost v oblasti informačních a telekomunikačních systémů.

EFTA European Free Trade Association
SWIFT Society for Worldwide Interbank Financial Telecommunications
EBA Euro Bankink Assocication

ECBS European Committee for Banking Standards

ECBS vydává standardy tak i technické příručky a zprávy pro implementaci standardů:

- TR 401 Sacure Banking over the Internet.
- TR 402 Certification Authorities.
- TR 405 Key recovery in Financial Systems (Ondrák, Sedlák, Mazálek, 2013).

2.5 Americké normalizační organizace zabývající se bezpečností IT

IEEE Institute ofElectrical and Electronics Engineers

Prostřednictvím svých členů je IEEE předním vedoucím orgánem v technických oblastech zahrnujících například počítačové inženýrství, biomedikální technologie, telekomunikace, elektrická energie, spotřební elektronika atd. Ve většině případů mají normy IEEE mezinárodní význam. Mimo jiné se organizace IEEE zaměřuje obzvlášť na normy bezpečnosti lokálních sítí a operačních systémů.

NIST National Institute for Standards and Technology

Je to vládní standardizační orgán, který působí v oblastech vývoje a podpory standardů, měřících technik a technologií, jehož účelem je zvýšení produktivity, usnadnění obchodu a zlepšení života.

CSD Computer Security Division

CSD se zabývá především bezpečností IT v rámci NIST a jeho práce je seskupena do pěti hlavních kategorií.

- Kryptografické standardy a aplikace.
- Testování bezpečnosti.
- Security Research/Emerging Technologies – výzkum cílený na zlepšení bezpečnostních služeb nových technologií.
- Security Management and Guindance – zaměřen na analýzy a správu rizik a školení.
- Outreach, Awareness and Education – zaměřen na podporu širšího uvědomění důležitosti a potřeby bezpečnosti IT.

(Ondrák, Sedlák, Mazálek, 2013)

3 PŘEHLED NOREM PRO SOUROMÉ SUBJEKTY

V této kapitole jsou představeny závazné a doporučené normy z oblasti bezpečnosti informací soukromých subjektů. Závazné normy jsou zde reprezentovány českou legislativou zabývající se předmětnou oblastí a normy doporučené jsou vyobrazeny širokou škálou norem z rodiny ISMS, přičemž je zde samotný model ISMS představen jako stěžejní doporučení pro řízení bezpečnosti informací soukromých subjektů.

3.1 Závazné normy soukromých subjektů

V této části je představena vybraná tuzemská legislativa, zahrnující oblast soukromých subjektů spolu s krátkým uvedením významu ke vztahu bezpečnosti informací.

Zákon č. 455/1991 Sb. o živnostenském podnikání

Tento zákon upravuje podmínky živnostenského podnikání a kontrolu nad jejich dodržováním. Ve vztahu k informacím, jež soukromé subjekty spravují prostřednictvím tohoto zákona lze zmínit živnostenský rejstřík, který je informačním systémem veřejné správy vedeným v elektronické podobě, ve kterém jsou ve vztahu k soukromým subjektům uvedeny údaje statistického a evidenčního charakteru související s provozováním živnosti. Za tímto účelem informace a údaje přebírány i z dalších informačních systémů a registrů.

Do živnostenského rejstříku se zapisují údaje jako např. jméno a příjmení fyzické osoby, státní občanství, adresa trvalého bydliště, rodné číslo, IČO, předmět podnikání, druh živnosti, provozovny, v nichž je živnost provozována, překážky provozování živnosti a další (Zákon č. 455/1991 Sb.).

Zákon č. 89/2012 Sb. občanský zákoník

Ve vztahu k bezpečnosti informací soukromých subjektů tento zákon definuje obchodní tajemství *„obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení“* (Zákon č. 89/2012 Sb., §504)

Zákon č. 110/2019 Sb. o zpracování osobních údajů

„Tento zákon zapracovává předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie (GDPR) a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů“ (§1). Dále se tento zákon zabývá postavením a pravomocemi Úřadu pro ochranu osobních údajů, zpracováním osobních údajů na základě nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR), zpracováním osobních údajů příslušnými orgány za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti a to včetně pátrání po osobách a věcech, zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky (Zákon č. 110/2019 Sb.).

GDPR neboli General Data Protection Regulation je obecné nařízení o ochraně osobních údajů, které vyvstalo z legislativy Evropské unie a jehož cílem je výrazné zvýšení ochrany osobních dat občanů. Do systému národní legislativy bylo GDPR přijato zákonem č. 110/2019 Sb. o zpracování osobních údajů. Představuje silný právní rámec ochrany osobních údajů v evropském prostoru, jež si klade za cíl co nejvíce hájit práva občanů EU proti neoprávněnému zacházení s jejich daty a to včetně osobních údajů. GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů. Nařízení GDPR míří tedy na ty, kdo zacházejí s osobními údaji zaměstnanců, zákazníků, klientů či dodavatelů napříč odvětvími. Zasahuje však i ty, kteří sledují či analyzují chování uživatelů na webu při používání aplikací nebo chytrých technologií. GDPR si klade za cíl chránit digitální práva občanů EU (Škorničková, b.r.).

Silnou stránkou těchto pravidel je to, že byla přijata formou evropského nařízení, což znamená především jejich jednotnou platnost v členských státech EU. To znamená, že je národní vlády zemí a jejich zákonodárci nemohou jakkoli ohýbat či přizpůsobovat místním zájmům nebo lobbistům. V ČR byl dosud v oblasti ochrany údajů hlavním regulátorem Úřad pro ochranu osobních údajů, který by měl zůstat ve funkci, ale přibudou mu pravomoci odrážející závažnost celé reformy a zároveň bude částečně Evropskému sboru pro ochranu osobních údajů (Škorničková, b.r.).

GDPR dává subjektům údajů (lidem, kterým údaje patří) do rukou nová práva. Nově budou moci po správcích údajů požadovat, co doposud nemohli. Například se jedná o právo vznést námitku proti zpracování, po které správce nebude moci údaje dále zpracovávat, pokud k tomu nebude mít závažné prokazatelné důvody. Novým elementem

je právo na výmaz a jeho rozšíření na právo být zapomenut, díky němuž může osoba požadovat výmaz svých osobních údajů bez zbytečného odkladu, neexistuje-li právní důvod pro jejich další zpracování (Škorničková, b.r.).

Dle stávající směrnice z roku 1995 tak i dle GDPR jsou osobní údaje definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě. Mezi obecné osobní údaje patří např. jméno, pohlaví, věk, datum narození, osobní stav, ale i IP adresa a fotografický záznam. Do kategorie citlivých údajů pak patří různé genetické dědičné znaky, biometrické údaje a osobní údaje dětí. Mezi osobní údaje PFO řadíme tzv. organizační údaje, mezi které patří e-mailová adresa, telefonní číslo či jiné státem vydané identifikační údaje. Do zvláštní kategorie řadíme údaje o rasovém či etnickém původu, politických názorech, náboženství, sexuální orientaci, členství v odborech, trestních deliktech či pravomocnému odsouzení (Škorničková, b.r.).

Nařízení GDPR je povinen dodržovat každý, kdo zpracovává osobní data či osobní údaje. Nařízení se tedy vztahuje na subjekty, které zaměstnávají byť jediného zaměstnance, či společnosti, které by měly byť jediného zákazníka ve věrnostním programu (GDPR Solutions, © 2021).

3.2 Doporučené normy soukromých subjektů

Níže je představen stěžejní model pro řízení bezpečnosti informací ISMS a dále škála vybraných norem, které se zabývají oblastí bezpečnosti informací pro soukromé subjekty.

3.2.1 Model ISMS

ISMS Information Security Managment System neboli systém řízení bezpečnosti informací. Jedná se o systém řízení bezpečnosti informací a to se všemi atributy, které to obnáší. Nutno zmínit, že ISMS je částí celkového systému řízení organizace. ISMS je dokumentovaný efektivní systém řízení a správy informačních aktiv, který má za cíl eliminovat jejich možnou ztrátu nebo poškození tím, že:

- Jsou určena aktiva, která se mají chránit.
- Jsou zvolena a řízena možná rizika bezpečnosti informací.
- Jsou zavedena opatření s požadovanou úrovní záruk a tato opatření jsou kontrolována (Ondrák, Sedlák, Mazálek, 2013).

ISMS lze zavést jak pro organizační složku společnosti, informační systém nebo jeho část, případně pro celou organizaci. Zavedení ISMS je strategickým rozhodnutím vedení společnosti.

ISMS se vztahuje na tyto základní okruhy:

- Bezpečnostní funkce a mechanizmy.
- Administrativní bezpečnost.
- Komunikační bezpečnost.
- Personální bezpečnost.
- Fyzická bezpečnost.
- IT bezpečnost.
- Dokumentace.

ISMS je založen na využití modelu PDCA (Demingova modelu), který má čtyři etapy:

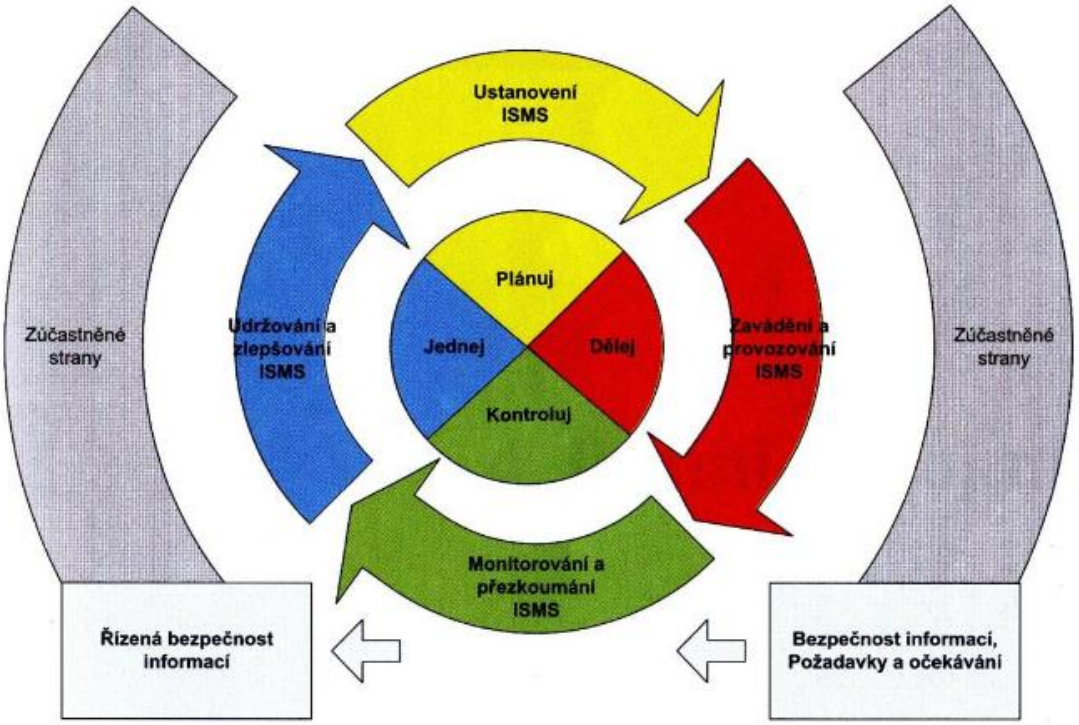
- Ustanovení ISMS (určuje rozsah a odpovědnosti).
- Zavádění a provoz ISMS (prosazení vybraných bezpečnostních opatření).
- Monitorování a přezkoumání ISMS (zajištění zpětné vazby a hodnocení řízení).
- Údržba a zlepšování (odstraňování slabin a soustavné zlepšování).

Model PDCA

Jedná se o metodu, představující postupné zlepšování kvality služeb, procesů, aplikací či dat formou opakovaného provádění čtyř základních činností:

- Plan (plánuj) plánování zamýšleného zlepšení.
- Do (dělej) realizace plánu.
- Check (kontroluj) ověření výsledku realizace s původním záměrem.
- Act (jednej) úpravu záměru a plošná implementace zlepšení do praxe.

Klíčovou součástí celého modelu PDCA je dokumentace každé jeho etapy. Procesy je potřeba identifikovat, popsat a zdokumentovat, řídit na základě dokumentace a následně optimalizovat jejich průběh (Ondrák, Sedlák, Mazálek, 2013).



Obr. 3 Model PDCA neboli životní cyklus ISMS (Ondrák, Sedlák, Mazálek, 2013

3.2.2 Normy řady 27000

V této podkapitole jsou uvedeny základní normy řady 27000 reprezentující systém managementu bezpečnosti informací a další normy reprezentující konkrétní oblasti.

ČSN ISO/IEC 27000:2018 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací (Přehled a slovník)

- Norma poskytuje přehled systémů řízení bezpečnosti informací a soubor souvisejících termínů. „Rodina norem“ si klade za cíl pomoci organizacím bez ohledu na jejich typ či velikost zavést a provozovat systém ISMS. Organizace tak mohou prostřednictvím norem ISMS vyvinout a implementovat rámec pro správu bezpečnosti vlastních bezpečnostních aktiv.

ČSN ISO/IEC 27001:2013 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací (požadavky)

- Norma prosazuje přijetí procesního přístupu k řešení ISMS a v tomto duchu zavádí model známý jako PDCA. Tento model lze aplikovat na všechny procesy zahrnuty v ISMS, tak jak je norma definuje (Ondrák, Sedlák, Mazálek, 2013).

ČSN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací (soubor postupů)

- Obsahuje přes 133 strukturovaných oblastí doporučení rozdělených do 11 kapitol, které obsahují přes 5000 přímých a odvozených bezpečnostních opatření, které podporují dosažitelnost podnikatelských cílů, přičemž odpovědnost za ně je přiřazována osobám s odpovídajícími funkcemi.

ČSN ISO/IEC 27003:2017 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

- Tato norma nabízí doporučení pro ustanovení a implementaci ISMS v souladu s požadavky normy ISO/IEC 27001. Lze ji použít pro všechny druhy organizací, které se rozhodli zavést ISMS.

ČSN ISO/IEC 27004:2016 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací (měření)

- Předmětem této normy jsou doporučení v oblasti vývoje a používání metrik pro měření účinnosti zavedeného ISMS.

ČSN ISO/IEC 2005:2018 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

- Předmětem této mezinárodní normy je doporučení pro řízení rizik bezpečnosti informací v organizacích a podpora konceptu, který je specifikován v ISO/IEC 27001, přičemž je tato norma strukturována za účelem dostatečné podpory implementace informační bezpečnosti, která je založená na přístupu řízení rizik.

ČSN ISO/IEC 27006:2015 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci ISMS

- Norma je určená primárně pro podporu procesu akreditace certifikačních orgánů, které poskytují certifikaci ISMS.

ISO/IEC 27010:2015 Information Technology – Security techniques – Information security management for inter-sector and inter-organizational communications

- Zde jsou obsažena doporučení, která řídí bezpečnost informací během interní a mimo firemní komunikace (Ondrák, Sedlák, Mazálek, 2013).

3.2.3 Vybrané normy ve vztahu ke konkrétné oblasti

Telekomunikační prostředí

ISO/IEC 27011:2016 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

- Norma je primárně určena pro telekomunikační operátory zavádějící ISMS. Cílem normy je primárně usnadnit naplnění bezpečnostních požadavků v rámci integrity, dostupnosti a důvěrnosti dat.

ISO/IEC 27032:2012 Information Technology – Security techniques – Guidelines for Cybersecurity

- Tato mezinárodní norma vysvětluje vztah mezi kybernetickou bezpečností a jinými typy zabezpečení, definuje zúčastněné strany a jejich role a vymezuje rámec, který umožňuje zúčastněným stranám spolupracovat na řešení problémů v oblasti kybernetické bezpečnosti.

Síťová bezpečnost

ISO/IEC 27033 Information technology – Security techniques – Network security

- Jedná se o soustavu norem, která obsahuje doporučení pro implementaci opatření vztahující se k bezpečnosti sítí.

(Ondrák, Sedlák, Mazálek, 2013)

4 PŘEHLED NOREM PRO VEŘEJNÉ SUBJEKTY

Tato kapitola obsahuje přehled závazných a doporučených norem pro veřejné subjekty v oblasti bezpečnosti informací. Závazné normy reprezentují především národní zákony zahrnující předmětnou oblast a je zde také krátce představena některá evropská legislativa. Oblast tzv. doporučených norem pak zahrnuje konkrétní vybrané normy z prostředí veřejného sektoru.

4.1 Závazné normy veřejných subjektů

V této části práce jsou zmíněny přední české zákony zahrnující oblast bezpečnosti informací.

4.1.1 České zákony zahrnující předmětnou oblast

Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů

Tento zákon upravuje výběr a evidenci archiválií, ochranu archiválií, práva a povinnosti vlastníků archiválií, práva a povinnosti držitelů a správců archiválií, využívání archiválií, zpracování osobních údajů pro účely archivnictví, soustavu archivů, práva a povinnosti zřizovatelů archivů, spisovou službu a působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisové služby (Zákon č. 499/2004 Sb.). Mimo samotného zákona č. 365/2000 Sb. o informačních systémech veřejné správy a jeho prováděcích přepisech je zákon č. 499/2004 Sb. o archivnictví a spisovné službě a o změně některých zákonů jedním z nejvýznamnějších zákonů ve vztahu k bezpečnostním požadavkům informačních systémů veřejné správy (Ondrák, Sedlák, Mazálek, 2013).

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

„Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy“ (§1). Dále se zabývá ochranou utajovaných informací, ale také například způsoby poskytování utajovaných informací a způsoby poskytování utajovaných informací Evropské unie v jejím rámci i mimo něj a způsoby přístupu k utajovaným informacím. Zákon dále definuje stupně újmy a hrožení České republiky, ke kterým by mohlo dojít v případě vyzrazení různých stupňů utajovaných informací. Definuje jednotlivé stupně utajení a

druhy zajištění ochrany utajovaných informací, mezi které patří personální bezpečnost, průmyslová bezpečnost, administrativní bezpečnost, fyzická bezpečnost, bezpečnost informačních nebo komunikačních systémů a kryptografická ochrana (Zákon č. 412/2005 Sb.).

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů

„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi“ (§1). Stanovuje také systém zajištění kybernetické bezpečnosti. Zákon také rovněž stanoví orgány a osoby, jimž se v oblasti kybernetické bezpečnosti ukládají určité povinnosti. Takovými orgány či osobami jsou poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací, orgány nebo osoby zajišťující významnou síť, správci a provozovatelé informačního systému kritické informační infrastruktury, správci a provozovatelé komunikačního systému komunikačního systému kritické informační infrastruktury nebo správce a provozovatel významného informačního systému. Dále se zabývá kybernetickými bezpečnostními událostmi a kybernetickými bezpečnostními incidenty, zpracovává jejich hlášení a vede o nich evidenci (Zákon č. 181/2014 Sb.).

Zákon o kybernetické bezpečnosti a související právní předpisy však ukládají povinnost pro zajišťování kybernetické bezpečnosti poměrně úzké skupině subjektů, pro které je bezpečnost v této oblasti vnímána jako nejvýznamnější, protože souvisí přímo se zajišťováním bezpečnosti státu a jeho funkcí. Především se jedná o subjekty z odvětví energetiky, telekomunikací, bankovnictví a podobně. Samotný zákon byl vytvořen především k zajištění veřejného zájmu na bezpečnosti kritické informační infrastruktury a významných informačních systémů. Subjekty, které nespadají pod zákon o kybernetické bezpečnosti, by přesto měly mít vlastní zájem na zavedení organizačních a technických opatření směrem k zajištění kybernetické bezpečnosti. Důvodem je především navyšující se počet útoků na menší společnosti (Antoš, 2020).

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy

„Tento zákon stanoví práva a povinnosti, které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných státními orgány nebo orgány územních samosprávných celků“ (§1). Tento zákon se však nevztahuje na informační systémy veřejné správy spravované pro potřeby zpravodajských služeb, pro potřeby nakládání s utajovanými informacemi, pro potřeby NBÚ nebo NUKIB. Dále se nevztahuje na ISVS spravované pro potřeby zajišťování obrany státu, podpory krizového řízení, pro potřeby bezpečnostních sborů nebo pro potřeby České národní banky. Ve vztahu k tomuto zákonu chápeme informační činnost jako získávání a poskytování informací, reprezentace informací prostřednictvím dat, shromažďování, vyhodnocování a ukládání dat na nosiče a jejich uchovávání, dále vyhledávání, úprava nebo i možné pozměňování dat, jejich následné šíření, předávání, výměna, zpřístupňování, vzájemné kombinování nebo třídění, následné blokování či likvidace dat ukládaných na různých nosičích. Tato informační činnost je prováděna prostřednictvím správců, provozovatelů a uživatelů ISVS za pomoci různých technických a programových prostředků. ISVS je v zákoně definován jako funkční celek nebo jeho část, který cílevědomě a systematický zabezpečuje informační činnost pro účely výkonu veřejné správy (Zákon č. 365/2000 Sb.).

4.1.2 Vybraná evropská legislativa zahrnující předmětnou oblast

- Směrnice Evropského parlamentu a Rady 2002/19/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací.
- Směrnice Evropského parlamentu a Rady 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice).
- Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.
- Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti.
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004.

- Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací.
- Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti webových stránek a mobilních aplikací subjektů veřejného sektoru.
- Směrnice evropského parlamentu a rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.
- Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- Směrnice Evropského parlamentu a Rady 2003/98/ES ze dne 17. listopadu 2003 o opakovaném použití informací veřejného sektoru.

4.2 Doporučené normy veřejných subjektů

Jako ideální prostředí v rámci veřejného sektoru se pro využití „doporučených norem“ nabízí oblast veřejné správy a zdravotnictví, přičemž je lze spravovat níže zmíněnými normami aplikujícími ISMS.

4.2.1 ISMS ve státní správě

Z pohledu ISMS a jeho zavádění se státní správa jeví jako nejpotřebnější a nejkritičtější oblast vzhledem k množství a členitosti zpracovávaných údajů. Abychom správně pochopili celou problematiku v této oblasti, je třeba zmínit následující členění:

- Převzetí celkové odpovědnosti za informační bezpečnost.
- Začlenění informační bezpečnosti do procesů státní správy.
- Správa a údržba informační bezpečnosti a integrace s jiným managementem.
- Nastavení dosažitelných cílů a ekonomická analýza informační bezpečnosti.
- Funkce politiky modelu bezpečnosti (Ondrák, Sedlák, Mazálek, 2013)

Samotné zavádění ISMS ve státní správě je specifická několika oblastmi:

- Převážná část dokumentů existuje v papírové formě.
- Komplikované hodnocení dopadů při analýze rizik.
- Komplikované meziresortní spolupráce.

Česká republiky i Evropská unie disponuje značným množstvím legislativy upravující požadavky na zpracování informací v rámci informačních systémů veřejné správy. Za nejvýznamnější legislativu ve vztahu k bezpečnostním požadavkům informačních systémů veřejné správy lze považovat výše zmíněný zákon o informačních systémech veřejné správy nebo zákon o archivnictví a spisové Ondrák, Sedlák, Mazálek, 2013).

Konkrétní normy zahrnující oblast státní správy

ISO/IEC 27014:2020 Information technology – Security techniques – Information security governance framework

- Cílem této normy je doporučovat organizacím návrh jejich vlastní „Information Security Governance“. Tímto pojmem se rozumí řízení informační bezpečnost v organizaci. Doporučení by měla zohledňovat strategie, cíle, politiky a legislativní povinnosti dané organizace. V této normě je nejlépe vystižena problematika státní správy a veřejného sektoru a je aplikovatelná pro organizace všech typů a velikostí Ondrák, Sedlák, Mazálek, 2013).

Britské normy zahrnující předmětnou oblast

BS ISO/IEC 38500:2015 Corporate governance of information technology

- Vedení organizací a podniků dostává prostřednictvím této normy praktické pokyny, jak při svých činnostech efektivně využívat používané informační technologie. Norma se vztahuje ke všem procesům zahrnujících služby komunikačních technologií a informací v organizacích. Celkově tedy představuje rámec pro řízení informačních technologií (Ondrák, Sedlák, Mazálek, 2013).

4.2.2 ISMS ve zdravotnictví

Zdravotnictví je třeba vnímat z hlediska provozního prostředí jako specifikum, které má na informační systémy odlišné požadavky. Z pohledu bezpečnosti zdravotních informací jsou vnímána aktiva jako např. lékařské informace, IT zařízení a lékařská zařízení zaznamenávající nebo poskytující data (Ondrák, Sedlák, Mazálek, 2013).

Zdravotnický informační systém dle normy ISO/TR 20514:2005 se dá definovat jako úložiště, které obsahuje informace o zdravotním stavu subjektu péče v počítačově zpracovatelné formě, které jsou uloženy a přenášeny bezpečně a jsou přístupné pro více autorizovaných uživatelů (Ondrák, Sedlák, Mazálek, 2013).

Normy zahrnující oblast zdravotnictví

ČSN ISO/IEC 27799:2016 Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.

- V této normě je specifikován soubor kontrol, kterými se řídí bezpečnost zdravotnických informací a rovněž norma poskytuje směrnice pro prověřené postupy v oblasti zabezpečení zdravotnických informací.

Existují však relevantní normy k výše zmíněné ČSN ISO/IEC 2779:2016. Důležitou je například norma:

ČSN ISO/TS 17090-1:2021 Zdravotnická informatika – Infrastruktura veřejného klíče – Část 1: Přehled služeb digitálních certifikátů

- Právě technologie infrastruktury veřejného klíče poskytuje hospodárný prostředek pro zabezpečení výměny informací prostřednictvím internetu, kdy nastává situace, že přenášená data, která jsou mnohdy osobní či důvěrná nejsou nijak zabezpečena.

Další normou využitelnou při přenosu zdravotnických informací je:

ISO 22857:2013 Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health informatics

- Na tuto normu jsou odkázáni pracovníci, kteří mají odpovědnost za národní, provinční nebo státní infrastrukturu zdravotnických informací a vyžadují, aby při přenosu zdravotnických informací mimo hranice působnosti byla zajištěna jejich bezpečnost.

Dále lze zmínit normu **ČSN P ENV 13608-1** Zdravotnická informatika – Bezpečnost komunikace ve zdravotnictví.

- Tato norma má tři části, přičemž první 13608-1 obsahuje pojmy a terminologie, druhá část 13608-2 obsahuje zabezpečené datové objekty a třetí část 13608-3 představuje zabezpečené datové kanály.

(Ondrák, Sedlák, Mazálek, 2013)

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Co si představíme, pokud se řekne doporučená norma. A co si představíme, pokud se řekne doporučená norma v oblasti bezpečnosti informací. Lze říci, že osoba neznalá tohoto prostředí by si mohla představit něco, co bude podobné zákonné regulaci a bude problematiku řešit. Bude se tedy pravděpodobně jednat o systém, postupy nebo opatření, která budou mít cíl zajistit informacím bezpečnost.

Zajištění bezpečnosti informací z pohledu zákonné regulace by se mohlo zdát laikovy automaticky přísnější, konkrétnější zkrátka dokonalejší. Přeci jen slovo „zákon“ si mnozí vyloží jako něco víc než například doporučenou normu.

Na základě provedené rešerše bylo představeno několik závazných norem v gesci národní legislativy předně zahrnující Zákon č. 181/2014 Sb. o kybernetické bezpečnosti nebo zákon o informačních systémech veřejné správy. Tyto zákony regulují předně veřejné subjekty. Pro veřejné subjekty je ale představena i možnost využití doporučených norem z rodiny norem ISMS. Soukromé subjekty se zase jeví jako vhodnější pro doporučené normy. Doporučené normy nejsou sami o sobě závazné jako zákony, ale jejich využití může být vyžadováno na základě právního předpisu.

Při tvorbě a vydávání „doporučených norem“ je určitě velkou předností možnost přizvat odborníky z konkrétních oblastí, provádět diskusi a přijímat a zapracovávat jejich poznámky, jako to dělají Britové nebo Němci.

II. PRAKTICKÁ ČÁST

6 KOMPARACE ZÁVAZNÝCH A DOPORUČENÝCH NOREM

V této kapitole se autor zaměřuje na porovnání konkrétních oblastí spojených s bezpečností informací. Mezi cílové oblasti patří např. bezpečnost lidských zdrojů, řízení přístupu, fyzická bezpečnost, klasifikace aktiv nebo kryptografické prostředky. Zmíněné odvětví jsou z jedné strany regulována závazným prováděcím předpisem zákona o kybernetické bezpečnosti a ze strany druhé doporučenou normou řady ISO/IEC 27000. Celá tato kapitola vyhází z vlastního zpracování s výjimkou tří doslovných citací.

6.1 Bezpečnost lidských zdrojů

Pro provedení samotné komparace se autor nejprve seznámil s regulací předmětné oblasti v gesci obou norem jak doporučených tak závazných a následně poukazuje na rozdíly a poskytuje své vlastní připomínky a postřehy.

Bezpečnost lidských zdrojů z pohledu vyhlášky o kybernetické bezpečnosti

Bezpečnost lidských zdrojů jako jedno z organizačních bezpečnostních opatření vyhláška řeší spíše tím způsobem, že ve stručnosti shrnuje tuto oblast do balíku povinností zahrnujících školení a obecně osvětu zaměstnanců v oblasti bezpečnosti informací. Tuto povinnost dává do rukou "povinné osobě", která je zodpovědná za průběh, evidování a dodržování plánu rozvoje bezpečnostního povědomí, stanovení osob odpovědných za dodržování jednotlivých konkrétních činností uvedených v plánu, za pravidelné hodnocení plánu nebo za určení postihů při porušení bezpečnostních pravidel. Obecně lze říci, že v této oblasti vyhláška pouze reguluje vzdělávací a školící proces, který se vztahuje na všechny uživatele a tento proces se individuálně přizpůsobuje konkrétním uživatelům dle jejich pracovní náplně, odpovědnosti a povinností.

Bezpečnost lidských zdrojů z pohledu normu ČSN ISO/IEC 27002

Norma ČSN ISO/IEC 27002 se oblastí samotného vzdělávání, školení a osvěty v oblasti bezpečnosti informací rovněž zabývá a v podstatě lze říci, že v případě "bezpečnosti lidských zdrojů" dojde použitím této normy k naplnění požadavků vyhlášky o KB. Norma je však v této oblasti daleko přísnější a konkrétnější. Zabývá se na příklad prověřováním minulosti uchazečů o zaměstnání a přesně stanovenými postupy od ověření životopisu, přes proklamované vzdělání až po podrobnější ověření jako je např. výpis z trestního rejstříku. Norma řeší i další přísnější a podrobnější prověřování v případě, že by přijatý zaměstnanec nastupoval na funkci, kde by pracoval se zařízením pro zpracování důvěrných

informací. Dále řeší bezpečnost informací po celou dobu pracovního poměru a poukazuje na povinnosti zaměstnance ve vztahu k bezpečnosti informací i po jeho odchodu.

6.2 Řízení přístupu

Řízení přístupu z pohledu vyhlášky o kybernetické bezpečnosti

Regulace zákonné normy je v tomto případě dosti obsáhlá stejně jako v případě normy (27002). V obou případech jsou zde především řešeny záležitosti jako přístupová práva a jejich přidělování na základě funkčního zařazení, dále samotné kontroly přidělování různých práv a pravidelné kontroly přístupových práv a oprávněnost jejich přidělování dle funkcí a činností uživatelů. Především se v tomto případě tedy jedná o minimalizování neoprávněného využívání informačních systémů či správu samotných informací neoprávněnými osobami, přičemž je za tímto účelem nastaven systém přístupů a kontrol. I zde je stejně jako v předchozím bodu (kapitola 6.1) rizikovým článkem lidský faktor, jehož činnost je tímto odvětvím vymezena směrem k bezpečnému využívání informačních systémů. V případě řízení přístupu je vyhláška specifičtější oproti normě například v oblasti samotných hesel, kde stanovuje minimální délku hesel jak pro běžné uživatele, tak pro administrátory, nebo systém obměňování hesel. Naproti tomu pokud bude vyžadována silná autentizace, norma zohledňuje i využití alternativy hesel v podobě kryptografických prostředků, čipových karet nebo biometrických prostředků.

Řízení přístupu z pohledu normy ČSN ISO/IEC 27002

Stejně jako u předchozího bodu (6.1) je i zde norma v některých bodech poněkud přísnější, konkrétnější a různé společné oblasti ve vztahu k vyhlášce reguluje obsáhleji. Například norma v úvodu části „řízení přístupu“ představuje model samotné politiky řízení přístupu, přičemž zde hovoří o myšlence, která zvažuje jak logické tak fyzické opatření pro řízení přístupů společně. Samozřejmě, že tím fyzická bezpečnost s pohledu normy nekončí, ale je jí stejně jako v případě vyhlášky věnována samostatná část. Norma při specifikaci pravidel řízení přístupu zakládá celý systém na faktu, že „*Obecně je vše zakázáno, pokud to není výslovně povoleno“, spíše než na předpokladu“Obecně je vše povoleno, pokud to není výslovně zakázáno“*(ČSN ISO/IEC 27002:2013). Z pohledu autora je tato myšlenka klíčová. Například pokud by se vždy předala nově nastupujícím zaměstnancům, kteří budou zastávat různé bezpečnostní a jiné funkce, byla by to první jasně stanovená hranice, které sama o sobě směruje k eliminaci bezpečnostních incidentů. Jednou z oblastí řízení přístupu, které se norma více věnuje, je přidělení tzv. privilegovaných práv. Vyhláška

v tomto případě pouze nařizuje minimalizovat tento proces na nejnutnější případy, kdy je to spojeno s činností uživatele, ale norma tento postup řeší mnohem podrobněji. Nejdříve se zabývá systém identifikace těchto práv, systémem jejich přidělování, rovněž také samotným přezkoumáváním kompetencí uživatelů, kterým byla tato práva přidělena. Oproti vyhlášce, která pouze obecně hovoří o povinnosti zajistit odebrání přístupových oprávnění při změně pozice nebo ukončení pracovního poměru, norma opět definuje konkrétní postupy a metody zahrnující také např. změny nebo odstranění používaných hesel.

6.3 Fyzická bezpečnost

Obecně pro zajištění kybernetické bezpečnosti a s tím spojené informační bezpečnosti můžeme rozdělit bezpečnostní opatření do dvou kategorií a těmi jsou organizační a technická opatření. Fyzická bezpečnost patří spolu s dalšími do kategorie technické. Sám zákon č. 181/2014 Sb. o kybernetické bezpečnosti odkazuje na fyzickou bezpečnost ve svém prováděcím předpise, který stanovuje onen obsah jednotlivých bezpečnostních opatření.

Fyzická bezpečnost z pohledu vyhlášky o kybernetické bezpečnosti

Z pohledu vyhlášky je fyzická bezpečnost velice úzce specifikována. Obsahuje pouze stručný a velice obecný výčet povinností ve vztahu k fyzickému zabezpečení. V podstatě definuje tento způsob ochrany jako systém proti poškození, krádežím či zneužití různých druhů aktiv a za tímto účelem nařizuje stanovení fyzického bezpečnostního perimetru, ve kterém je uchováváno vše cenné jako informace nebo různá technická aktiva ICT.

Fyzická bezpečnost z pohledu normy ČSN ISO/IEC 27002

Komparace tohoto odvětví byla pro autora velice zajímavá, neboť z výše zmíněného pohledu vyhlášky se jedná v kostce a zabezpečený kus něčeho, v čem se nachází něco cenného co je potřeba chránit, přičemž za tímto účelem nejsou specifikovány žádné konkrétní činnosti. Norma však podrobně specifikuje jednotlivé oblasti způsobů fyzické ochrany počínaje fyzickým bezpečnostním perimetrem, přes fyzickou kontrolu vstupu, zabezpečení kanceláří, jednotlivých místností a vybavení, ochranu před vnějšími a přírodními hrozbami, zabezpečení oblastí pro nakládku a vykládku, činnost v zabezpečených oblastech až zabezpečení zařízení, jeho umístění a ochranu. Norma specifikuje i postupy pro fyzickou ochranu zařízení a aktiv mimo prostory organizace, tedy

mimo samotný bezpečnostní perimetr. Veškerá zmíněná odvětví fyzické ochrany jsou normou konkrétně definována až detailně specifikována.

6.4 Kryptografické prostředky

Kryptografické prostředky z pohledu vyhlášky o kybernetické bezpečnosti

Tato oblast je v podstatě shrnuta jak vyhláškou, tak normou poměrně úzce. Ve vyhlášce je používání kryptografie svěřeno do rukou „*povinné osoby pro ochranu aktiv informačního a komunikačního systému"*(Vyhláška č. 82/2018 Sb., §26), přičemž jsou jí uloženy povinnosti jako bezpečné nakládání s kryptografickými prostředky a obecné zajištění jejich správného fungování v organizaci. Zajímavou povinností odpovědné osoby je fakt, že musí zohledňovat doporučení v oblasti kryptografických prostředků, která se zveřejňují na stránkách Úřadu.

Kryptografické prostředky z pohledu normy ČSN ISO/IECC 27002

Využitím normy i v tomto případě dojde k naplnění zákona o kybernetické bezpečnosti jako u všech výše porovnávaných oblastí. Oproti vyhlášce, kde musí povinná osoba sledovat doporučení vydaná Úřadem, je zde tato činnost rozvedena o něco více. Zmiňuje se rovněž sledování národních nařízení a omezení v oblasti kryptografie, ale norma také hovoří o monitorování aktualit v oblasti, které se vztahují na používání kryptografických technik ve světě „*a na problematiku oběhu zašifrované informace přes hranice"* (ČSN ISO/IEC 27002:2013). Co se týká samotné správy kryptografických klíčů, tato oblast je oproti vyhlášce opět rozvedena. Nejen že je zde široce popsán systém správy klíčů zahrnující jejich distribuci, vydávání, ukládání, výměny, zálohování či zničení, ale také je zde zmíněna fyzická ochrana zařízení, která slouží pro jejich generování. Za účelem zvýšení bezpečnosti jako takové je zmíněna i možnost využití kryptografických technik k ochraně samotných kryptografických klíčů.

6.5 Klasifikace/hodnocení aktiv

V této části je poukázáno na to, jakým způsobem jsou klasifikována data prostřednictvím normy (27002) a vyhlášky o kybernetické bezpečnosti. Přičemž toto je oblast, kde vyhláška převyšuje normu v oblasti konkrétních opatření a postupů.

Klasifikace aktiv z pohledu vyhlášky o kybernetické bezpečnosti

V tomto případě vyhláška přesně definuje stupnice hodnocení pro jednotlivé stupně úrovní informací. Aktiva jsou zde hodnocena podle důvěrnosti, integrity, a dostupnosti. Každé kritérium obsahuje formou přílohy samostatnou tabulku s uvedením přesného popisu aktiva a způsobu jeho odpovídající ochrany, přičemž při hodnocení aktiv dle důvěrnosti se vychází s TLP protokolu viz kapitola 1.8.

Klasifikaci aktiv z pohledu normy ČSN ISO/IEC 27002

Norma v podstatě nemá přesná kritéria stanovující pevně určený postup. Ve svém znění popisuje systém pro klasifikaci informací na základě obecných požadavků, jako jsou zájmy z hlediska činností organizace na sdílení nebo omezení informací. Norma uvádí, že by informace měli být rovněž hodnoceny z hlediska důvěrnosti, integrity a dostupnosti jako je tomu ve vyhlášce. Schéma klasifikace informací v této normě v podstatě popisuje fungující systém vyhlášky o kybernetické bezpečnosti.

7 ZPŮSOBY BEZPEČNÉHO CHOVÁNÍ V KYBERPROSTORU A OCHRANY INFORMACÍ

V této kapitole je představeno několik způsobů pro zvýšení bezpečnosti informací v kyberprostoru zahrnujících různá opatření a činnosti uživatelů, kteří využívají ICT. Opatření zahrnují činnosti spojené s bezpečným chováním na internetu, šifrování dokumentů nebo různých zpráv a informací nebo nástroje pro obnovu smazaných dat. Tato kapitola pracuje s naprostým miniem zdrojů, přičemž použití zdroje zde slouží pouze pro odborné specifikum daných problémů.

7.1 Zabezpečené spojení protokolem HTTPS

Tato část je věnována protokolu HTTPS a jeho výhodám oproti protokolu HTTP a zároveň je zaměřena na správnou a bezpečnou činnost uživatelů webových stránek. Ať už se jedná o domácí osobní stolní počítače, notebooky, nebo různé firemní počítače v podnicích jak v soukromém tak veřejném sektoru, vždy jsou obsluhovány lidmi-uživateli. Níže je v jednoduchosti vysvětleno, jak uživatel pozná, že se při práci s internetem pohybuje v bezpečném a šifrovaném prostředí a chrání tak své informace.

Protokol HTTPS versus protokol HTTP

Jako jedné z možností zabezpečení informací potažmo jejich samotné ochrany je využíváno protokolu „HTTPS“, což znamená Hypertext Transfer Protokol Secure. Představuje novější verzi protokolu, která zajišťuje komunikaci probíhající mezi prohlížečem uživatele a serverem. Oproti předchozí verzi protokolu „HTTP" (Hyper Text Transfer Protocol) tato novější verze představuje jeden zásadní a klíčový rozdíl a tím je to, že přenášená data šifruje a tím pádem výrazně snižuje riziko jejich zneužití. Toto riziko může spočívat například ve zneužití osobních údajů, odposlechu naší komunikace, případně pozměnění obsahu samotné komunikace. Lze jednoduše říci, že protokol HTTPS je vlastně protokolem HTTP, který je zašifrovaný prostřednictvím certifikátů SSL (Secure Socket Layer) nebo TLS (Transport Layer Security). V obou případech těchto bezpečnostních vrstev jde o stejný cíl a tím je šifrování v tomto případě pomocí asymetrické kryptografie (Koďousková, 2021).

Téměř všichni uživatelé internetu dnes již využívají různých webů, kde je nutno se registrovat a následně přihlašovat, přičemž je toto spojeno s opakovaným zadáváním různých osobních údajů. Dále jsou využívány internetové obchody, kde dochází k přímým online platbám a jsou tedy s různými weby sdíleny i citlivé údaje např. o platebních

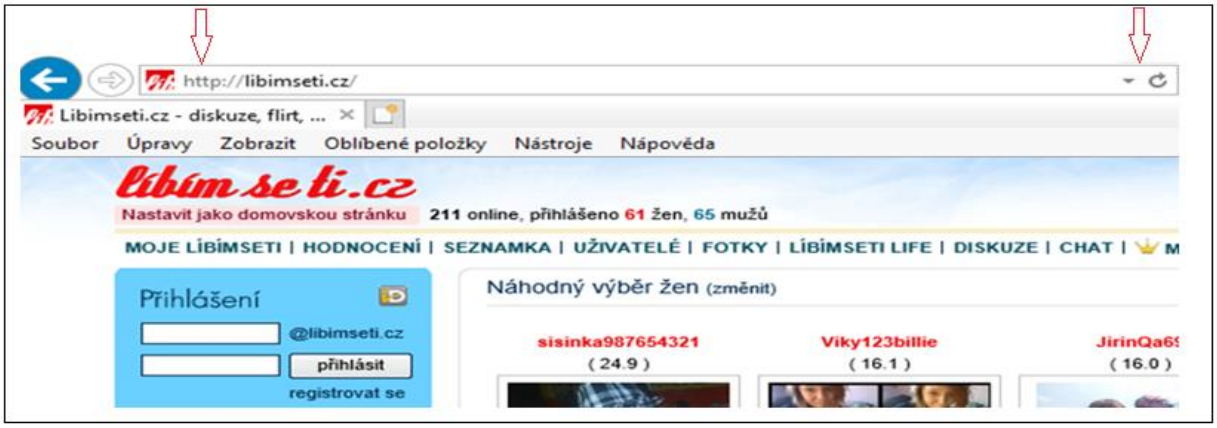
kartách. Komunikace mezi počítačem uživatele a serverem samozřejmě probíhá v kyberprostoru a může být zachycena a zneužita třetí stranou. Za tímto účelem však protokol HTTPS informace a komunikaci šifruje. Aby uživatel poznal, že se pohybuje v zabezpečeném prostředí využívající protokolu HTTPS, internetové prohlížeče toto signalizují v řádku pro zadávání URL adresy. Níže je na snímcích ukázáno, kde a jakým způsobem signalizují prohlížeče HTTPS protokol čili bezpečný server. Za tímto účelem jsou představeny uživateli nejčastěji používané prohlížeče: Internet Explorer, Mozila Firefox, Google Chrome a Opera (zdroj vlastní).

Internet Explorer – šifrované připojení

Obr. 4 Signalizace zabezpečeného prohlížeče v Internet Explorer (zdroj vlastní)

Na snímku výše poukazují červené šipky na jasné ukazatele toho, že pracujeme s protokolem HTTPS. Tento fakt, je zmíněn dvěma indikátory, přičemž první je v levém horním rohu samotný nápis „https“ a dále v pravém horním rohu ikona zámku, který značí, že připojení k serveru je šifrováno tedy zabezpečeno.

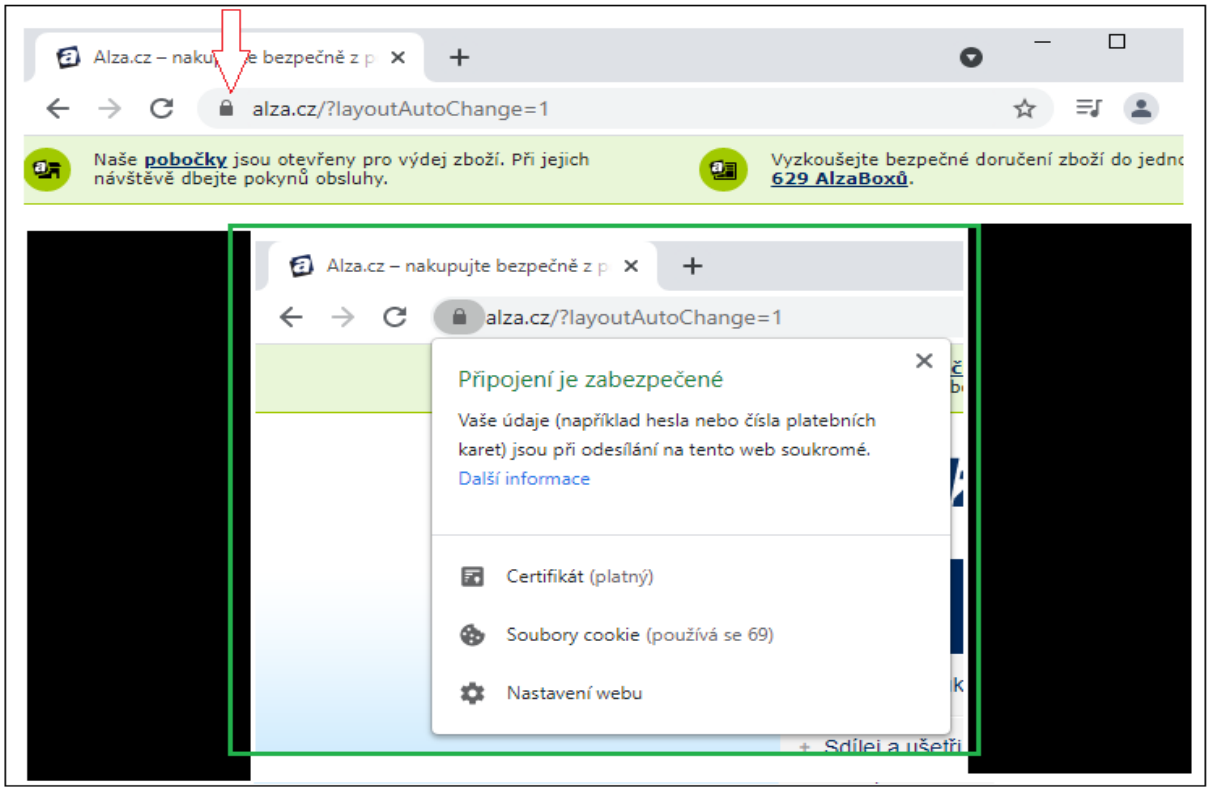
Internet Explorer – nezašifrované připojení



Obr. 5 Signalizace nezabezpečeného prohlížeče v Internet Explorer (zdroj vlastní)

Na snímku výše je pro srovnání příklad, kde se uživatel pohybuje v nezabezpečeném serveru. Indikátory ukazují, že uživatel v tomto případě využívá protokol HTTP a s tím zmizela i ikona zámku signalizující zabezpečené připojení. Lze si povšimnout, že tento server chce po uživateli rovněž přihlášení, avšak v tomto případě po kliknutí na tlačítko přihlásit dojde k tomu, že citlivé uživatelské informace budou po cestě v kyberprostoru nešifrovány a může dojít k jejich zachycení případně zneužití třetí stranou. Níže je ukázáno připojení pomocí protokolů HTTPS a HTTP v prohlížeči **Google Chrome**. I v tomto případě jsou vyznačeny jasné indikátory signalizující uživateli informace o protokolu, který zabezpečuje prohlíženou internetovou stránku (zdroj vlastní).

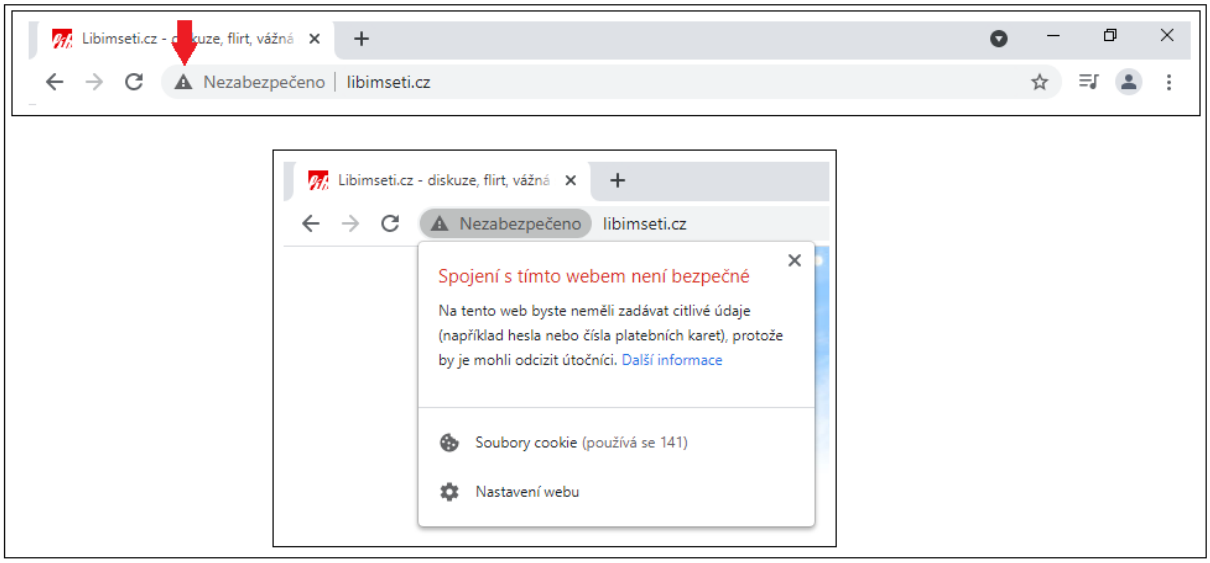
Google Chrome – zašifrované připojení



Obr. 6 Signalizace zabezpečeného připojení v prohlížeči Google Chrome (zdroj vlastní)

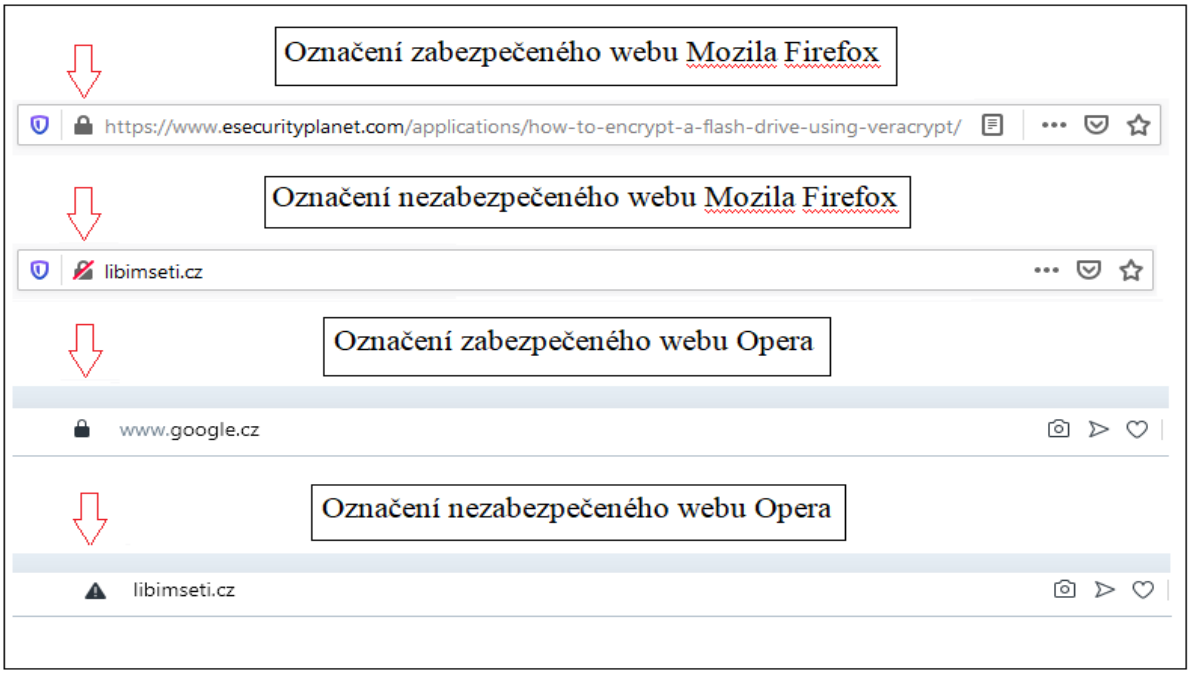
Na snímku je pro uživatele patrné, že ikona zámku v adresovém řádku znamená, že se jedná o zabezpečené připojení tedy o HTTPS protokol. V případě, že uživatel klikne na samotnou ikonu zámku, objeví se malý informační panel, kde je uvedeno, že připojení je bezpečné. Rovněž se v případě prohlížeče Google Chrom na panelu objeví i údaj o platném certifikátu, který po otevřené poskytuje i informace o době trvání platnosti (zdroj vlastní).

Google Chrome - nezašifrované připojení



Obr. 7 Signalizace nezabezpečeného připojení v prohlížeči Google Chrome (zdroj vlastní)

Ikona výstražného trojúhelníku signalizuje nezabezpečený server využívající protokol HTTP. Uživatel, který chce chránit své informace (přihlašovací údaje, online platby nebo komunikaci s jiným uživatelem), by měl toto prostředí opustit. Následující snímek zobrazuje umístění indikátorů o zabezpečení v prohlížečích Mozila Firefox a Opera.



Obr. 8 Signalizace bezpečnostního prostředí u prohlížečů Mozila Firefox a Opera (zdroj vlastní)

7.2 Hashovácí funkce

Představme si, že někomu posíláme nějaký druh dat, ať už se jedná o obrázek, jakkoliv dlouhý text např. v MS Word nebo video. Tento přenos uskutečňujeme digitálně a v kyberprostoru může naši komunikaci zachytit třetí strana (útočník). Budeme-li posílat elektronicky cenná a důležitá data, budeme logicky chtít, aby adresát obdržel přesně to, co jsme odeslali, neboť útočník může zprávu zachytit a přepsat či pozměnit. Aby bylo možné mezi odesílatelem a příjemcem ověřit integritu komunikované informace, lze k ní vytvořit tzv. „hash“ neboli otisk (zdroj vlastní).

Co je to Hash

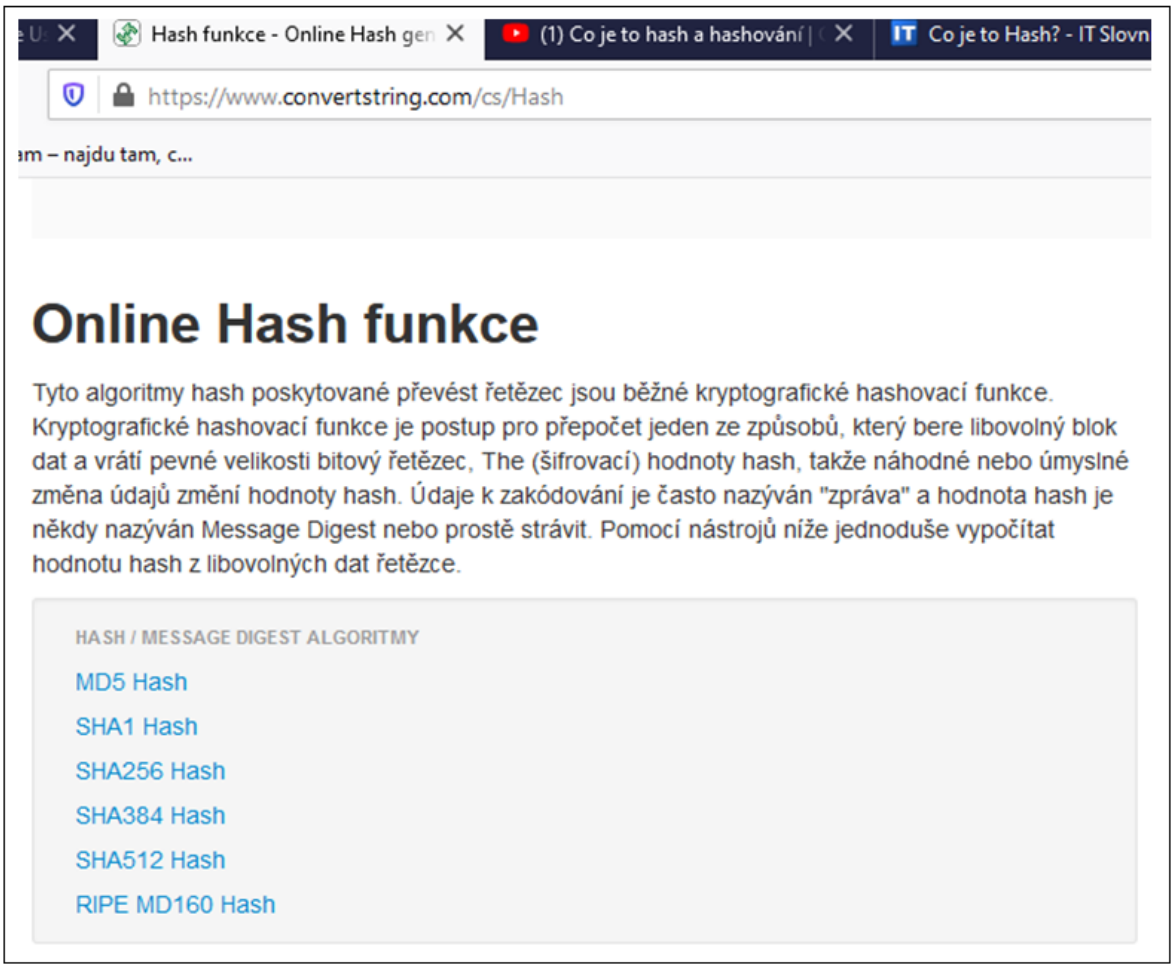
Můžeme říci, že se jedná o digitální otisk dané komunikované informace. Hash má podobu shluku čísel a písmen, která jsou vždy jedinečná. Lze jej použít v případech, kdy nechceme, aby došlo odhalení zprávy třetí stranou. Hash je jedinečný a bezpečný a to z několika důvodů:

- Hash bude vždy stejně dlouhý a nelze z něj rozpoznat např. délku hesla.
- Pokud např. v heslu nebo komunikovaném dokumentu přepíšeme byť jen jediný znak, hash se kompletně změní.
- Z hashe není možné rekonstruovat původní komunikovanou informaci.
- Je krajně nepravděpodobné, že by např. dvě stejná hesla nebo jiné informace měly stejný hash (Lujka, Řezníček, © 2018).

Budeme-li chtít ke komunikované informaci v jakékoliv podobě vytvořit hash, není to nic složitého. V současnosti jsou dostupné různé hashové online generátory, které jsou zdarma. Existuje také několik hash algoritmů, přičemž každý má jinou výslednou délku jedinečného (otisku-kódu čísel a písmen). Je tedy nutné, aby při porovnávání integrity informace jak odesílatel, tak příjemce použili stejnou hashovaní funkci se stejným algoritmem (zdroj vlastní).

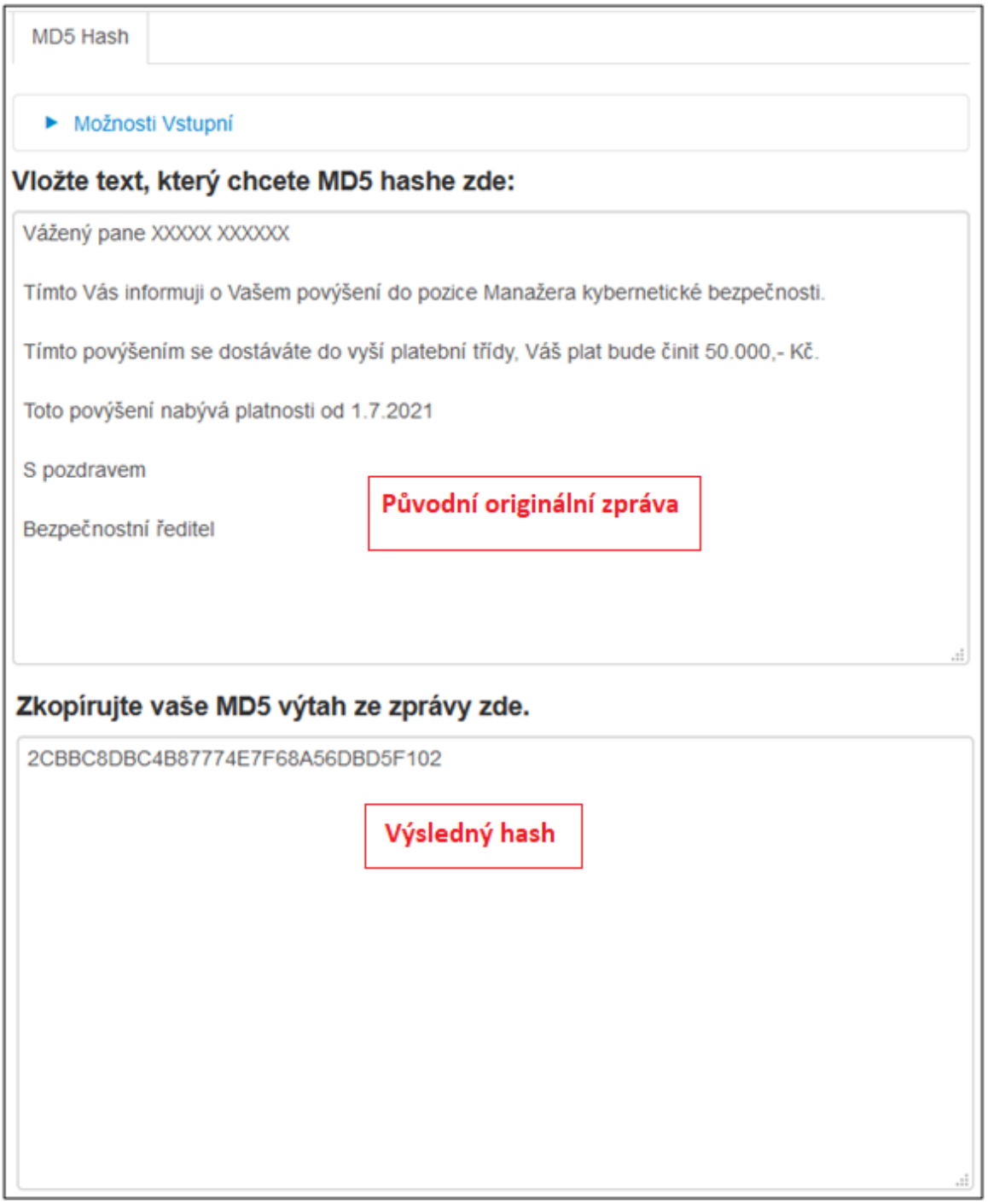
Níže je za pomoci různých online hash generátorů představen model toho, jak vytvořit hash k obyčejné textové zprávě nebo např. klasickému textovému dokumentu.

Příklad vytvoření „Hashe“ z generátoru dostupného na zabezpečeném webu https://www.convertstring.com/cs/Hash. Po otevření zmíněného odkazu se objeví titulní stránka s možností volby algoritmu kryptografické hashovaní funkce.



Obr. 9 Online generátor hashovacích funkcí (zdroj vlastní)

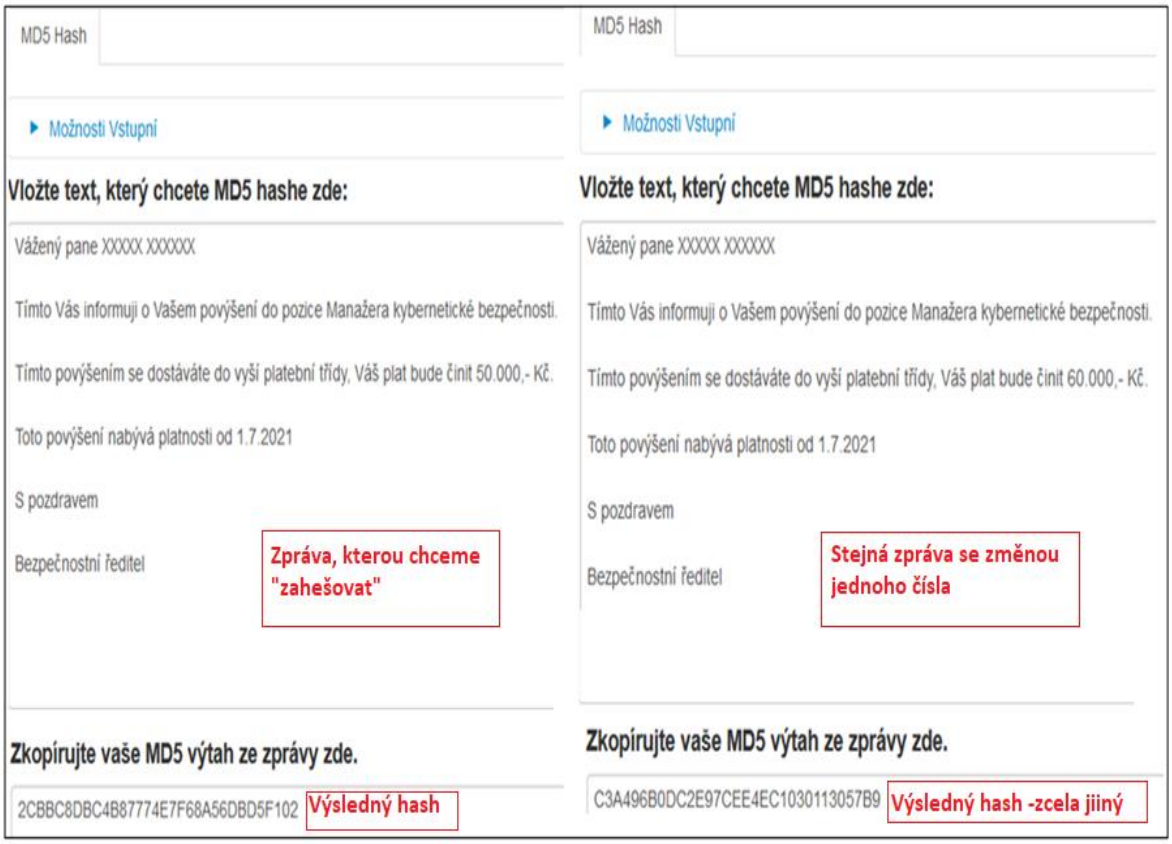
Všimněme si, že v případě této webové stránky se jedná o zabezpečení pomocí protokolu HTTPS viz kapitola 7.1. Jednotlivé hash algoritmy představují ve výsledku svého jedinečného otisku různou délku znaků a je tedy nutné, aby obě komunikující strany zvolily stejný algoritmus. Například hash zprávy: „*došlo k bezpečnostnímu incidentu*“, by v případě MD5 funkce byl jiný než v případě SHA 256 funkce. Pro příklad budeme používat hashovaní funkci MD5 , která se nám na snímku nabízí. Představme si, že posíláme jako nadřízený stupeň svému zaměstnanci emailem informaci o tom, že bude povýšen do pozice manažera kybernetické bezpečnosti a za tímto účelem mu posíláme informace o jeho novém platebním tarifu. Zobrazeno na snímku níže (zdroj vlastní).



Obr. 10 Hash zprávy v online generátoru (zdroj vlastní)

V případě zvolení funkce MD5 Hash, má výsledný jedinečný otisk délku 32 znaků. Odesílatel může příjemci pro ověření integrity odeslat hash například pomocí SMS zprávy na mobilní telefon. Příjemce po obdržení zprávy následně taktéž za využití funkce MD5 zkopíruje znění zprávy do generátoru a dostane hash který porovná s obdrženým od odesílatele, jenž jej vytvořil před odesláním zprávy. Jsou-li tyto dva hashe shodné jedná se o autentickou zprávu a je jisté, že nebyla během přenosu kyberprostorem pozměněna či

jinak znehodnocena třetí stranou. Pokud by došlo k zachycení zprávy a útočník by pozměnil její obsah, vygenerovaný hash by se neshodoval s tím, který příjemce obdržel v SMS správě. Hash je tak dokonalý, že pokud ve zprávě dojde ke změně byť jediného čísla/písmene, tak výsledný otisk bude absolutně odlišný od původního, který byl vytvořen z originální zprávy (zdroj vlastní).

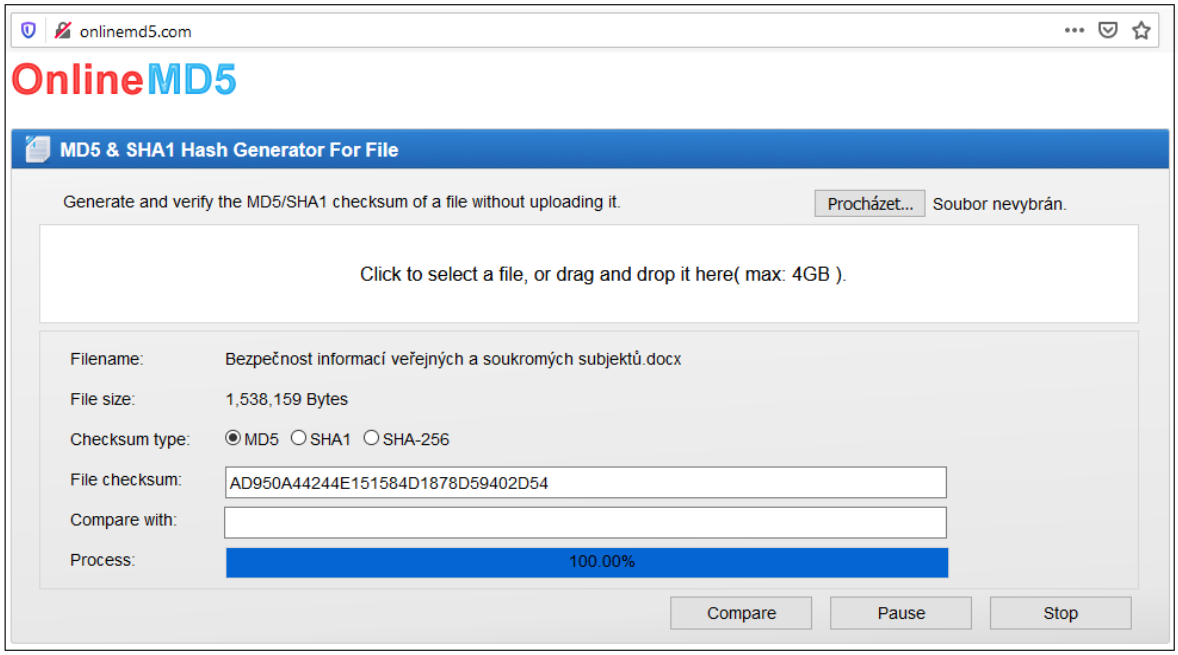


Obr. 11 Příklad rozdílného hashe při zásahu do původní zprávy (zdroj vlastní)

Na tomto snímku bylo ve zprávě pozměněno pouze jediné číslo. V původním znění zprávy došlo pouze ke změně z 50.000 na 60.000 (z čísla 5 na číslo 6). Můžeme tedy vidět, že vlivem minimálního zásahu do předávané informace došlo k vytvoření naprosto rozdílného otisku-hashe (zdroj vlastní).

Existují i online generátory, kde lze vkládat přímo konkrétní soubory pomocí přetažení buď z pracovní plochy počítače, nebo z jiného uživatelského úložiště či přes vyhledávač na samotném serveru. Lze tedy vytvořit hash například ze zaslaného dokumentu. Jako modelový příklad si představme odevzdání bakalářské práce vedoucímu (zdroj vlastní).

Pro vygenerování hashe využijeme tentokrát generátor z webu využívající protokol HTTP a to konkrétně z:http://onlinemd5.com/

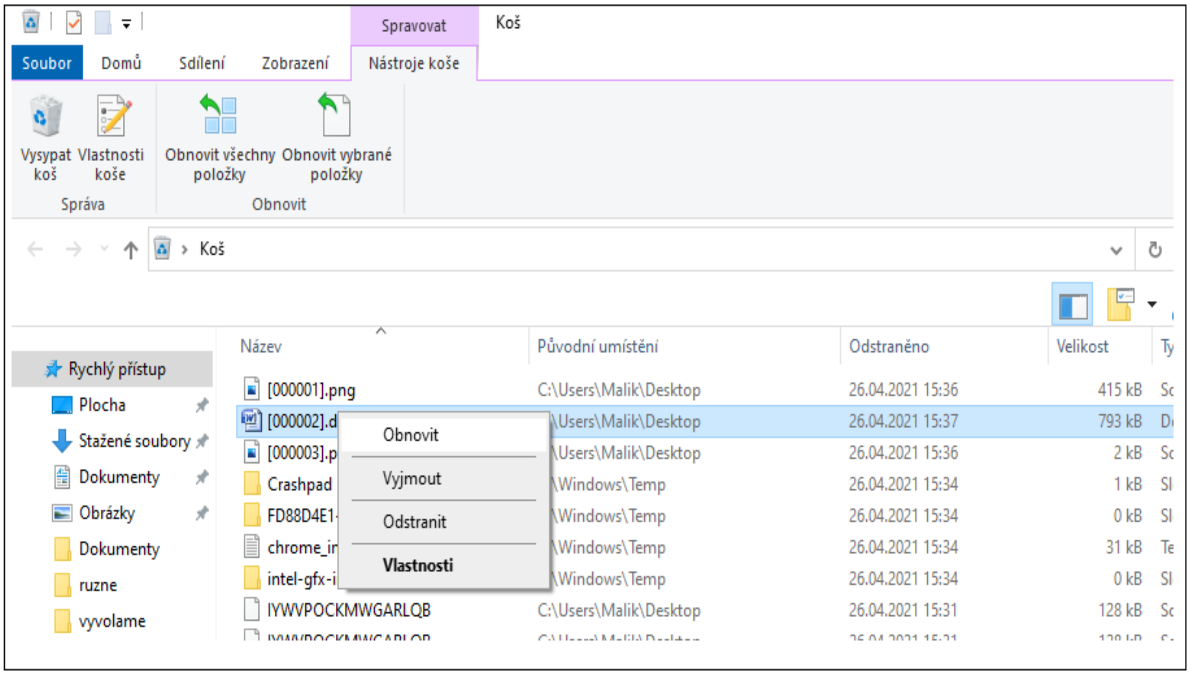


Obr. 12 Online hash generátor umožňující kódovat soubory (zdroj vlastní)

Pro vytvoření hashe byla v případě tohoto dokumentu opět vybrána funkce MD5 Hash. Odesílatel příjemci odešle emailem textový soubor a i v tomto případě hash odešle pomocí SMS zprávy. Příjemce soubor následně stáhne a vloží do téhož generátoru s využitím stejné hash funkce. Pokud se bude „otisk“ shodovat s tím v SMS zprávě, tak komunikace proběhla v pořádku bez zásahu třetí stranou. Pokud by ovšem během přenosu byla narušena integrita pozměněním obsahu dokumentu, příjemce by po obdržení takové zprávy při zpětné kontrole vygeneroval odlišný hash než odesílatel. I v tomto případě stačí, aby útočník, který by dokument během komunikace zachytil, pozměnil pouze slovo, přidal háček, či změnil v dokumentu datum a hash, který by vyšel příjemci při generování s takovýmto pozměněným souborem, by byl opět zcela odlišný. Lze tedy říci, že hash slouží k ověření pravosti zaslané informace (zdroj vlastní).

7.3 Obnova smazaných dat

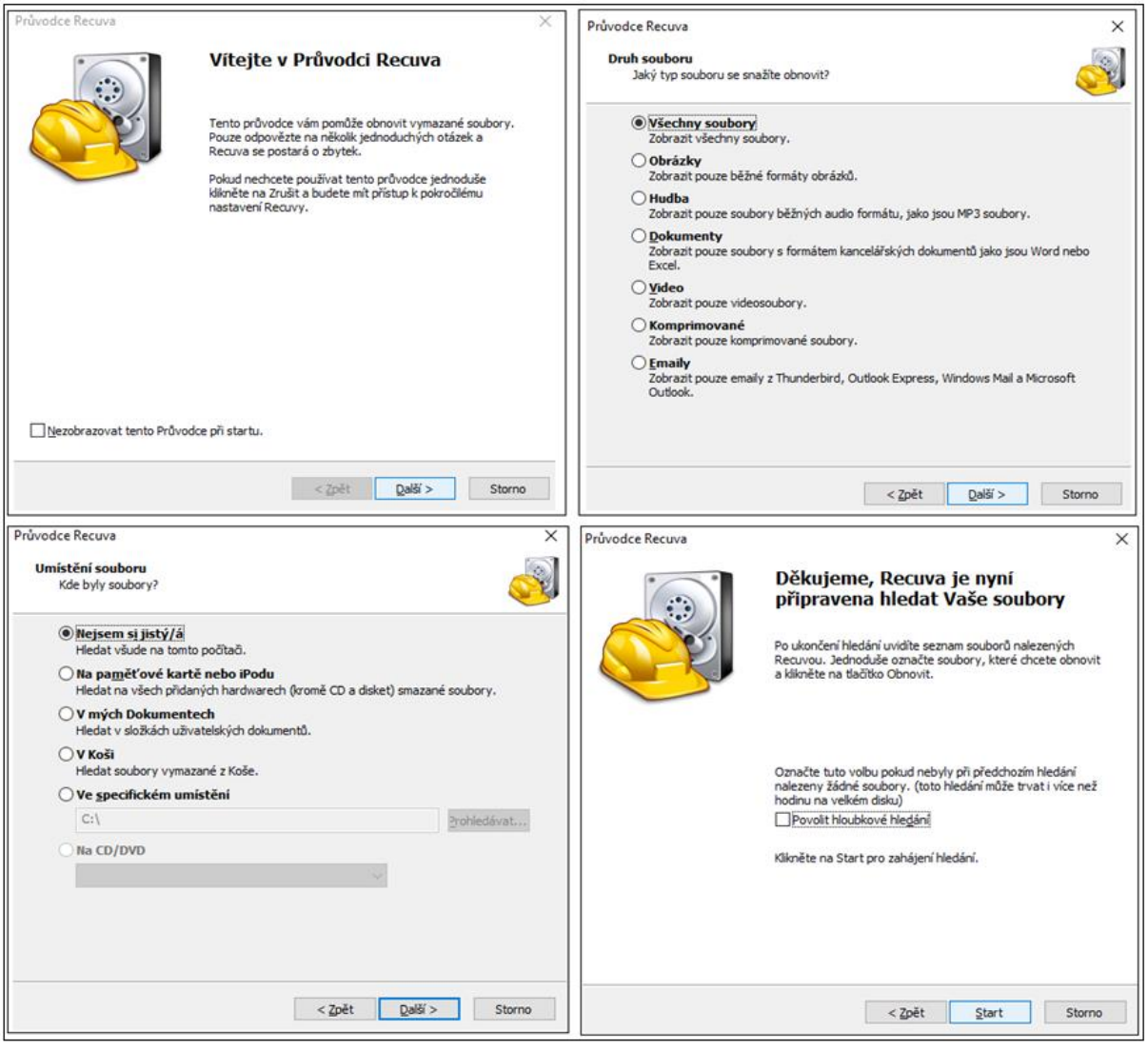
Tato část se zabývá možností jak obnovit a znovu využít smazaná data, která byla odstraněna z pevného disku nebo z přenosového média. Položme si ale otázku, proč a kdy bychom chtěli smazaná data obnovit. Základní myšlenka spočívá v tom, že cesta dat např. souborů, obrázků, písniček a jiných různých uživatelských aktiv nekončí přesunutím do „koše ani jeho vysypáním“. Smazáním jako takovým sice soubory odstraníme a uvolníme místo na pevném disku, ale ve skutečnosti je počítač pouze připraví k přepsání. Z pohledu souborového systému se soubor na disku již neobjevuje a sektory, které obsahují jeho data, jsou považovány za volné místo a jsou obnovitelné do doby, než dojde k přepsání těchto sektorů novými daty. Odstraněné soubory bychom mohli chtít obnovit například v případě, že jsme je odstranili omylem. Příkladem může být mazání dat ve složce, která obsahuje vícero druhů souborů a my spolu s těmi, které chceme odstranit, smažeme omylem i ty, které jsme si chtěli ponechat pro další užívání. V tomto případě, pokud mažeme pouze tlačítkem „delete“ na klávesnici (soubor putuje přímo do koše), nebo přes pravé tlačítko myši zvolíme v nabídce odstranit (rovněž jde soubor do koše), je nejjednodušší způsob pro obnovení souborů ten, že otevřeme na pracovní ploše „koš“ naše zájmové soubory vybereme a přes pravé tlačítko myší zvolíme „obnovit“. V tomto případě zaujmou své původní umístění v počítači. Tento nejjednodušší proces obnovy smazaných dat je zobrazen na snímku níže (zdroj vlastní).



Obr. 13 Průvodce obnovením smazaných dat z koše (zdroj vlastní)

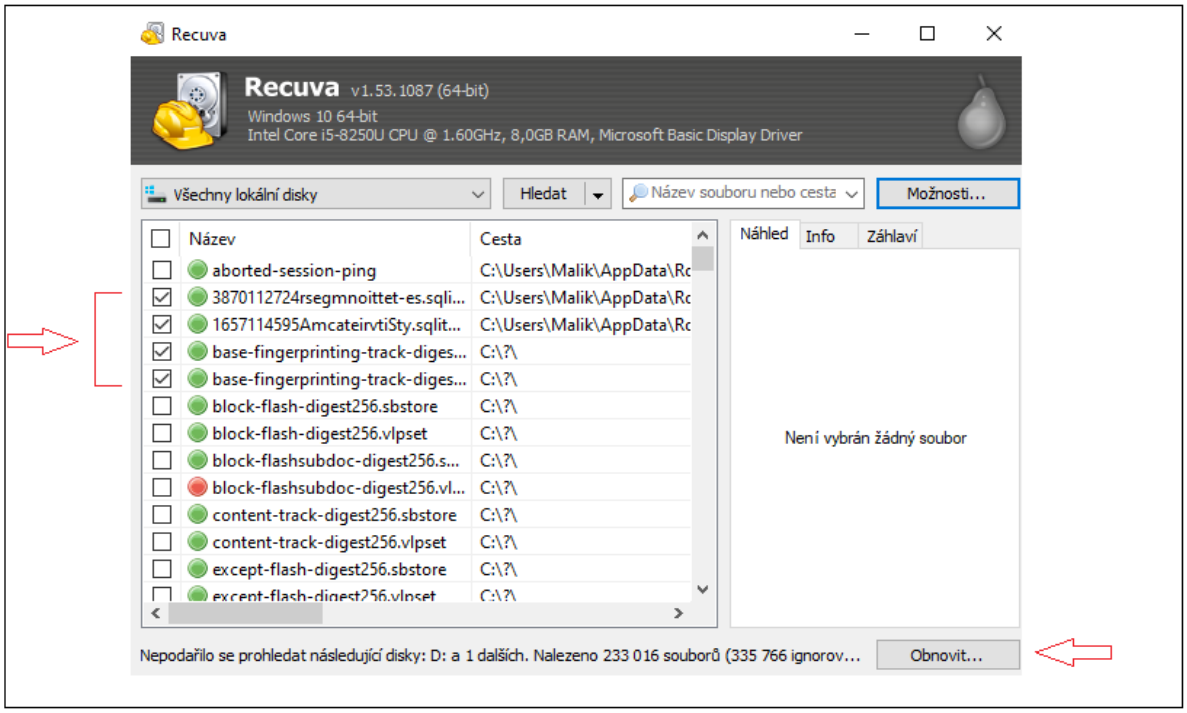
Tento proces obnovy však nefunguje v případě, že soubory smažeme stiskem kombinace kláves „Shift+Delete“. V tomto případě jsou soubory trvale odstraněny a přes koš neputují. Ovšem ani v tomto případě nejsou odstraněny trvale. Zatím jsou stále obnovitelné pomocí níže zmíněného programu. Ovšem, chceme-li tyto data obnovit, měli bychom s diskem pracovat pokud možno co nejméně a pokusit se o obnovu v co nejkratší době (zdroj vlastní).

Systém Windows sice nemá v základu nástroj, který by skenoval na pevném disku odstraněné soubory, ale jsou externí programy. Mezi snadno dostupný a uživatelsky přívětivý můžeme zařadit program „Recuva“. Tento program je zdarma dostupný např. na serveru: https://stahuj.cz. Níže na snímku je zobrazen průvodce programu, díky kterému uživatel dokáže vyfiltrovat, jaká akce bude probíhat (zdroj vlastní).



Obr. 14 Průvodce programu Recuva před prvotní analýzou (zdroj vlastní)

Po absolvování zmíněných kroků na snímku výše se v okně programu zobrazí všechny dostupné obnovitelné soubory, které byly nalezeny na těch úložných prostorech, které jsme vybrali v průvodci na začátku, včetně externích úložišť připojených k počítači.

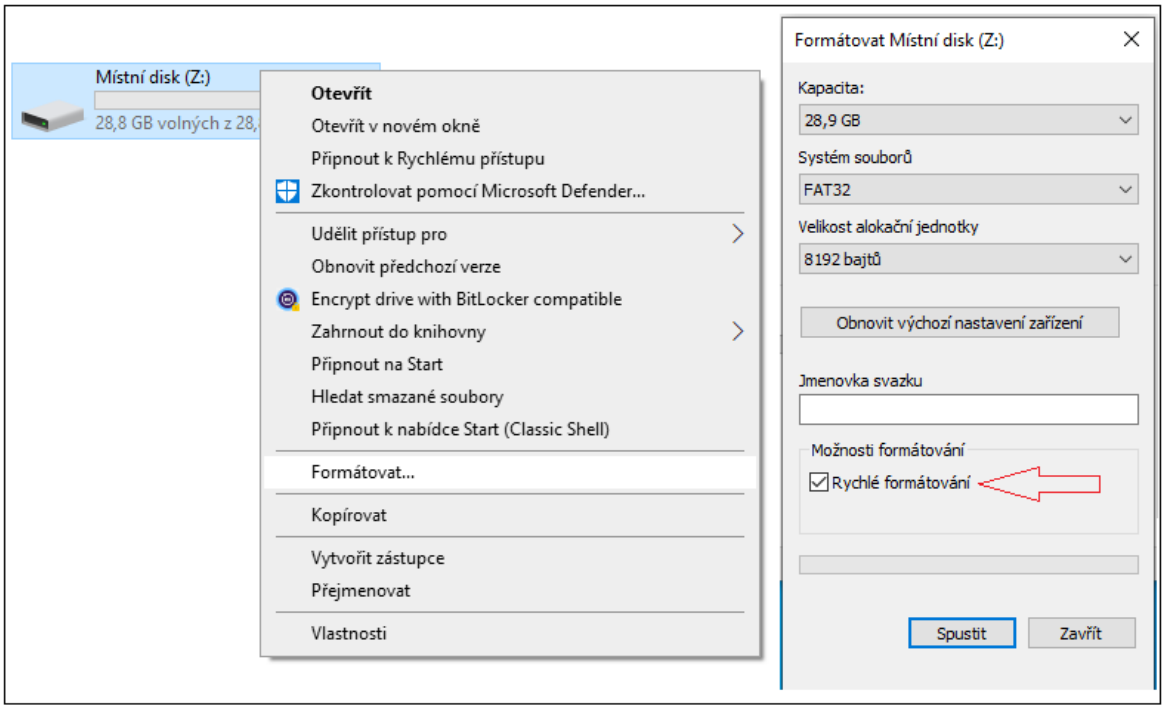


Obr. 15 Výsledky analýzy smazaných dat v programu Recuva (zdroj vlastní)

Po ukončení vyhledávání můžeme s programem dále pracovat, např. zvolit znovu konkrétní úložiště, které bude prohledáno, případně lze zadat funkci hloubkového hledání, přičemž je ale doba analyzování podstatně delší i v řádu několika hodin vzhledem k velikosti harddisku a ostatních úložišť. Soubory, které budeme chtít obnovit, jednoduše označíme jako na výše zmíněném snímku a následně po kliknutí na tlačítko „obnovit“ vybereme konkrétní místo v počítači nebo externím úložišti, kam budou data převedeny.

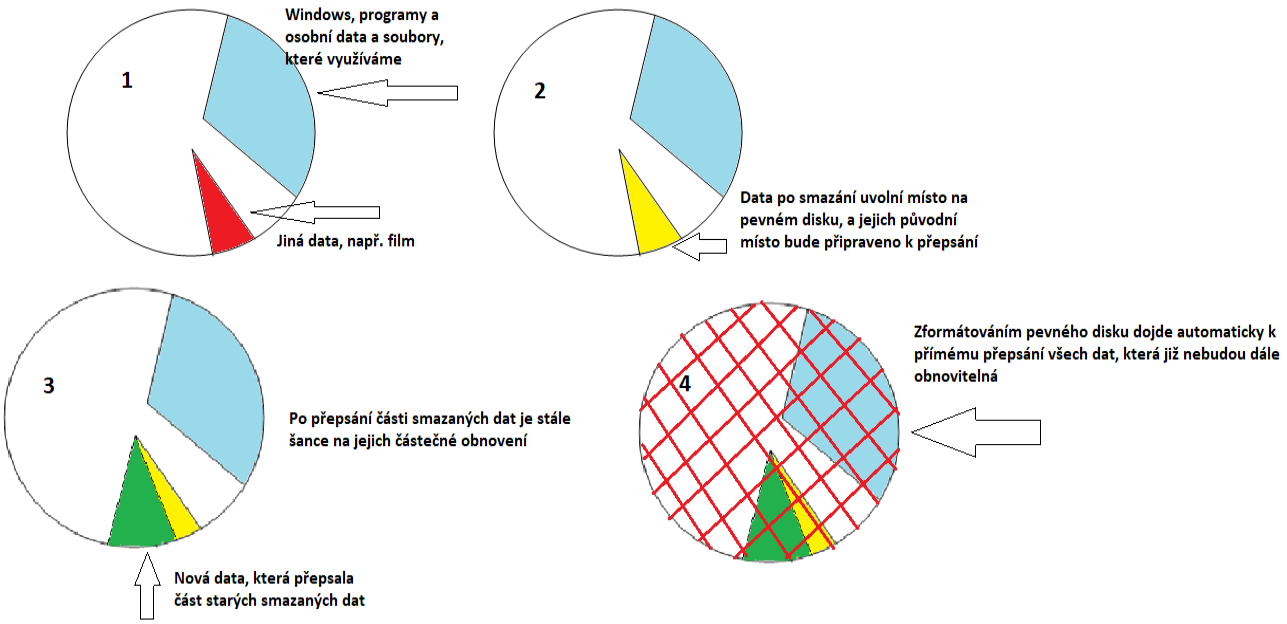
Problém nastává v případě, kdy nejsme dost opatrní při mazání různých citlivých dat. Představme si, že opouštíme pracovní pozici, na které jsme pracovali s citlivými nebo dokonce s utajovanými dokumenty a informacemi a předáváme počítač nebo např. flash disk jiné osobě, která s ním bude dále pracovat. Nyní již víme, že nestačí tyto informace smazat, ale je třeba je smazat tak, aby nebyla možná jejich rekonstrukce. V tomto případě je efektivním nástrojem formátování. Zformátujeme-li pevný disk, data z něj již neobnovíme. Pozor si však musíme dát při formátování flash disků. Zde v případě volby

formátování musíme provést hloubkové formátování, nikoli tzv. „rychlé formátování“, které se bude nabízet automaticky jako na snímku níže (zdroj vlastní).



Obr. 16 Formátování flash disku (zdroj vlastní)

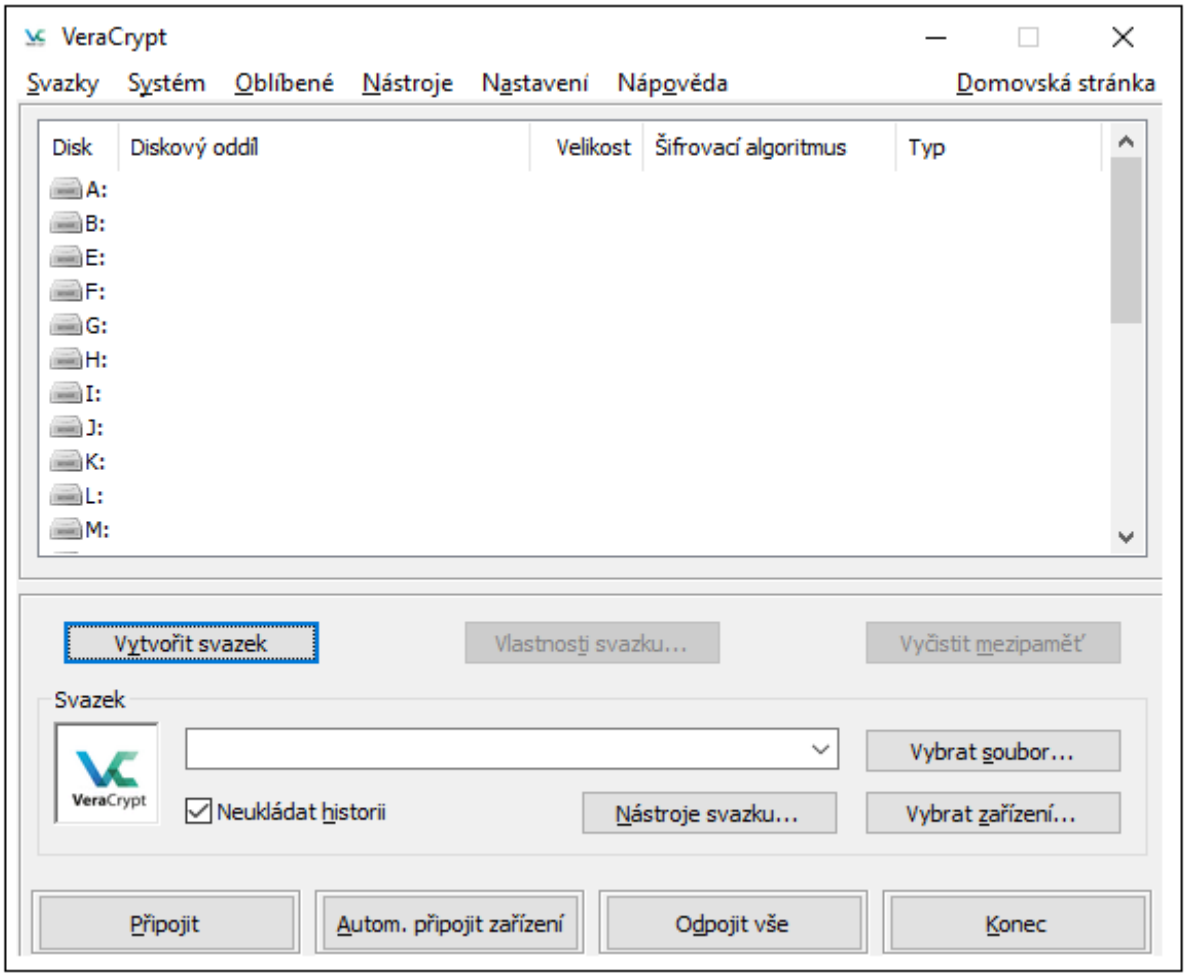
Pokud ponecháme při formátování flash disku automaticky nabídnutou volbu „rychlého formátování“, takto smazaná data budou poté programem „Recuva“ i nadále obnovitelná. Pro trvalé a neobnovitelné odstranění souborů je nutné tuto volbu nevyužívat (zdroj vlastní).



Obr. 17 Koloběh života dat (zdroj vlastní)

7.4 Šifrování dat

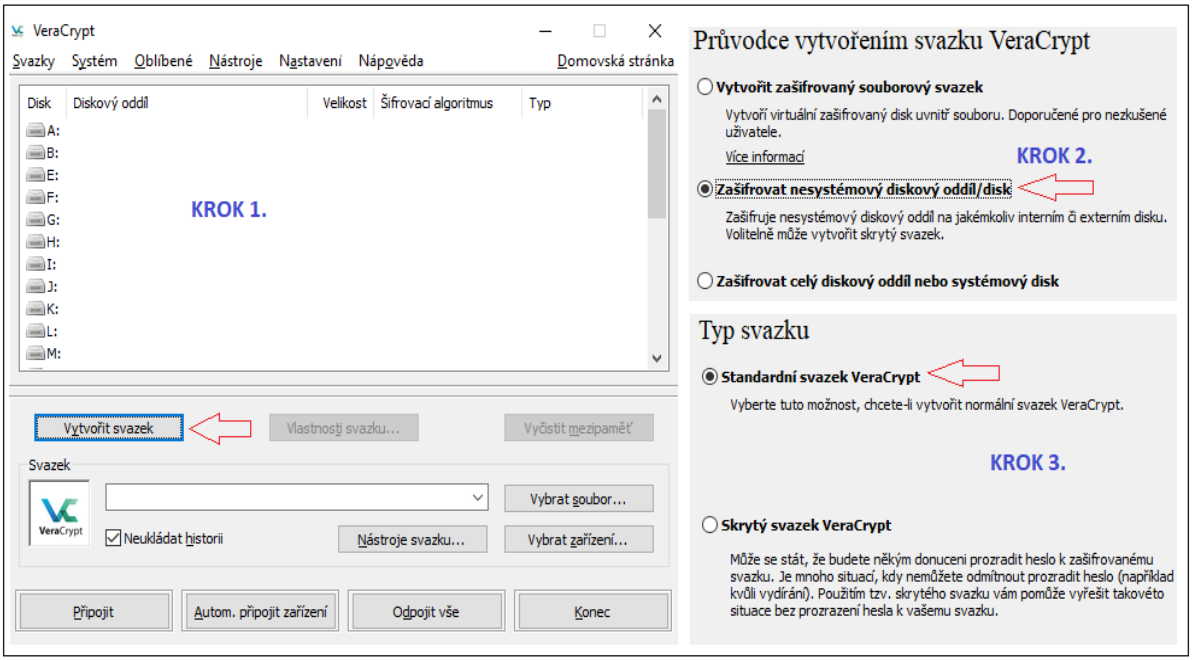
Jako jednu z možností ochrany informací a dat lze zvolit šifrování. Můžeme zašifrovat samotné soubory či složky nebo i celý harddisk či externí úložiště. Některé verze operačního systému Windows obsahují ve svých nástrojích šifrovací funkce, pomocí kterých lze šifrovat pevné disky. Pokud splňujeme za tímto účelem verzi operačního systému, nemusí však podmínky pro šifrování splňovat naše fyzické zařízení (počítač jako takový). I v tomto případě existuje několik programů, které mohou šifrovat pevné disky i externí úložiště. Pro následující model je vybrán program „VeraCrypt“, který je jako programy zmíněné v předchozích kapitolách dostupný zdarma ke stažení. I v tomto případě jej lze stáhnout z webu: https://stahuj.cz (zdroj vlastní).



Obr. 18 Představení rozhraní programu VeraCrypt (zdroj vlastní)

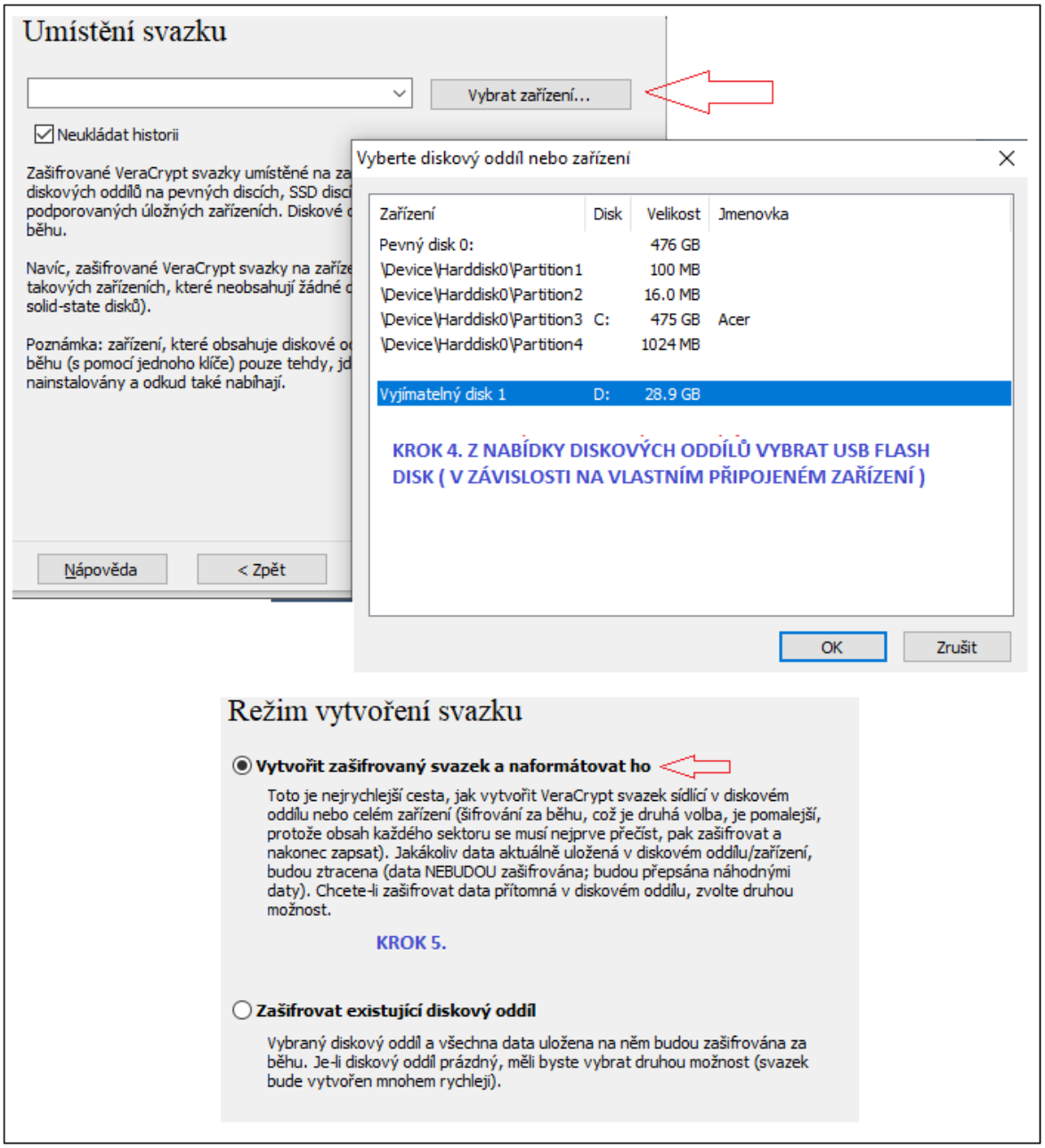
Představme, že pracujeme pro nás s cennými informacemi, které chceme utajit a které pro svou potřebu přenášíme na flash disku, díky čemž jsou nám dostupné vždy a všude. Nemusíme tedy šifrovat jednotlivé soubory, ale lze jednoduše zašifrovat celý flash disk, který se tak stane nečitelným v případě, že by jej někdo nalezl a chtěl přečíst jeho obsah ve svém vlastním zařízení. Takto uzamčený disk lze odemknout pouze opět v programu VeraCrypt, přičemž k samotnému odemknutí je třeba znát heslo, které jsme si samozřejmě vygenerovali před šifrováním. Co ale v případě, že budeme chtít přenosné médium rozjet v jiném zařízení (zdroj vlastní). V tomto případě umožňuje program Veracrypt vytvoření tzv. „cestovatelského disku“ (nebo přenosného/traveler disku). Tato funkce spočívá v nainstalování kopie VeraCryptu na samotný flash disk, což umožní fungování USB disku i v jiném počítači se systémem Windows, přičemž při vytváření takovéhoto přenosného zařízení nastavíme funkci „automatické spuštění“, která spustí program VeraCrypt v cizím zařízení bez nutnosti jej instalovat (Rubens, 2016).

Grafické znázornění tvorby šifrovaného USB flash disku:



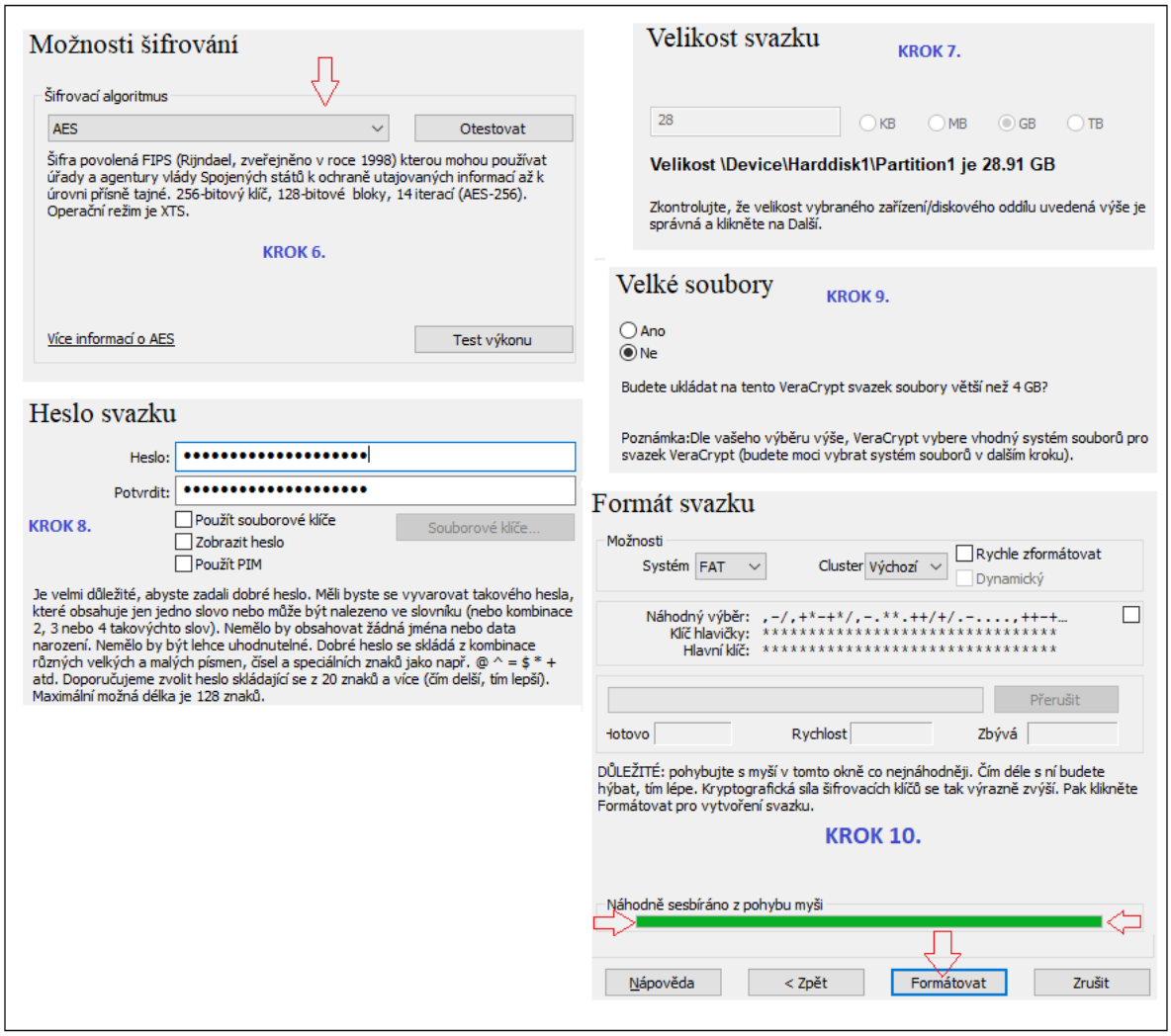
Obr. 19 Postup při šifrování v programu Veracrypt (zdroj vlastní)

Následující snímky zobrazují jednoduché kroky, které uživatel podstoupí pro zašifrování USB disku. Celý postup je graficky a popisově zpracován tak, aby dle něj mohl postupovat běžný uživatel ICT.



Obr. 20 Postup při šifrování v programu Veracrypt (zdroj vlastní)

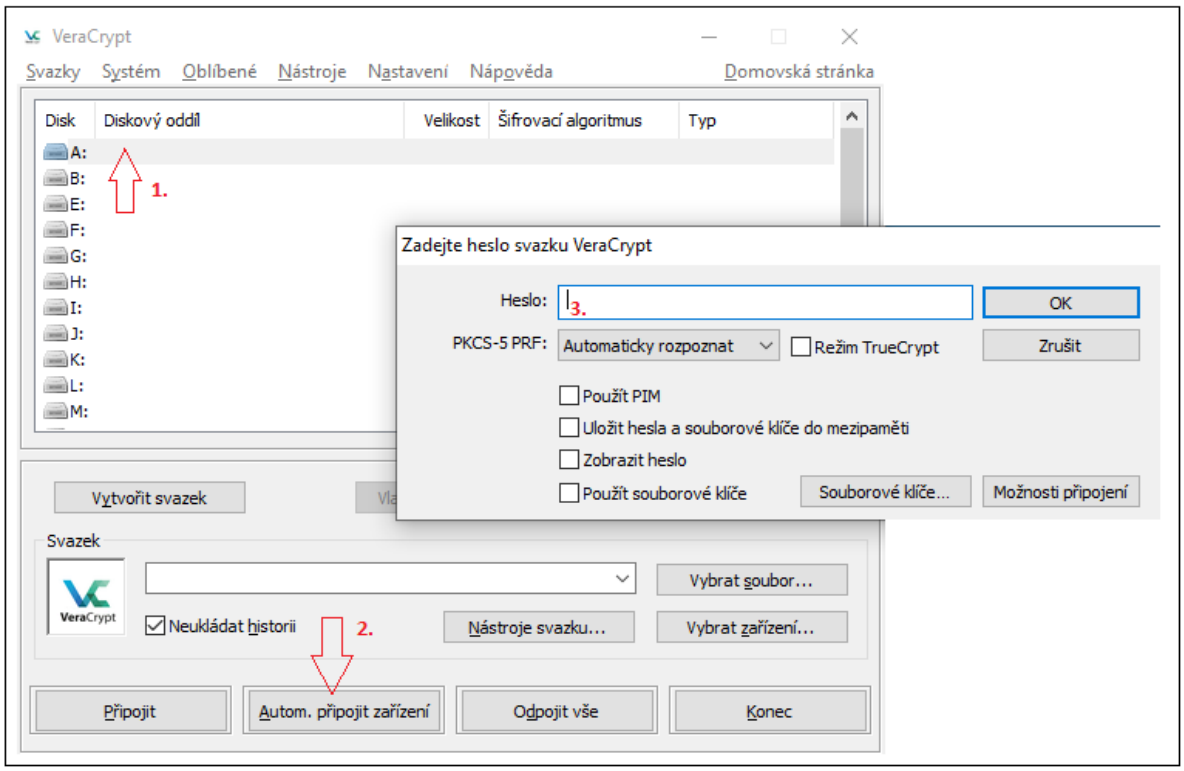
V kroku č. 4 je nutné vybrat správné zařízení, aby uživatel skutečně zašifroval cílený USB disk. Jako pomocné informace pro správné zvolení mohou sloužit v tomto případě data o velikosti jednotlivých disků, přičemž se pravděpodobně v případě notebooků a stolních počítačů s připojenými USB disky budou pohybovat v rozmezí několika set gigabyte až po desítky gigabyte. Při klasických velikostech USB flash disku 16, 32, 64 gigabyte bude správná volba zřetelná. V případě české verze programu pak bude klíčová informace „Vyjímatelný disk“ s označením jednotky (zdroj vlastní).



Obr. 21 Postup při šifrování v programu Veracrypt (zdroj vlastní)

V kroku č. 6 ponecháme zvolený šifrovací algoritmus „AES“. Sedmý krok je kontrolní a slouží k tomu, abychom potvrdili, že se skutečně jedná o flash disk, který chceme šifrovat. Pro kontrolu porovnání lze také využít údaj o kapacitě na samotném tělese USB disku. Při zadávání hesla (krok č. 8) program sám vybízí k silnému heslu a specifikuje i jeho délku a druh znaků, ale uživatel v tomto případě může užít jemu známého hesla, které podmínky uvedené programem splňovat nebude. V tomto případě bude ale upozorněn, že zadal slabé heslo, ale bude moci pokračovat dál. Volba v následujícím kroku je čistě individuální vzhledem k datům, které budou na disk později nahrávány. V posledním kroku se budeme řídit výhradně pokyny programu v daném pracovním okně a zakončíme klikem na tlačítko formátovat. Pro představu bylo vyzkoušeno zašifrování USB flash disku o kapacitě 32 gigabyte a doba trvání byla 3 hodiny (zdroj vlastní).

Pro opětovné využívání zašifrované USB disku je zapotřebí opět interakce v programu VeraCrypt. Níže na snímku je postup jak zašifrovanou jednotku otevřít.



Obr. 22 Odšifrování flash disku v programu VeraCrypt (zdroj vlastní)

Po vložení zašifrovaného USB disku do počítače se jednotka načte pod klasickým označením diskového oddílu, jako tomu bylo před zašifrováním. Ale bude neaktivní a bude hlásit, že disk musí být před použitím naformátován, čímž by se ale ztratily veškerá uložená data (zdroj vlastní).

Postup pro aktivaci zašifrovaného disku dle snímku výše:

- Nejprve zvolíme volnou jinak nepoužívanou jednotku, pod kterou bude šifrovaný disk v počítači vystupovat.
- Jako druhý krok zvolíme možnost automatického připojení zařízení, přičemž program sám aktivuje jím zašifrované médium.
- V poslední řadě zadáme heslo, které jsme si vytvořili výše při kroku č. 8 str. 64.

Disk bude nyní v počítači vystupovat pod označením jednotky, kterou jsme zvolili během kroku č. 1 na snímku výše (zdroj vlastní).

8 DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI

Překvapivým zjištěním je fakt, že doporučené normy i přesto že nejsou nadřazeny závazným zákonným normám, regulují některé oblasti přísněji konkrétněji a detailněji. V mnohých případech tedy dojde užitím norem automaticky k naplnění povinností vyplývajících ze zákona. V případě bezpečnosti informací to jasně vyplývá z provedené komparace. Naskýtá se tedy otázka, zda subjekty které jsou povinny se řídit zákonem o kybernetické bezpečnosti, mohou zvýšit účinnost zabezpečení dodatečnou aplikací některou z norem řady ISO 27000.

V části zahrnující samotné uživatelské praktiky, které mají za cíl zvýšit bezpečnost dat a komunikovaných informací jsou přestaveny zajímavé programy, které autor využil prvně až při zpracovávání této práce. Zde zmíněné techniky jsou efektivní a poměrně snadno uživatelsky ovladatelné.

Samotné šifrování je účinné, ale ve své podstatě pouze „zakóduje“ komunikaci, nebo komunikovanou informaci. Ovšem existují i další metody. Představme si, že nechceme, aby kdokoliv věděl, že nějaká komunikace potažmo přenos informací vůbec probíhá. Způsob, který za tímto účelem ukrývá samotnou komunikaci, se nazývá „steganografie“ a spočívá v ukrytí dat uvnitř jiných dat. Můžeme například poslat textový dokument obsahující tajné informace, který bude vložen do obyčejné fotografie ve formátu „jgp“, na které naše kočka pije vodu z vany. Případný útočník by pak tuto komunikaci ignoroval, protože by nejspíš nejevil zájem o bezcenné fotografie domácích mazlíčků. Tento postup je však uživatelsky náročnější a zahrnuje znalosti příkazových řádků.

ZÁVĚR

Tato práce přinesla autorovi mnohá obohacení, neboť téma samotné široce zahrnuje oblast informačních a komunikačních technologií jako takových, přičemž v tomto odvětví nikdy předtím nic nezpracovával. Od začátku to bylo „pohybování se v nových vodách“ a každý zjištěný poznatek byl přínosem v podobě zajímavé a hodnotné informace. Sám autor se plně ztotožňuje s myšlenkou, že využívání moderních digitálních informačních technologií je nezbytné pro fungování v současné společnosti a je nutno držet krok s vývojem v této oblasti a plně s ním korespondovat.

Moderní digitální svět se neustále plní novými technologiemi, které se stávají nedílnou součástí fungování všech odvětví jako např. průmyslu, ekonomiky a samozřejmě především informačních a komunikačních technologií. Množství informací ve všech jejich formách se tak rovněž dramaticky navyšuje. Tyto informace se tak stávají velice atraktivním lákadlem pro zneužití nebo krádež.

Tato práce se zabývá především možnostmi regulace široce zavedených postupů a opatření směrem k bezpečnosti informací jako takových. Výsledná rešerše v oblasti závazných a doporučených norem, které regulují tuto předmětnou oblast, pak přináší přehledy konkrétních zákonů a rozsáhlé řady ISO norem.

Komparace samotná pak spočívá v nalezení diferencí v konkrétních oblastech zabezpečení mezi závaznými a doporučenými normami, přičemž lze tímto způsobem zhodnotit, jak která norma konkrétně řeší samostatná odvětví, která jsou ve své podstatě zaměřena na zabezpečení informací potažmo kybernetické bezpečnosti.

Celkově se práce věnuje bezpečnosti informací z širší perspektivy. Závazné a doporučené normy jsou zde sice na primární úrovni, ale představují pouze první část oné myšlenky bezpečného chování v současném světě řízeném informačními technologiemi. Druhým krokem je pak představení jednotlivých praktik, které vedou opět pouze k jedinému cíli a tím je maximalizovat bezpečné chování uživatelů v rámci využívání informačních technologií.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje

BASL, Josef a Roman BLAŽÍČEK, 2012. *Podnikové informační systémy: Podnik v informační společnosti*. 3., aktualizované a doplněné vydání. Praha: Grada. ISBN 978-80-247-4307-3.

DEATH, Darren, 2017. *Information Security Handbook: Develop a threat model and incident response strategy to bulid a strong information secuity network* [online]. Birmingham: packtpub [cit. 2020-11-17]. ISBN 978-1-78847-833-0. Dostupné z: https://vufind.katalog.k.utb.cz/Record/91175

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary* [online]. Třetí aktualizované vydání. Praha: Národní centrum kybernetické bezpečnosti [cit. 2020-11-14]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

KOLOUCH, Jan, 2016. *CYBERCRIME* [online]. Praha: CZ.NIC [cit. 2021-4-26]. ISBN 978-80-88168-16-4. Dostupné z: https://www.bookport.cz/e-kniha/cybercrime-510716/#

KOLOUCH, Jan a Pavel BAŠTA a spol., 2019. *CyberSecurity* [online]. Praha: CZ.NIC [cit. 2020-11-13]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

LINDOVSKÝ, Vít a kol., 2008. *EGovernment bezpečně* [online]. Praha: Grada [cit. 2020-11-19]. ISBN 978-80-247-2462-1. Dostupné z: https://vufind.katalog.k.utb.cz/Record/bkp01527

LUDĚK, Lukáš a kol., 2013. *Bezpečnostní technologie, systémy a managment III*. Zlín: VeRBuM. ISBN 978-80-87500-35-4.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK, 2013. *Problematika ISMS v manažerské informatice*. Brno: CERM. ISBN 978-80-7204-872-4.

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk. ISBN 80-86898-38-5.

SINGER, P.W. a Allan FRIEDMAN, ©2014. *Cybersecurity and Cyberwar: what everyone needs to know*. I. Title. New York: Oxford University. ISBN 978-0-19-991809-6.

SMEJKAL, Vladimír a Karel RAIS, 2006. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualizované a rozšířené vydání. Praha: Grada. ISBN 80-247-1667-4.

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

WHITMAN, Michael E. a Herbert J. MATTORD, ©2012. *Principles of Information Security: International Edition*. Fourth Edition. Canada: Course Technology. ISBN 978-1-1111-3823-3.

Internetové zdroje

ANTOŠ, Michal, 2020. Regulace kybernetické bezpečnosti v soukromém sektoru. *Právní prostor* [online]. Šetina Komendová & Partners [cit. 2020-12-12]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/regulace-kyberneticke-bezpecnosti-v-soukromem-sektoru#note-1

ČESKO. Zákon č. 365/2000 Sb. o informačních systémech veřejné správy. In: *Sbírka zákonů*. 99/2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-365?text=365%2F2000

ČESKO. Zákon č. 412/2005 Sb. ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů*. 143/2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Sbírka zákonů*. 75/2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO. Vyhláška č. 82/2018 Sb. (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. 43/2018. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82?text=vyhl%C3%A1%C5%A1ka+o+kybernetick%C3%A9#f6229263

ČESKO. Zákon č. 89/2012 Sb. občanský zákoník. In: *Sbírka zákonů*. 33/2012. Dostupné také z: https://www.zakonyprolidi.cz/cs/2012-89?text=obchodn%C3%AD%20tajemstav%C3%AD

ČESKO. Zákon č. 110/2019 Sb. o zpracování osobních údajů. In: *Sbírka zákonů*. 47/2019. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

ČESKO. Zákon č. 455/1991 Sb. o živnostenském podnikání. In: *Sbírka zákonů*. 87/1991. Dostupné také z: https://www.zakonyprolidi.cz/cs/1991-455

ČESKO. Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů*. 173/2004. Dostupné také z: https://www.zakonyprolidi.cz/cs/2004-499

ČSN ISO/IEC 27002, 2014. *ČESKÁ TECHNICKA NORMA ČSN ISO/IEC 27002: Informační technologie-Bezpečnostní techniky-Soubor postupů pro opatření bezpečnosti informací*. Úřad pro technickou normalizaci.

FUKÁRKOVÁ, B., 2019. Rizika a úskalí informační společnosti: A digitální propast je to jediné, co informační společnost trápí? *Medium.com* [online]. [cit. 2021-4-26]. Dostupné z: https://medium.com/edtech-kisk/rizika-a-%C3%BAskal%C3%AD-informa%C4%8Dn%C3%AD-spole%C4%8Dnosti-85b916f50cf0

KOĎOUSKOVÁ, Barbora, 2021. HTTPS v kostce: co to je, jak funguje a jak na něj přejít: Co je to HTTPS. *Rascasone* [online]. Praha [cit. 2021-4-27]. Dostupné z: https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls

LUJKA, Miloslav a Pavel ŘEZNÍČEK, (c) 2018. Hash. *Digitální pevnost: Bojujeme za bezpečnější digitální svět* [online]. [cit. 2021-4-27]. Dostupné z: https://www.digitalnipevnost.cz/viki/hash

Národní strategie informační bezpečnosti ČR (NSIB ČR). Verze 0.8, 4. 10. 2005.

NAŘÍZENÍ GDPR: Vše co potřebujete vědět o GDPR na jednom místě, (c) 2021. *GDPR solutions* [online]. ANT Studio [cit. 2021-03-20]. Dostupné z: https://www.gdprsolutions.cz/narizeni-gdpr/

Doporučení k používání protokolu TLP ke sdílení chráněných informací, 2020. *NÚKIB* [online]. Brno [cit. 2021-4-29]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/

RUBENS, Paul, 2016. How to Encrypt a Flash Drive Using VeraCrypt. *ESecurity Planet* [online]. Nashville [cit. 2021-4-28]. Dostupné z: https://www.esecurityplanet.com/applications/how-to-encrypt-a-flash-drive-using-veracrypt/

ŘEHKA, Karel, 2020. Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025. *NÚKIB* [online]. Brno [cit. 2020-12-12]. Dostupné z: https://nukib.cz/cs/

ŠKORNIČKOVÁ, Eva, b.r. Co je GDPR? *Gdpr.cz* [online]. Praha [cit. 2021-01-12]. Dostupné z: https://www.gdpr.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	-	Confidentiality, Integrity, Availability
EU	-	Evropská unie
GDPR	-	General Data Protection Regulation
HTTP	-	Hyper Text Transfer Protocol
HTTPS	-	Hyper Text Transfer Protocol Secure
ICT	-	Information and Communication Technology
INFOSEC	-	Information Security
ISVS	-	Informační systém veřejné správy
KB	-	Kybernetická bezpečnost
MŠMT	-	Ministerstvo školství mládeže a tělovýchovy
NATO	-	North Atlantic Treaty Organization
NBÚ	-	Národní bezpečnostní úřad
NSIB ČR	-	Národní strategie informační bezpečnosti
NUKIB	-	Národní úřad pro kybernetickou a informační bezpečnost
OUI	-	Ochrana utajovaných informací
PFO	-	Podnikající fyzická osoba
PO	-	Právnická osoba
SPOF	-	Single Point of Failure
SW	-	Software
TLP	-	Traffic Light Protocol
URL	-	Uniform Resource Locator
USB	-	Universal Serial Bus
VIS	-	Významný informační systém

SEZNAM OBRÁZKŮ