Informační bezpečnost z pohledu uživatele osobního počítače

Bc. Lukáš Navrátil

Diplomová 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 DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Lukáš Navrátil**
Osobní číslo:	**L19256**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Informační bezpečnost z pohledu uživatele osobního počítače**

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k dané problematice.
2. Proveďte analýzu informační bezpečnosti uživatele osobního počítače.
3. V návaznosti na předchozí analýzu navrhněte možná opatření na zvýšení informační bezpečnosti uživatele osobního počítače.
4. Vytvořte příručku pro zvýšení informační bezpečnosti uživatele osobního počítače.

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

Seznam doporučené literatury:

1. DE GUISE, Preston, 2020. *Data protection: ensuring data availability*. Second edition. New York: Taylor & Francis. ISBN 978-036-7256-777.
2. DIOGENES, Yuri a Erdal OZKAYA. *Cybersecurity – attack and defense strategies: infrastructure security with Red Team and Blue Team tactics*. Birmingham: Packt, 2018, viii, 367 s. ISBN 9781788475297.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

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

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 6. srpna 2021

Jméno a příjmení studenta: Bc. Lukáš Navrátil

…….

podpis studenta

ABSTRAKT

Tato diplomová práce byla zpracována za účelem zefektivnit a zlepšit informační bezpečnost uživatele osobního počítače. Což zahrnuje objasnění věcí týkajících se tohoto tématu zjištění bezpečnostní situace u běžných uživatelů a návrhu opatření.

V teoretické části je řešeno definování základních pojmů z oblasti kybernetické a informační bezpečnosti pro uvedení čtenáře do dané problematiky. Jedná se především o kyberprostor, kybernetickou bezpečnost či data a informace. Pochopení těchto pojmů je základním stavebním kamenem pro orientaci v předmětu kybernetické bezpečnosti a samozřejmě informační bezpečnosti, která je součástí kybernetické bezpečnosti. Velký prostor je věnován také kybernetickým útokům, které nejsou v dnešní době ničím výjimečným. Pro přehlednost bylo vybráno pouze několik typů útoků, jež jsou nejčastěji prováděny, ať už se jedná o ransomware, phishing či další uvedené. Znalost principu kybernetických útoků pomáhá ke zvýšení informační bezpečnosti.

Praktická část je zaměřena na identifikování hrozeb pro informační bezpečnost na což navazuje následné vyhodnocení aktuální informační bezpečnosti u běžných uživatelů osobního počítače, které odhalilo závažné nedostatky v této oblasti, načež byla formulována opatření ke zvýšení informační bezpečnosti. Šifrování, zálohování dat, nastavení silného hesla či používání anti-malwaru jsou ochranná opatření, která zvyšují informační bezpečnost a měla by být základem ochrany dat každého uživatele. Celkovým výstupem této práce je vytvořená bezpečnostní příručka, která má sloužit ke zvýšení informační bezpečnosti uživatele osobního počítače.

Klíčová slova: bezpečnost informací, kybernetický útok, malware, silné heslo, šifrování, zálohování.

ABSTRACT

This diploma thesis was prepared in order to streamline and improve the information security of personal computer users. This includes clarifying matters related to this topic, determining the security situation of ordinary users and proposing measures.

The theoretical part deals with the definition of basic concepts in the field of cyber and information security to introduce the reader to the issue. These are mainly cyberspace, cyber security or data and information. Understanding these concepts is the basic building block for orientation in the subject of cyber security and, of course, information security, which is part of cyber security. A large space is also devoted to cyber-attacks, which are nothing special nowadays. For the sake of clarity, only a few types of attacks have been selected, which are the most frequently carried out, be they ransomware, phishing or others listed. Knowledge of the principle of cyber-attacks helps to increase information security.

The practical part is focused on identifying threats to information security, which is followed by a subsequent evaluation of current information security for ordinary personal computer users, which revealed serious shortcomings in this area, after which measures were formulated to increase information security. Encryption, data backup, strong password settings or the use of anti-malware are protective measures that increase information security and should be the basis for protecting every user's data. The overall output of this work is a security manual, which is to serve to increase the information security of personal computer users.

Keywords: information security, cyber-attack, malware, strong password, encryption, backup

Poděkování

Ze všeho nejdříve bych chtěl poděkovat svému vedoucímu diplomové práce panu Ing. Petru Svobodovi, PhD., který měl mnoho trpělivosti při vedení této diplomové práce a také pro poskytnuté konzultace a cenné rady. Velké poděkování musí mířit také mé rodině, která mě po celou dobu studia podporovala a díky které bylo možné tuto práci vytvořit.

OBSAH

ÚVOD

Informační bezpečnost je stále se rozvíjející oblast, která se netýká jen státních orgánů a institucí či obchodních korporací. Dnes již téměř každý člověk ve vyspělých zemích vlastní počítač. Dříve se používala truhla pro cennosti, dnes je to právě počítač a cennosti jsou ve formě dat, jež jsou v něm uložené. Fotky, videa, dokumenty nebo smlouvy mohou být uložena v počítači a při neopatrném zacházení uživatel riskuje jejich ztrátu případně vydírání ze strany crackera. Právě proto by měl i běžný uživatel znát základy z oblasti bezpečnosti informací a měl by dbát na dodržování určitých zásad, které zvyšují bezpečnost dat v počítači.

Informační a komunikační technologie jsou čím dál rozšířenější a pracují s nimi i lidé, kteří umí jen základy, což nahrává crackerům, kteří takto mohou tyto lidi vydírat. Nebo může takovýto uživatel jednoduše přijít o svá cenná data kvůli špatnému zacházení. Je tedy na místě, aby se každý vzdělával v oblasti bezpečnosti informací a zabránil tak ke ztrátě, poškození či vydírání.

Cílem této práce je zjistit jaká je úroveň informační bezpečnosti u běžných uživatelů a v návaznosti na tato zjištění navrhnout opatření ke zvýšení bezpečnosti a vytvořit bezpečnostní příručku pro uživatele osobního počítače.

Teoretická část je zaměřena na definici a vysvětlení pojmů z oblasti kybernetické a informační bezpečnosti. Druhá část je pak věnována malwaru a jeho rozdělení podle vektoru útoku a způsobu útoku.

V praktické části byly nejprve identifikovány hrozby pro informační bezpečnost, které byly následně popsány. V návaznosti na to bylo provedeno dotazníkové šetření. Cílem bylo analyzovat současnou úroveň informační bezpečnosti u běžných uživatelů. Po vyhodnocení byla navržena ochranná opatření pro zvýšení informační bezpečnosti. A na závěr byla vytvořena Příručka pro zvýšení informační bezpečnosti uživatele osobního počítače, která obsahuje opatření a zásady, které pomohou zvýšit informační bezpečnost každému uživateli.

I. TEORETICKÁ ČÁST

1 TERMÍNY Z OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

Současná doba je definovaná hlavně rychlostí. Ať jde o rychlost běhu v práci, rychlost klimatických změn díky působení člověka nebo rychlostí vývoje nových technologií, které naopak mají dopad na lidstvo.

Jde především o informační a komunikační technologie (dále jen „ICT“), které používá čím dál vyšší počet lidí po celé planetě. Jedná se zejména o mobilní telefony, tablety, chytré technologie (tzv. Smart Technologies) a samozřejmě počítače. Vše má sloužit jako nástroj ke zjednodušení každodenního života, ale poslední dobou mají i jinou funkci. Místo aby lidé tyto technologie pouze použili k usnadnění života, jimi bývají „ovládáni“. Nejedná se o doslovné ovládání, ale o závislost, kdy už i malé děti mají své mobilní telefony či počítače a mnohdy tráví veškerý čas právě u nich, místo aby se šli bavit s rodiči nebo přáteli. Tím se vytrácí sociální kontakty a základy společenského chování, což může chybět při pohovoru do práce.

Informační a komunikační technologie zkrátka ovlivňují širokou oblast lidského života. Ale hlavní oblast, ve které ICT dominuje a pomáhá je práce s daty a informacemi, kdy ve většině případů už nahrazují tužku a papír. Pokud s ICT pracuje osoba znalá této práce, tak jsou ICT velká pomoc. Na druhou stranu v rukou neznalého člověka se může neznalost obrátit proti němu. Existují totiž i lidé, kteří jsou schopni získat od neznalých a naivních obětí jejich data a začít je vydírat nebo po nich vymáhat peníze.

Je tedy důležité znát alespoň základy zacházení s ICT, základní terminologii a také základní typy útoků, které mohou lidé zažít. Proto se tato kapitola věnuje základní terminologii v oblasti ICT a bezpečnosti dat.

1.1 Kyberprostor (Cyberspace)

Téměř každý se dnes a denně pohybuje v kyberprostoru, jen ho moc nevnímá. Mnoho obyčejných lidí by ani neumělo tento pojem celistvě popsat. Proto i lidé z oboru nejsou jednotní v definici a každý ji uvádí lehce jiným způsobem. Avšak než se dostaneme k definici, je třeba uvést první použití samotného slova.

Slovo cyberspace (česky „kyberprostor“) bylo prvně použito umělkyní Susanne Ussingovou (1940* – 1998†) a architektem Carstenem Hoffem (1934*). CYBERSPACE je napsáno v pravém dolním rohu koláže vytvořenou právě výše zmíněnými umělci v letech 1968 – 1970. Tyto koláže vydávali oba umělci pod falešným jménem Atelier Cyberspace.

Na obrazech jsou vyobrazeny lidské postavy umístěné v prostoru tvořeném geometrickými a organickými formami. (The (Re)invention of Cyberspace, 2015)

Obr. 1 – Koláž nazvaná CYBERSPACE z let 1968 – 1970 (The (Re)invention of Cyberspace, 2015)

Co se týká prvního použití slova cyberspace v literatuře, tak o to se postaral americko-kanadský autor sci-fi William Gibson. Tento termín použil ve svých dílech Neuromancer a Burning Chrome. Cyberspace použil nejdříve ve své povídce Burning Chrome, kterou napsal pro magazín Omni. Ta byla publikována v roce 1982. Samostatná kniha Burning Chrome byla vydána až v roce 1986. Každopádně William Gibson tento termín označil jako „evokativní a v podstatě nesmyslné“ módní slovo, které mělo sloužit jako šifra pro jeho kybernetické myšlení. (March 17, 1948: William Gibson, Father of Cyberspace, 2009)

Termín byl také použit v knize Neuromancer z roku 1984, za kterou obdržel cenu Nebula Award v roce 1984 za nejlepší novelu, v tomtéž roce Philip K. Dick Award za nejlepší novelu a v roce následujícím také Hugo Award taktéž za nejlepší novelu. Ta se stala jeho nejvíce oceňovaným dílem. (Neuromancer, © 2008 - 2021)

Právě v knize Neuromancer definoval cyberspace jinak než dříve. Má jít o vytvoření počítačové sítě ve světě plné uměle inteligentních bytostí. (Bussell, 2013)

Další definice se ujal John Perry Barlow, který byl také spoluzakladatelem společnosti Electronic Frontier Foundation (EFF). John Perry Barlow sepsal „*A Declaration of the Independence of Cyberspace*" (česky „Deklarace nezávislosti kyberprostoru") z roku 1996, kde vymezil kyberprostor takto: *„Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live."* (Barlow, 1996) Barlow tvrdil, že komunita v kyberprostoru by měla vytvořit svá pravidla, která by byla jako zákon, jímž by se komunita řídila. Z toho vyplívalo, že kyberprostor nemá být pod vlivem žádné vlády či země na Zemi. (Bussell, 2013)

V neposlední řadě je také zajímavá definice v americkém dokumentu „DOD Cyberspace Operations Lexicon". Zde se uvádí, že kyberprostor je: *„Doména charakterizovaná využitím elektroniky a elektromagnetického spektra k ukládání, úpravám a výměně dat prostřednictvím síťových systémů a souvisejících fyzických infrastruktur."*(United States, s. 7)

Existuje nepřeberné množství definic, co to kyberprostor je, z nichž je jen několik zde uvedeno. V podstatě lze říct, že kyberprostor je nehmotný prostředí sestávající z komunikačních a informačních technologií, které jsou síťově propojené, ve kterém se vytvářejí, zpracovávají, ukládají a šíří data.

Již samotná definice kyberprostoru je velmi složitá a nejasná. Na přesné definici se nemohou shodnout ani experti z oboru. S tím jsou spojené další věci, které nelze přesně definovat. A to:

- rozměr,
- hranice,
- pravomoc a odpovědnost.

Co se týká **rozměru**, je jasné, že ho nelze přesně vymezit. Je kyberprostor konečný nebo nekonečný? Na tuto otázku zatím nelze přesně odpovědět, a proto se dá předpokládat, že kyberprostor je síť navzájem propojených počítačů a dalších informačních a

komunikačních technologií bez konce. Z toho lze také položit otázku, zda by šel rozměr určit podle počtu zařízení, která spolu komunikují? Ale prozatím ani na tuto otázku není žádná odpověď.

Pokud se podíváme na **hranice** kyberprostoru, tak i ty nelze přesně vytyčit. Kyberprostor nezná hranice, což je na jednu stranu pozitivní pro všechny uživatele, kteří se v něm mohou pohybovat bez omezení. Negativní stránka věci je kybernetická kriminalita, která zde probíhá. Problémem bývá to, že každý stát má jinou legislativu týkající se kybernetické kriminality a také jinou veřejnou politiku. Proto se jeví otázka, zda by se nemělo i v kyberprostoru dodržovat státní hranice? Prozatím je tato otázka nezodpovězená a tudíž i hranice kyberprostoru nejsou známé.

Pravomoc a odpovědnost jsou témata velice podstatná a diskutovaná po celém světě. V kontextu celého světa nelze přesně určit, kdo by měl mít pravomoc, například vypnout Internet. Zato je velmi jasné, že každý stát má odpovědnost za svou kybernetickou bezpečnost. Každý stát má jinak zpracované právní normy a jiný politický postoj k tomuto tématu. Z toho vyplývá, že v celosvětovém měřítku nelze určit nikoho, kdo by měl hlavní pravomoc či odpovědnost v kybernetickém prostoru. Na druhou stranu lze přesně určit, že kybernetickou bezpečnost si každý stát spravuje sám, svými nástroji tak, aby byl kyberprostor v tomto státu bezpečný, a to nejen pro státní aktéry, ale také pro veřejné aktéry (např. soukromé organizace či obyčejné obyvatele). (Hrůza, 2013)

1.2 Kybernetická válka (Cyber war, Cyber warfare)

Kyberprostor s sebou nepřinesl pouze nové příležitosti ke komunikaci, obchod, sdílení dat a podobně, ale také hrozby. Závažnou hrozbou, která se ukazuje zejména v posledních letech, je tzv. kybernetická válka. Kybernetická válka je už dnes brána jako závažná hrozba pro většinu států. Jedním z důvodů proč tomu tak je, je závislost současné společnosti na kyberprostoru a informačních a komunikačních technologiích. (Hrůza, 2013)

Kybernetická válka by se odehrávala oproti té běžné v kyberprostoru tedy přes Internet. Místo zbraní by bylo použito množství škodlivých programů a dovedností při práci s počítačem. Škoda, která by mohla být způsobena primárně, by nebyla fyzická či materiální, ale virtuální (např. vyřazení krádež dat, infikování ICT pomocí malware, vyřazení důležitých webových stránek, atd.). Ovšem sekundární dopady by mohly být fyzické nebo materiální, protože mnoho technologií ovlivňuje chod kritické infrastruktury, bez které by mohly být ohroženy lidské životy (např. v nemocnicích, domovech pro

seniory a podobných institucích). Také by byl ohrožen běžný chod státu, hospodářství nebo by hrozil blackout. (Hrůza, 2013)

Výkladový slovník kybernetické bezpečnosti definuje kybernetickou válku takto: *„Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.“* (Jirásek a kolektiv, 2015, s. 70)

Metody kybernetické války

Možnost kybernetické války se začala rozšiřovat až s narůstajícím počtem uživatelů kybernetického prostoru. V současnosti se již jedná o skutečnou a významnou hrozbu zejména pro státy. Jak konvenční válku, tak i tu kybernetickou lze vést různými metodami a to jak těmi mírnými, tak i velmi ničivými. Jedná se o:

- Vandalismus – Jak název napovídá, jde o metodu útoku nejčastěji na vládní webové stránky. Hlavní charakteristiky jsou rychlost vedení útoku a malá škoda, kterou po sobě zanechají.
- Propaganda – Internet je mocný nástroj pro šíření jakéhokoliv druhu propagandy. Většinou jde o politickou anebo teroristickou (dále v podkapitole Kybernetický terorismus) propagandu. Oproti běžné propagandě je využití kyberprostoru velmi efektivní a zprávy se dostanou k velkému počtu lidí, což se například u letáků nemůže stát.
- Sběr dat – Tím je myšleno shromažďování důvěrných dat, které jsou cenné pro jejich majitele. Provádí se to u dat, která nebývají dobře zabezpečena a je tudíž snadné se k nim dostat.
- Odepření přístupu – Podstatou této metody je buďto úplné zablokování komunikace protivníka (například útokem na počítač či satelit důležitý pro komunikaci) nebo zachycení a pozměnění zprávy. Může to být útok jak na ozbrojené síly protivníka, tak i na další důležité sektory (např. energetika, ekonomika apod.).
- Síťové útoky na infrastrukturu – Útok je veden na přenosovou soustavu, kterou vybraná společnost používá. Jde o metodu používanou na cíle podnikající v energetice (elektrárenství, plynárenství, teplárenství, ropný průmysl) a také v komunikační infrastruktuře. Jde tedy o společnosti závislé na ICT.
- Nesíťové útoky na infrastrukturu – Nesíťové útoky jsou opakem síťových, z čehož vyplývá, že využívají běžného hardware či software. Škodlivý program je už

zabudovaný v hardware nebo software ještě před tím, než ho společnost začne používat. Tím útočník zamezí odhalení malware. (Hrůza, 2013)

Dále lze kybernetickou válku rozdělit stejně jako konvenční na:

- Útočnou – Na rozdíl od konvenční války, kdy by docházelo k přímému ohrožení životů obyvatelstva, je v případě kybernetické války dopad mírnější. Veřejnost z toho může nabýt dojmu, že nejde o tak vážnou hrozbu, ale je třeba si uvědomit, že mnoho sektorů figurujících v každodenním fungování společnosti je ohroženo právě útokem na ICT. Velmi vážný dopad může být zejména při útoku na kritickou infrastrukturu. Příkladem ztrát na životech při kybernetické válce může být útok na nemocnice či jiná sociální zařízení, kde je pečováno o nemocné obyvatele, kteří často bývají závislí na přístrojích, které může útočník vyřadit z provozu. Dalším prvkem kritické infrastruktury, jehož vyřazení by mělo katastrofální dopad na všechny sektory a každého člověka je energetika. Takový blackout je významná hrozba, na kterou jsou pořádána i cvičení Integrovaného záchranného systému a dalších zainteresovaných subjektů. Dá se tedy říci, že ač se útočná kybernetická válka zdá jako méně závažná než ta konvenční, tak důsledky mohou být velmi podobné a v některých případech i horší.
- Obrannou – U této metody je velmi důležité vytyčit strategické objekty při vzniku kybernetické války. Při přípravě na konvenční válku se určují důležité objekty, které mají strategický význam a v případě kybernetické války jde o totéž až na to, že objekty mohou být i virtuální. Poté je u těchto objektů nutná mitigace slabých míst, kterými by bylo možné do nich vniknout. Mezi činnosti k mitigaci patří například hardwarové a softwarové zabezpečení, proškolení personálu, atd. Zajištění kybernetické obrany je a bude i do budoucna velmi složitý úkol, protože se technologie neustále vyvíjejí. Při obraně je nejdůležitější poté, co je proveden útok, co nejdříve reagovat, stabilizovat systém, detekovat útok, pochopit záměr útočníka a provést přiměřený protiútok. Nesmí také chybět následná analýza útoku pro budoucí posílení zabezpečení. (Hrůza, 2013)

Všechny metody kybernetické války jsou používány také útočníky, mezi které patří hackerské organizace či jednotlivci („hackeři“), při útocích na obyčejné obyvatelstvo pro kterýkoliv účel.

1.3 Kybernetický terorismus (Cyberterrorism)

Terorismus je pojem, který v této době rezonuje v celém světě. Řadí se mezi největší hrozby pro společnost. Terorismus se stejně jako vše ostatní vyvíjí, což je zřetelné zejména na použitých zbraních. Dříve to bývaly chladné zbraně, poté střelné a výbušniny a v posledních letech se jedná zejména o dopravní prostředky jako dopravní automobily či letadla.

Teroristickým skupinám se také nevyhýbá používání informačních a komunikačních technologií. S čímž se dostáváme k další odnoži terorismu a to kybernetickému terorismu.

FBI definuje kyberterorismus jako jakýkoli *„promyšlený, politicky motivovaný útok proti počítačovým systémům, počítačovým programům a datům, který má za následek násilí proti nebojujícím cílům ze strany subnárodních skupin nebo tajných [skrytých, nelegálních] agentů.“ „Kyberteroristický útok „by mohlo vést k rozsáhlému narušení počítačových sítí, telekomunikačních systémů nebo internetových služeb a mělo by mít za následek vážné nebo rozsáhlé ekonomické škody nebo fyzické dopady na komunitu.“*(TERRORISM, c2021)

Definici kyberterorismu má i Česká republika a to ve Výkladovém slovníku kybernetické bezpečnosti, která zní takto: *„Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků.“* (Jirásek a kolektiv, 2015, s. 71)

1.4 Kybernetická bezpečnost

Kybernetická bezpečnost je spojena s několika dalšími pojmy. Zejména se jedná o kybernetický prostor, kybernetickou hrozbu (hrozba nacházející se v kybernetickém prostoru) a kybernetické riziko (pravděpodobnost vzniku kybernetické hrozby a následné škody). Kybernetická bezpečnost je tedy vztažena ke kybernetickému prostoru. (Doucek, Konečný a Novák, 2019)

Kybernetická bezpečnost je aplikace technologií, procesů a ovládacích prvků k ochraně systémů, sítí, programů, zařízení a dat před kybernetickými útoky. Cílem kybernetické bezpečnosti je snížit pravděpodobnost vzniku kybernetických útoků a chránit před neoprávněným zneužitím systémů, sítí a technologií. (What is Cyber Security? Definition and Best Practices, © 2003-2021)

Jiná definice je od Jirovského a spol. a to že kybernetická bezpečnost je: *„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* (Jirásek a kolektiv, 2015, s. 69)

Kybernetická bezpečnost se ovšem nevztahuje jen na firmy, organizace či stát, ale především začíná u každého uživatele. Každý by měl dbát na informační bezpečnost a chránit svá data proti jejich zneužití ze strany útočníka. Právě informační bezpečnost je jakousi podmnožinou kybernetické bezpečnosti.

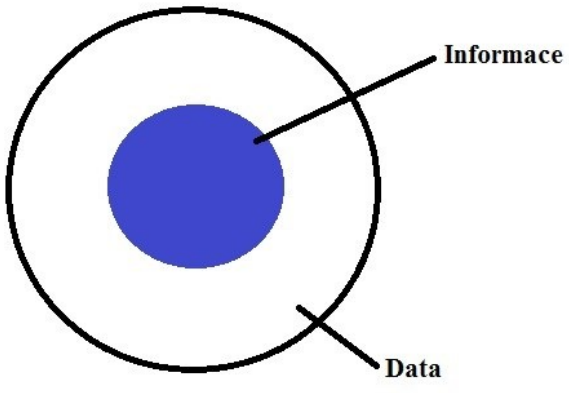
1.5 Data a informace

Pojem data a informace mnoho lidí považuje za synonyma, ale není tomu tak. Proto je nutné tyto dva pojmy od sebe odlišit. Data bývají chápána jako statická fakta, která nejsou časově závislá. Data se obvykle označují jako údaje. Naproti tomu informace odrážejí stav reality a nemohou být měněna. Informace vznikají zpracováním dat. Informace obsahují data, ale to neznamená, že jakákoli data se mohou stát informací. Tou se data stávají, až když přinesou něco nového příjemci. Data lze chápat jako čísla, text, zvuk, obraz či další smyslové vjemy.

Požár uvádí jasné definování dat a informací, pro pochopení jejich odlišného významu:

„1. Údaje, data jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.

2. Informace jsou údaje, které byly zpracovány do podoby užitečné pro příjemce.“ (Požár, 2005, s. 24-25)



Obr. 2 – Zobrazení dat a informací

Životní cyklus dat

I když to zní poněkud divně, tak i data mají svůj životní cyklus. Vše začíná vytvořením dat a končí jejich smazáním, ale je důležité si ujasnit, jak celý cyklus vypadá. Ten je znázorněn na obrázku dole.

Obr. 3 – Životní cyklus dat (Masschelein, 2019)

1) Vytvořit/získat (Create/Acquire)

První fáze životního cyklu dat. Data mohou mít formu čísla, textu, zvuku, obrazu nebo i databáze. Data mohou být vytvořena a zadávána manuálně do počítače, mohou být získána nebo je lze sesbírat z používaných zařízení (toto se týká nějaké organizace, která používá různá zařízení, která generují data).

2) Skladovat (Store)

Další fází je uložení a skladování dat a k tomu patří i jejich zabezpečení před ukradením či jinou nežádoucí manipulací. Nesmí být zapomenuto ani na zálohování a obnova dat při jakémkoliv problému.

3) Použít (Use)

Ais nejdůležitější fáze, kdy jsou data používaná k čemukoliv, co je třeba. Do používání se řadí prohlížení, zpracování, úprava a ukládání. Co se týče úpravy, je nutné vždy mít data

zálohovaná a možnost úpravy by měli mít pouze vybraní z důvodu chtěné či nechtěné změny důležitých dat.

4) Sdílet (Share)

Fáze sdílení je také velmi důležitá. Sdílení je velké usnadnění pro uživatele, ať ve směru rychlosti šíření dat nebo rozsah šíření, kdy sdílení může probíhat pro miliony uživatelů.

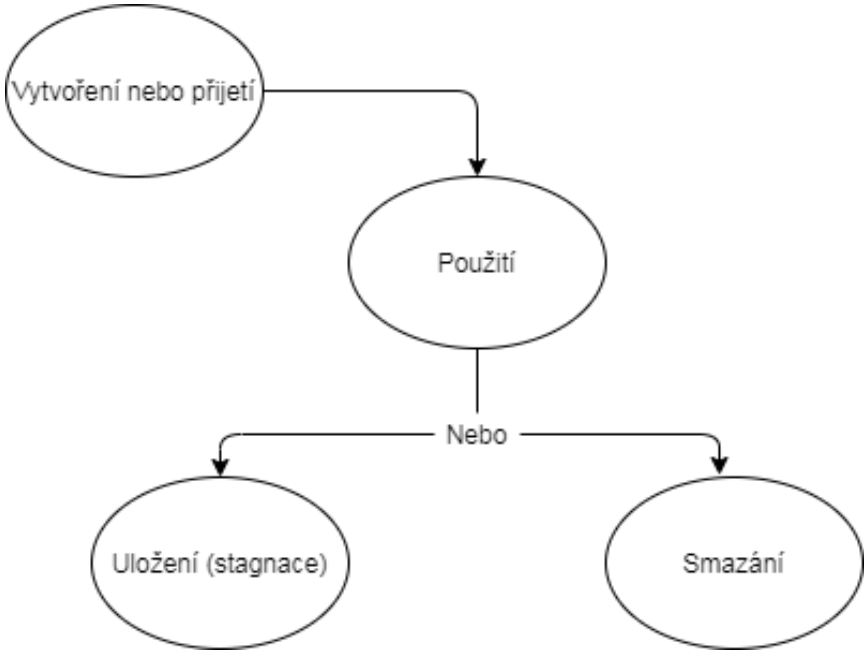
5) Archiv (Archive)

Archiv dat je místo, kde jsou data zkopírována a uložena bez dalšího použití. Jde o bezpečnostní krok pro případ, že je bude uživatel ještě někdy v budoucnu potřebovat. I u archivu je nutnost zabezpečení dat.

6) Zničit (Destroy)

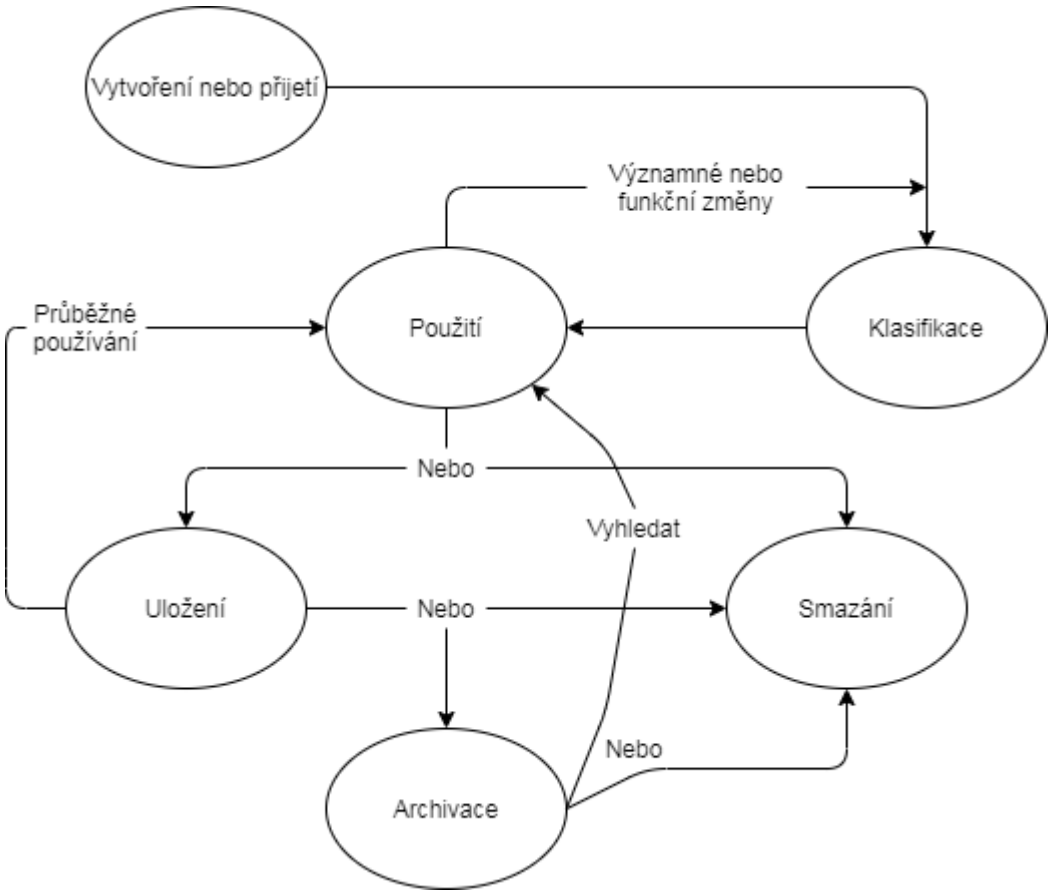
Poslední krok životního cyklu dat je jejich zničení. I přesto, že si uživatel chce uchovat všechna data, která kdy získá, tak to není možné. Je totiž limitován velikostí úložiště a nákladů na něj. Při zničení dat je nutné zkontrolovat, že budou zničeny řádně. Toto je většinou prováděno v archivu. (Integrity in the Data LifeCycle, c2021)

Životní cyklus dat je důležitý zejména v organizacích, ale i pro obyčejného člověka. Protože správné zacházení s daty, předchází jejich zneužití ze strany případného útočníka, je důležité se vyvarovat případným chybám, které přichází se špatným zacházením. De Guise uvádí dva obrazce, na nichž je vyobrazen životní cyklus dat, který není vhodný, ale v mnoha případech je používán (buď ze strany organizace, nebo jedince). Jde o obrázek č. 4**.** To je typický příklad špatného životního cyklu dat. Ten je otevřený a data, která jsou uložená, stagnují a nejsou fakticky využívána (kromě těch stále používaných). To je největší chyba většiny uživatelů i firem. (De Guise, 2020)



Obr. 4 – Schéma špatného životního cyklu dat (upraveno, De Guise, 2020, s. 28)

Obrázek č. 5 naproti tomu představuje správný životní cyklus dat. Rozdílů v porovnání s předchozím cyklem je několik, ale tím hlavním je uzavření celého cyklu. Není totiž možné, aby se data po použití buď ukládali, nebo mazali. Protože uložená data bývají nejčastějším problémem v informační bezpečnosti. Většina uživatelů se při práci s daty rozhoduje právě mezi těmito dvěma možnostmi a poté již neřeší, co s uloženými daty dělat dál a ty jsou tím pádem vystavena hrozbě kybernetického útoku. Správné řešení je uložená data buďto archivovat anebo ty, které již nejsou potřeba smazat. Tím se zabrání stagnaci dal v úložišti nebo jeho možnému zaplnění.



Obr. 5 – Schéma správného životního cyklu dat (upraveno, De Guise, 2020, s. 28)

Rozdíl je především v nedokončení celého cyklu, kdy je ukončen uložením nebo zničením. Pokud jsou data řádně zničena, tak není příliš o čem přemýšlet, ale při jejich uložení a skladování bez zabezpečení muže dojít hned ke dvěma negativním možnostem. První je zaplnění úložiště, kdy uživatel musí stejně nějaká data smazat, ale musí je všechny projít a uspořádat. Tou horší variantou je, že je útočník ukradne nebo pozmění. Nakonec uchování dat bez jejich použití nemá smysl a jen vystavuje uživatele riziku útoku. Proto je důležité myslet na to, že je lepší data klasifikovat a podle toho s nimi poté pracovat. Specialisté na správu a klasifikaci dat se často zmiňují o problému „ROT“ (Redundant, Obsolete, Trivial), což je klasifikace na redundantní, zastaralá a triviální data. Účelem správy a klasifikace dat je účinně eliminovat „ROT“ z podnikového úložiště se zaměřením na:

- Redundantní data – Patří sem kopie dat, která jsou například archivována nebo uložena jinde. Problémem je to, že nejsou používání, majitel o nich víceméně neví a mohou se stát snadným terčem pro krádež.
- Zastaralá data – Data, která jsou uchovávána, ale už nemusí. I toto má stejný problém, navíc zbytečně zabírají místo v úložišti a majitel o nich již často ani neví.

- Triviální data – Patří sem dočasná data, data k jednomu použití, nepracovní data a podobně. Zde jde především o data, která majitel potřebuje jen při jedné aktivitě či jednomu použití a následně jsou víceméně uchovávány zbytečně. (De Guise, 2020)

Klasifikace dat je dále jen na majiteli. Klasifikace je důležitá pro další práci s daty. Totiž pokud data majitel vyhodnotí jako zbytečná, tak je může odstranit. Při zařazení do důležitých následuje uložení, které by mělo být následováno archivací a odstraněním kopií těchto dat pro větší zabezpečenost. Každopádně je důležité se o data starat, aby se k nim nedostal nikdo nepovolaný a nezpůsobil tak majiteli škodu.

Informační bezpečnost

Informační bezpečnost (Information Security) je sada opatření a postupů určených k ochraně během celého životního cyklu. Také to lze nazvat jako zabezpečení dat. Jde o zabezpečení dat před neoprávněným přístupem, změnami či krádeži jak v počítači, tak při přenosu z jednoho zařízení do druhého. Zajištění informační bezpečnosti by měla být priorita pro každého člověka, protože data uložená v počítači mají pro majitele určitou cenu a určitě o ně nechce přijít.

Často se také zaměňuje kybernetická bezpečnost s informační bezpečností. Rozdíl je především v tom, že kybernetická bezpečnost řeší celkové zabezpečení prostředků ICT před útokem a informační bezpečnost je přímo specifickou disciplínou, která spadá pod kybernetickou bezpečnost. (Fruhlinger, 2020)

Bezpečnost informací je udržena, pokud jsou zachovány důvěrnost, integrita a dostupnost informací. K bezpečnosti informací je třeba přistupovat zodpovědně už jen proto, aby se zabránilo zneužití citlivých dat a informací každého občana pohybujícího se nejen na Internetu, ale také v digitálním prostředí. Proto je dobré řídit se následující triádou CIA. (Jirásek a kolektiv, 2015)

Triáda CIA

V názvu stojí tři písmena, která značí **C** (**Confidentiality**=důvěrnost), **I** (**Integrity**=celistvost) a A (Availability=dostupnost). Tato triáda představuje principy, které mají za cíl kybernetickou bezpečnost, ale je především vztahována na informační bezpečnost. Každý pojem má svůj význam při ochraně dat a informací.

<u>Důvěrnost</u>

Mezi základní druhy ochrany dat a informací patří ochrana důvěrnosti. Ne každá osoba by měla mít přístup k určitým informacím. Většinou to bývá zajištěno tak, že jsou data a

informace rozděleny do různých kategorií (např. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti rozděluje informace na vyhrazené, důvěrné, tajné a přísně tajné). Je tedy důležité zajistit, aby byly data a informace přístupné pouze vybraným osobám, které s nimi pracují. (Kolouch a Bašta, 2019)

Celistvost

Celistvost nebo také integrita má zajistit, že data a informace zůstanou nezměněné a nepoškozené. A pokud ke změně dojde ze strany osoby, která s nimi pracuje, tak aby byla možnost změnu vrátit. Celistvost tudíž zajišťuje, že data a informace nemůže změnit či poškodit osoba, která k tomu nemá oprávnění. (What is the CIA Triad?, © 2021)

Dostupnost

Poslední část triády CIA, která se stará o to, že budou data a informace dostupné tehdy, když je oprávněná osoba potřebuje. Dostupnost se zajišťuje informačními a komunikačními technologiemi (ICT). Právě ona dostupnost je důležitá pro práci s informacemi, protože systém, který má zabezpečenou důvěrnost a celistvost nemůže bez dostupnosti fungovat. (Kolouch a Bašta, 2019)

1.6 Hacker

Informační server Novinky.cz uvedl dne 5. 3. 2021 zprávu, jejíž úryvek zní: *„Hackerskému útoku čelily ve čtvrtek systémy veřejné správy. Přitom Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) varoval před závažnými zranitelnostmi již ve středu, nebylo to ale evidentně k ničemu platné. Přitom záplaty dotčených chyb byly k dispozici již od úterý.“*(Fišer, 2021)

Hacker je pojem často slýchaný především ve zprávách. V úryvku výše lze vidět, jak této pojem média používají. Označují jím člověka, který spáchal kybernetický trestný čin, avšak toto označení není zcela oprávněné.

Jargon File – The New Hackers Dictionary je v podstatě slovník pojmů, které hackeři používají. Proto je zde uvedeno několik bodů, které definují kdo je hacker:

1. Osoba, kterou baví prozkoumávat podrobnosti programovatelných systémů a rozšiřovat svoje schopnosti, na rozdíl od většiny „běžných“ uživatelů.
2. Ten, kdo nadšeně (až posedle) programuje nebo ho programování baví, na rozdíl od teorie.
3. Osoba schopná ocenit hackerskou hodnotu.
4. Osoba, která umí rychle programovat.
5. Expert na konkrétní program nebo ten, kdo na něm často pracuje.

6. Odborník nebo nadšenec jakéhokoli druhu.
7. Ten, kdo má rád intelektuální výzvu tvořivého překonávání nebo obcházení omezení.
8. Zlomyslný všetečka, který se snaží získat choulostivé informace špiclováním. Správný termín pro tento smysl je cracker. (The Online Hacker Jargon File, verze 5.0.1, 2012)

Hacker může být i člověk, který je tímto označen jako příslušník celosvětové komunity v kyberprostoru. Hackeři se sami označují za uživatele kyberprostoru, kteří pomocí samostudia ovládli technologické znalosti, které používají k odhalování chyb v ICT. Svými schopnostmi objevují bezpečnostní nedostatky a zranitelná místa, čímž do jisté míry uspokojují svou touhu o překonávání limitů v tomto prostředí. (Jirovský, 2007)
Z výše uvedených charakteristik tedy vyplývá, že používání pojmu hacker v souvislosti s kybernetickou kriminalitou je nevhodné. Pro široký okruh dopadu médií většina obyvatelstva používá taktéž nesprávně pojem hacker. Pro vyšší povědomí je dobré vědět, že pokud je zmíněna trestná činnost v souvislosti s kyberprostorem, tak pachatel se nazývá cracker.

1.7 Malware

Malware je zkrácenina anglických slov malicious software, což lze přeložit jako škodlivý software. Malware je software, který je určen k různým druhům škodlivé činnosti v počítačovém systému. Může jít o získávání dat, přístupu k uživatelským účtům, k obohacení crackera a podobně. (Kolouch, 2016)
O jednu z definic se postaral Jirásek a kolektiv a ta zní, že malware: *„Je obecný název pro škodlivé programy. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software.“* (Jirásek a kolektiv, 2015, s. 115)
Cambridge Dictionary uvádí lehce odlišnou definici: *„Software, který je navržen tak, aby poškodil informace na počítačích jiných lidí a zabránil normálním funkcím počítačů.“* (Malware, c2021)
Malware je v podstatě souhrnný název pro různé škodlivé softwary. V minulosti se nejprve používaly názvy samotných škodlivých programů, ale postupem času se zavedlo označení právě pojmem **MALWARE**. Níže je uvedeno jen několik druhů malwaru, které dnes existují.

1) Adware.

2) Spyware.
3) Keylogger.
4) Viry.
5) Červi.
6) Trojské koně.
7) Ransomware.
8) Backdoor.
9) Rootkity a jiné. (Kolouch, 2016)

1.8 Internet věcí (Internet of Things – IoT)

Internet věcí, zkráceně IoT je fenomén poslední doby, který označuje oblast komunikace a kontroly technologií, které člověk běžně užívá. Tato zařízení jsou spolu propojena a komunikují prostřednictvím Internetu či bezdrátového přenosu dat.

IoT umožňuje sběr velkého množství dat, která jsou poté využívána např. v logistice, zdravotnictví, meteorologii apod. Ovšem nejčastěji je pod pojmem IoT myšlena „chytrá" domácnost. Dnes je již mnoho zařízení propojených dohromady a člověk je může odkudkoliv ovládat pomocí chytrého telefonu.

Pokud jde o „chytrou" domácnost jsou to zařízení jako dálkově ovládané zásuvky, osvětlení, klimatizace, pračky, reproduktory, atd. Je to v podstatě docela mladá oblast, ve které by se mohla objevovat později i kybernetická kriminality, protože zmíněná zařízení nebývají dostatečně zabezpečena proti možným útokům. (Co je IoT?, © 2021)

2 KYBERNETICKÉ ÚTOKY (CYBER ATTACKS)

Kybernetické útoky jsou dnes velmi časté a už nebývají zaměřeny pouze na korporace či státní orgány, ale čím dál častěji na obyčejné občany. Proto je dobré vědět, co to vůbec kybernetický útok je. Níže jsou uvedeny různá pojetí kybernetického útoku a jejich porovnání.

Dobrá definice je opět uvedena ve Výkladovém slovníku kybernetické bezpečnosti. Jedná se o: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“* (Jirásek a kolektiv, 2015, s. 71)

Jiné pojetí zpracoval americký Národní institut standardů a technologií (NIST) a to že kybernetický útok je: *„Útok prostřednictvím kyberprostoru zaměřený na plánované využití kyberprostor za účelem narušení, deaktivace, ničení nebo zlomyslné ovládání počítačového prostředí / infrastruktury; nebo zničí integrity dat nebo krádež kontrolovaných informací.“* (Ross, 2012)

Pokud se obě definice porovnají, tak je zřetelné, že každá má mírně jiné pojení směrem ke kontextu útoku. Jirásek a kolektiv uvádí, že útoky bývají politicky či vojensky motivované a naproti tomu americký Národní institut standardů a technologií bere definici více ze široka, kdy není zaměřena na žádný kontext, ale spíše na cíle útoku (např. narušení počítačového prostředí či počítačové infrastruktury,…). Kolouch a spol. pojali kybernetický útok jako: *„jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby.“* (Kolouch a Bašta, 2019, s. 82)

Kybernetický útok nelze vykonat pouze pro politické či vojenské motivy, ale i pro vlastní obohacení útočníka (Ransomware, Phishing,…), získání citlivých informací (Spyware, Sociální inženýrství,…) nebo i pro získání dalších zařízení, které poté využije k dalším útokům (Botnet). I přes uvedené definice je třeba říci, že v této práci jsou řešeny kybernetické útoky z hlediska bezpečnosti informací.

Ve společnosti nyní používá počítač většina lidí, kteří nemusí nutně být znalí v oblasti ICT, a proto bývají pro útočníky snadnou kořistí. Z tohoto důvodu by se každý uživatel měl vzdělávat v této oblasti a vědět, jaké typy útoků existují, aby se proti nim mohl chránit a předešel tak ztrátě cenných dat či peněz.

Kybernetické útoky se dělí na několik typů, přičemž každý z nich má jinou mechaniku fungování a také odlišný cíl. Proto jsou níže popsány ty nejznámější a v posledních letech

nejvíce objevované, na které by s trochou smůly mohl narazit vysoký počet uživatelů počítačů.

odborná veřejnost popisují vektor útoku jako cestu, kterou používá útočník (cracker) k tomu, aby si zajistil přístup do napadeného zařízení. Tímto způsobem se do cílového zařízení dostane škodlivý kód, který dále páchá různým způsobem další škody v tomto zařízení. Mezi kybernetické útoky řazené dle vektoru útoku jsou:

- Botnet.
- Červi.
- SPAM.
- Trojské kně.
- Viry. (Attack Vector, ©2021)

A dle **způsobu útoku,** což znamená už konkrétní typ útoku. Nejde o způsob jeho šíření, ale o samotný druh. Na příkladu adwaru, jde o to, že se může do počítače dostat jako trojský kůň, ale jeho hlavní funkce je zobrazování reklam v počítači. Mezi kybernetické útoky řadící se podle způsobu útoku jsou:

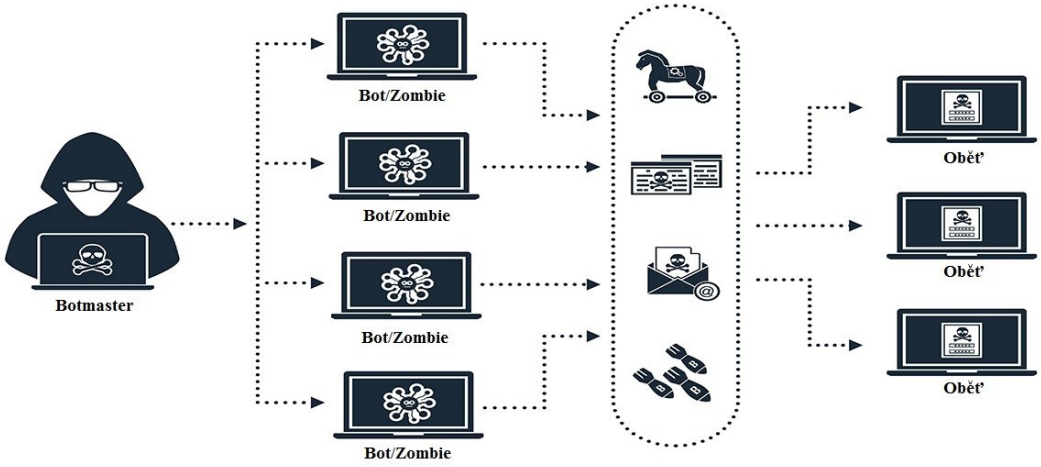
- Adware.
- DoS/DDoS.
- Phishing.
- Ransomware.
- Spyware.
- Sociální inženýrství.
- Zero-day-attack.

2.1 Botnet

Jako Botnet bývá označena síť tzv. „zotročených zařízení“, čímž jsou myšleny nejvíce počítače, ale také chytrá (SMART) zařízení mezi, která patří televize, mobilní telefony, tablety či další zařízení připojená k Internetu. (Botnet, © 2018)

Botnet je složen z botů (jednotlivých zařízení), kterým se říká zombie. Tuto síť ovládá cracker, což je člověk, který má přístup ke všem zařízením a může je využívat k další nezákonné činnosti. Součástí sítě bývají stovky až tisíce zařízení, která bývají používána zejména k DDoS útokům nebo distribuci spamu. Botnety si lze také pronajmout na

Darkwebu nebo si rovnou objednat zmíněný DDoS útok či distribuci spamu. (Jirásek a kolektiv, 2015)



Obr. 6 – Ukázka, jak funguje Botnet (upraveno, Yatziv, 2020)

2.2 Červi

Červ (anglicky Worm) je škodlivý kód, který se nejčastěji dostane do počítače elektronickou poštou ve formě přílohy. Pokud uživatel stáhne a otevře tuto přílohu, kterou bývá stejně jako u trojského koně program, tak se červ okamžitě aktivuje, skryje se v systému, namnoží se a rozešle se dále (použije kontakty, které má uživatel v e-mailu). Oproti trojskému koni je červ schopen sám sebe rozmnožit a rozeslat přes Internet. Může způsobit i úplný kolaps systému čehož dosáhne tak, že se rozmnožuje do doby, kdy už je úložiště zcela zaplněné a počítač již nemůže pracovat. (Požár, 2005)

Červi se zaměřují na slabá místa v operačním systému (dále jen „OS“), aby se mohli namnožit a rozeslat dále. Využívají slabá místa v zabezpečení, zadních vrátek (tzv. backdoors) nebo mohou být nainstalováni ručně. Infikované počítače lze využít pro vytvoření botnetu a posléze útokům DDoS atd. (Baker, 2021)

2.3 SPAM

Jednoduše řečeno nevyžádaná pošta, též nazývaná junk mail nebo unsolicited mail. SPAMem je každý nevyžádaný e-mail, který dorazí uživateli e-mailové schránky. Nemusí to být jen nabídka zboží či služeb, u nichž nebyl společnosti uživatelem uveden souhlas se zasíláním e-mailů, ale i další nevyžádaná pošta. Do SPAMu spadá i phishing, jelikož to

bývá dost často spojená činnost útočníků (phishingové útoky bývají součástí spamu) a další druhy. Až 95 % veškeré pošty je spam. To, že veškeré SPAMy nedorazí do určené schránky je zásluha antispamových filtrů, které nedovolí projít e-mailu z nedůvěryhodného zdroje nebo obsahující určité slovní spojení. Ne vždy však tento filtr zastaví všechen SPAM. Záleží na jeho nastavení. Pokud se nějaký spam dostane do e-mailu je už na uživateli, aby vyhodnotil, zda jde o spam nebo ne. Toto je ale poněkud ošemetné, protože pokud je SPAM vyhodnocen jako obyčejný e-mail, tak při jeho otevření útočník zjistí, že je e-mailová schránka aktivní a začne na ni posílat ještě více spamu, proto je důležité, aby byl antispamový filtr nastaven dobře. Uživatel musí být také ostražitý při probírání pošty. (Šulc, 2018)

Druhy SPAMu:

1) Reklamní SPAM – hlavním cílem je doručení reklamy. SPAM propaguje konkrétní služby či zboží, které ale nebývají z relevantních eshopů a většinou se jedná o napodobeniny značkových výrobků apod.
2) HOAX – také nevyžádaná pošta, která na rozdíl od reklamního SPAMu obsahuje buďto nepravdivou informaci nebo jde o tzv. dopisy štěstí. K šíření pomáhají samotní uživatelé, kteří zprávě uvěří a šíří ji dále. Dopisy štěstí obsahují krátký text a varují, že pokud ho uživatel neodešle dále, tak už nebude mít nikdy štěstí. V případě šíření nepravdivé informace je jen na lidech, zda si informace ověří nebo jim uvěří a rozšíří je dále.
3) SCAM – již není neškodný, ale jde o praktiku, kdy se útočník snaží člověka podvést od samého začátku. Bývá to nabídka zboží, loterie, výhra nějaké ceny apod., ale nakonec se podvedený ničeho nedočká. Útočník používá i sociální inženýrství k přesvědčení své oběti a komunikuje pouze přes e-mail. (Šulc, 2018)

Phishing – je zaměřen na neoprávněné získání citlivých údajů od své oběti (více o phishingu je uvedeno v kapitole 2.4).

2.4 Trojské koně

Trojský kůň je pojmenován podle Trojského koně z řecké mytologie. Stejně jako zmíněný Trojský kůň z trojské války (jež byl navenek neškodný, ale uvnitř byli vojáci čekající na moment útoku) se i tento program maskuje za užitečný program, ale jinak je to škodlivý software. Při spuštění program většinou nainstaluje zadní vrátka, která může poté používat útočník. Ten se tak dostane do infikovaného počítače a může z něj udělat zombie do svého

botnetu (dále k použití k DDoS), ukrást z něj citlivá data, nainstalovat další malware, upravovat nebo mazat soubory, sledovat obrazovku uživatele, způsobit havárii počítače apod. Mezi příklady populárních trojských koní patří: Emotet, Trickbot, Kovter, ZeuS, NanoCore a Redyms. (Trojan Horse, © 2021)

Trojské koně fungují podle toho, jak je naprogramoval útočník. Trojský kůň může způsobit:

- Zpomalení systému, jeho poškození (nebo poškození jeho částí) nebo úplné vyřazení.
- Krádež citlivých dat a přihlašovacích údajů (které jsou uložené v prohlížeči).
- Mohou mít funkci keyloggeru (případně mohou umožnit útočníkovi instalaci keyloggeru) – tedy zaznamenávat stisknuté klávesy, shromažďovat snímky obrazovky a toto odesílá útočníkovi.
- Ovládání počítače útočníkem na dálku.
- Zablokovat antivirový program či další bezpečnostní nástroje.

Trojský kůň se do počítače dostane přímo jako program, které se nejeví škodlivě. Také se může do počítače dostat, když uživatel navštíví infikovaný web nebo pokud klikne na vyskakovací okno a tím se trojský kůň automaticky nainstaluje. Útočník může také trojského koně připojit k legitimnímu softwaru (kdy o něm tvůrce neví) nebo ho nainstaluje ručně. (Trojan (trojský kůň), c2018)

2.5 Viry

Počítačovým virem je škodlivý kód nebo škodlivý program, který je určen k páchání škody v cílovém zařízení bez vědomí uživatele. Cílem viru bývá poškození počítačového systému, převzetí kontroly nad počítačem nebo i smazání či přepsání některých souborů. Šířen je pomocí jiných souborů, do kterých se zkopíruje, ale oproti červům se není schopen šířit přes síť sám. Potřebuje, aby ho uživatel rozšířil pomocí souboru či programu, do kterého se zkopíroval. Může to být program, dokument či samo spustitelná příloha v emailu. Viry jsou dnes již méně časté, protože je většinou zachytí anti-malware (v tomto případě antivir). (Počítačové viry, červi a trojské koně, © 2018)

2.6 Adware

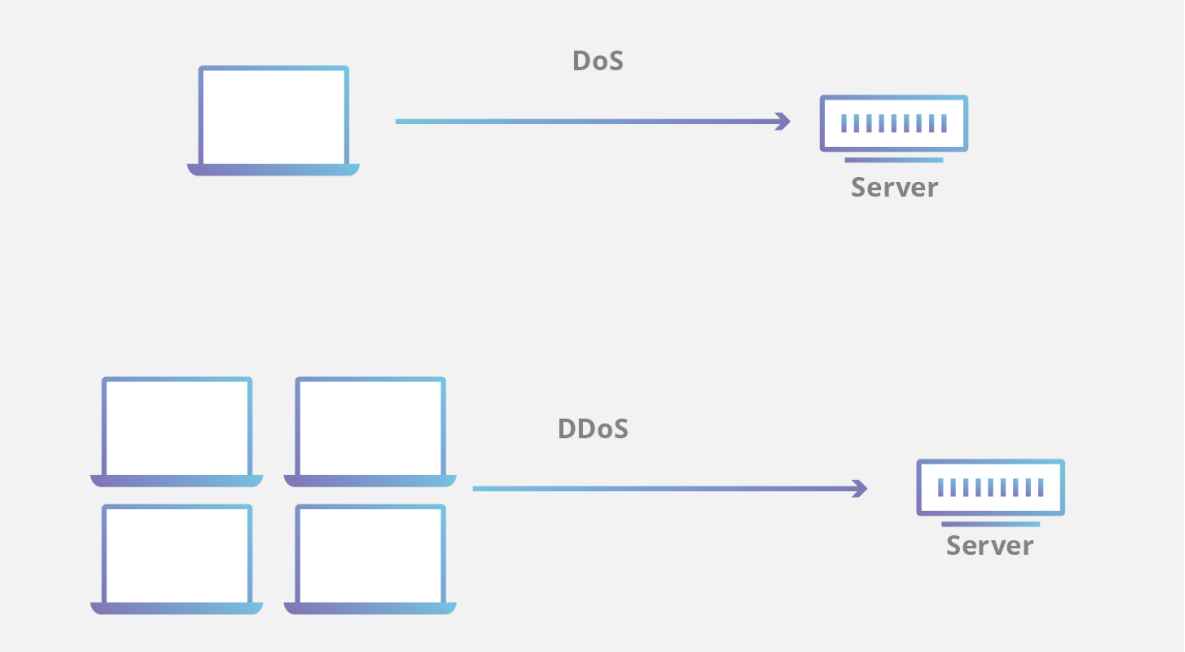
Celým názvem je to *advertising supported software* a jde o malware. Je to software, který zobrazuje reklamu proti vůli uživatele a jedná se o méně nebezpečný typ malwaru. Adware

může kromě reklam být propojen i se spywarem, pro získání citlivých dat od uživatele. (cybercrime)

Prioritně nemusí být adware zaměřen na získávání citlivých dat od uživatele, ale spíše na zobrazování reklam. Proto má také schopnost sledovat aktivitu uživatele na Internetu, aby mohl adware zobrazovat relevantní reklamy (podle toho, jaké webové stránky uživatel navštěvuje). Adware může mít formu vyskakovacích oken, reklamy mohou překrývat část obrazovky nebo obsah webové stránky. Adware může být také použit k odkazu na phishingové stránky. Některé druhy umí i změnit nastavení v internetovém prohlížeči. Celkově jde spíše o malware, který je otravný a ztěžuje uživateli práci na počítači. (Adware, © 1992 – 2021)

2.7 DoS/DDoS

Denial-of-Service (zkráceně DoS) hrubě přeloženo jako odmítnutí služby je útok zaměřující se na znepřístupnění buďto internetové nebo jiné služby, díky opakujícím se odesíláním požadavků, které nakonec službu zahltí a ta přestane fungovat. (Kolouch, 2016) Oproti tomu DDoS, čili *Distributed Denial-of-Service* je rozdílný v distribuci, jak již stojí v názvu. Jde o stejný princip útoku na vybranou službu jen s tím rozdílem, že požadavky jsou posílány z více zařízení. K tomuto účelu slouží dříve zmíněný botnet. K vyřazení služby se používá botnet o velikosti 1 000 až 10 000 zombie. DDoS si lze také koupit například na Darkwebu. DDoS útoky mohou být provedeny tzv. hacktivisty (člověk, který má politický nebo společensky motivovaný důvod k útoku na počítačový systém určité společnosti) proti nadnárodním korporacím či vládním organizacím. Útočí na jejich webové stránky a síťovou infrastrukturu. Tím chtějí ukázat svou sílu. Dalším druhem útoku může být útok na síťovou infrastrukturu vybraného státu, který může mít závažné následky a dopad na celkovou funkci státu a poskytování služeb veřejnosti. A v neposlední řadě může DDoS použít také konkurence. Cílem je vyřazení webových stránek obchodu tak, aby zákazníci šli nakupovat k nim. Může se to dít zejména o Vánocích nebo jiných svátcích. (Šulc, 2018)



Obr. 7 – Ukázka DoS a DDoS útoku (What is a denial-of-service (DoS) attack?, © 2021)

V závěru je tedy jediným rozdílem v těchto útocích počet zařízení, které jsou k němu využity. Jde taky o dobrý výdělek pro majitele botnetů, kterým se tak vyplácí získávat další a další zařízení do své sítě zombie.

2.8 Phishing/Spearphishing/Pharming

Česky rybaření přesně vyjadřuje hlavní náplň tohoto typu útoku. Je to jeden z nejstarších triků, který crackeři používají. Phishing je i po letech stále velmi úspěšný a stále se objevuje. Je používán k získávání citlivých informací o subjektu (společnosti nebo častěji osobě). Princip spočívá v posílání podvodných e-mailů osobám, přičemž útočník předstírá, že je renomovaná společnost. E-mail obsahuje zprávu, kde je vysvětleno, že je potřeba přihlášení k účtu pro ověření údajů nebo podobný důvod. V e-mailu je také odkaz na podvodnou webovou stránku, která má ovšem všechny náležitosti jako pravá webová stránka. Cílem je získat přihlašovací údaje k účtu či jiné citlivé údaje. Převážně se jedná o přihlašovací údaje k internetovému bankovnictví, čísla sociálního zabezpečení nebo jiné přihlašovací údaje. (Diogenes a Ozkaya, 2018)

Českou definici lze opět najít ve Výkladovém slovníku kybernetické bezpečnosti, který ho definuje jako: *„Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z*

uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN." (Jirásek a kolektiv, 2015, s. 82)

Existuje několik druhů phishingu z nichž každý se provádí trochu jinak. Jsou to Spear Phishing, Pharming, Vishing a Smishing. Níže jsou rozvedeny pouze dvě a to Spear Phishing a Pharming, protože zbylé dvě využívají mobilní telefony a ne počítač.

Spear Phishing

Spear Phishing je stejně jako phishing zaměřena na získávání citlivých údajů, ale rozdíl je v tom, že u tohoto typu je útok zaměřen na určitou osobu. Je to namáhavější pro útočníka, protože musí zjistit více informací o cíli (co ho zajímá) a poté mu posílá podvodné e-maily, které ho nutí z nějakého důvodu otevřít. Úspěšnost phishingu je asi 3%, zatímco spear phishing má 70% úspěšnost. Také je známo, že přibližně 5 % lidí, kteří otevírají phishingové e-maily klikají na odkazy nebo stahují přílohy, zatímco u spear phishingu je to celá polovina. (Diogenes a Ozkaya, 2018)

Pharming

Pharming je daleko propracovanější než phishing a pro své oběti je daleko nebezpečnější. Útočník vede útok na DNS (Domain Name System) server, kde dochází k překladu doménového jména na IP adresu, v podstatě útočník doménové jméno přesměruje na podvodnou IP adresu, kterou vytvořil jako repliku stejně jako tomu je u phishingu. V tomto případě je téměř k nerozeznání, zda je oběť na originální nebo na podvržené webové stránce. Dále pak probíhá opět žádost o zadání přihlašovacích údajů, které tím získá útočník. U pharmingu bývají časté útoky na internetové bankovnictví. (Kolouch, 2016)

2.9 Ransomware

Podle Jiráska a kolektivu je to: *„Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (např. virus, trojský kůň)."* (Jirásek a kolektiv, 2015, s. 97)

Patří do skupiny tzv. vyděračského malwaru. Funguje na principu omezení funkčnosti počítačového systému, který je nedostupný do té doby, než je zaplaceno „výkupné". Do

počítače se nejčastěji dostane pomocí malware, který bývá součástí přílohy u e-mailu. Další možnost je také návštěva „infikované“ webové stránky nebo díky využití reklam (postačí zobrazení reklamy). Jakmile se dostane do počítače, tak v něm zašifruje data. Ransomware využívá strachu oběti ze ztráty cenných dat. (Kolouch, 2016)

Ransomware se dále dělí podle toho, co v počítači zašifruje. Prvním je ransomware šifrující soubory, kdy počítač funguje, ale jsou zašifrované pouze soubory na disku (kromě systémových souborů). Druhým typem je ransomware blokující počítač. Při tomto typu se na monitoru objeví obrazovka, která žádá heslo k odemčení a „výkupné“. Počítač nelze vypnout a nereaguje na klávesové zkratky. (Šulc, 2018)

Nejčastější je první typ, který se také nazývá crypto-ransomware. Bývá zaměřen na zašifrování soukromých souborů v počítači, a to obrázků, videí a textových dokumentů. Jak již bylo řečeno, tak pro dešifrování (odemčení souborů zpět pro normální použití) je žádaná určitá částka, většinou v Bitcoinech (aby nešlo útočníka vystopovat) a k tomu běží časová lhůta k odemčení. Pokud se do konce lhůty soubory nedešifrují, tak dojde k jejich smazání. (Kolouch, 2016)

Velmi často oběť zaplatí, protože o data nechce přijít, i když je doporučeno neplatit. Zaplacením se totiž podporuje tato nekalá praktika nezákonného výdělku.

2.10 Spyware

Spyware je dalším typem malwaru, který se snaží získávat a shromažďovat data o uživateli bez jeho souhlasu. Mezi jeho funkce patří zaznamenávání stisknutých kláves, snímků obrazovky, ověřovacích údajů, e-mailových adres, údajů z webových formulářů a dalších citlivých údajů uživatele. Během používání program odesílá získaná data útočníkovi a ten je může zneužít k trestné činnosti. Ať už sám nebo prodejem údajů další osobě, která je může použít k jakýmkoliv účelům. Spyware se do počítače dostane stejně jako většina malwaru a to tak, že uživatel stáhne aplikaci či soubor z nedůvěryhodného zdroje nebo stáhne nakaženou přílohu z mailu. (Spyware, 2005)

Pro upřesnění toho, co je spyware je zde uvedena definice zpracovaná Jiráskem a spol.: *„Program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.“* (Jirásek a kolektiv, 2015, s. 115)

Spyware může mít různé podoby a funkce, jsou to:

- Adware (součástí adwaru může být i spyware).
- Keylogger (klasický příklad spywaru, který zaznamenává stisknuté klávesy, snímky obrazovky, někdy také zvuk z mikrofonu).
- Infostealers (jsou spíše zaměřeny na prohlížeče – získávání informací z webových stránek).
- Password Stealers (podobné jako infostealers, avšak zaměřená na získávání hesel – dokáží získat uložená hesla z prohlížeče případně heslo k počítači).
- Trojské koně. (What is Spyware? The 5 Examples You Need to Know, © 2014-2021)

2.11 Sociální inženýrství (Social Engineering)

Jde o jednu z nejobávanějších útoků, které se používají, protože se proti němu v podstatě nelze připravit. Oproti různým útokům, které jsou vedeny přes počítačové sítě a lze se proti nim bránit za pomoci softwarového zabezpečení se proti sociálnímu inženýrství nelze úplně ubránit. Sociální inženýrství využívá lidské přirozenosti. Tento aspekt přesahuje veškeré bezpečnostní nástroje, které se běžně používají. Při použití jakéhokoliv malwaru ho jde detekovat pomocí nainstalovaného anti-malwaru. Lidská složka je na druhou stranu otevřená manipulaci. Lidé se rádi předvádějí, důvěřují přátelům, jsou podřízeni vyšším autoritám apod. a to je to čeho využívá sociální inženýrství. (Diogenes a Ozkaya, 2018)
Sociální inženýrství využívá manipulace s člověkem a útočník používající tuto techniku je sociotechnik. Ten se snaží přesvědčit svou oběť k tomu, aby mu poskytla důležité informace nebo udělala to, co chce. Vše se snaží udělat tak, že si oběť nepřijde zneužitá. Sociotechnik využívá svou důvěryhodnost, charisma, popřípadě se snaží zapůsobit jako autorita. (Šulc, 2018)
Kolouch uvádí, že je sociální inženýrství vedeno třemi způsoby, které bývají často kombinované a jsou to:

- *„Sběr volně (veřejně) dostupných dat o cíli útoku.*
- *Fyzický útok (útočník se například vydává za pracovníka servisní agentury – např. servis tiskáren, pracovník údržby aj.), při kterém se útočník snaží získat co nejvíce informací „zevnitř“ společnosti, případně citlivé informace o jednotlivých pracovnících (včetně např. prohledávání odpadků aj.).*
- *Psychologický útok*

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:

1) *Podvodný e-mail či falešná webová stránka*
2) *Telefonický hovor*
3) *Útok „tváří v tvář“*
4) *Prohledávání odpadků („Dumpster diving“ a také „cezení dat“)*
5) *Prohledávání webu, sociálních sítí aj. (jedná se o jednoduše dosažitelný otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá zjistit, případně ověřit informace o potenciálním cíli). Veřejné informace dostupné online (např. životopisy, práce, teze, návrhy aj. uveřejněné na Internetu). Výroční zprávy a jiné veřejně dostupné informace o společnosti*
6) *Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči*
7) *Ponechání paměťového média (USB aj.) v zájmové oblasti (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware)*
8) *Nabídka vyzkoušení služby online (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.)*
9) *Dodávka či nalezení zařízení (počítačového systému)*
10) *Falešný servisní technik*
11) *Jiné“* (Kolouch, 2016, s. 187,188)

2.12 Zero-day-attack

Označovaný též jako Day Zero, česky *útok nultého dne* je útok fungující na principu využití slabého místa v softwaru, o kterém vývojář ještě neví. Softwarový vývojář musí co nejdříve opravit tato slabá místa vydáním aktualizace či patche. Zero-day-attack lze použít i na IoT (internet věcí), protože ty nemívají časté aktualizace softwaru. Název je odvozen ode dne, kdy vývojář o slabině nevěděl (tedy nultý den). Útok nultého dne může zahrnovat malware jako například adware či spyware.

Jak se bránit útokům nultého dne? Nejlepší možnost je nastavení automatických aktualizací, ať už u OS, internetového prohlížeče, antivirového programu a dalších aplikací, protože právě aktualizacemi se snaží vývojáři spravovat slabá místa, která by potenciálně mohl využít útočník. Je proto důležité stále udržovat vše aktuální. Ovšem někdy ani aktuální software nedokáže zabránit takovémuto útoku, protože pokud není známé místo, kterým se do něj útočník dostane, tak není vydaná záplata, která toto napraví. Zranitelnosti nultého dne jsou zneužívány především crackery, ale mohou být využívány i státními bezpečnostními agenturami pro sledování či útoky. Existuje i samotný trh poptávky po zranitelnostech nultého dne, i ze strany vládních bezpečnostních agentur.

Slabé místo může být zpřístupněno vývojáři nebo třetí straně. Pokud jde o prodej třetí straně tak se tak děje bez souhlasu vývojáře a informace mohou být zneužity k zločinným účelům. Nejlepší pro vývojáře je pokud je na zranitelnost upozorní etický hacker nebo bílý klobouk (white hat – hacker, který hledá zranitelnosti, aby o nich posléze informoval vývojáře). (Frankenfield, 2020)

3 CÍLE A POUŽITÉ METODY

Cílem teoretické části práce je shromáždit a definovat co nejvíce důležitých pojmů z oblasti kybernetické a informační bezpečnosti, které tak čtenáře uvedou do dané problematiky. Následně uvést a definovat různé typy malwaru pro lepší pochopení útoků a informační bezpečnosti.

Cílem praktické části je analyzovat informační bezpečnost uživatele osobního počítače a zjistit tak jaká je úroveň informační bezpečnosti u běžných uživatelů. Na základě výsledků navrhnout ochranná opatření pro zvýšení informační bezpečnosti a vytvořit bezpečnostní příručku pro uživatele osobního počítače.

Použité metody při zpracování práce

K dosažení již výše zmíněných cílů diplomové práce bylo využito několik metod vědeckého zkoumání. První z nich byla literární rešerše, která byla použita v teoretické části, kdy byly nashromážděny literární a internetové zdroje pro lepší pochopení dané problematiky. Dále byla použita obsahová analýza také v teoretické části zejména k analýze textů, což dopomohlo k následnému vysvětlení pojmů tak, aby ho pochopil i neodborný čtenář. Komparace neboli srovnávání bylo použito v teoretické části, kdy se komparovaly definice pojmů od různých autorů, protože některé pojmy každý autor definuje jinak a vychází to především z úhlu pohledu a zkušeností daného autora. Komparace byla využita i v praktické části a to v případě šifrovacích programů, druhů zálohování a anti-malwarů. V tomto případě sloužila komparace k ukázání výhod a nevýhod ve výše zmíněných případech a podle toho také vybrat tu nejlepší volbu. Ke zjištění úrovně informační bezpečnosti bylo použito dotazníkové šetření, které bylo v elektronické formě. Dotazník se skládal z 33 otázek, které byly zaměřeny na 5 oblastí. Asi poslední metodou bylo statistické zpracování dat. Tato metoda byla užita při zpracování výsledků dotazníkového šetření do podoby grafů, které zobrazovaly výsledky jednotlivých otázek.

II. PRAKTICKÁ ČÁST

4 HROZBY PRO INFORMAČNÍ BEZPEČNOST

V této kapitole je sestavena tabulka hrozeb pro informační bezpečnost, která je dále rozvedena podle určených hrozeb. Hrozby jsou určena podle subjektivního pocitu a mají ukázat, jaké jsou nebo mohou být hrozby v různých prostředích, jaké mohou způsobit následky, způsob provedení útoku za pomoci této hrozby a opatření, která minimalizují riziko vzniku.

Tabulka 1 – Hrozby pro informační bezpečnost s dalšími specifiky (vlastní)

Hrozby	Následek	Způsob provedení	Prostředí	Opatření
Spolupracovníci	Spatření hesla či jiných citlivých informací	Fyzická krádež dat; krádež peněz; vydírání; prodej hesla od internetového bankovnictví či citlivých dat	Pracoviště	Prověrka, obezřetnost.
Opuštění počítače	Krádež citlivých dat	Fyzická krádež dat; krádež peněz; vydírání; prodej hesla od internetového bankovnictví či citlivých dat	Pracoviště	Zamknutí počítače při jeho opuštění.

Hrozby	Následek	Způsob provedení	Prostředí	Opatření
Podvodný email	Odkazy na podvodné stránky, neznámé přílohy	Krádež přihlašovacích údajů (krádež peněz); krádež dat; vydírání; poškození softwaru	Pracoviště	Mazání neznámých emailů.
Použití soukromého USB Flash disku nebo HDD	Nakažení počítače či sítě	Vytvoření zombie; poškození softwaru; zašifrování dat	Pracoviště	Používání pracovních USB Flash disků nebo sdílení přes Internet či cloudové služby.
Stažení souboru z neověřených webových stránek	Nakažení počítače či sítě	Vytvoření zombie; poškození softwaru; zašifrování dat	Pracoviště	Stahování souborů pouze z oficiálních stránek.
Podvodný email	Odkazy na podvodné stránky, neznámé přílohy	Krádež přihlašovacích údajů (krádež peněz); krádež dat; vydírání; poškození softwaru	Domácnost	Mazání neznámých emailů.

Hrozby	Následek	Způsob provedení	Prostředí	Opatření
Použití USB Flash disku nebo HDD	Nakažení počítače či sítě	Vytvoření zombie; poškození softwaru; zašifrování dat	Domácnost	Častá kontrola anti-malwarovým softwarem nebo formátování.
Stažení souboru z neověřených webových stránek	Nakažení počítače či sítě	Vytvoření zombie; poškození softwaru; zašifrování dat	Domácnost	Stahování souborů pouze z oficiálních stránek.
Cizí lidé	Spatření hesla či jiné důležité informace	Krádež dat (krádež peněz); vydírání; prodej hesla od internetového bankovnictví či citlivých dat	Veřejné místo	Obezřetnost.
Opuštění počítače	Krádež počítače	Fyzická krádež zařízení; krádež dat (počítač je odemknutý); rozbití zařízení	Veřejné místo	Vzít si počítač s sebou nebo ho nechat pohlídat kamarádem.

Pracoviště

Kancelář nebo jiné místo, kde uživatel pracuje. Není tím myšlen home office.

a) Riziko: spolupracovníci

Od spolupracovníků může hrozit to, že spatří heslo či jiné citlivé údaje, které mohou použít pro své účely. Nemusí ovšem jít nutně jen o spolupracovníky, ale také o návštěvy na pracovišti či kontroly. U přihlašování ať už do počítače nebo do jakéhokoliv jiného účtu či práce s citlivými daty může hrozit, že toto spatří spolupracovník či jiný výše zmíněný a může je použít pro svůj prospěch.

Opatření: Nejúčinnějším opatřením se v tomto případě nabízí prověrka zaměstnanců, což může přispět k informační bezpečnosti na pracovišti. Dále je dobré být obezřetný a dávat si pozor na bezpečnost přihlašovacích údajů a dalších důležitých informací.

b) Riziko: opuštění počítače

Při opuštění počítače může hrozit krádež citlivých dat podniku, osobních citlivých dat či jiných důležitých dat z počítače. Nebezpečí může hrozit ze strany spolupracovníků, ale také návštěv na pracovišti či jiných lidí, kteří mají přístup do budovy. Nebezpečné je opuštění počítače zejména, pokud jej před odchodem nezamkneme.

Opatření: Při opuštění počítače je nejlepší počítač jej vždy uzamknout, aby se do něj nikdo nedostal. Pro podporu tohoto opatření je také dobré mít silné heslo, případně heslo jednou za čas změnit.

c) Riziko: podvodný email

Neznámý email je jedním z nejčastěji používaných metod crackery. Může nést podvodné odkazy (phishing) či nakažené přílohy (mohou nést ransomware, trojské koně, viry, apod.), které slouží k získání přihlašovacích údajů nebo k nakažení počítače. I přes to, že je tato metoda známá i nadále je počet osob, které na ni „skočí“ vysoké. Proto by měl být každý na vědom této metody a být obezřetný.

Opatření: Nejlepší způsob ochrany je neznámé emaily vůbec neotevírat a okamžitě je smazat. Samotné otevření emailu sice nic nezpůsobí, ale je lepší je ihned smazat, nebo pokud je to již několikátý stejný email tak ho nahlásit.

d) Riziko: použití soukromého USB Flash disku nebo HDD

USB Flash disk je velice používané přenosné úložiště, a proto je také vysoké riziko jeho nakažení nějakým druhem malwaru. Obzvláště u soukromých Flash disků je tato pravděpodobnost dost vysoká, protože většina uživatelů jej nečistí od malware. Infikovaný Flash Disk může počítač nakazit spywarem, ransomwarem či jinými druhy malwaru.
Opatření: Zde bývá většinou na pracovišti zakázáno používat soukromá přenosná úložiště, což je asi nejúčinnější opatření a používají se pouze firemní. Je také možnost používat cloudová úložiště apodobně.

e) Riziko: stažení souboru z neověřených webových stránek

Velmi nebezpečné je také stahování souborů či aplikací z neověřených webových stránek. Největší riziko je to, že soubor může obsahovat skrytý malware, který se při stažení dostane do počítače a může napáchat mnoho škody. Nejčastěji jde o spyware, adware, viry či ransomware a další.
Opatření: Stahovat soubory a aplikace pouze z oficiálních webových stránek. Případně, pokud se jedná o soubory a aplikace volně přístupné, tak pouze z ověřených webových stránek.

Domácnost

Může jít o byt, rodinný dům, chatu či jiné obydlí, kde člověk bydlí.

f) Riziko: podvodný email

Na podvodné emaily si každý musí dávat pozor nejen na pracovišti, ale i doma. Doma si navíc emaily prohlíží celá rodina a je tudíž vyšší riziko, že někdo otevře podvodný odkaz nebo stáhne neznámou přílohu z emailu. Další věc je, že doma si lidé v mnoha případech data nezálohují, takže při možném infikování počítače malwarem mohou o data natrvalo přijít.
Opatření: Neotevírat email a ihned ho smazat. Pokud se jedná o email, který již někdy přišel nebo email od stejného adresáta, tak nahlásit.

g) Riziko: použití USB Flash disku nebo HDD

Používání přenosného úložiště je vždy rizikové kvůli jeho snadnému nakažení malwarem. Většina uživatelů jej preventivně nekontroluje přes anti-malware což ještě zvyšuje riziko nakažení dalších zařízení.
Opatření: Kontrola přenosného úložiště anti-malwarem případné formátování, aby se předešlo infikování některým druhem malwaru.

h) Riziko: stažení souboru z neověřených webových stránek

Stahování souborů a aplikací z Internetu doma je dnes již standart a právě neověřené webové stránky mohou skrývat soubory či aplikaci ke stažení, ke kterým jsou skrytě připojeny různé druhy malwaru.

Opatření: Stahovat soubory či aplikace z oficiálních webových stránek nebo z ověřených webových stránek.

Veřejné místo

Veřejné místo lze definovat jako místo s vyšším výskytem obyvatel. Může se jednat o veřejné prostranství, restauraci, kavárnu, park a jiné. Na těchto místech je vysoká anonymita, která nahrává snadnému sledování nebo krádežím.

i) Riziko: cizí lidé

Veřejná místa jsou ideální pro nenápadné pohybování a je tudíž těžké neustále pozorovat kolemjdoucí lidi. Avšak o to větší pozornost by měl každý věnovat skrytí přihlašovacích údajů, pokud je zadává na nějakém veřejném místě. Je totiž jednoduché pro zkušeného zloděje či někoho podobného zpozorovat tyto údaje a využít je ve svůj prospěch.

Opatření: Jediné opatření se v tomto případě jeví obezřetnost a všímavost svého okolí. Ovšem nejbezpečnější by bylo počítač na veřejném místě vůbec nepoužívat.

j) Riziko: opuštění počítače

Dalším rizikem na veřejných místech, je opuštění počítače z čehož plyne hrozba jeho krádeže nebo poškození či úplného zničení.

Opatření: V tomto případě jde o notebook. Počítač nechat někomu z rodiny či kamarádovi, který ho pohlídá. Pokud je člověk sám, tak si jej vzít s sebou.

Zranitelná místa uživatele osobního počítače

Zranitelná místa jsou místa, která mohou být zneužita v neprospěch nějaké osoby za účelem způsobení újmě (v tomto případě duševní nebo finanční), vydírání nebo zneužití. Útočník může způsobit poškození softwaru počítače, ztrátu dat uživatele, vydírání s pomocí citlivých dat uživatele (většinou za účelem obohacení) nebo zneužití počítače bez vědomí jeho majitele pro konání nelegální či trestné činnosti. V návaznosti na tabulku 1 je zde vytvořena tabulka zranitelných míst uživatele osobního počítače. Zranitelná místa přímo vyplývají z předešlé tabulky a jsou k nim doplněny další upřesňující údaje. První je důvod, proč je místo zranitelné. A dále je to možný následek při zneužití zranitelného místa crackery nebo někým jiným.

Tabulka 2 – Zranitelná místa informační bezpečnosti (vlastní)

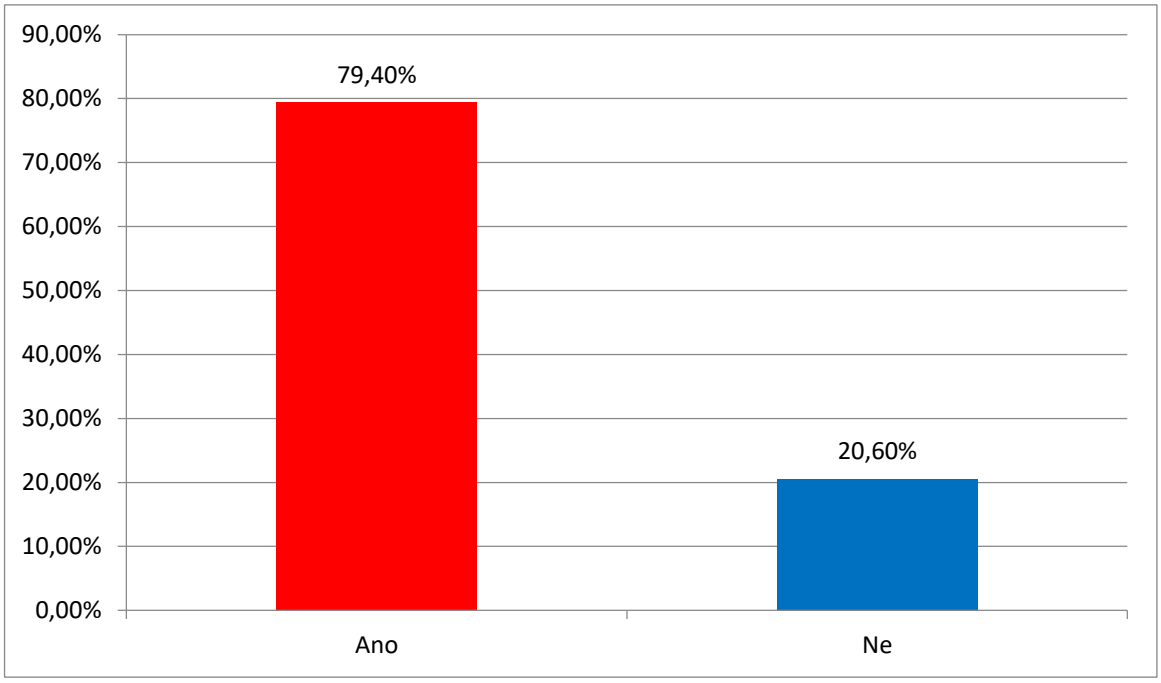
Zranitelné místo	**Důvod**	**Možný následek**
Heslo	Špatné heslo	Krádež dat; vydírání
Člověk	Nepozornost; naivita	Zpozorování citlivých informací – vydírání; krádež dat; dobrovolné poskytnutí přihlašovacích údajů či citlivých dat (sociální inženýrství)
Software	Zastaralý OS; počítač bez anti-malwaru	Ztráta dat; infikování malwarem
Špatné zvyky	Nezamknutí počítače při jeho opuštění; otevírání každého emailu a v něm přiložených odkazů či příloh	Krádež dat; krádež přihlašovacích údajů (od internetového bankovnictví, emailu, apod.)

5 ANALÝZA INFORMAČNÍ BEZPEČNOSTI UŽIVATELE OSOBNÍHO POČÍTAČE

Analýza byla provedena formou dotazníku. Dotazník se zaměřuje na zabezpečení dat v počítači a na zvyky s ním spojené. Dotazník probíhal anonymně za pomoci webového portálu Survio a to od 27. Dubna 2021 do 7. Května 2021. Dotazník se skládá z celkem 33 otázek. Některé otázky vyžadovaly pouze jednu odpověď, jiné umožňovaly respondentům více odpovědí. V dotazníku bylo použito logické pravidlo, které umožňuje podle toho, která odpověď je označena přejít na další určenou otázku tak, aby byly odpovědi co nejrelevantnější a předcházelo se tak podobným otázkám pro respondenta. Dotazník vyplnilo celkem 141 respondentů. Oslovení respondenti byly z Fakulty logistiky a krizového řízení UTB. Dotazník byl rozeslán formou e-mailů za velké pomoci studijního oddělení Fakulty logistiky a krizového řízení UTB. Cílem bylo zjistit stav bezpečnosti informací studentů na Fakultě logistiky a krizového řízení UTB, která sídlí v Uherském Hradišti. Dotazník byl vyhodnocen a výsledná data zpracována díky programu Microsoft Excel do grafů.

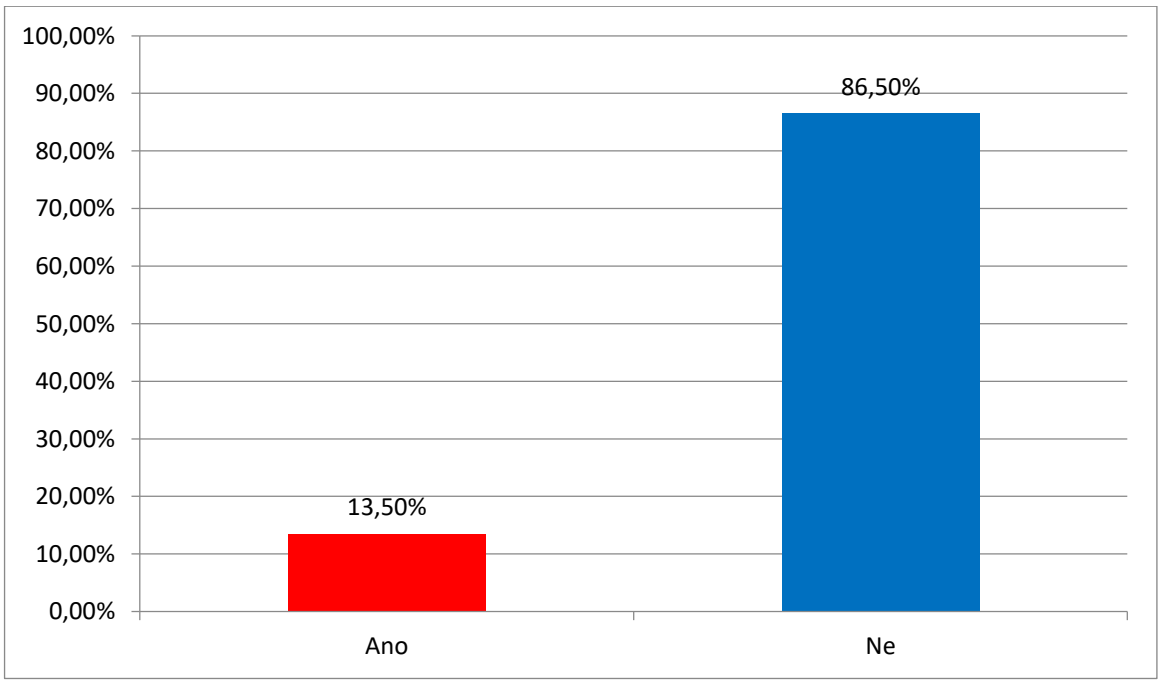
Dotazníkové šetření se týkalo bezpečnosti informací a otázky byly rozděleny podle určených témat, která právě zahrnuje bezpečnost informací. První téma bylo **zabezpečení počítače**, které zahrnovalo otázky 1 – 10 a tyto otázky se zaměřují zejména na nastavení hesla pro účty v počítači, zadávání hesla v přítomnosti jiné osoby, či na uzamykání počítače v různých prostředích. Druhý okruh otázek se týkal **heslové politiky** a šlo o otázky 11 – 18, zaměřené na podobu hesla, případně zda a k jakým účtům je jedno heslo používáno, na správce hesel nebo na to, kdo by heslo prozradil jiné osobě. Dále bylo **pokročilé zabezpečení dat v počítači**. Téma zahrnovalo otázky 19 – 26 dotýkající se šifrování, šifrovacích softwarů a zálohování. **Malware a zabezpečení** je okruh otázek 27 – 31, jež je zaměřen na anti-malwary (laicky antiviry), které respondenti používají či znají. Poslední dvě otázky 32 a 33 zaměřené na neznámé emaily a stahování souborů z neznámých webových stránek.

Vyhodnocení první otázky, která se týkala nastavení hesla pro přihlášení na počítač, dopadlo tak, že 112 respondentů (79,4 %) odpovědělo *„Ano“* a 29 (20,6 %) odpovědělo *„Ne“*. Z toho je jasné, že většina respondentů má nastavené heslo pro přihlášení do počítače.



Graf 1 – Nastavení hesla pro přihlášení do počítače (vlastní)

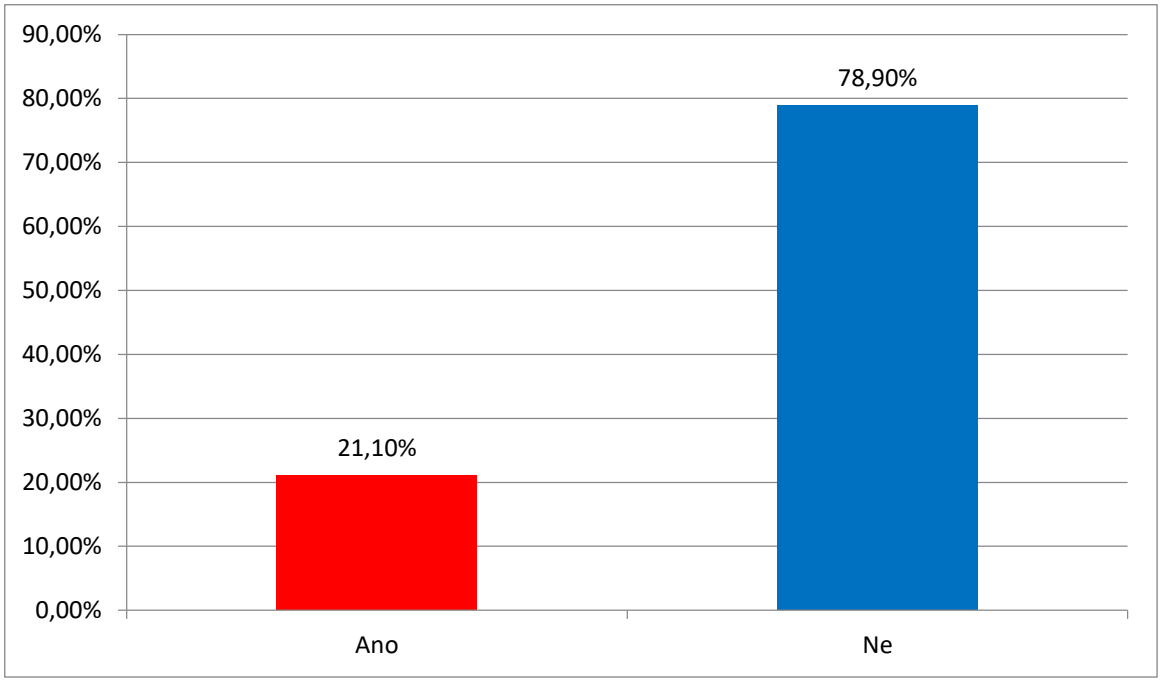
Vyhodnocení 2. otázky: Druhá otázka se zaměřovala na to, zda má respondent vytvořeno více účtů ve svém počítači. Výsledky jsou v grafu 2.



Graf 2 – Nastavení více účtů v počítači (vlastní)

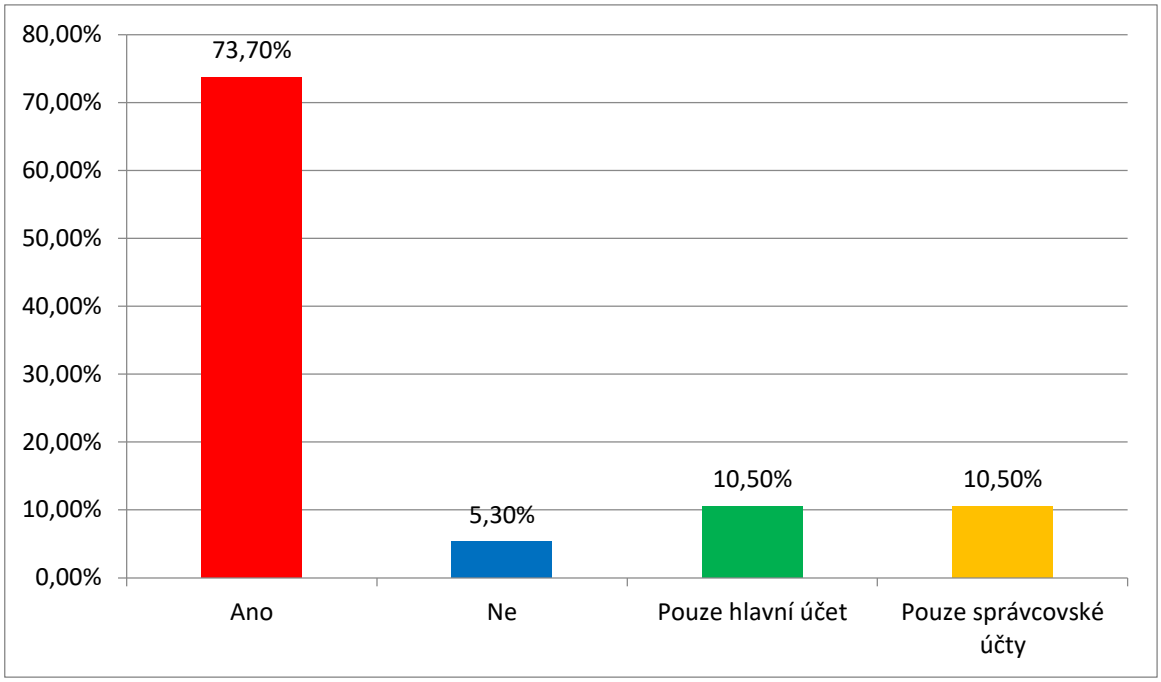
Z výsledku vyplývá, že více účtů má 19 respondentů (13,5 %) a zbylých 122 (86,5 %) má jen jeden účet. Respondenti, kteří odpověděli *„Ano“* byli přesunuti k 3. otázce a ostatní, čili ti, kteří odpověděli *„Ne“* až k 5. otázce.

Vyhodnocení 3. otázky: Ta se týkala toho, zda má respondent vytvořeno více správcovských účtů. Pouze 4 odpověděli *„Ano“* (21,1 %) a 15 *„Ne“* (78,9 %). Takže z devatenácti respondentů, kteří mají vytvořeno více účtů jich má většina pouze jeden účet správcovský.



Graf 3 – Více správcovských účtů (vlastní)

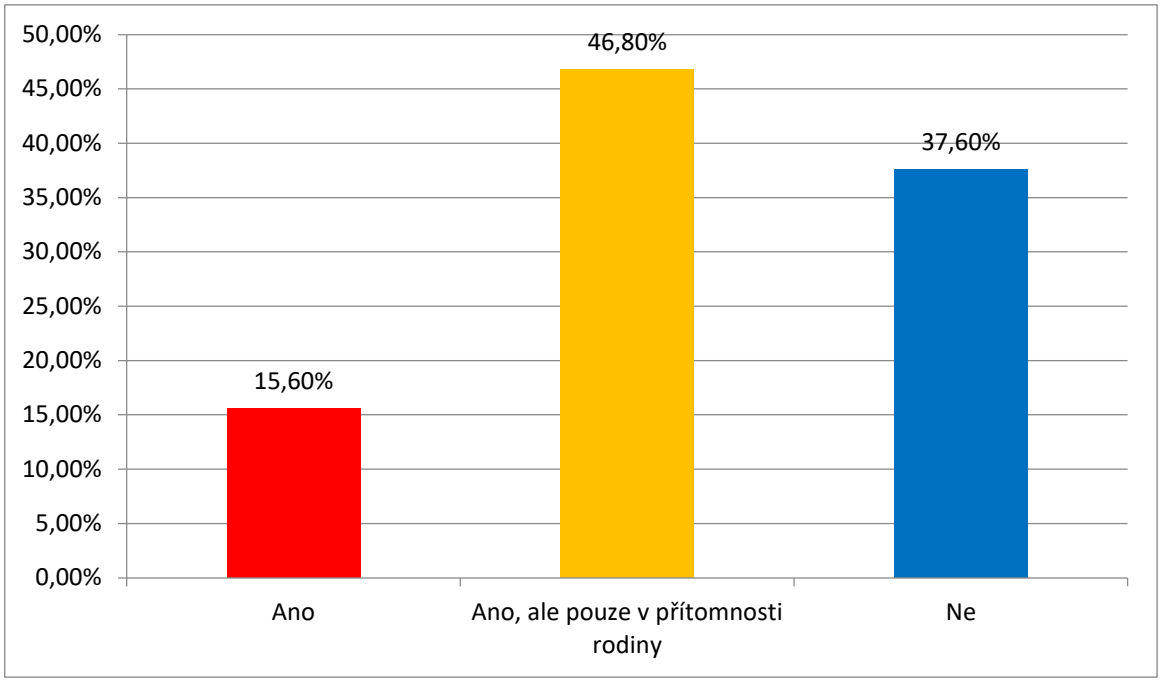
Vyhodnocení 4. otázky: Otázka zněla, zda má respondent zabezpečeny všechny účty heslem. Výsledek je vidět na grafu 4.



Graf 4 – Zabezpečení všech účtů heslem (vlastní)

14 odpovědělo ano a 1 ne. Další 2 mají heslem zabezpečen pouze hlavní účet a 2 mají zabezpečeny pouze správcovské účty. Celkově tedy 14 respondentů má zabezpečeny všechny účty heslem a zbylých 5 má zabezpečeny pouze některé.

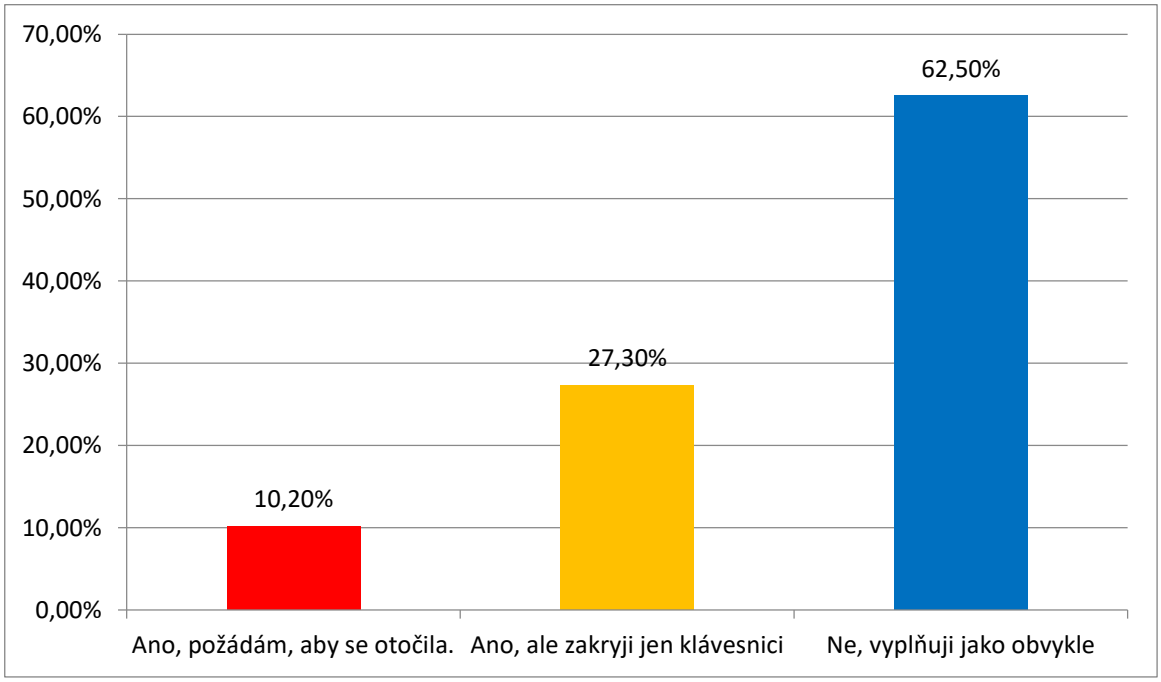
Vyhodnocení 5. otázky: Další otázka měla zjistit, jestli respondent zadává heslo v přítomnosti jiné osoby. Na toto odpovědělo *„Ano“* 22 dotazujících a jako *„Ne“* 53. Variantu *„Ano, ale pouze v přítomnosti rodiny“* odpovědělo 66 respondentů. Z čehož vyplývá, že ve většině případů heslo zadávají tak, aby je nikdo neviděl případně v přítomnosti rodiny.



Graf 5 – Zadávání hesla v přítomnosti jiné osoby (vlastní)

Zde bylo opět použito logické pravidlo, které respondenty, kteří vybrali *„Ano“* nebo *„Ano, ale pouze v přítomnosti rodiny“* byl odkázán na 6. otázku a zbytek na 7. otázku.

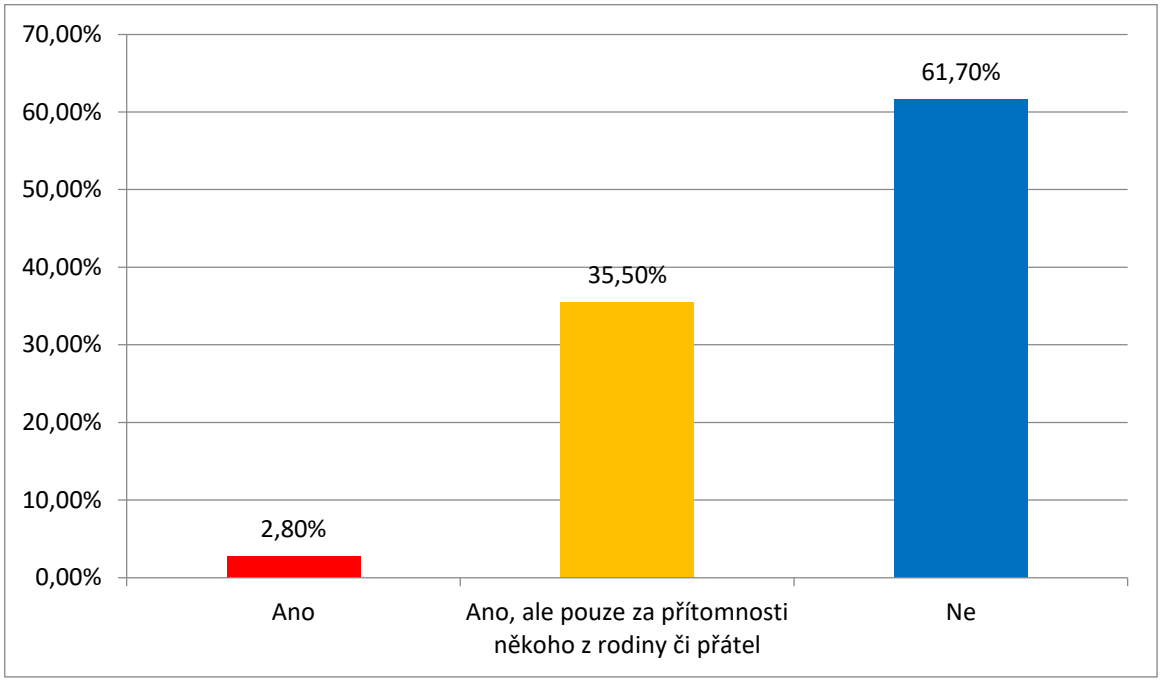
Vyhodnocení 6. otázky: Hned navazující otázka se dotazovala na to, jestli si respondent dává pozor, aby heslo, co zadává, daná osoba neviděla. Výsledek můžete vidět v grafu 6.



Graf 6 – Pozornost, aby heslo nikdo neviděl (vlastní)

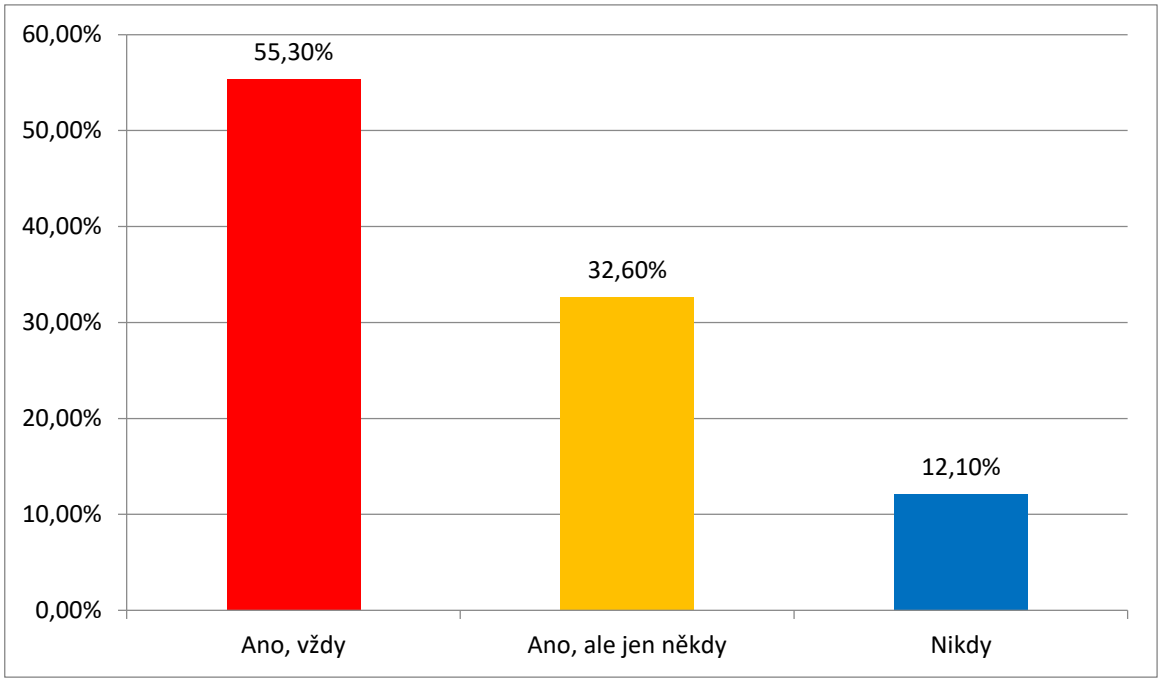
Nejvíce odpovědí bylo jako „Ne, vyplňuji jako obvykle“ a to 55. Se zakrytou klávesnicí vybralo 24 respondentů a 9 respondentů požádá, aby se osoba otočila. Nadpoloviční většina tedy vyplňuje heslo jako obvykle a nestará se, jestli ho přítomná osoba může vidět.

Vyhodnocení 7. otázky: Nechal/a byste svůj notebook na veřejném místě (kavárna, vlak, lavička v parku apod.) chvíli bez dozoru či pozornosti? Takto zněla 7. Otázka, na kterou *„Ano“* odpověděli 4 respondenti (2,8 %), *„Ano, ale pouze za přítomnosti někoho z rodiny či přátel“* označilo 50 dotazujících (35,5 %) a zbývajících 87 (61,7 %) označilo *„Ne“*. Skoro všichni tedy jsou obezřetní se svým notebookem na veřejnosti.



Graf 7 – Odložení notebooku na veřejném místě (vlastní)

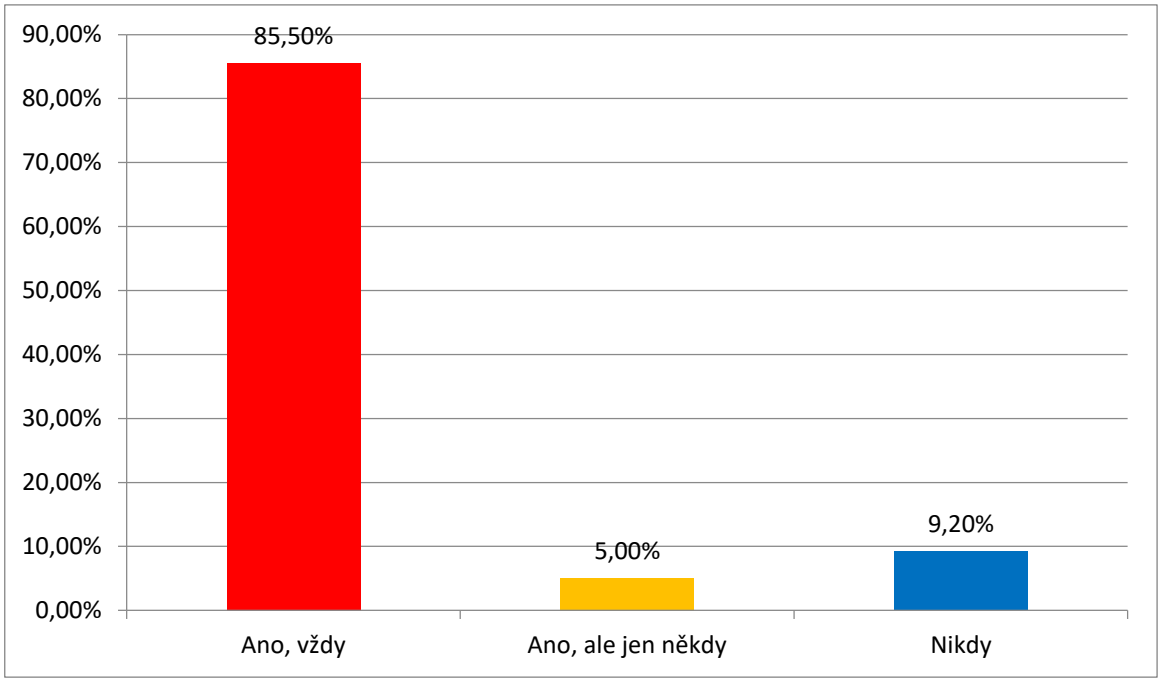
Vyhodnocení 8. otázky: Otázka se ptá, zda respondent uzamyká počítač v kontrolovaném prostředí, kdež od něj odchází. Kontrolovaným prostředím je myšleno místo jako práce či škola, kde se nachází pouze lidé, kteří zde jsou pravidelně. Výsledek je zřetelný v grafu 8.



Graf 8 – Uzamykání počítače v kontrolovaném prostředí (vlastní)

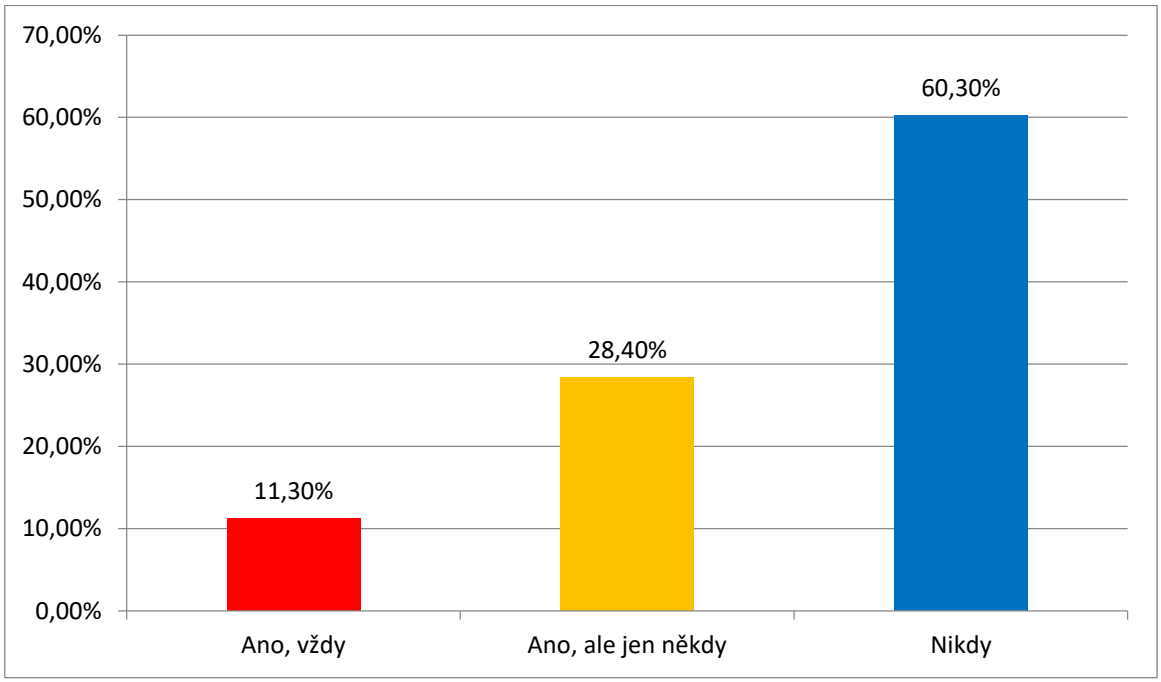
Většina (tedy 78 dotazujících) svůj počítač uzamyká vždy, když od něj odchází. 46 jej uzamyká jen někdy a 17 svůj počítač v těchto prostorách nikdy neuzamyká. Z těchto výsledků vyplývá, že ne každý je opatrný a i přesto, že 55,3 % respondentů svůj počítač uzamyká, tak jsou i tací, kteří se cítí bezpečně.

Vyhodnocení 9. otázky: Dále byla otázka položena také na uzamykání počítače, ale tentokrát v nekontrolovaném prostředí, což může být kavárna, restaurace a další místa, na kterých se pohybuje mnoho neznámých lidí a jde o veřejná místa. Zde byly odpovědi více jednoznačné a to tak, že 121 respondentů počítač zamyká vždy, 7 jen někdy a 13 nikdy. Opět je vidět, že jsou i lidé, kteří si nedávají tak velký pozor i na veřejných místech, kde je vysoké nebezpečí.



Graf 9 – Uzamykání počítače v nekontrolovaném prostředí (vlastní)

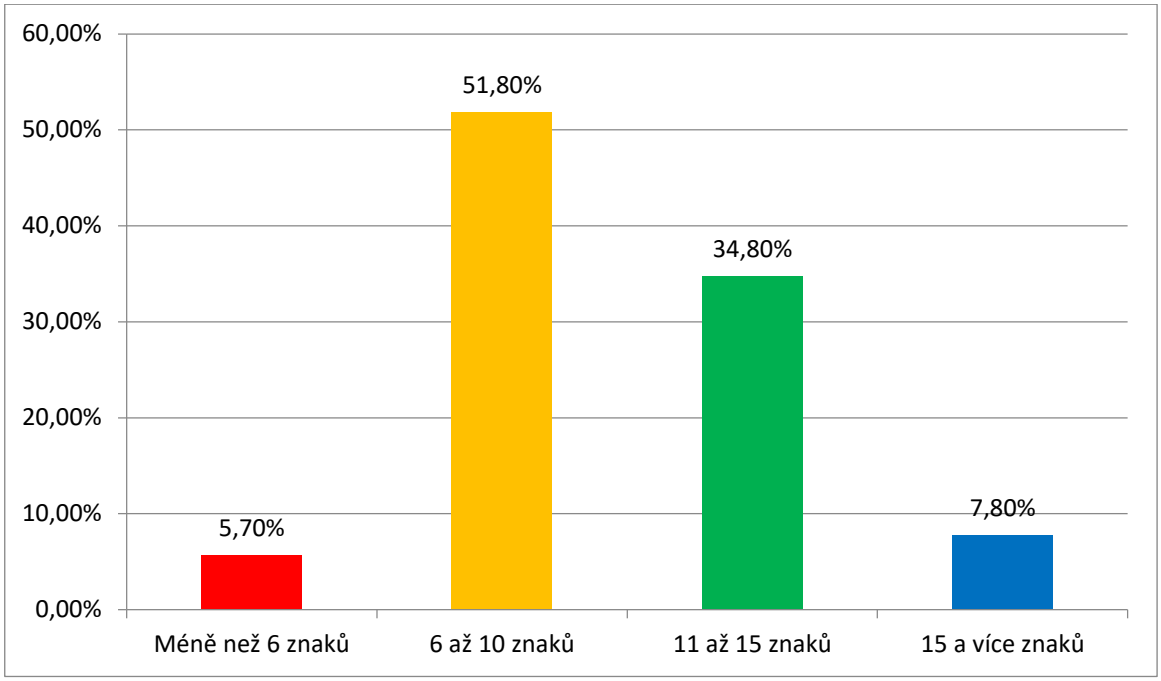
Vyhodnocení 10. otázky: *„Uzamykáte svůj počítač doma, když od něj odcházíte?“* Další otázka na téma uzamykání počítače, tentokrát doma. Výsledek této otázky lze vidět na grafu 10.



Graf 10 – Uzamykání počítače doma (vlastní)

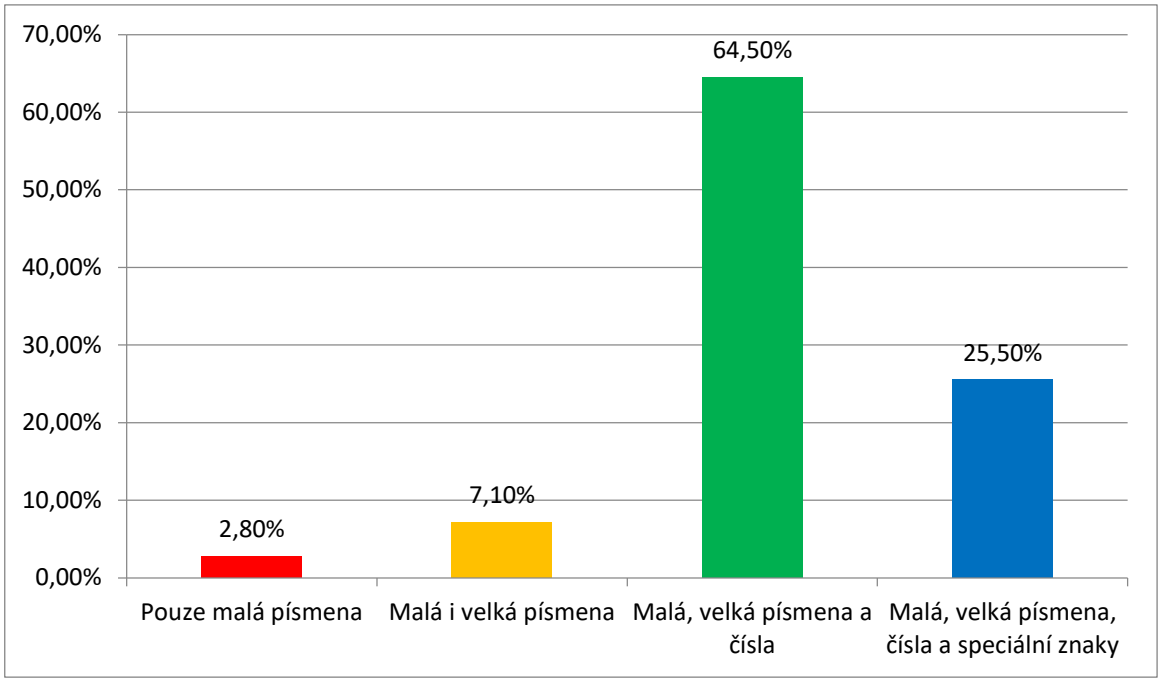
Zde jsou odpovědi naprosto jiné než u předchozích dvou otázek. Ovšem výsledek se dal předvídat, protože doma si počítač nezamyká 85 respondentů, jak se dalo čekat. 16 si zamyká počítač vždy a 40 jen někdy.

Vyhodnocení 11. otázky: Otázka týkající se heslové politiky zjišťovala, jak dlouhá hesla dotazující používá. Počet respondentů používajících hesla s délkou menší než 6 znaků je 8, v rozpětí 6 až 10 jich je 73, 11 až 15 znaků používá 49 a 15 a více znaků 11 dotazovaných.



Graf 11 – Délka používaných hesel (vlastní)

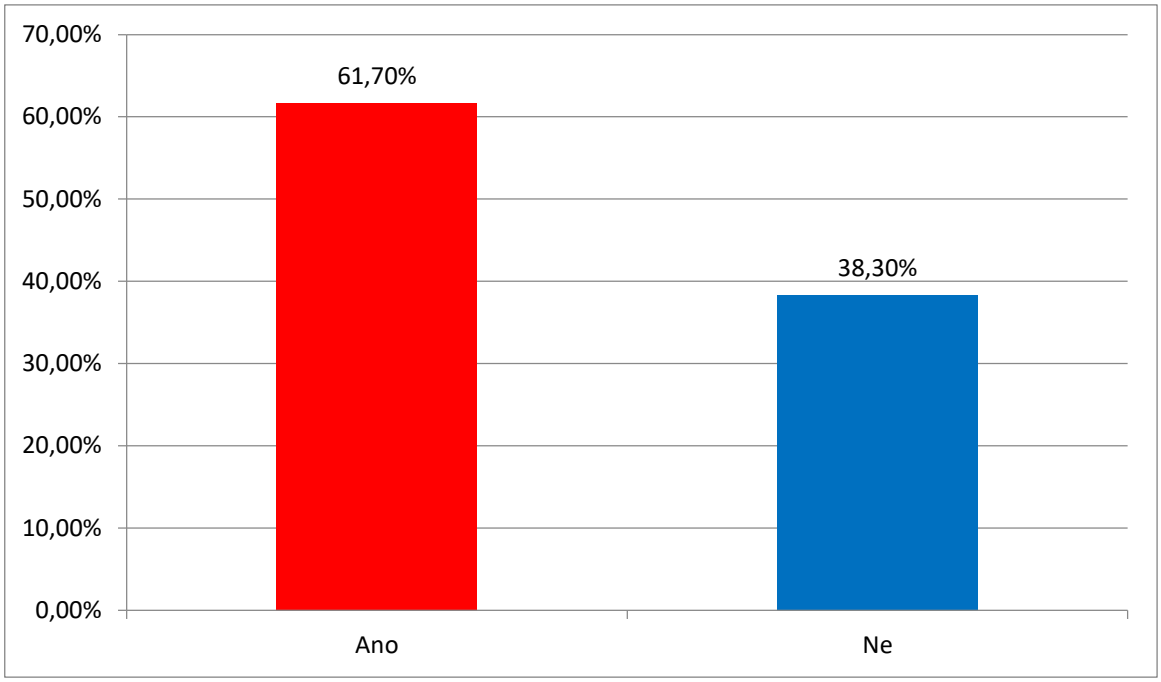
Vyhodnocení 12. otázky: Otázka byla zaměřena na to, jak složitá hesla respondent používá. Složitost ve smyslu použití malý, velkých písmen čísel a speciálních znaků a v jejich kombinaci. Výsledek můžete vidět na grafu 12.



Graf 12 – Složitost používaných hesel (vlastní)

Nejméně bezpečná hesla skládající se pouze z malých písmen používají 4 respondenti. Dalších 10 používá malá i velká písmena, která ovšem nejsou také příliš bezpečná. Největší část respondentů a to 91 používá kombinaci malých, velkých písmen a čísel. A nejbezpečnější kombinaci písmen, čísel a speciálních znaků používá 36 dotazujících. Celkově lze tedy říci, že téměř všichni používají bezpečné kombinace. Toto však neznamená, že hesla složená v těchto kombinacích ještě nemusí být zcela bezpečná. Vždy záleží na podobě hesla.

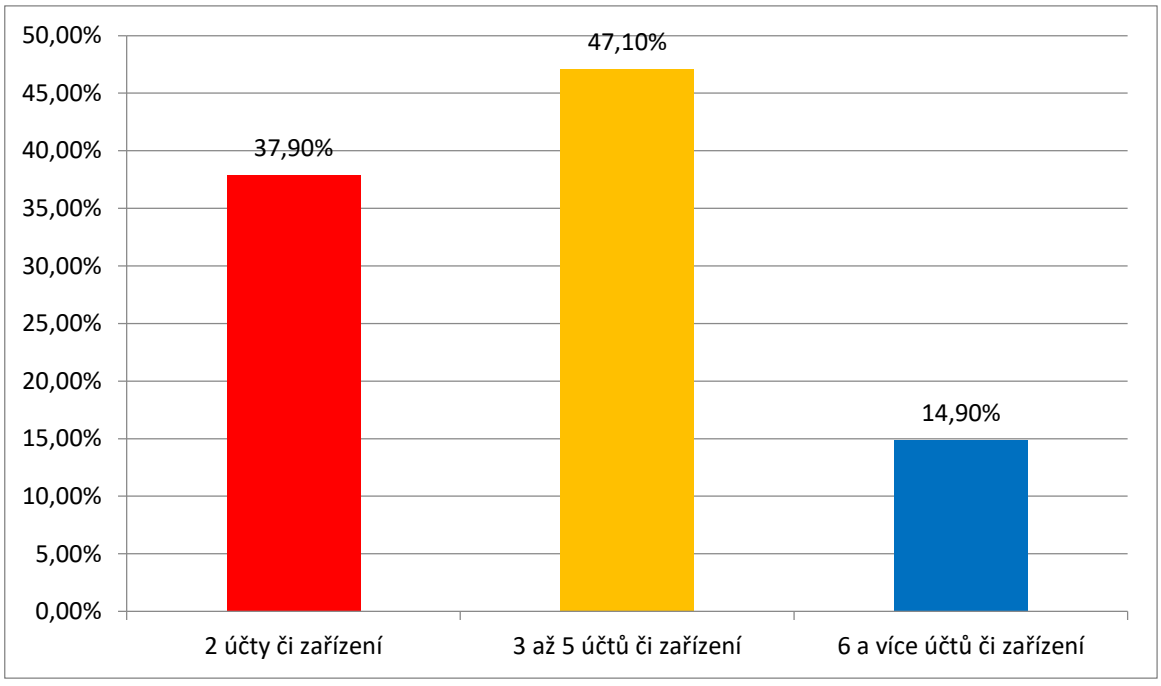
Vyhodnocení 13. otázky: Respondent měl odpovědět, zda používá jedno heslo k více účtům či zařízením. Tím je myšleno, že uživatel používá heslo k počítači, Facebookovém účtu a k emailu. „Ano“ odpovědělo 87 a „Ne“ 54 respondentů. Čili více jich používá jedno heslo k více zařízením nebo účtům.



Graf 13 – Používání jednoho hesla k více účtům či zařízením (vlastní)

Respondenty, kteří vybrali *„Ano“* byli přesměrování na 14. otázku a ostatní, tedy ti co dali *„Ne“* na 15. otázku.

Vyhodnocení 14. otázky: Tato navazovala na předešlou a ptala se na to, ke kolika účtům či zařízením dotazující používá jedno heslo. Zde byly odpovědi následující: 33 vybralo *„2 účty či zařízení“*, 41 *„3 až 5 účtů či zařízení“* a 13 dalo *„6 a více účtů či zařízení“*.

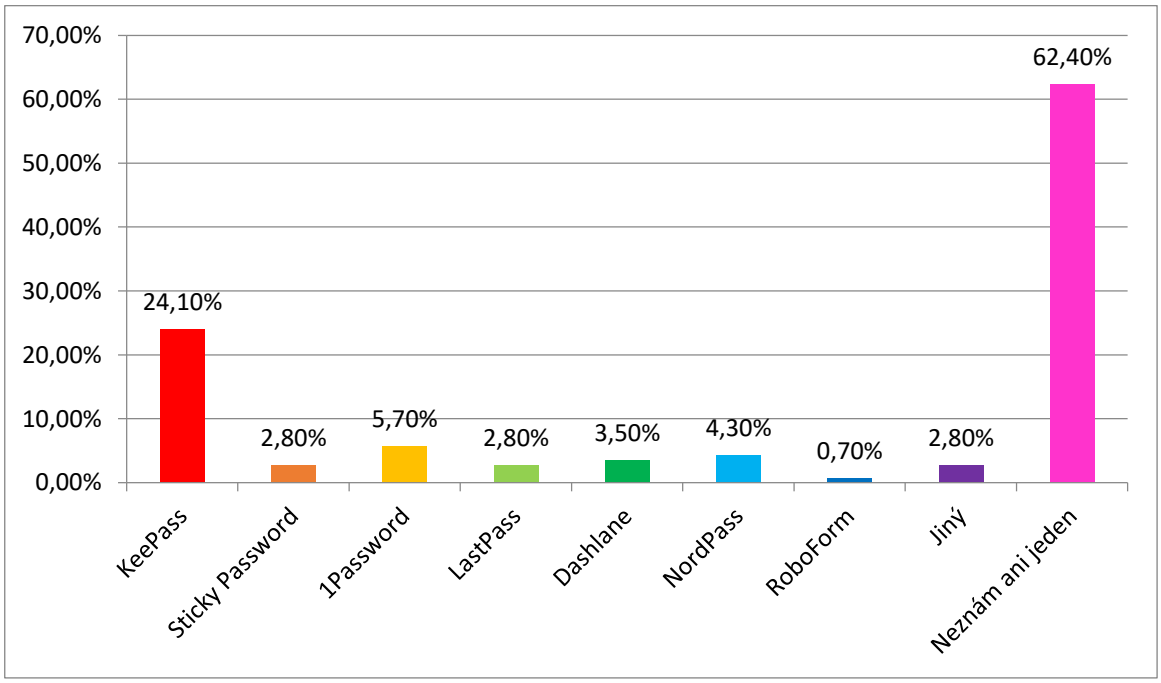


Graf 14 – Množství účtů či zařízení při použití jednoho hesla (vlastní)

Vyhodnocení 15. otázky: Ta se zabývá správci hesel. Přesněji se ptá na to, jaké respondent zná nebo používá. U této otázky šlo vybrat více odpovědí. Nejvíce volená možnost byla *„Neznám ani jeden“* a to 88 výběrů. Druhá nejvíce volená byla odpověď *„KeePass“* v počtu 34.

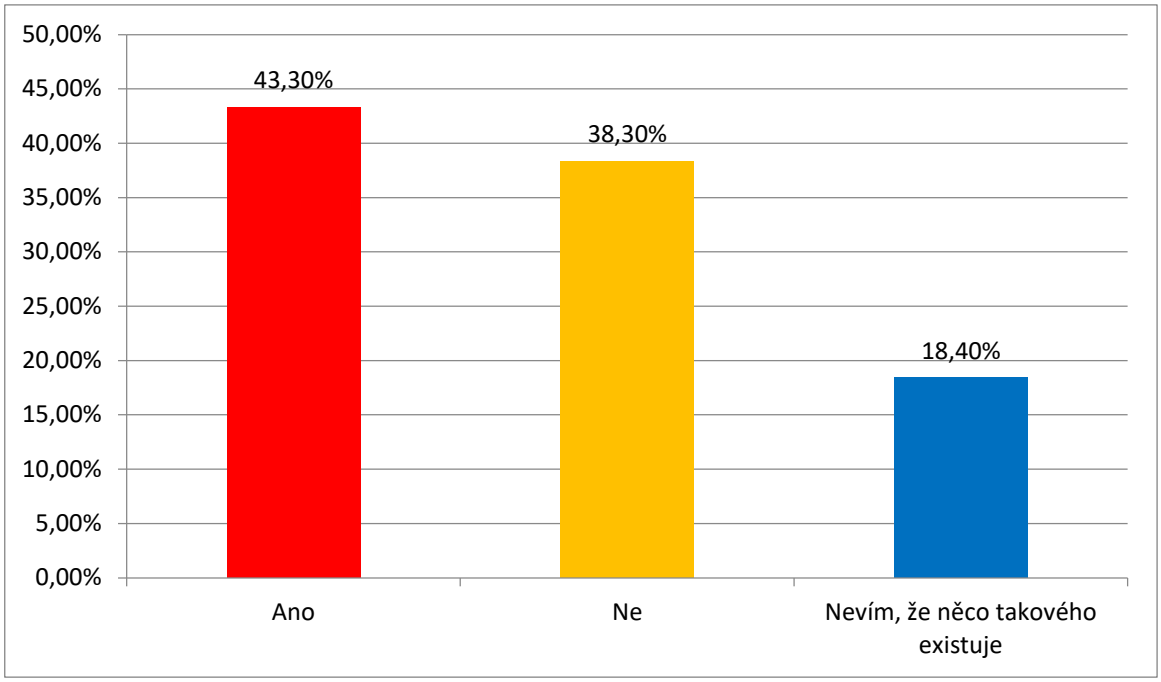
Další odpovědi byly v těchto počtech:

- Sticky Password – 4×.
- 1Password – 8×.
- LastPass – 4×.
- Dashline – 5×.
- NordPass – 6×.
- RoboForm – 1×.
- Jiný – 4 (Avira 1×, Google password 1×, Apple správa hesel 2×).



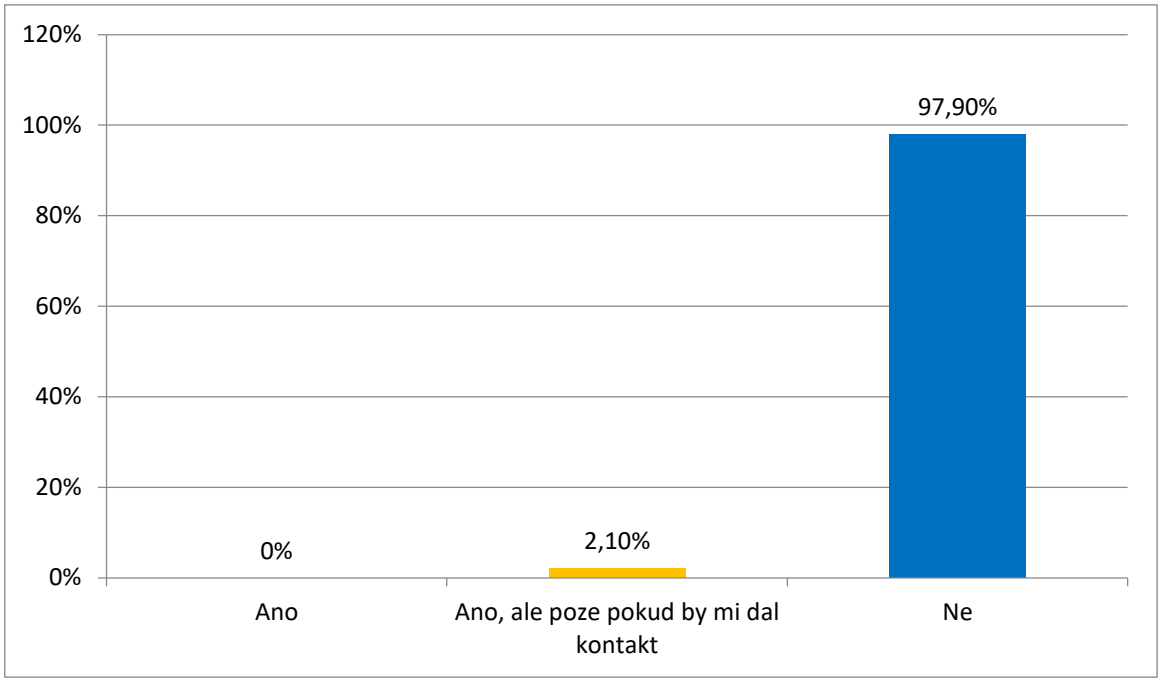
Graf 15 – Software pro správu hesel (vlastní)

Vyhodnocení 16. otázky: Tato otázka zjišťovala, jestli dotazovaný používá správce hesel v prohlížeči. 61 jich odpovědělo *„Ano“*, 54 vybralo *„Ne“* a dalších 26 označilo odpověď *„Nevím, že něco takového existuje“*.



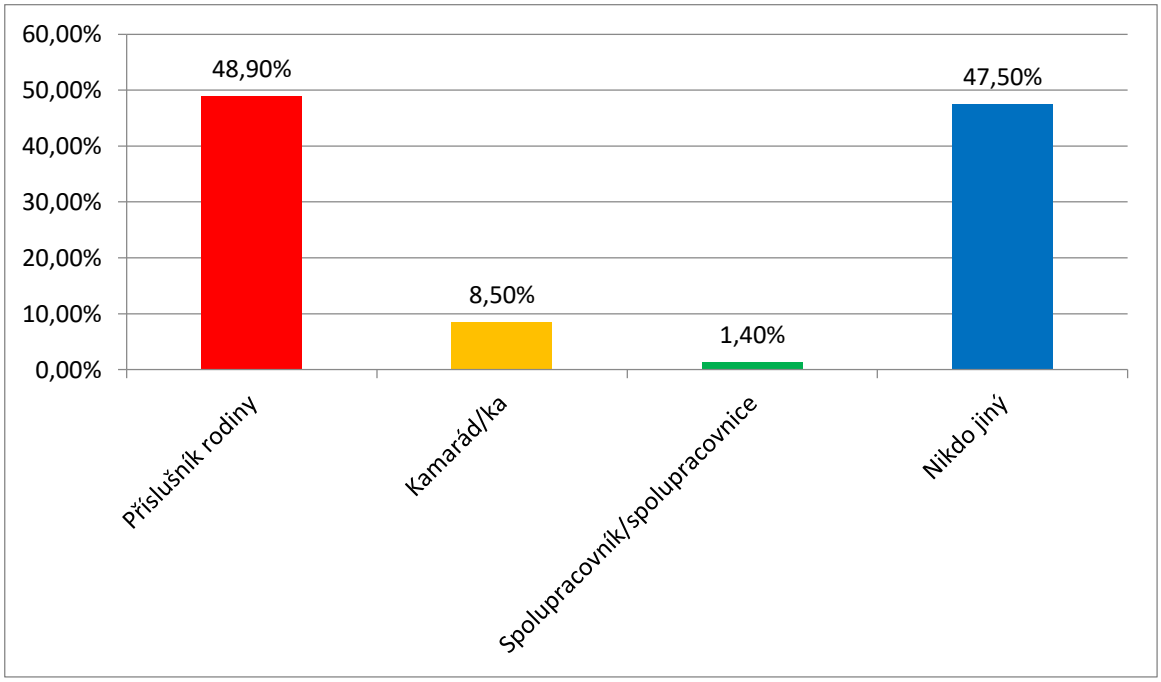
Graf 16 – Používání správce hesel v prohlížeči (vlastní)

Vyhodnocení 17. Otázky: *„Byl/a byste schopen/a prozradit heslo či jiné citlivé údaje člověku, který by vystupoval (v telefonu, SMS nebo emailu) jménem organizace (např. banky, sociálních sítí, pojišťovny apod.), kterou znáte, a uváděl by různé důvody, proč po Vás tyto informace chce?“* Toto je celé znění otázky, která je zaměřena na sociální inženýrství. Výsledek ukázal, že by nikdo neprozradil své heslo či citlivé údaje. 3 lidé by tyto informace prozradili, ale pouze pokud by jim osoba nechala kontakt a 138 odpovědí bylo jasně pro *„Ne“*. Zde tedy vyšlo, že by téměř nikdo nic neprozradil, což přispívá k bezpečnosti informací.



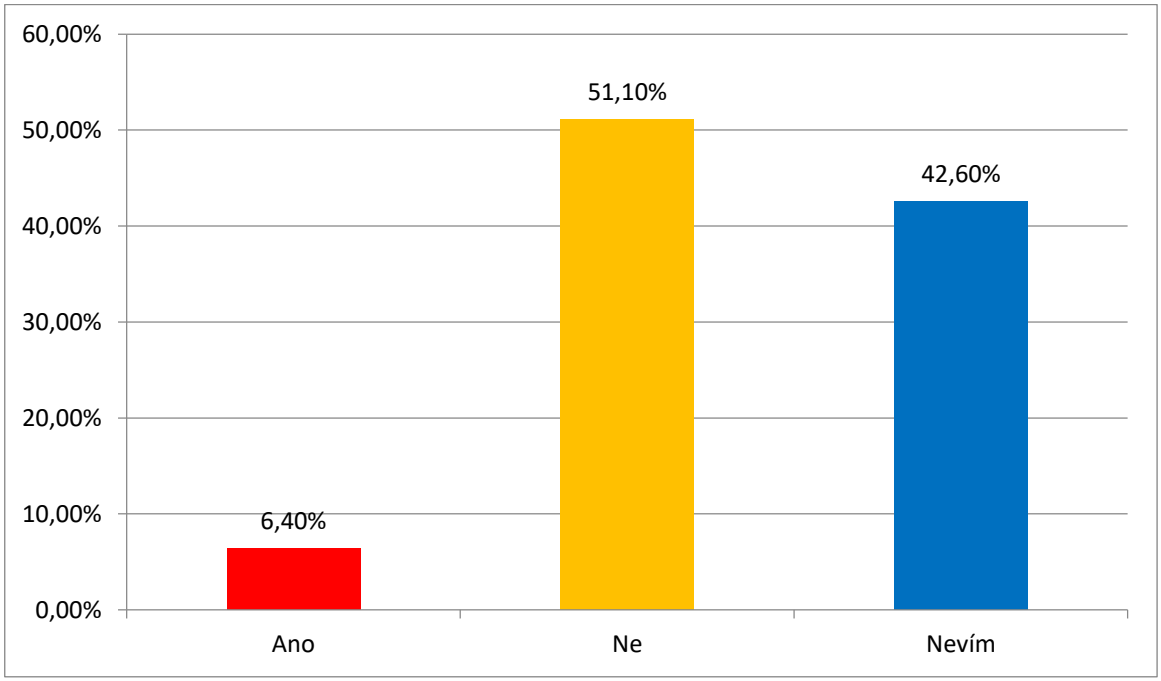
Graf 17 – Prozrazení hesla či citlivých údajů neznámé osobě (vlastní)

Vyhodnocení 18. otázky: Ptá se dotazovaných, jestli jejich heslo nebo PIN zná někdo jiný. Nejvíce respondentů vybralo možnost *„Příslušník rodiny“* celkem 69. Pro kamaráda/ku hlasovalo 12, spolupracovník/spolupracovnice 2 a 67 určilo, že jejich heslo nezná nikdo.



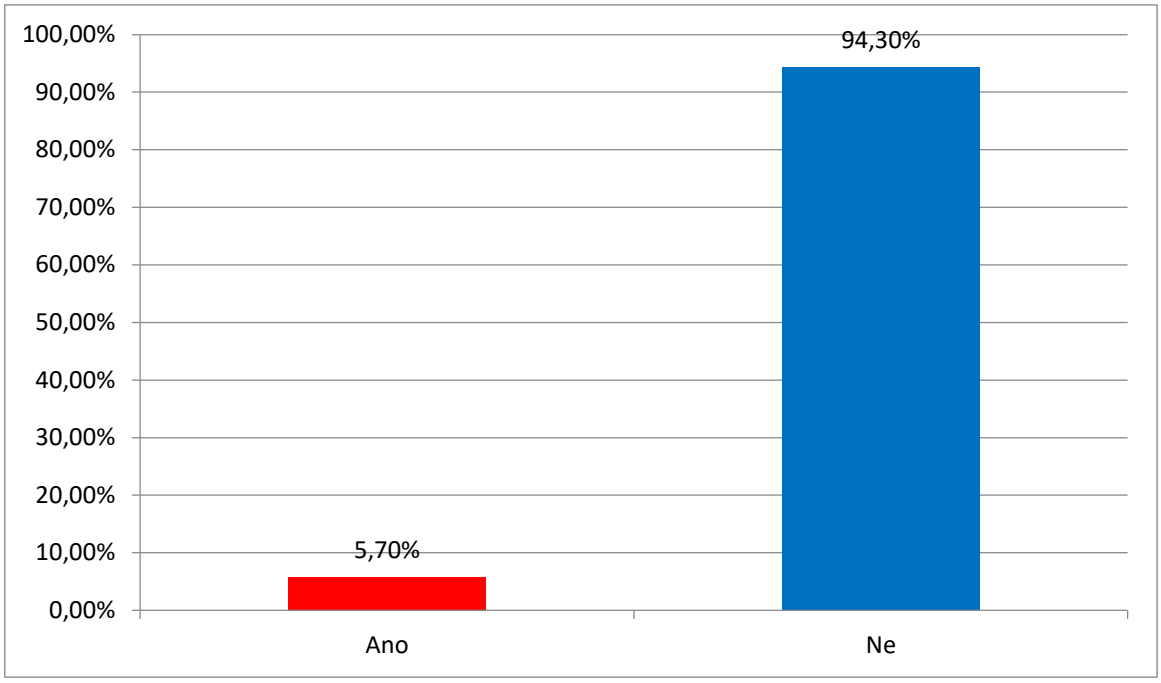
Graf 18 – Znalost hesla (vlastní)

Vyhodnocení 19. otázky: Další sada otázek se týká šifrování a otázka č. 19 se ptá respondentů, zda mají šifrovaný disk v počítači. Pouze 9 odpovědělo *„Ano“*. Negativních odpovědí bylo 72 a 60 neví.



Graf 19 – Šifrovaný disk v počítači (vlastní)

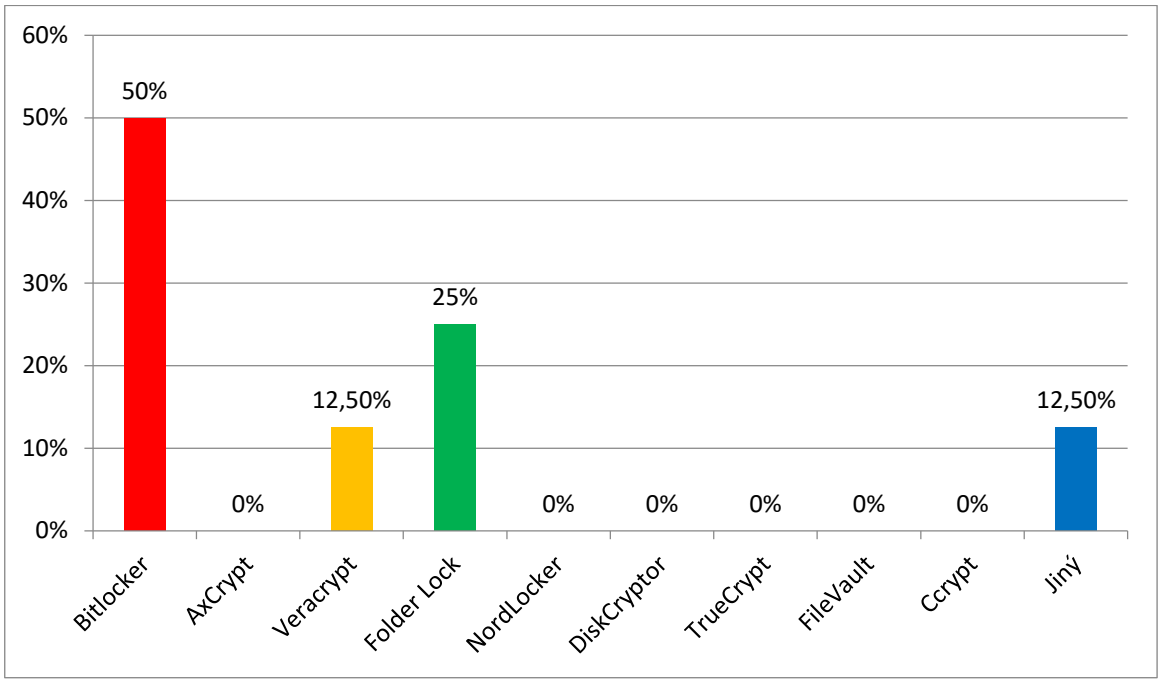
Vyhodnocení 20. otázky: Tato otázka se zaměřila na šifrování cenných dat. 8 respondentů šifruje a 133 nešifruje svá cenná data. Z toho vyplývá, že si svá data chrání menšina, což neukazuje dobrou ochranu dat.



Graf 20 – Šifrování dat (vlastní)

Ti, kteří odpověděli *„Ano“* přešli na 21. otázku a ostatní na 22. otázku.

Vyhodnocení 21. otázky: Otázka navazuje na předchozí a ptá se na šifrovací program, který respondent používá. Výsledek je v grafu 21.

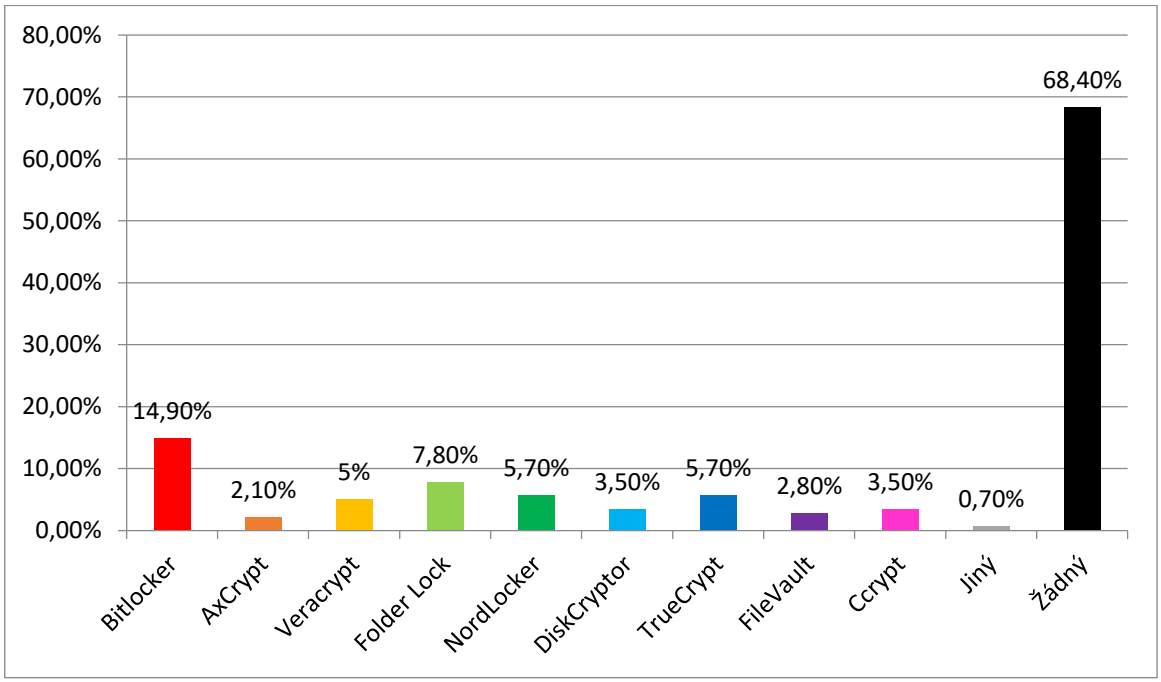


Graf 21 – Používaný šifrovací software (vlastní)

Z 8 respondentů vybrali:

- 4× Bitlocker.
- 1× Veracrypt.
- 2× Folder Lock.
- 1× Jiný (zde respondent z osobních důvodů nechtěl uvést).

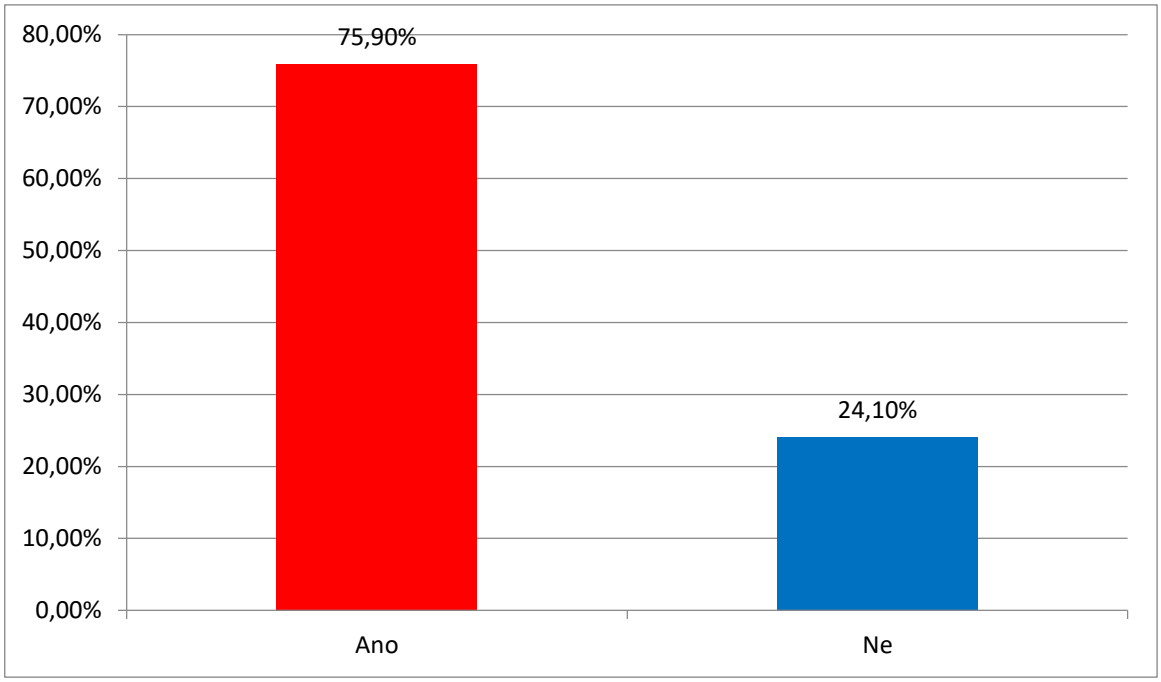
Vyhodnocení 22. otázky: Tato otázka byla položena pro všechny a zjišťovala, jaký šifrovací program znají dotazující. Graf 22 ukazuje výsledek.



Graf 22 – Známý šifrovací software (vlastní)

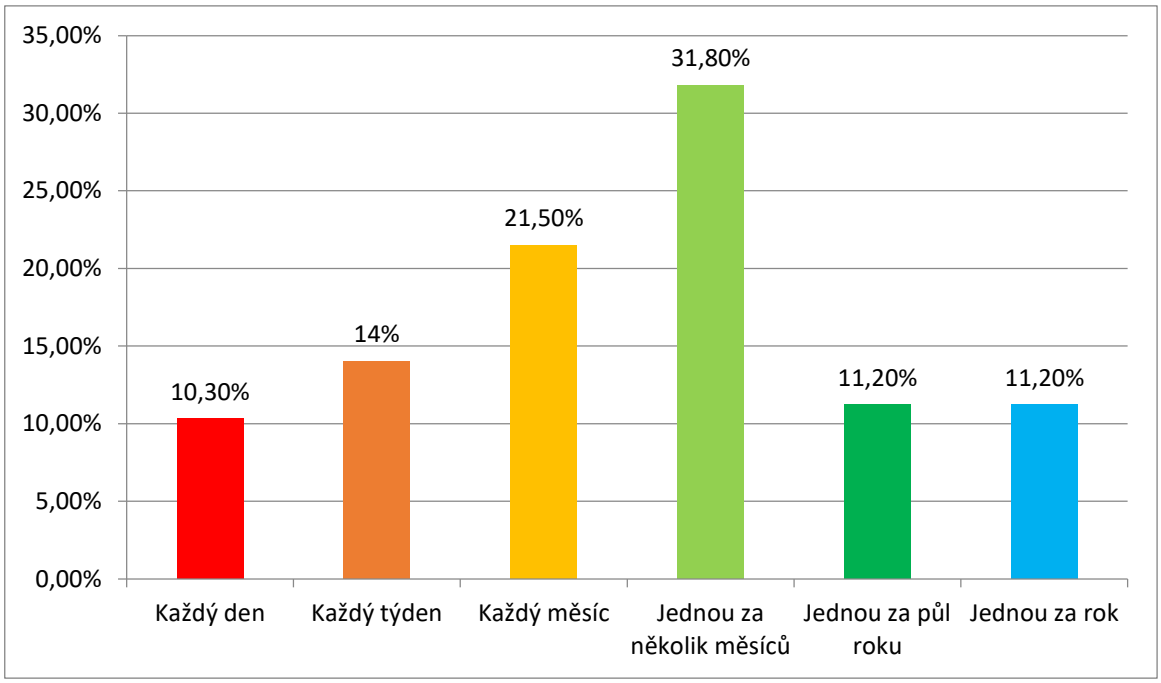
Nejvíce respondentů uvedlo, že nezná žádný šifrovací program a to v počtu 96. Na druhém místě skončil BitLocker, který vybralo 21 lidí. Další programy mají 11 a míně hlasů.

Vyhodnocení 23. otázky: Otázka dotazující se na zálohování. Zde 107 respondentů odpovědělo kladně a 34 záporně. Při odpovědi *„Ano“* přešli respondenti na otázku č. 24 a u *„Ne“* na 26. otázku.



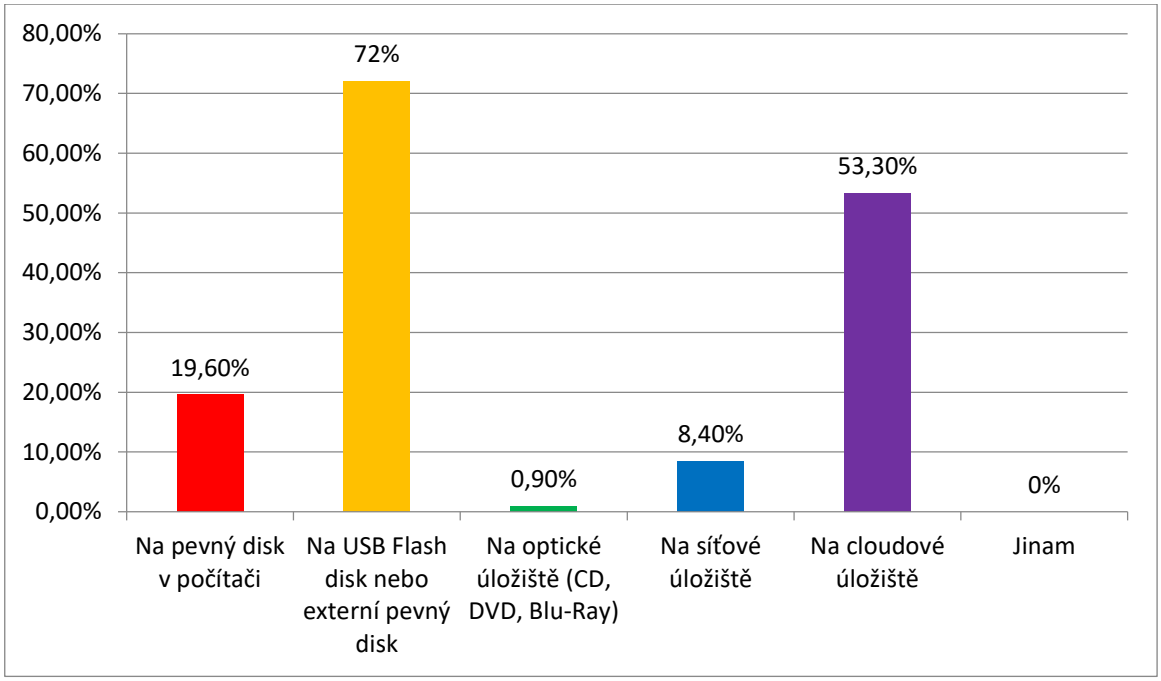
Graf 23 – Zálohování dat (vlastní)

Vyhodnocení 24. otázky: *„Jak často zálohujete?“* Výsledky jsou na grafu 24. Ale je třeba zmínit, že nejvíce respondenti vybírali, že zálohují jednou za několik měsíců a to 34×. Zato nejméně, 11× bylo voleno každý den. Výsledky jsou pochopitelné, ale ne příliš bezpečné pro data svých uživatelů. Bezpečné a rozumné by bylo zálohovat každý týden až každý měsíc.



Graf 24 – Četnost zálohování (vlastní)

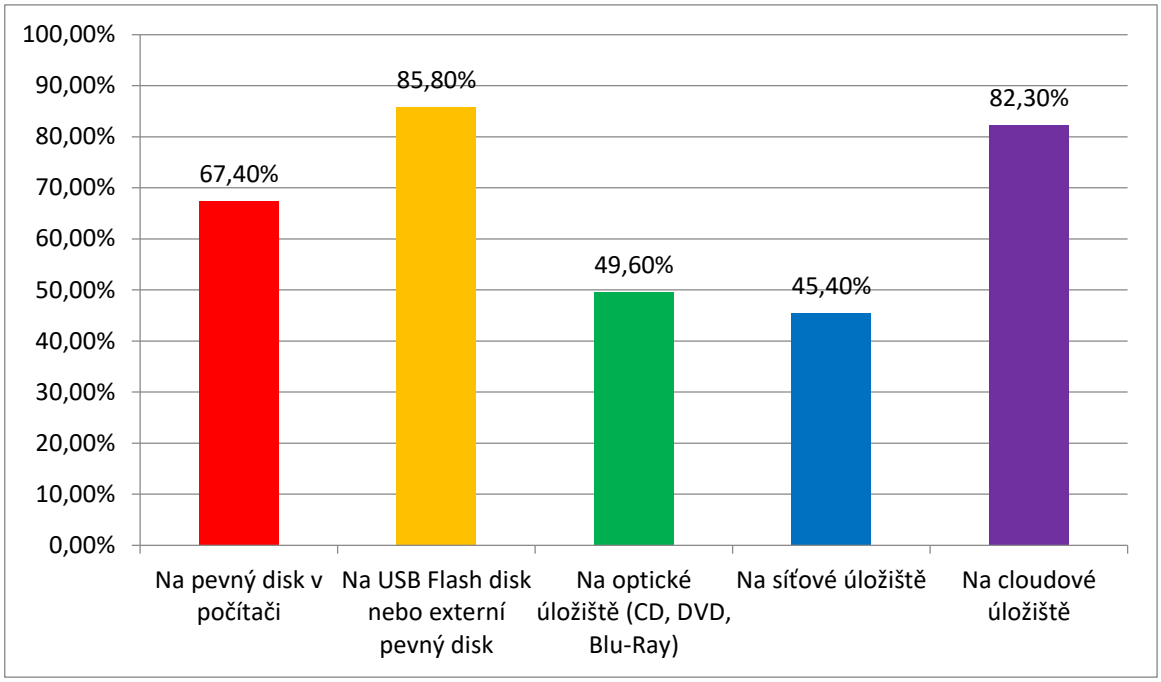
Vyhodnocení 25. otázky: Kam zálohují dotazující? Následný graf 25 ukáže odpověď.



Graf 25 – Místo kam zálohovat (vlastní)

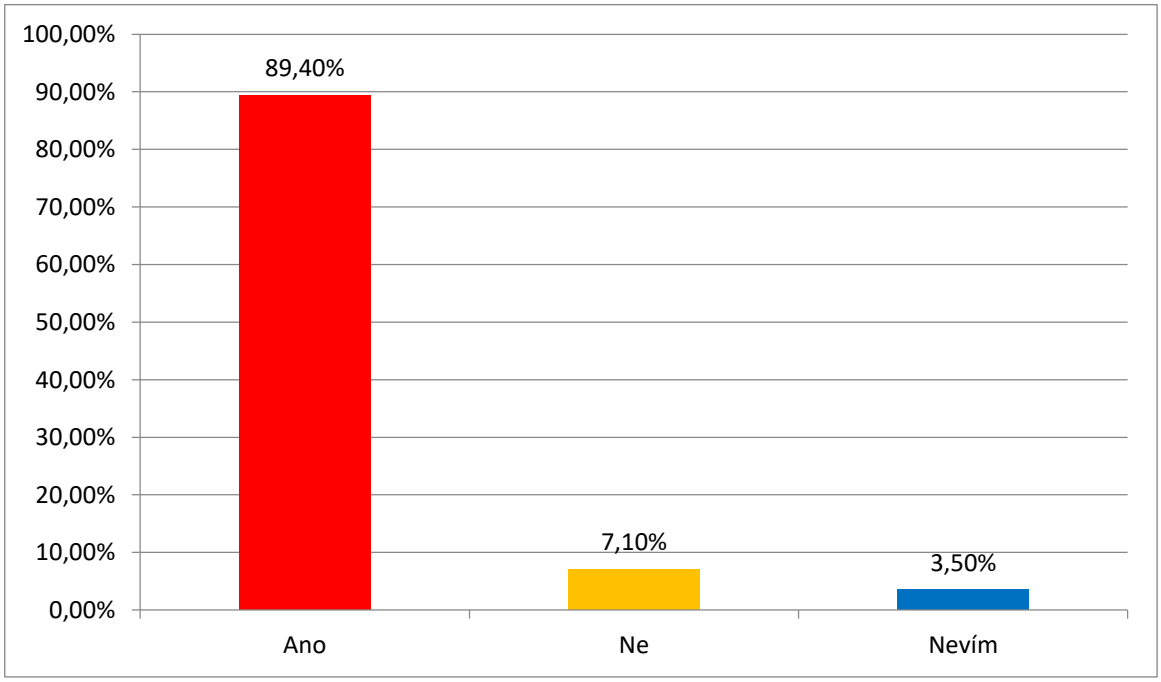
Zde byl možný výběr více odpovědí. Z výsledných odpovědí lze zpozorovat, že nejvíce respondentů zálohuje data na přenosné úložiště a to v počtu 77 odpovědí. Na druhém místě je cloudové úložiště v počtu 57, na pevný disk zálohuje 21 respondentů, na síťové 9 a na optické úložiště 1.

Vyhodnocení 26. otázky: Tato otázka navazuje na předchozí v tom smyslu, že se dotazuje na to, jaké způsoby zálohování dotazovaný zná. Byl možný výběr více odpovědí. Na prvním místě se 121 odpověďmi skončili přenosná úložiště. Následně vybralo 116 respondentů cloudové úložiště. Pevný disk vybralo 95 lidí, 70 optické úložiště a 64 síťové úložiště.



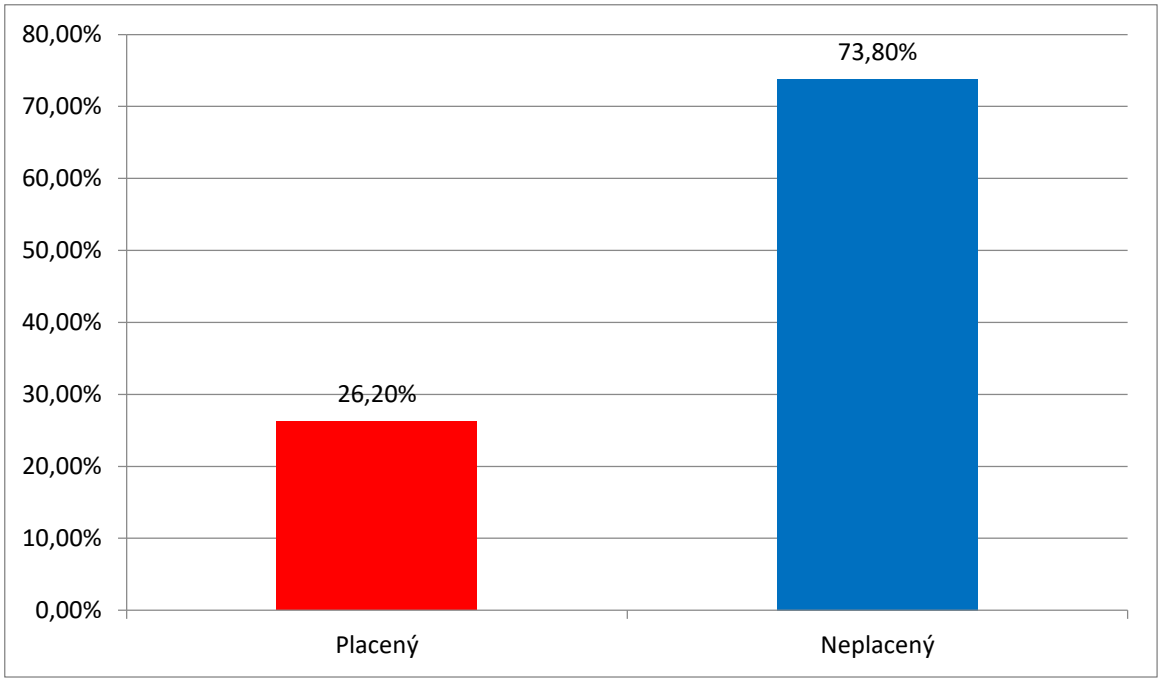
Graf 26 – Známé způsoby zálohování (vlastní)

Vyhodnocení 27. otázky: *„Máte v počítači nainstalovaný anti-malware/antivir?“* Výsledek je takový, že 126 respondentů vybralo *„Ano“*, ti byli následně přesměrování na 28. otázku. 10 dotazujících anti-malware nemá, ty dotazník posunul na 29. otázku a pět, kterých neví, jestli ho má nainstalovaný šli až na otázku 30.



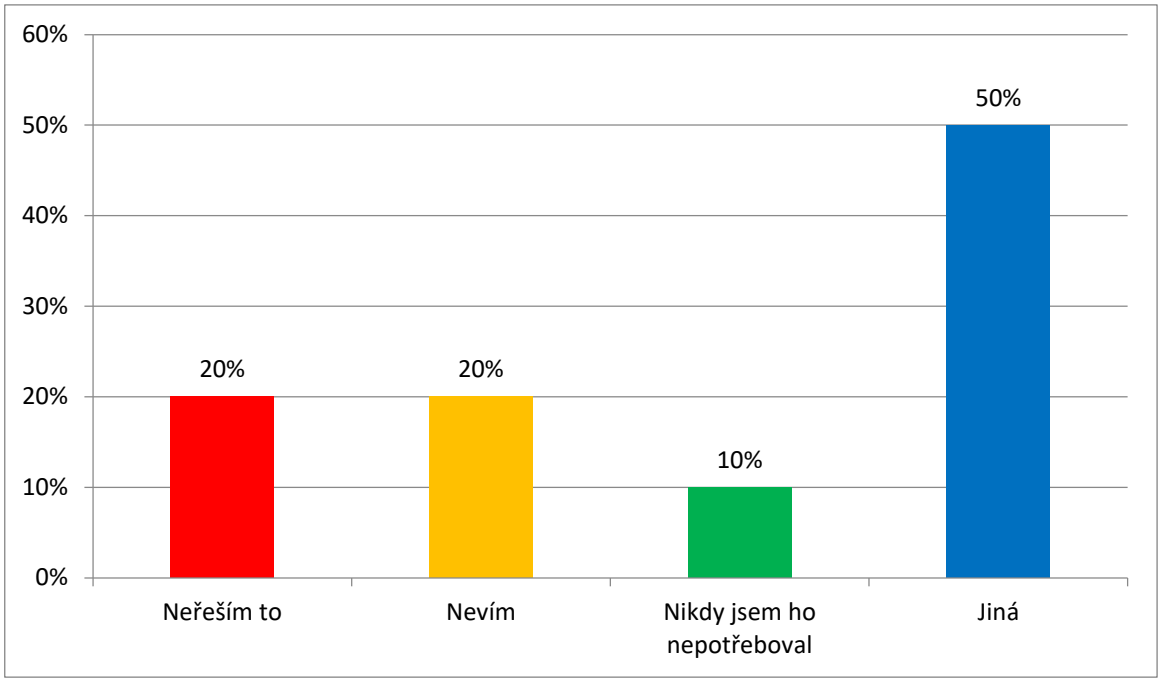
Graf 27 – Nainstalovaný anti-malware (vlastní)

Vyhodnocení 28. otázky: Ti, kteří odpověděli, že mají nainstalovaný anti-malware, vybírali, zda se jedná o placenou či neplacenou verzi. V převážné většině (tedy 93 odpovědí) to byl neplacený, jen 33 respondentů si platí anti-malware. Z této otázky byli dále přesměrování na 31. otázku.



Graf 28 – Verze anti-malwaru (vlastní)

Vyhodnocení 29. otázky: Respondenti, kteří nemají anti-malware měli uvést důvod, proč tomu tak je. Výsledek nám ukazuje graf 29.

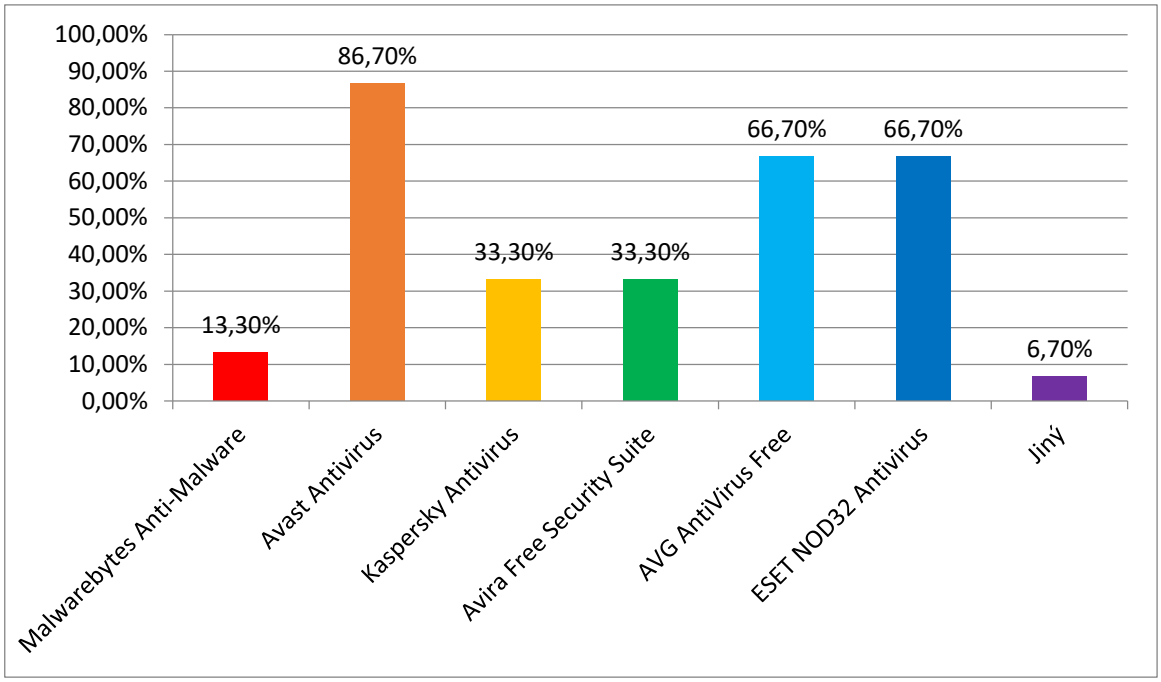


Graf 29 – Důvod nenainstalování anti-malwaru (vlastní)

„Neřeším to“ a *„Nevím“* vybralo po dvou respondentech a jeden vybral *„Nikdy jsem ho nepotřeboval“*. Odpověď „Jiná“ vybralo 5 respondentů, zde jsou uvedeny jejich důvody:

- „Pro OS iOS se nedoporučují antiviry, protože sám o sobě je to uzavřený systém.“
- „Nemusím ho instalovat.“ – iOS nebo Microsoft již mají přímo zabudovanou ochranu, nejspíš proto respondent uvedl tuto odpověď.
- „Dělám ho on-line na internetu.“
- „Různé odborné práce ukazují, že při správném užívání počítače může antivirus napáchat víc škod než užitku. Uživateli, který nestahuje z neoficiálních“ – zde respondent využil při odpovědi plnou kapacitu znaků, proto je odpověď zdá se neúplná.
- „Blokuje některé cracky.“

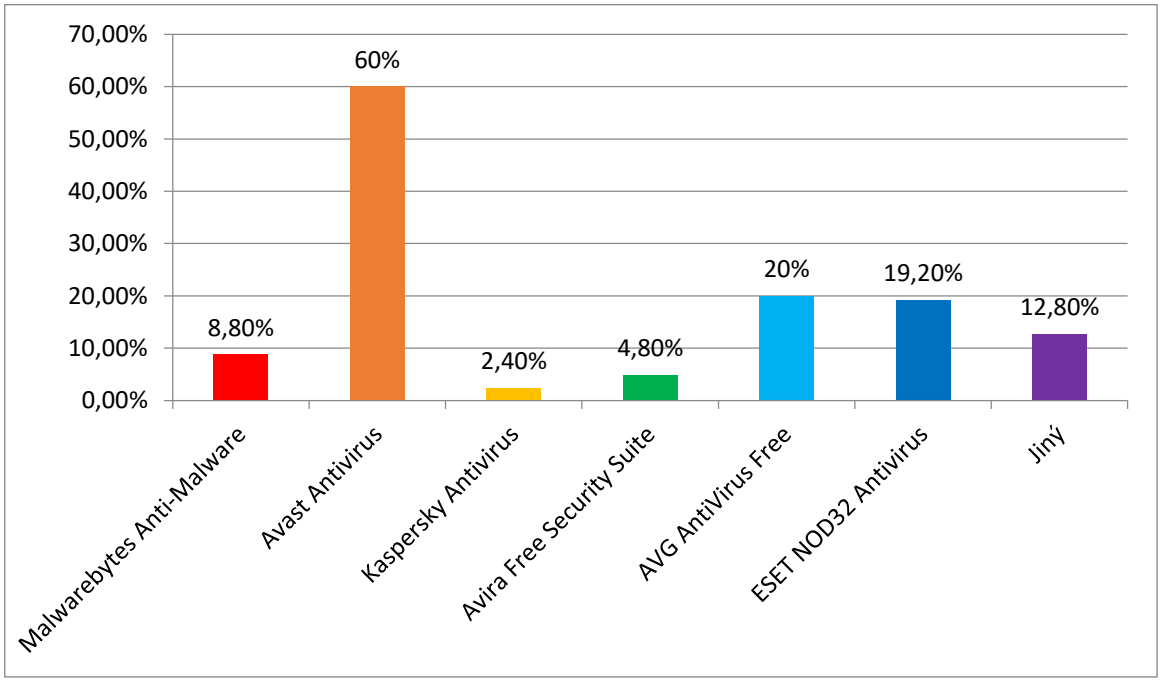
Vyhodnocení 30. otázky: Tato otázka byla určena těm respondentům, kteří odpověděli v otázce č. 27 *„Ne“* nebo *„Nevím“*. Respondenti také mohli vybrat více odpovědí. Otázka se ptala na to, které anti-malwary zná dotazující. Nejvíce hlasů má Avast Antivirus, pro který hlasovalo 13 lidí. Po deseti odpovědích mají AVG AntiVirus Free a ESET NOD32 Antivirus. Pět respondentů vybralo Kaspersky a Aviru, Malwarebytes se dvěma hlasy a jeden respondent zvolil *„Jiný“*, kde uvedl McAfee.



Graf 30 – Známé anti-malwary (vlastní)

Od 30. otázky byli dotazující přesměrování na otázku č. 32.

Vyhodnocení 31. otázky: Tato otázka byla zacílena na ty, kteří mají anti-malware a ptá se jich, jaký používají. Dotazovaný mohl vybrat více odpovědí, protože nemusí mít jen jeden počítač a může na každém používat jiný program. Graf 31 zobrazuje výsledek.

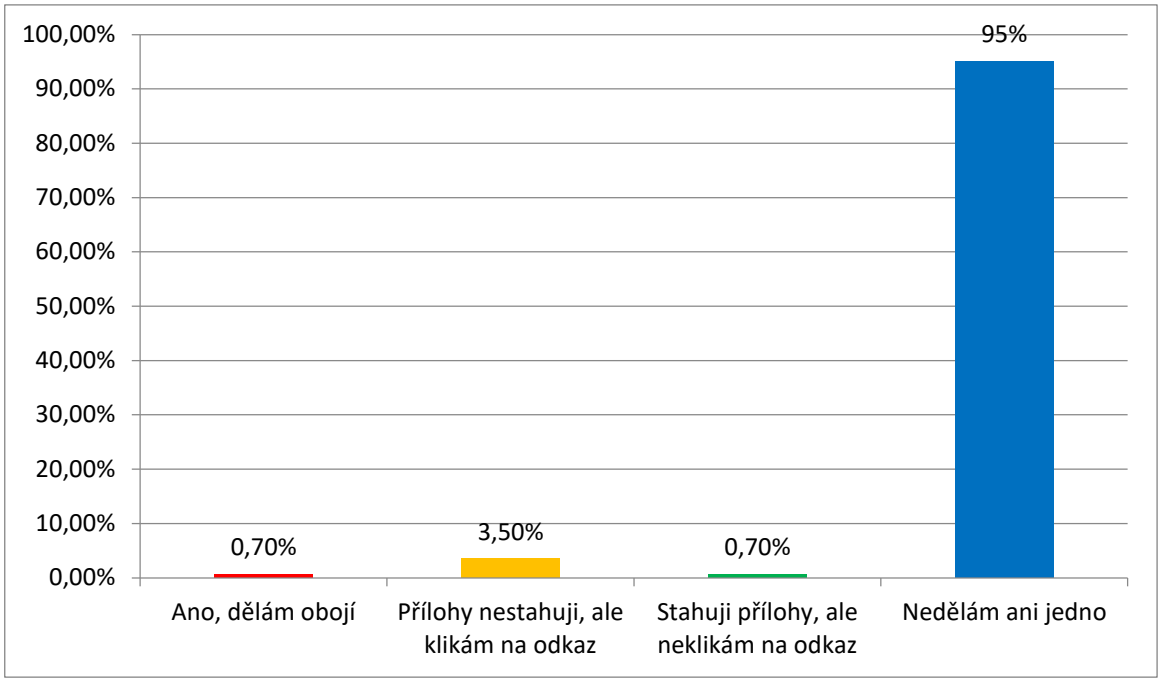


Graf 31 – Užívané anti-malwary (vlastní)

Nejvíce respondentů používá Avast Antivirus a to v počtu 75. Další programy dopadly následovně:

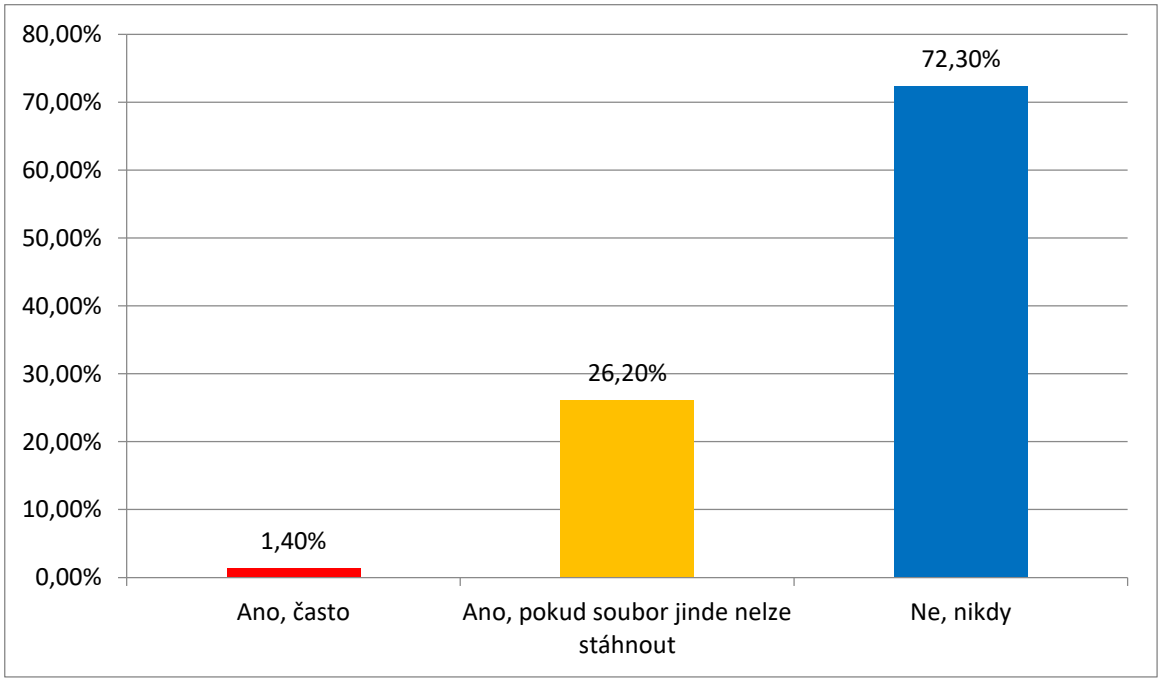
- Malwarebytes Anti-Malware – 11×.
- Kaspersky Antivirus – 3×.
- Avira Free Security Suite – 6×.
- AVG AntiVirus Free – 25×.
- ESET NOD32 Antivirus – 24×.
- Jiný – 16×, a to:
    - 7× Microsoft Defender.
    - 1× Norton 360.
    - 1× Adaware.
    - 1× *„Nevím, využívám firemní počítač“*.
    - 1× F-Secure Client Security Premium.
    - 1× Essentials.
    - 1× *„Nevím“*.
    - 1× *„Nevím, byl v PC při pořízení“*.
    - 1× Palo Alto.
    - 1× Bitdefender.

Vyhodnocení 32. otázky: *„Stahujete neznámé přílohy nebo klikáte na uvedené odkazy, když Vám přijde neznámý email?“* Velice důležité téma, které i přes to, že bývají lidé informování o tomto problému, i tak se to objevuje. 134 respondentů ovšem bezpečně odpovědělo, že nedělá ani jedno, což je správný přístup. Pět odpovědělo, že přílohy nestahuje, ale kliká na odkazy a po jednom respondentovi stahuje přílohy a dělá obojí.



Graf 32 – Stahování neznámých příloh či otevírání odkazů (vlastní)

Vyhodnocení 33. otázky: Poslední otázka byla zaměřena na téma stahování souborů z neznámých a podezřelých webových stránek. Zde odpovědělo 102 dotazujících, že nikdy nestahuje, 37 jich stahuje soubor, pouze pokud je nelze jinde stáhnout a 2 se přiznali, že stahují často.



Graf 33 – Stahování souborů z neznámých webových stránek (vlastní)

I přes tyto odpovědi, které vypadají dobře a ukazují, že mezi respondenty jsou lidé, kteří ke stahování přistupují bezpečně a vše si kupují, tak realita většinou bývá jiná. Nelze ovšem hned zpochybnit výsledek této otázky, jen je třeba ji brát s rezervou.

Celkové vyhodnocení

Na závěr této kapitoly týkající se dotazníkového šetření bude dobré udělat celkové vyhodnocení výsledků. Vyhodnocení je podle tematických okruhů, ze kterých byly položeny otázky.

1) Zabezpečení počítače

Z průzkumu vyplynulo, že většina respondentů má počítač zabezpečen heslem, což ukazuje na dobrý základ pro bezpečnost dat. V návaznosti na to téměř všichni uvedli, že mají pouze jeden účet v počítači a pokud jich někdo má víc, tak je má všechny zabezpečeny heslem. Při zadávání hesla necelá polovina uvedla, že toto dělá v přítomnosti někoho z rodiny, o něco méně ho zadává tak, aby ho nikdo neviděl a zbytek v jakékoliv situaci. Toto zjištění naznačuje, že při zadávání hesla nebývají mnozí opatrní. U uzamykání počítače jsou respondenti opatrní zejména v nekontrolovaném prostředí, jinak v kontrolovaném uzamykání moc neřeší a doma vůbec.

2) Heslová politika

U heslové politiky se ukázalo, že nejvíce respondentů používá heslo dlouhé 6 až 10 znaků, což ovšem není příliš bezpečné. Nejlepší by bylo mít heslo s 15 a více znaky, ale postačí i 11 a více. V heslu je nejčastěji používána kombinace malých a velkých písmen a čísel, což ukazuje na dobrou úroveň bezpečnosti hesla. Takto bezpečné ale není používání jednoho hesla k více účtům. Toto zjištění je velice alarmující a lidé by neměli používat jedno heslo k více účtům či zařízením. U předmětu správce hesel nebylo nic neobvyklého, že převážná většina nic takového nezná. Při otázce na sociální inženýrství byl předpoklad, že lidé budou odpovídat tak, že by nikomu heslo či jiné citlivé údaje neprozradili, je ale otázkou zda jsou odpovědi zcela pravdivé, protože sociální inženýrství je technikou, která je velmi účinná a stále používaná. Je tedy třeba i přes uvedené výsledky upozornit na opatrnost při komunikaci s cizí osobou, když jde o takto citlivé údaje. Obzvláště když vyplynulo, že heslo u velké skupiny zná i někdo z rodiny.

3) Pokročilé zabezpečení dat v počítači

Toto téma zahrnovalo otázky na šifrování, kde se ukázalo, že polovina dotazujících nemá šifrovaný disk, další velká skupina neví, jestli má šifrovaný disk, což ale ve většině případů nejspíše nebude, protože při obyčejném používání počítače nebývá disk šifrovaný, pouhých několik jedinců má šifrovaný disk. I v další otázce se ukázalo, že až na pár výjimek nikdo data nešifruje. Proto i většinu šifrovacích programů nikdo nezná. U zálohování dat je to však zcela jiné. Téměř všichni uvedli, že data zálohují. Tento výsledek je dobrý bezpečnost informací, ale zjištění za jak dlouhou dobu to je není příliš povzbudivé. V únosných mezích normálního uživatele je dobré zálohovat jednou týdně až jednou měsíčně. A místem kam zálohovat je především přenosné úložiště a cloudové úložiště, což je dobrá volba.

4) Malware a zabezpečení

Proti malwaru je nutné mít nainstalovaný anti-malware neboli antivir v laické řeči. Ten mají téměř všichni respondenti. Ve většině jde o neplacenou verzi. Nejvíce oblíbený je Avast Antivirus, dále AVG AntiVirus Free a ESET NOD32 Antivirus. Případně software již nainstalovaný v počítači. Zjištění že anti-malware používají téměř všichni je uspokojivé a ukazuje na v dnešní době již nutnost toto mít.

5) Email a stahované soubory

Neznámé emaily chodí snad každému a mohou skrývat odkazy na podvodné stránky nebo přílohy nakažené malwarem. Skoro všichni odpověděli, že neotevírají odkazy ani nestahují přílohy, našlo se však několik jedinců, kteří buď jedno, nebo druhé dělají. Přesněji 7 respondentů by mělo být více opatrných. A poslední otázka směřovala na stahování souborů z neznámých webových stránek. Očekávalo se, že všichni vyberou možnost, že nikdy nestahují z neznámých webových stránek, ale nakonec se pár respondentů nebálo a šlo o 39 lidí, kteří se tímto přiznali. Ale z běžného života lze říci, že pravda bude taková, že takto stahuje většina uživatelů, jen se tím nechtějí chlubit. Navíc to obnáší nebezpečí nákazy počítače malwarem, který může být na stránkách nebo součást stahovaného souboru.

6 OCHRANY PROTI ÚTOKŮM NA OSOBNÍ POČÍTAČ

Tato kapitola navazuje na výsledky dotazníkového šetření, které ukázaly, v čem dělají lidé největší chyby při běžném používání počítače, čímž vystavují svá cenná data nebezpečí poškození či krádeže. Jsou zde navržená opatření pro zvýšení bezpečnosti informací. Mezi tato opatření byla vybrána šifrování, zálohování dat, nastavení silného hesla a používání anti-malwaru.

6.1 Šifrování a šifrovací nástroje

Šifrovacích nástrojů je na výběr mnoho a k velkému štěstí je jich i mnoho zdarma. Každý program také slouží k něčemu jinému. Může to být šifrování disku, oddílu nebo jen souboru. Další programy mohou šifrovat dokumenty typu PDF či Excel. Některé umí dokonce šifrovat vytvořené webové stránky. Zkrátka programů pro šifrování je nepřeberné množství a každý uživatel si může vybrat ten, který se mu bude zamlouvat nejvíce. Je mnoho kritérií podle, který si může každý uživatel vybrat.

Nejprve jsou programy, které jsou podle elektronického časopisu PCMag vyhlášeny jako *„The Best Encryption Software for 2021“*, tedy nejlepší šifrovací software pro rok 2021.

AxCrypt Premium (1. místo)

Opět jde o placenou verzi, která má ovšem oproti neplacené více funkcí. AxCrypt používá šifrování AES-256, což je americký federální standart. Program šifruje především soubory a složky. Jeho další funkce jsou správa hesel, generátor hesel, sdílený klíč (pokud by uživatel chtěl soubor někomu přeposlat) a zálohování na cloud. Program je určen jak pro OS Windows (Vista, 2008, 7, 8, 10), OS X, Android a iOS. Cena tohoto programu je přibližně 95,00 Kč za měsíc, přičemž je první měsíc zdarma. (AxCrypt Premium, c2021)

Folder Lock (2. místo)

Folder Lock má mnoho funkcí jako zamykání a skartování složek, zamykání a šifrování souborů, USB Flash Disků, CD a DVD, případně šifrování e-mailových příloh. Ještě má jednu funkci, která je velmi zajímavá a to je možnost vytvoření virtuální peněženky, do které si může uživatel ukládat např. adresy, bankovní údaje a lze také data zálohovat do cloudu. Folder Lock má mnoho funkcí, ale je to za cenu toho, že je placený. Pořizovací cena je 30,79 USD. Program je v angličtině, jako většina a funguje na OS Windows (XP, Vista, 7, 8, 10) a iOS. (Folder Lock, © 1997-2021)

InterCrypto Advanced Encryption Package 3 (3. místo)

Další program pro šifrování souborů a textů. Lze si vybrat z více šifer, podle preferencí uživatele. Je velmi jednoduchý pro používání, bezpečně maže data, lze použít USB Flash Disk pro uložení šifrovacích klíčů. Výhodou je i šifrování e-mailových příloh tzv. šifrovaného samorozbalovacího souboru, kdy druhá strana nepotřebuje žádný software. Pro OS Windows (7, 8, 10). Zdarma je na 30 dní jinak stojí 49,95 USD. (Encryption Software…, c2014-1998)

Ranquel Technologies CryptoForge (4. místo)

Program CryptoForge šifruje soubory a složky. Největší možná velikost na svazcích NTFS (souborový systém) je 16 TB. Pokud se zašifrovaný soubor posílá, druhá strana jen použije aplikaci, která je zdarma, aby soubor dešifrovala. Taktéž používá šifru AES a umožňuje bezpečnou skartaci souborů (překračuje specifikace amerického ministerstva obrany). Program nemá žádná „zadní vrátka“, proto pokud uživatel zapomene heslo, už se nedostane k souborům. Program šifruje i názvy souborů. CryptoForge pracuje na OS Windows (XP, Vista, 7, 8, 10) a cela plné verze je 39,70 USD. (Encryption Software, © 2001-2021)

NordLocker (5. místo)

Program šifruje soubory za pomoci AES-256, Argon2 či ECC šifer. Vývojáři na svých oficiálních webových stránkách uvádí argumenty, proč nepoužívat cloud (např. možné „hacknutí“ cloudu, důvěra v dobré jednání poskytovatele?, apod.). NordLocker je určen pro OS X a OS Windows pro všechny typy souborů a velikostí. Program lze propojit i s účtem Dropbox a bezpečně sdílet data. Verze zdarma je jen pro 2 GB jinak měsíčně stojí 1 USD. (About NordLocker, © 2021)

Steganos Safe (6. místo)

Německý program pro šifrování souborů v nejnovější verzi Safe 22. Používá jedno z nejmodernějších šifrování tedy AES-XEX. Program vytváří šifrovanou jednotku a maximální bezpečná velikost uváděná vývojáři je 2 TB. Podporuje šifrování v Dropboxu, OneDrive, Google Drive a MagentaCLOUD. Jde o placený program, jehož nynější měsíční cena je 13,99 USD. (Steganos Safe 22, c2021)

InterCrypto CryptoExpert8 (7. místo)

CryptoExpert8 vytváří jednotku o velikosti 10 GB a více. Počet vytvořených jednotek je neomezený. Program má na výběr více šifer, a to BLOWFISH, ČÁST, 3DES nebo AES-256. Je možné mít klíče k odemčení jednotek na USB Flash Disku, kde budou chráněné

jedním heslem. Jako většina pracuje na OS Windows (7, 8, 10) a má bezplatnou 30denní verzi. Plná verze je k dispozici za 59,95 USD. (CryptoExpert 8…, c2016)

Cypherix Cryptainer PE (8. místo)

Na rozdíl od SecureIT je tento program zaměřen na vytváření kontejnerů (jednotek) o velikosti 32 GB. Používá 448bitové šifrování, což je vysoce bezpečné. Nefunguje jen na počítači, ale lze s ním také šifrovat soubory na USB Flash Disku, CD či DVD. Opět funkční na OS Windows (XP, Vista, 7, 8, 10). K vyzkoušení je zdarma na 30 dní, placená verze stojí 45 USD. (Cryptainer PE, © 1999-2021)

Cypherix SecureIT (9. místo)

Následující dva programy jsou od firmy Cypherix. Hlavní funkce tohoto programu jsou šifrování souborů, složek, komprese souborů a skartace. Stejně jako předešlý CryptoForge nemá „zadní vrátka“. Umí vytvořit také samorozbalovací šifrované soubory. Opět určené pro OS Windows (XP, Vista, 7, 8, 10). Opět zdarma na 30 dní, nebo ke koupi za 29,95 USD. (Secure IT, © 1999-2021)

Dále jsou popsané ty nejznámější programy určené k šifrování dat, které nebyly zařazeny do předešlého výběru. Jsou to zejména programy, které jsou dlouhodobě vysoce užívané pro jejich dobré vlastnosti a uživatelsky příjemné prostředí. Navíc je většina z nich k dispozici zcela zdarma.

DiskCryptor

Program, který šifruje oddíly. Dokáže šifrovat všechny diskové oddíly včetně systémového. Jelikož se jedná o open source program (program s otevřeným zdrojovým kódem), tak se nedoporučuje k šifrování opravdu důvěrných dat. Program podporuje šifrování AES-256, Twofish a Serpent. Lze použít i dva algoritmy dohromady pro případ, že by byl jeden narušen. Program zvládne šifrovat také přenosná média jako USB Flash Disk, CD a DVD. A je zcela zdarma. (DiskCryptor, © 2021)

TrueCrypt

Jeden z úplně nejznámějších programů určených k šifrování dat je TrueCrypt. Naneštěstí již od roku 2014 vývojáři ukončily činnost. Od té doby není bezpečné TrueCrypt používat. Program byl určen k šifrování celých oddílů nebo jen souborů. Měl na výběr více šifrovacích algoritmů jako AES, Twofish,…. Program sice lze pořád stáhnout, ale na oficiálních stránkách http://truecrypt.sourceforge.net/ mají uvedené varování: *„WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues“*. Používání již

není bezpečné, a proto by ho neměl už nikdo používat, ale na druhou stranu je řada programů, které stojí na TrueCryptu, jako třeba doporučený VeraCrypt. (Zima, 2011)
A naposled jsou uvedeny šifrovací nástroje, které bývají zabudované přímo v OS. Jsou zde uvedeny tři nástroje a každý je z jiného OS. Figurují zde tedy Windows, OS X a Linux.

BitLocker (Windows)

BitLocker je nástroj OS Windows. Nyní je dostupný ve verzi Windows 10, ale výjimkou je edice Windows 10 Home. BitLocker dokáže šifrovat soubory, ale také jednotky. Lze u něj také nastavit PIN, pokud nějaký uživatel má zašifrovanou nějakou jednotku. PIN poté musí uživatel zadat při spouštění systému. Místo PINu lze využít USB Flash Disk, na kterém bude klíč k odemčení, ale je třeba ji vždy připojit při spouštění. Optimální je podle Microsoft kombinace BitLockeru s modulem Trusted Platform Module (TPM) ve verzi 1.2 a novější. Dohromady dokáží zajistit bezpečí pro data, i když je počítač vypnut. Nástroj BitLocker je zdarma a je jedním z nejznámějších šifrovacích nástrojů. (BitLocker, 2018)

FileVault (OS X)

FileVault je šifrovací nástroj zabudovaný v každém Macu. Slouží k šifrování svazků a vyměnitelných úložných zařízení. Používá šifrování XTS-AES-128. Klíč se uloží na iCloud. Pokud je FileVault zapnutý musí uživatel zadat při spouštění přihlašovací údaje nebo klíč. Bez těchto údajů se nelze k datům dostat, a to i když je disk připojen k jinému počítači. (Šifrování startovacího disku Macu pomocí FileVaultu, © 2021)

Ccrypt (Linux)

Tento nástroj je téměř v každé verzi Linuxu. Ve výchozí instalační verzi se pracuje v příkazovém řádku. Lze s ním zašifrovat text, soubory či celý disk. (Rippl, 2013)

6.1.1 Doporučení pro uživatele

Šifrovacích nástrojů je mnoho a mnohé jsou zdarma, což je velmi výhodné pro běžného uživatele, který chce zabezpečit svá data, ale nechce utrácet peníze. V úvahu se braly pouze programy, které jsou k dispozici zdarma, protože běžný uživatel většinou nechce utrácet peníze za jakýkoliv software. V tomto případě je doporučení velmi složité. I přese všechny programy, které jsou uvedeny výše, je logické pro běžné uživatele doporučit šifrovací nástroje, které jsou již zabudované v OS. To znamená, že pro uživatele Microsoft Windows 10 je doporučeno používat BitLocker. Majitelům Apple zařízení je doporučeno používat integrovaný software FileVault. Apple si zakládá na propojení všech zařízení a

sám právě nabízí uživatelům své řešení různých problémů a je tudíž zbytečné hledat něco jiného než to, co samotná firma nabízí většinou zcela zdarma.

Autor by doporučil šifrovací software VeraCrypt. Má mnoho výhod i přesto, že není integrovaný v OS. Dalším důvodem, proč lze software doporučit je to, že někteří uživatelé nemusí mít verzi Microsoft Windows, která obsahuje BitLocker. V tabulce níže jsou uvedeny výhody a nevýhody, které vedli autora k doporučení softwaru.

Tabulka 3 – Šifrovací software VeraCrypt (vlastní)

VeraCrypt	
Výhody	**Nevýhody**
Šifrování složek, oddílu, celého disku nebo připojeného přenosného zařízení.	Pouze anglický jazyk.
Možnost přenosné verze softwaru.	Není integrovaný jako BitLocker či FileVault.
Přehlednost a uživatelská přívětivost.	
Bezpečnost – možnost výběru z mnoha šifrovacích a hashovacích algoritmů.	
Program je zdarma.	

VeraCrypt - návod

Program je určen k šifrování oddílů nebo úložných zařízení jako USB Flash Disků. Má na výběr mnoho šifrovacích algoritmů a uživatel si může vybrat, jak velký zašifrovaný oddíl chce vytvořit. Jedná se o open source program, který funguje na OS Windows, OS X a Linux. Je založený na dříve velmi populárním TrueCryptu, který již není bezpečné používat. (Home, c2021)

Vše začalo výběrem verze. Byla zvolena přenosná, ale program má i verzi, která se nainstaluje na počítač. Program byl po stažení spuštěn a bylo vybráno místo na disku, kam program rozbalit.

Latest Stable Release

For Windows: 1.24-Update6 (Tuesday March 10, 2020)

For FreeBSD, Linux and MacOSX: 1.24-Update4 (Thursday January 23, 2020)

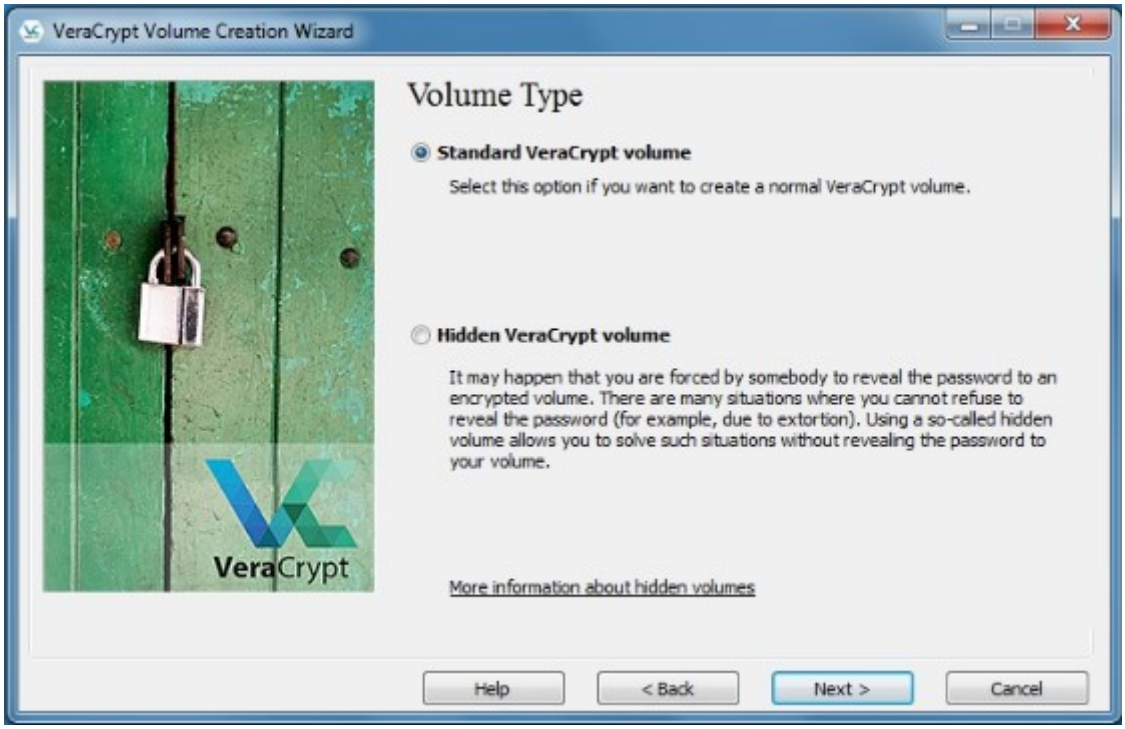
- *Windows*:
  - Installer: VeraCrypt Setup 1.24-Update6.exe (34.5 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.24-Update6.exe (34.3 MB) (PGP Signature)
  - Debugging Symbols: VeraCrypt_1.24-Update6_Windows_Symbols.zip (9.51 MB) (PGP Signature)
- *Mac OS X*:
  - OS X Mavericks 10.9 and later: VeraCrypt_1.24-Update4.dmg (6.23 MB) (PGP Signature)
  - OS X Lion 10.7 and OS X Mountain Lion 10.8: VeraCrypt_Legacy_1.24-Update4.dmg (9.45 MB) (PGP Signature)
  - OSXFUSE 2.6 or later must be installed.
- *Linux*:
  - Generic Installers: veracrypt-1.24-Update4-setup.tar.bz2 (14.5 MB) (PGP Signature)
  - Linux Legacy installer for 32-bit CPU with no SSE2: veracrypt-1.24-Update4-x86-legacy-setup.tar.bz2 (7.19 MB) (PGP Signature)
  - Debian/Ubuntu packages:
    - Debian 9:
      - GUI: veracrypt-1.24-Update4-Debian-9-amd64.deb (PGP Signature)
      - console: veracrypt-console-1.24-Update4-Debian-9-amd64.deb (PGP Signature)

Obr. 8 – Výběr verze programu (Downloads, c2021)

Program byl poté spuštěn a začal se vytvářet svazek (Volume), který bude zašifrovaný. Byla vybrána první možnost, kdy je vytvořen šifrovaný „kontejner“. Možno také vybrat šifrování USB Flash Disku či celého disku.

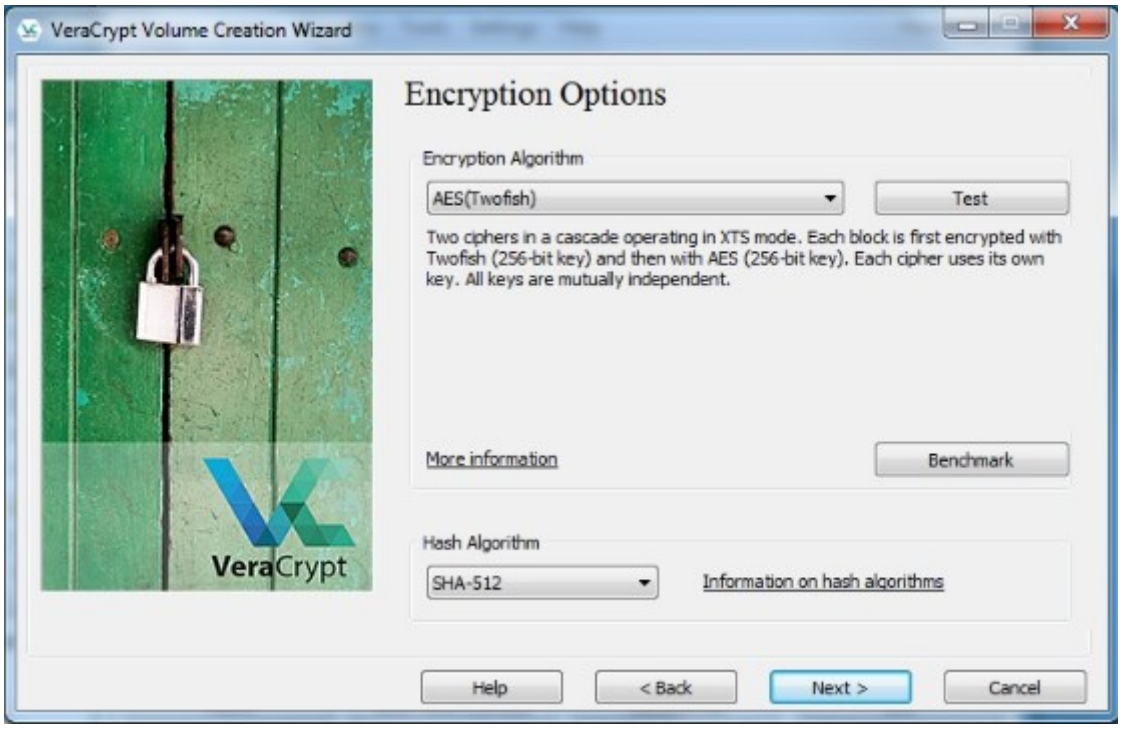
Obr. 9 – Okno s výběrem šifrovaného formátu (vlastní)

Pokračovalo se výběrem standartního svazku.



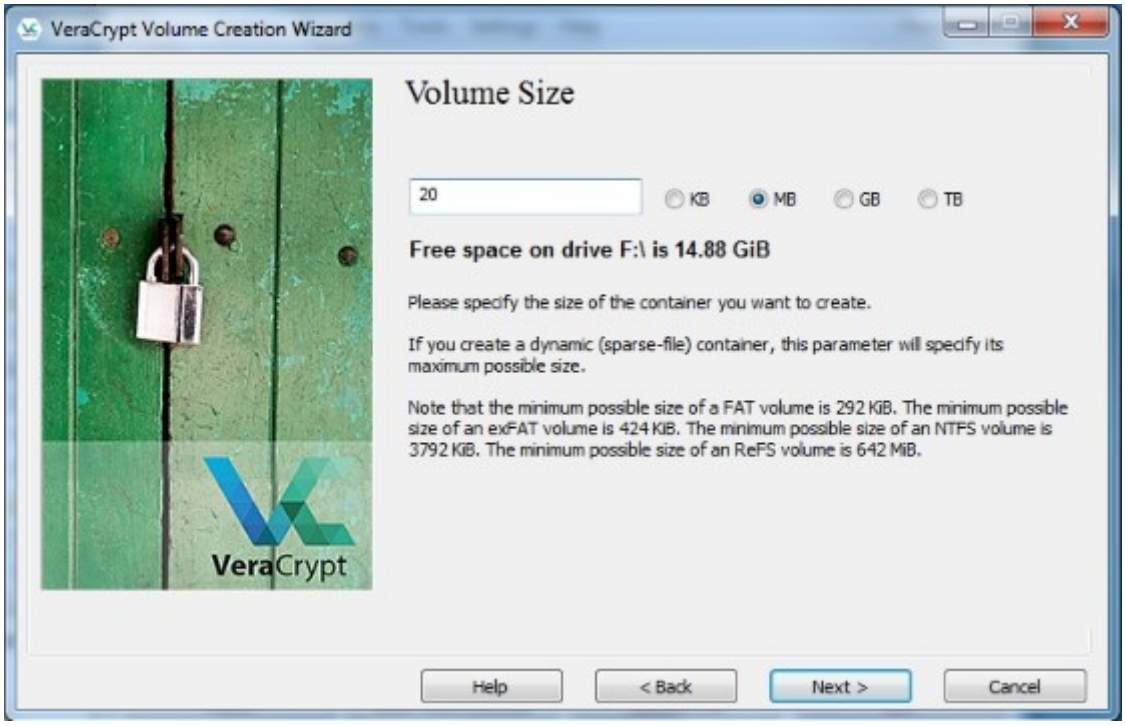
Obr. 10 – Okno s výběrem typu šifrovaného svazku (vlastní)

Dále byla nabídka výběru šifrování. Pro test byl vybrán šifrovací algoritmus AES Twofish. Ovšem je zde celá řada algoritmů na výběr podle preferencí uživatele. Dále byl na výběr také hashovací algoritmus, který byl ponechán jako SHA-512.



Obr. 11 – Okno s možnostmi šifrování (vlastní)

Pro účel testu byl vytvořen „kontejner“ o velikosti 20 MB.

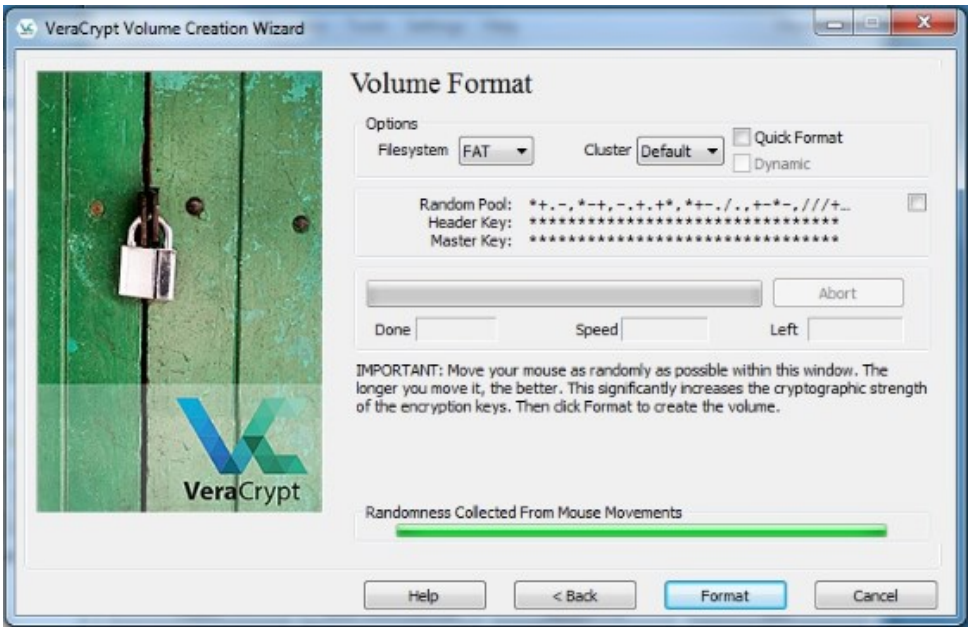


Obr. 12 – Okno, kde se zadávala velikost svazku (vlastní)

Na řadu přišlo i zadání hesla. Na obrázku níže je vidět vyplněné heslo a okénko, které varuje, že aby bylo heslo bezpečné, mělo by mít délku minimálně 20 znaků.

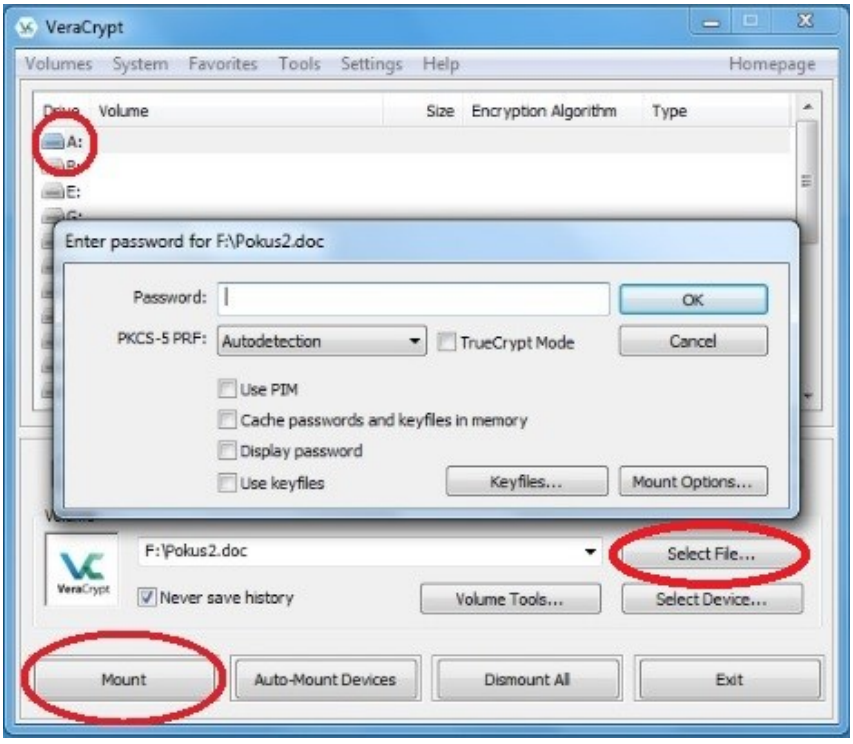
Obr. 13 – Okno s upozorněním, že délka hesla je nedostatečná (vlastní)

Nyní již přišlo na vytvoření „kontejneru“. V tomto kroku bylo možné změnit formátování souborového systému, ale bylo ponecháno FAT, které je nejčastější.



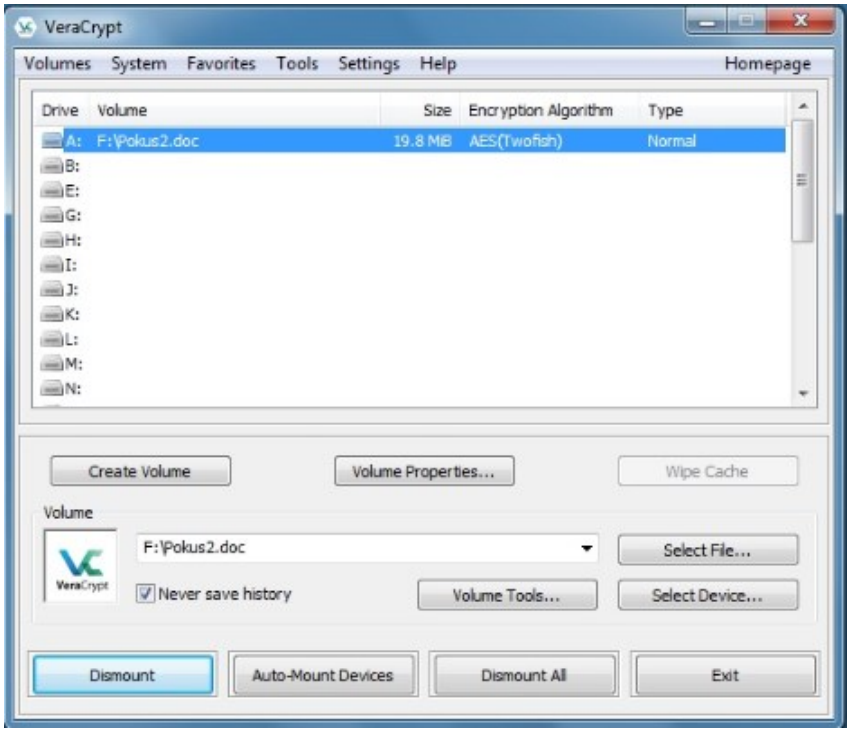
Obr. 14 – Okno, kde se formátoval svazek (vlastní)

V tomto kroku byl již zašifrovaný „kontejner“ spolu s testovacími soubory vytvořen. V kroku, který je vidět na obrázku dole je vidět postup, jak se k zašifrovaným souborům dostat. Nejprve bylo třeba vybrat soubor, poté zvolit jednotku (zde byla zvolena jednotka A) a následně připojit („Mount“). Pak už je stačilo zadat heslo.



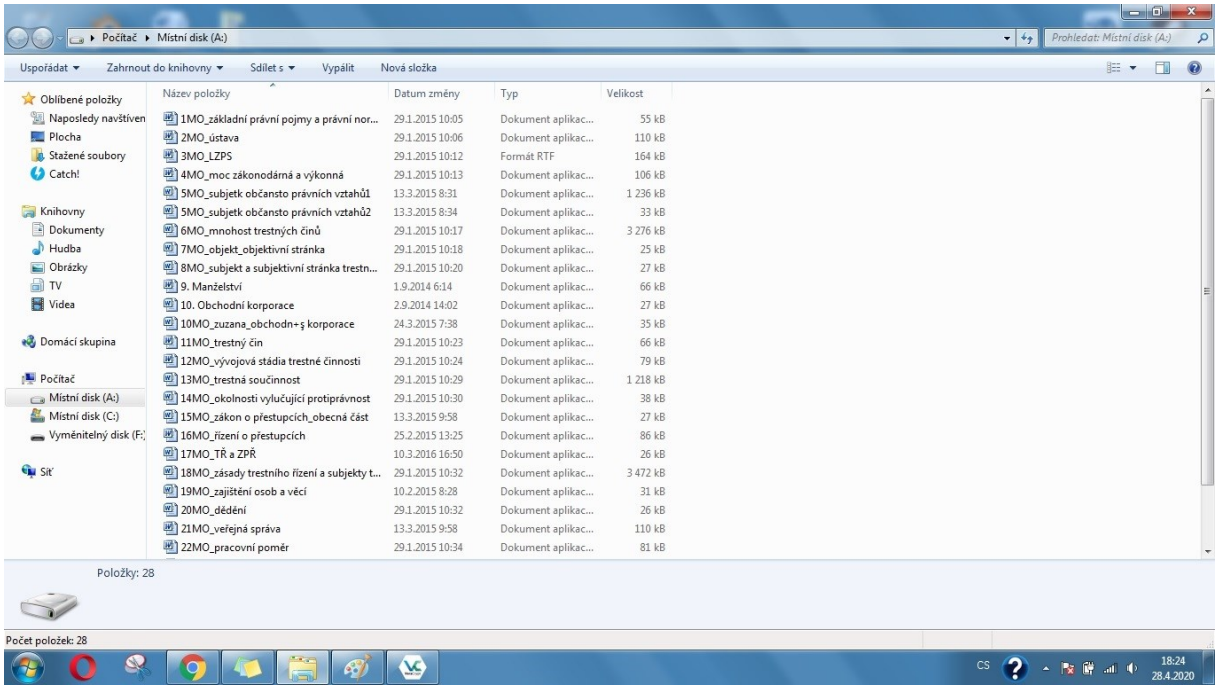
Obr. 15 – Okno s postupem, jak otevřít zašifrovaný svazek (vlastní)

Soubor byl odemknut a dvojklikem byl otevřen.



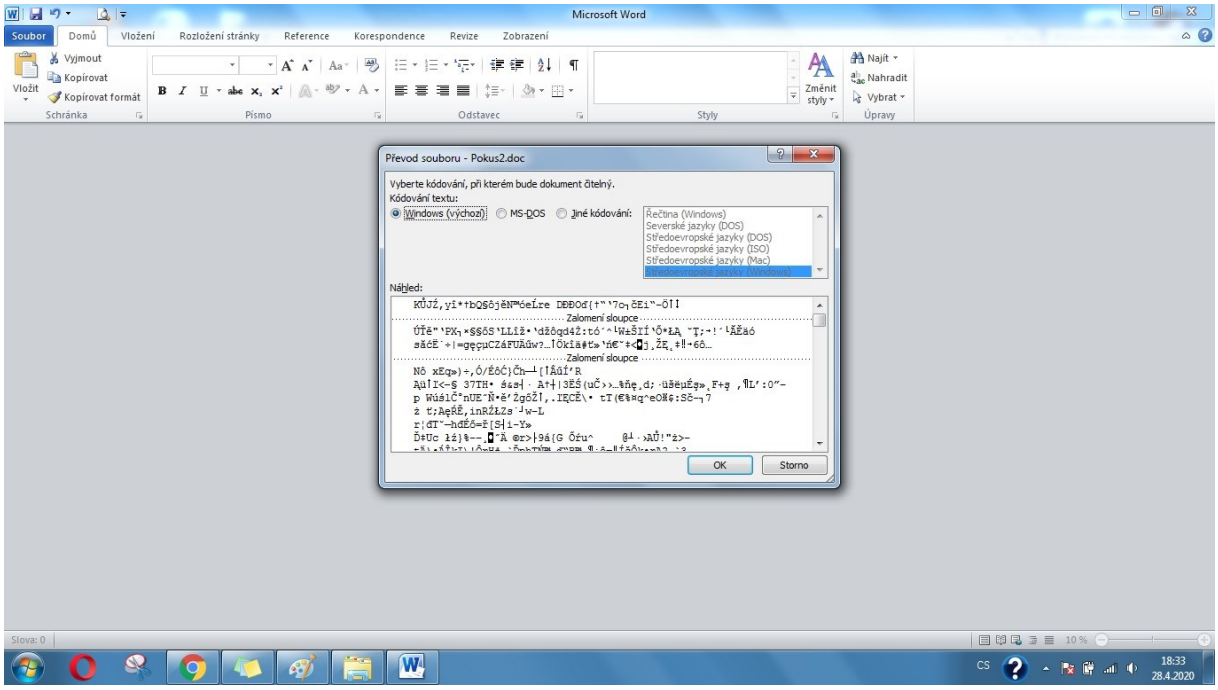
Obr. 16 – Okno s odemknutým svazkem (vlastní)

Zde je možné vidět obsah složky.



Obr. 17 – Obsah svazku (vlastní)

Poslední obrázek ukazuje, co se stane, pokud by se někdo snažil soubor otevřít bez programu VeraCrypt. (Pozn. Otevření v MS Word je proto, že testovací „kontejner“ měl příponu .doc).



Obr. 18 – Podoba svazku, když se otevře bez programu VeraCrypt (vlastní)

Program VeraCrypt je uživatelsky příjemný, ale než uživatel zašifruje soubory, tak to chvíli trvá. Jinak je příjemná možnost zašifrovat i USB Flash Disk nebo celý disk. Zkrátka VeraCrypt nabízí mnoho možností, takže si zde vybere snad každý uživatel. Jediná možná chyba je, že přenosná verze má velikost 55,3 MB, což je trochu víc, ale i tak je to výborný šifrovací program, který je navíc zdarma.

6.2 Zálohování dat

Zálohování dat (anglicky „*Data Backup*“) je v podstatě digitální kopie dat v počítači. Ty jsou uloženy v jiném úložišti či počítačovém systému a v případě ztráty těch originálních je lze velice snadno obnovit. (Drake, 2020)

Zálohovat by se měla důležitá data, jejichž ztráta je nenahraditelná pro majitele nebo by to způsobilo výrazné komplikace pro jeho práci nebo finanční stránku. Zálohovat lze veškerá data od fotek, videa, dokumentů, aplikací, až po smlouvy, výpisy či přístupové údaje. (Zálohování, © 2021)

Zálohování může probíhat na:

- Cloudové úložiště.

- Pevný disk (interní, externí).
- USB flash disk.
- Optické médium (CD, DVD, Blu-ray).
- Síťové úložiště (NAS).

Úložné médium se volí podle toho několika kritérií. Asi nejdůležitější je vědět velikost zálohovaných dat. Protože optická média mají oproti ostatním variantám velmi omezenou velikost, navíc se tak často už nepoužívají. Dalším důležitým faktorem je jak často se bude zálohovat. Dále je dobré mít na mysli, jak dlouho má smysl zálohovaná data přechovávat. Zda je například užitečné mít zálohovaná data stará 5 let a více. A v neposlední řadě jak moc je obsah dat důvěrný. (Zálohování, © 2021)

Cloudová úložiště

Pro zálohování je cloudové úložiště velice dobrou volbou. Není třeba mít doma další hardware, čímž lze ušetřit místo u počítače, lze se k němu dostat odkudkoliv s připojením k Internetu a má i další výhody. Co se týče bezpečnosti, tak dnes již většina provozovatelů cloudových úložišť garantuje bezpečné uložení dat, některé navíc používají šifrovanou komunikaci, která zajišťuje, že při ukládání dat na cloud je nemůže nikdo *„zvenčí“* přečíst. Níže jsou uvedena některá cloudová úložiště, která jsou nejpoužívanější a nejznámější.

Tabulka 4 – Výhody a nevýhody cloudu (vlastní)

Cloudové úložiště	
Výhody	**Nevýhody**
Přístup odkudkoliv s připojením k Internetu.	Přístup pouze online.
Velikost lze přizpůsobit potřebám uživatele.	Měsíční pronájem úložného místa.
Šifrování souborů.	

OneDrive je cloudové úložiště, které provozuje firma Microsoft a bývá již součástí OS Microsoft Windows 10. Zdarma je 5 GB a za každý další GB je cena 1 – 0,05Kč podle toho, jak velké úložiště chcete. Menší slabinou je to, že soubory nelze šifrovat, to tato služba nenabízí. Lze zde uložit soubor o maximální velikosti 15 GB, což je také nevýhoda, ale jinak je to ideální řešení pro někoho, kdo chce mít ke cloudu přístup přímo z plochy počítače a využívá případně další produkty od Microsoftu. (Nejlepší cloudové úložiště 2021, © 2016 - 2021)

Doporučení pro uživatele: OneDrive je určen zejména pro uživatele OS Microsoft Windows 10. Právě díky jeho zabudování v OS je použití velice jednoduché. Tento cloud je také určen těm, kteří používají produkty Microsoft 365, protože je součástí balíčku těchto produktů. Jediný důvod, proč si nevybrat tento cloud je to, že nenabízí šifrování souborů.

Google Disk je také velmi populární a známá služba od firmy Google, jež je součástí Google účtu a nabízí zdarma 15 GB prostoru s možností šifrování souborů. Nevýhodami je maximální velikost souboru, což je 5 GB. Toto je již docela velká nevýhoda, protože například filmy a jiná další média dnes již zabírají větší místo. Zde si lze za větší úložný prostor připlatit 0,60 – 0,30 Kč za 1 GB. Toto řešení je ideální pro většinu uživatelů, protože dnes již každý má Google účet a může této služby využít. (Nejlepší cloudové úložiště 2021, © 2016 - 2021)

Doporučení pro uživatele: Google Disk je dobrou volbou pro všechny uživatele, kteří používají Google účet. Šifrování souborů je výhodou. Co může odradit od pořízení je limit velikosti ukládaného souboru 5 GB.

iCloud je také nepřehlédnutelný, protože je součástí mikroklima iOS a MacOS. Apple staví zejména na propojení všech jejich zařízení a iCloud je téměř jistou volbou pro uživatele jakéhokoliv zařízení od Applu. Zdarma je k dispozici 5 GB a nabízí i šifrování souborů. Maximální velikost ukládaného souboru je bez limitu a při navýšení velikosti je měsíční cena za 1 GB 0,50 Kč. (Nejlepší cloudové úložiště 2021, © 2016 - 2021)

Doporučení pro uživatele: iCloud je jasná volba pro každého s Apple zařízením, jelikož je stejně jako OneDrive pro Microsoft integrovaný přímo v systému. Zahrnuje také šifrování a sdílení souborů. I když je pro zařízení Apple, tak se může používan i na jiných OS.

DropBox je dalším velkým hráčem v oblasti cloudu. I když jde o službu mimo provozovatele OS, tak nabízí aplikaci pro lepší přístup k souborům a zdarma jsou 2 GB a s bonusy to může být až 20 GB. Disponuje také šifrováním souborů. Cena 0,16 Kč za GB je jedna z nejnižších a bez limitní velikost ukládaných souborů je také výhodou. DropBox je tedy velmi zajímavou variantou a nabízí se otázka, jaká je nevýhoda. Snad jen webové stránky bez možnosti českého jazyka. (Nejlepší cloudové úložiště 2021, © 2016 - 2021)

Doporučení pro uživatele: DropBox je zajímavou volbou pro ty, kteří chtějí vyzkoušet něco jiného než výše zmíněné. Cenově je velice výhodný, navíc zahrnuje šifrování souborů, jejich sdílení a možnost obnovení souborů 30 dní zpětně.

Mega je v poslední době velmi využívána a 20 GB volného místa zdarma je další ukázkou, proč je tak oblíbený. Opět splňuje možnost šifrovat soubory a ukládat soubory bez limitu velikosti. Cena za 1 GB měsíčně je od 0,60 Kč a stejně jako u DropBoxu jsou webové stránky v angličtině. (Nejlepší cloudové úložiště 2021, © 2016 - 2021)

Doporučení pro uživatele: Mega je dnes již známé cloudové úložiště, které není pozadu v porovnání s ostatními. Šifrování souborů a jejich sdílení je zde standard. Navíc Mega zaručuje, že při útoku ransomwarem o data napřijdete. Je to tedy zajímavá volba zejména díky bezpečnosti.

Pevní disk

Pevný disk je možnou variantou úložiště pro zálohování dat. V dnešní době je velice jednoduché sehnat harddisk až interní nebo externí a na výběr je z mnoha výrobců, kapacit a dalších vlastností, které mohou harddisky mít. Nejprve je ale třeba si uvědomit, že pro větší bezpečnost zálohovaných dat a jistotu jejich zachování není příliš dobré mít data zálohovaná na stejném počítači, na kterém jsou i originální. Důvodů je hned několik a prvním z nich je samozřejmě napadení počítače malwarem či jiným způsobem, kdy může dojít k jejich zničení či znepřístupnění pro majitele. Dalším důvodem je předcházení rizika při možné technické závadě zařízení nebo poškození zařízení způsobené kolísavým elektrickým proudem (např. při bouřce, zásahu blesku do trafostanice apod.).

Na výběr je interní a externí pevný disk. Pro porovnání jsou níže uvedeny výhody a nevýhody u obou variant.

Tabulka 5 – Rozdíly mezi interním a externím pevným diskem (vlastní)

Interní pevný disk		Externí pevný disk	
Výhody	**Nevýhody**	**Výhody**	**Nevýhody**
Nižší cena.	Nízká bezpečnost.	Připojení a přenosnost.	Vyšší cena.
Zabudování do počítače.	Nižší odolnost, při externím použití.	Vyšší odolnost.	Použité materiály.
Lze použít i jako externí.		Váha.	Bezpečnost.
		Velikost a rychlost	
		Bezpečnost.	

Interní pevný disk

Mezi výhody interních disků patří levnější pořizovací cena. Také to, že je zabudován do počítače, čímž nikde nezavazí a není slyšet. Jasnou výhodou je i to, že ho lze použít jako externí, jen je potřeba mít adaptér, který je zakončen USB konektorem. Nevýhodou je zejména bezpečnost, protože při zapojení v počítači se většinou nakazí všechny disky. A při externím používání má nižší odolnost, protože je vyroben pro interní použití.

Obr. 19 – Interní pevný disk (Interní pevný disk HDD 320GB…, © 2021)

Obr. 20 – Adaptér pro interní pevný disk při externím použití (USB 3.0 - SATA3…, © 2021)

Externí pevný disk

Hlavní výhodou je připojení a přenosnost. Uživatel si jej může vzít kamkoliv a nezabere ani moc místa. Když jde o přenos, tak další nespornou výhodou je vyšší odolnost proti poškození, která je závislá od použitých materiálů. Některé disky z levných materiálů ale nemusí být tak odolné, proto jsou použité materiály také nevýhodou. Externí disky jsou navíc docela lehké a malé. Dnes je navíc rychlost připojení velkou výhodou. A při správném zacházení je to také bezpečnost, což může být i nevýhoda právě při špatném používání. Asi největší nevýhodou je vyšší cena.

Obr. 21 – Externí pevný disk (vlastní)

USB Flash disk

USB Flash disk je oproti pevnému disku omezený kapacitou úložiště, což ovšem nebrání jej využít k zálohování dat. Flash disky jsou ve variantách velikosti úložiště od několika gigabytů (dále jen GB) až do 2 terabytu (dále jen TB).

Výhodou pořízení flash disku je dobrá skladnost, kdy se vleze i do kapsy a člověk jej může mít stále u sebe. Výhodou i nevýhodou je potom kapacita úložiště, která nepojme velké množství dat (např. 5 TB). Ale pokud majitel potřebuje zálohovat jen menší množství dat je to výhoda.

Tabulka 6 – Výhody a nevýhody USB Flash disku (vlastní)

USB Flash disk	
Výhody	**Nevýhody**
Skladnost.	Menší úložný prostor.
Bezpečnost.	Bezpečnost.
Nízká cena.	Nízká odolnost.

Obr. 22 – USB Flash disk (USB flash disk 16GB, © 2010 – 2021)

Optické médium

Optická média jako CD, DVD či Blu-ray se již tak často nepoužívají. Jsou nahrazeny právě nějakou z předchozích variant. Hlavním důvodem je jejich snadné poškození a malá úložná kapacita.

Tabulka 7 – Výhody a nevýhody optických médií (vlastní)

Optické médium	
Výhody	**Nevýhody**
Bezpečnost proti malwaru.	Již zastaralé.
	Nízká odolnost.
	Omezená velikost úložiště.

Obr. 23 – Optická média (Datová média (CD, DVD, Blu-ray), © 2021)

Síťové úložiště (NAS)

NAS neboli Network Attached Storage je datové úložiště, které je s počítačem spojeno přes LAN nebo může být připojen do WiFi routeru, čímž k němu může mít přístup například celá domácnost. Je ideální pro zálohování dat a v dnešní době také pro ukládání mediálních souborů jako jsou filmy, videa, hudba či dokumenty. Jde tedy o dobrou variantu pro zálohování.

Tabulka 8 – Výhody a nevýhody síťového úložiště (vlastní)

Síťové úložiště (NAS)	
Výhody	**Nevýhody**
Může sloužit více zařízením.	Cena.
Velikost.	Další hardware v domě.

Obr. 24 – Síťové úložiště (DiskStation DS220+, © 2021)

6.3 Silné heslo - Autentizace

Tím nejzásadnějším opatřením, které zvýší bezpečnost zašifrovaných dat je zvolit SILNÉ HESLO, které nepůjde tak lehce „prolomit“ vnějším útokem. Může se jednat o brute force útok, slovníkový útok nebo například sociální inženýrství. Každý by tedy měl mít silné heslo, kterým zabezpečí zašifrovaná data, ale silné heslo by nemělo být pouze u takovéhoto zabezpečení dat, ale nejlépe na všech účtech, které člověk má. Nicméně zde jsou uvedena kritéria, která charakterizují silné heslo.

- **Délka hesla** – délka hesla by měla začínat na nejméně 10 znacích, ale úplně nejlepší je 15 a více znaků.
- **Kombinace znaků** – nejlépe je doporučeno použít velká a malá písmena, číslice a speciální znaky, jež bývají v kombinaci velice silné proti prolomení.
- **Nepoužívání běžné náhrady znaku** – dnešní útoky již znají nahrazování znaků, proto je lepší použít náhodné nahrazování (např. BRNOJENEJ – 8RN0J3N3J).
- **Nepoužívat po sobě jdoucí klávesy** - je to stejně nebezpečné jako nahrazování znaků (např. qwerty).

Bezpečné bývá použití fráze či věty, kterou si uživatel pamatuje a nemusí ani obsahovat číslice či zvláštní znaky. Může to být z knihy, filmu nebo seriálu, který má uživatel v oblibě. Jako poslední řešení je generátor hesel, který vygeneruje heslo, ale obyčejný člověk by si ho většinou nezapamatoval. (Empey, 2019)

Obr. 25 – Generované náhodné heslo (Generátor náhodných hesel, © 1988–2021)

Je zde i jiná možnost, a to ta, že pokud uživatel chce mít silné heslo, které si nepamatuje, může za tímto účelem využít správce hesel, do kterého si hesla uloží a bude mu stačit, aby si pamatoval pouze hlavní heslo, kterým se dostane ke všem heslům, které se akorát zkopírují. Tím odpadá zapamatování a uživatel si může vymyslet či vygenerovat opravdu silné heslo, které může vypadat naprosto nesmyslně (příkladně obrázek výše). Je mnoho správců hesel, zde jsou uvedeny pouze některé: KeePass, LastPass, Avast Passwords, 1Password, Dashlane…

Pro představu je zde uvedena tabulka, která zobrazuje časy prolomení při použití různého počtu znaků a různé kombinace.

Tabulka 9 – Časy prolomení různě dlouhých a kombinovaných hesel (upraveno,Mills, 2020)

Počet znaků	**Pouze čísla**	**Malá písmena**	**Malá a velká písmena**	**Čísla, malá a velká písmena**	**Čísla, malá, velká písmena a speciální symboly**
4	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
5	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
6	Okamžitě	Okamžitě	Okamžitě	1 sekunda	5 sekund
7	Okamžitě	Okamžitě	25 sekund	1 minuta	6 minut
8	Okamžitě	5 sekund	22 minut	1 hodina	8 hodin
9	Okamžitě	2 minuty	19 hodin	3 dny	3 týdny

Počet znaků	Pouze čísla	Malá písmena	Malá a velká písmena	Čísla, malá a velká písmena	Čísla, malá, velká písmena a speciální symboly
10	Okamžitě	58 minut	1 měsíc	7 měsíců	5 let
11	2 sekundy	1 den	5 let	41 let	400 let
12	25 sekund	3 týdny	300 let	2 tisíce let	34 tisíc let
13	4 minuty	1 rok	16 tisíc let	100 tisíc let	2 miliony let
14	41 minut	51 let	800 tisíc let	9 milionů let	200 milionů let
15	6 hodin	1 tisíc let	43 milionů let	600 milionů let	15 miliard let
16	2 dny	34 tisíc let	2 miliardy let	37 miliard let	1 bilion let
17	4 týdny	800 tisíc let	100 miliard let	2 biliony let	93 bilionů let
18	9 měsíců	23 milionů let	6 bilionů let	100 bilionů let	9 biliard let

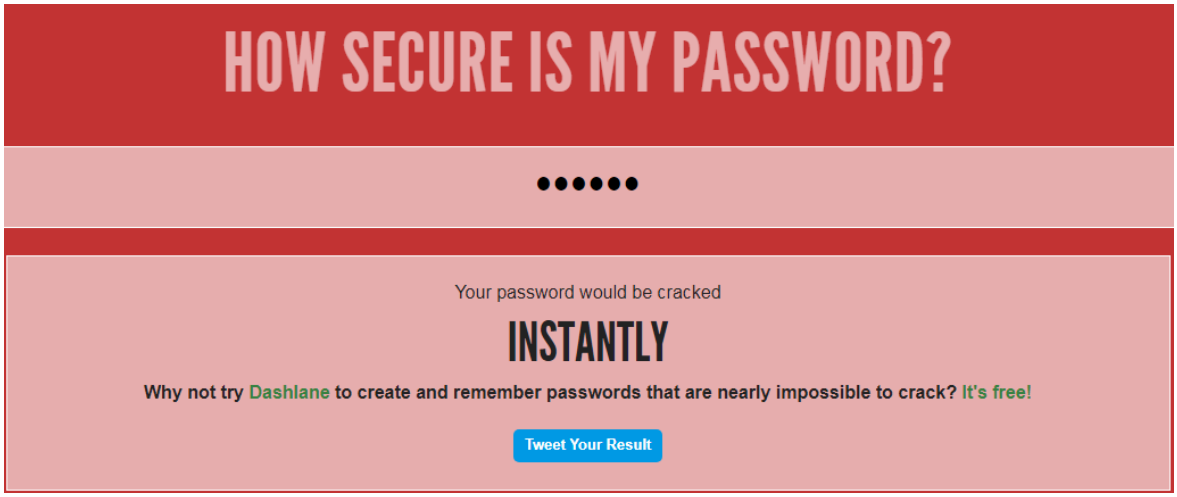
Fialově označená pole jsou prolomena okamžitě, červená již trvá nějaký ten čas, ale bývají to sekundy až hodiny. Oranžová pole již představují silnější hesla, ale lze je také prolomit v řádu dnů až měsíců. Žlutě jsou označeny kombinace pro silná hesla, která jen tak nelze prolomit. V tomto případě je heslo již použitelné. A zelená jsou hesla, která nelze prolomit. Heslo, které má takovouto kombinaci je velice bezpečné a nelze ho prolomit.

Hesla jsou jednou z nejrozšířenějších způsobů autentizace uživatelů, ať už na různých webových stránkách, tak i u zašifrovaných dat. Ale přesto jsou hesla také jednou z největších bezpečnostních hrozeb. Důvodů je hned několik: jednoduchost hesla (př. heslo123), krátký tvar hesla (př. 123456) a podobně. Je to způsobené hlavně kvůli množství hesel, které každý má. Aby si člověk nemusel pamatovat mnoho složitých hesel, tak si vymyslí menší množství krátkých a jednoduchých hesel. (Kolouch a Bašta, 2019)

Pro velké množství hesel je důležitá správa hesel. Je to sada zásad a osvědčených postupů, jak účinně ukládat a spravovat hesla tak, aby byly maximálně zabezpečeny. K tomuto

účelu slouží počítačové aplikace pro správu hesel. (What is password management?, © 2021)

Pokud si uživatel chce ověřit sílu svého nynějšího hesla, existují webové stránky, kde se vyplní a ukáže se, za jak dlouho by bylo heslo „prolomeno“. Příkladně lze uvést nejpoužívanější heslo podle serveru CNN – 123456. Druhé heslo bude delší a bude obsahovat i speciální znaky – UTB_flkr-ochrana2020. Rozdíl je zřetelný a ukazuje, proč by měl každý uživatel, nejen šifrovacího programu, ale i jiných aplikací či webových portálů mít silné heslo.



Obr. 26 – Kontrola „prolomitelnosti“ hesla „123456“ (HOW SECURE IS MY PASSWORD?, © 2021)

Obr. 27 – Kontrola „prolomitelnosti“ hesla „UTB_flkr-ochrana2020“ (HOW SECURE IS MY PASSWORD?, © 2021)

Software pro správu hesel

Tedy tzv. správce hesel je aplikace, která slouží ke správě hesel. Ve správci hesel je možné mít mnoho hesel na jednom místě zabezpečených tak, aby k nim neměl nikdo přístup. Takováto aplikace ukládá hesla v šifrované podobě a k jejich přečtení si majitel nastaví hlavní heslo. Existuje více typů správců hesel, přičemž se liší především způsobem šifrování. (Password Manager, © 2021)

Hlavní předností správce hesel je to, že si majitel nemusí pamatovat mnoho hesel, ale jen hlavní, které mu odemkne všechna ostatní. V aplikaci jsou uloženy přihlašovací údaje od uložených účtů. Takže při přihlašování se údaje doplní sami a je menší riziko útoků (např. keylogger, apod.).

Na druhou stranu ani správce hesel není odolný proti všemu. Bylo provedeno testování, jak bezpečné jsou vybraní správci hesel. Jednalo se o 1Password, Dashlane, KeePass a LastPass. Výsledky byly takové, že při spuštění byly hesla chráněná. Ve stavu nespuštěném a uzamčeném to bylo stejné. Docela jinak tomu bylo s uložením dat v paměti, kdy se takto dalo zjistit buď hlavní heslo, nebo také všechna ostatní. Nakonec ani jeden program nebyl zcela neproniknutelný a alespoň jeden aspekt ochrany nebyl naplněn. (Zorze, 2019)

6.4 Anti-malware

Anti malware je software, který chrání počítač před malwarem, jako je spyware, adware a červy. Naskenuje systém, zda neobsahuje všechny typy škodlivého softwaru, který se dokáže dostat k počítači. Program proti malwaru je jedním z nejlepších nástrojů k ochraně počítače a osobních údajů.

Antimalwarový program je navržen tak, aby eliminoval malware z počítače. Přestože se program proti malwaru podobá antiviru, liší se od antiviru. Program proti malwaru má pokročilejší funkce a širší pokrytí. Řeší spyware, spam a další problémy s hrozbami, které antivirus ne. (What is Anti Malware?, © 2021)

Rozdíly mezi anti-malwarem a antivirem

Mezi lidmi se při ochraně počítače před malwary používá především pojem antivirus. Jeho použití ale není v mnoha případech správné. Proto je dobré vysvětlit tyto rozdíly.

Antivirus se zpravidla zabývá staršími, zavedenými hrozbami typu trojských koní, virů a červů. Anti-malware je rozdílný v zaměření na nové věci, které ještě nejsou známé nebo se objevují v malém počtu. Jsou to například polymorfní malware a malware dodávaný zneužitím nulového dne (Zero-day attack). Antivirus funguje jako ochrana před

přetrvávajícím, předvídatelným a přesto nebezpečným malwarem. Anti-malware oproti tomu chrání uživatele před nejnovějšími, aktuálními a ještě nebezpečnějšími hrozbami. Kromě toho anti-malware většinou aktualizuje svá pravidla rychleji než antivirus, což znamená, že je to nejlepší ochrana proti novému malwaru, se kterým se můžete setkat. Antivirový program je zase nejlepší proti malwaru, který se může do počítače dostat z tradičních zdrojů jako je USB nebo e-mailová příloha. (Zamora, 2015)

Nástroje pro ochranu před malwarem

Jelikož je k výběru nepřeberné množství různých a různě kvalitních softwarů a proto je zde uveden žebříček *„Best malware removal software 2021: free and paid anti-malware tools and services“* z webvých stránek Techradar. Všechny softwary jsou stručně popsané, ale jde pouze o výčet. Každý uživatel má jiné preference, takže tento seznam slouží jako inspirace pro možnost výběru.

1. **Malwarebytes Anti-Malware**

Malwarebytes je anti-malwarový software, který velmi jednoduchý na ovládání a populární. Jeho nespornou výhodou je aktualizace každý den, což zajišťuje aktuálnost ochrany a vysokou míru odhalitelnosti malwaru. Malwarebytes je stejně jako u většiny dalších volně ke stažení, ale neoplývá tolika funkcemi jako placená verze. Prémiová verze je placená, ale při první instalaci je uživateli k dispozici na vyzkoušení bezplatně na 14 dnů. Bezplatná verze disponuje pouze funkcí pro ochranu počítače proti základním formám malwaru. (Marshall a kolektiv, 2021)

Malwarebytes funguje na principu shody chování malwaru, ne na jeho jednoduchých podpisových shodách. Proto chrání i proti neznámým typům malwaru. Placená verze obsahuje funkce:

- Varování před infikovanou webovou stránkou a reklamou.
- Automatické skenování počítače.
- Detekce malwaru v reálném čase a ochrana proti němu.
- Ochrana proti ransomwaru. (Anderson, 2019)

2. **Avast Antivirus**

Avast je velmi známý software používaný miliony uživatelů po celém světě. Je známí především svou bezplatnou verzí, ale existují i placené, které mají navíc další funkce. Hlavní výhodou placených verzí je úplná ochrana více zařízení. Chrání proti všem druhům

malwaru včetně ransomware. Avast si zakládá také na funkčnosti nejen na počítačích, ale i na dalších zařízení jako je Mac, mobilní telefon či tablet. (Marshall a kolektiv, 2021)
Samotný software má dobrou funkčnost a nezabírá mnoho výkonu počítače, což je velké plus. Mezi funkce patří:

- Detekce a odstranění malwaru.
- Ochrana proti ransomwaru.
- Zabezpečení hesel a ochrana webového prohlížeče. (Anderson, 2019)

3. Kaspersky Antivirus

Kaspersky je známý software zejména díky kauze v Evropském parlamentu. V roce 2018 europoslanci žádali, aby se přestal používat veškerý software od Kaspersky Lab. Důvodem byla nebezpečnost a škodlivost. Firma je ruská a po obviněních se dala slyšet, že přesune některá aktiva do Švýcarska, což se také stalo. (Slížek, 2018)
I přes tuto kauzu je Kaspersky Antivirus stále velmi populární mezi uživateli. Zaměřuje se na blokování škodlivých webových stránek, detekci a ochranu před malwarem,… Kaspersky Antivirus je dobře hodnocen od uživatelů i na webech jako AV-Comparatives. (Marshall a kolektiv, 2021)
Kaspersky Antivirus je placený a podle toho jaký balíček si uživatel vybere, tak tolik má funkcí k dispozici.

4. Trend Micro Antivirus+ Security

Další placený software, který je účinným pomocníkem pro ochranu počítače. Ovšem jsou zde pozitiva i negativa. Zejména AV-Comparatives upozorňuje na vysoký počet falešně pozitivních výsledků, což není ku prospěchu firmy ani softwaru. Na druhou stranu AV-TEST poukazuje na vysokou přesnost a žádné falešné poplachy. Software je podobný Bitdefenderu. Celkově jsou falešné poplachy jen nepatrně vyšší a software neovlivňuje výkon systému téměř vůbec. Antivirus lze vyzkoušet na 30 dní zdarma. Většinu funkcí má jako výše uvedené:

- Ochrana před ransomware.
- Ochrana před phishingem.
- Detekce a ochrana před malwarem.
- Zabezpečení dat proti krádeži na webových stránkách. (Marshall a kolektiv, 2021)

5. F-Secure SAFE

F-Secure SAFE je také dobře hodnocený software, který je taktéž placený, ale má velké množství funkcí, které uživatele chrání. Jde především o internetovou ochranu, ale nezapomíná ani na základní ochranu před malwarem. F-Secure umožňuje ochranu více zařízení. Od AV-TESTu software dostal vynikající hodnocení a i u AV-Comparatives dosahuje také vysokého skóre. Velkou výhodou je snadná obsluha, nízké ovlivnění výkonu počítače. Hlavními funkcemi jsou:

- Ochrana při internetovém bankovnictví a online nakupování.
- Možnost vyhledání polohy zařízení (týká se mobilních telefonů).
- Blokuse škodlivé webové stránky.
- Ochrana proti ransomwaru.
- Rodičovská kontrola. (Marshall a kolektiv, 2021)

Další nástroje k ochraně proti malwaru, které se zde neobjevily, jsou například: Bitdefender Antivirus Free Edition, Avira Free Security Suite, AVG AntiVirus Free, SpyBot Search & Destroy, Emsisoft Emergency Kit, ESET NOD32 Antivirus a mnoho dalších.

Aby zde bylo uvedeno kvalitní hodnocení anti-malwarů, tak byly použity testy z oficiální instituce, která se zabývá testováním těchto programů a to AV-TEST. AV-TEST je výzkumný ústav pro bezpečnost IT, který sídlí v německém Magdeburgu. Firma má více než 15 letou zkušenost a jejím hlavním předmětem činnosti je srovnávání všech mezinárodně relevantních bezpečnostních produktů pro IT. Firma tedy garantuje kvalitu srovnávacích testů a je možné se řídit výsledky. V tabulce níže jsou uvedeny programy, které byly testovány v dubnu 2021, což je nyní nejaktuálnější verze. Pro aktuální testy je nejlepší se podívat na webové stránky https://www.av-test.org/en/. Testovány byly nejnovější verze programů. Hodnoceny byly tři oblasti a to ochrana, výkon a použitelnost. Nejvíce bodů je 6. Když byly všechny tři oblasti hodnoceny nejvýše, případně i se ztrátou půl bodu u jedné oblasti dostali od AV-TESTu certifikát *„Top produktu“*. (About the AV-TEST Institute, © 2021)

Tabulka 10 – test anti-malwaru organizací AV-TEST (upraveno, The best Windows antivirus software for home users, © 2021)

Produkt	Certifikát	Ochrana	Výkon	Použitelnost
AhnLab V3 Internet Security	Top produkt	6	6	6

Produkt	Certifikát	Ochrana	Výkon	Použitelnost
9.0				
Avast Free AntiVirus 21.10 & 21.2	Top produkt	6	6	6
AVG Internet Security 21.10 & 21.2	Top produkt	6	6	6
Avira Internet Security for Windows 1.0 & 1.1	Top produkt	6	5,5	6
Bitdefender Internet Security 25.0	Top produkt	6	6	5,5
BullGuard Internet Security 21.0	Top produkt	6	6	6
ESET Internet Security 14.0	Top produkt	6	6	6
F-Secure SAFE 17	Top produkt	6	6	6
G Data Total Security 25.5	Top produkt	6	6	6
K7 Security Total Security 16.0	AV certifikát	5,5	6	5,5
Kaspersky Internet Security 21.3	Top produkt	6	6	6

Produkt	Certifikát	Ochrana	Výkon	Použitelnost
Malwarebytes Premium 4.3.0	Top produkt	6	6	6
McAfee Total Protection 24.1 & 24.2	Top produkt	6	6	6
Microsoft Defender 4.18	Top produkt	6	6	6
eScan Internet Security Suite 14.0	AV certifikát	4	6	5,5
Northguard Security 20.0	Top produkt	6	6	6
Norton 360 22.21	Top produkt	6	6	6
PC Matic 3.0	AV certifikát	4,5	6	4
Total AV 5.14	Top produkt	6	6	6
Trend Micro Internet Security 17.0	Top produkt	5,5	6	6
VIPRE AdvancedSecurity 11.0	AV certifikát	4,5	6	5,5

6.4.1 Doporučení pro uživatele

Doporučení jen jednoho anti-malwaru je velmi složité kvůli jejich různorodosti a také dalším parametrům. Každý uživatel totiž preferuje něco jiného a doporučení je tudíž čistě subjektivní. Předem lze říci, že dnes již mívají OS anti-malware integrovaný a v mnohých případech lidé nemusí nic řešit. Příkladem je Microsoft Windows 10, který obsahuje Defender, což je právě anti-malware přímo od výrobce. Ale ne každému může vyhovovat již nainstalovaný program. V potaz je při doporučení bráno zejména to, že běžný uživatel

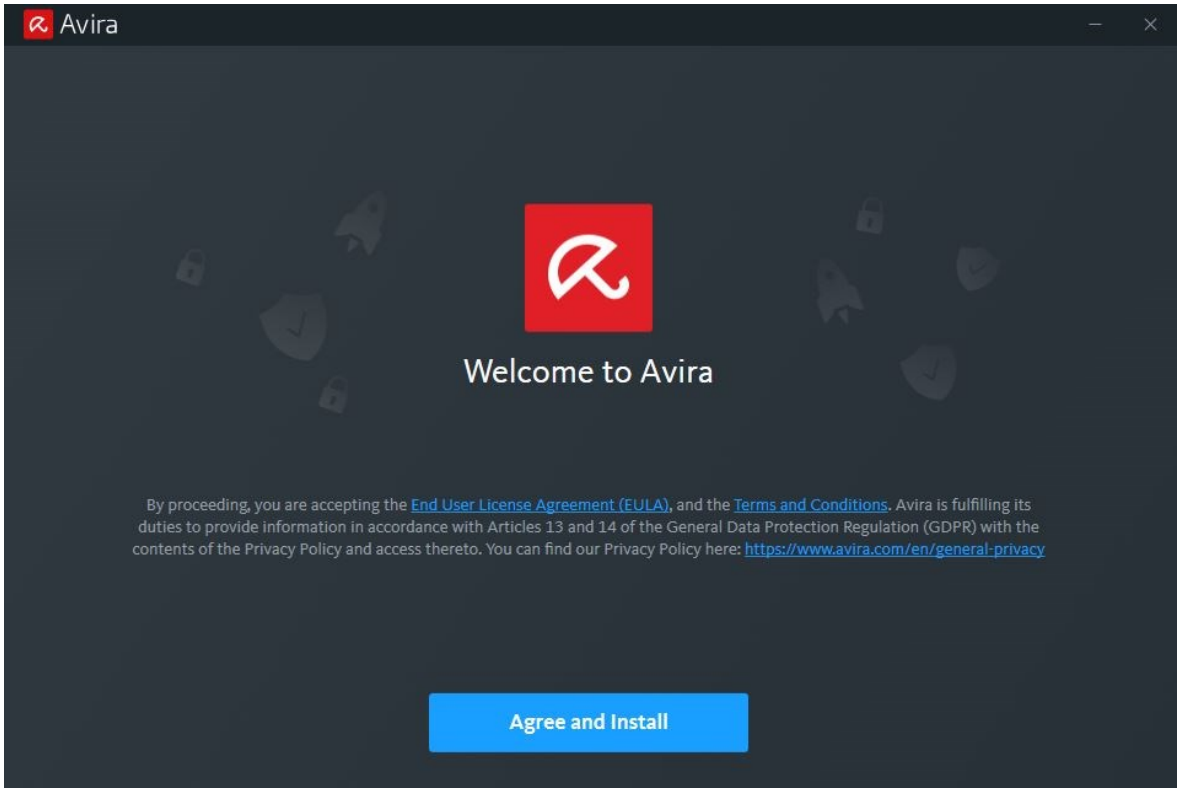
většinou nechce platit za tento program, takže výběr probíhal z těch, které lze stáhnou zdarma. Autor by tedy s přihlédnutím k této skutečnosti a dalším, které se odrážejí na bezpečnosti a funkčnosti programu doporučil Aviru Free Antivirus. Je namístě zdůraznit, že verze programů zdarma nemívají takové vybavení a některé funkce bývají omezené. V tabulce dole jsou uvedeny výhody a nevýhody, které k této volbě přispěli.

Tabulka 11 – Anti-malware Avira Free Antivirus (vlastní)

Avira Free Antivirus	
Výhody	**Nevýhody**
Zdarma.	Není v české verzi.
Po instalaci a spuštění pracuje sám.	Neobsahuje ochranu proti ransomwaru ani spamu.
Upozorňuje na nebezpečné webové stránky.	Neblokuje webové reklamy.
Součástí je i správce hesel v prohlížeči.	
Nezatěžuje počítač, protože nepotřebuje tolik výkonu.	

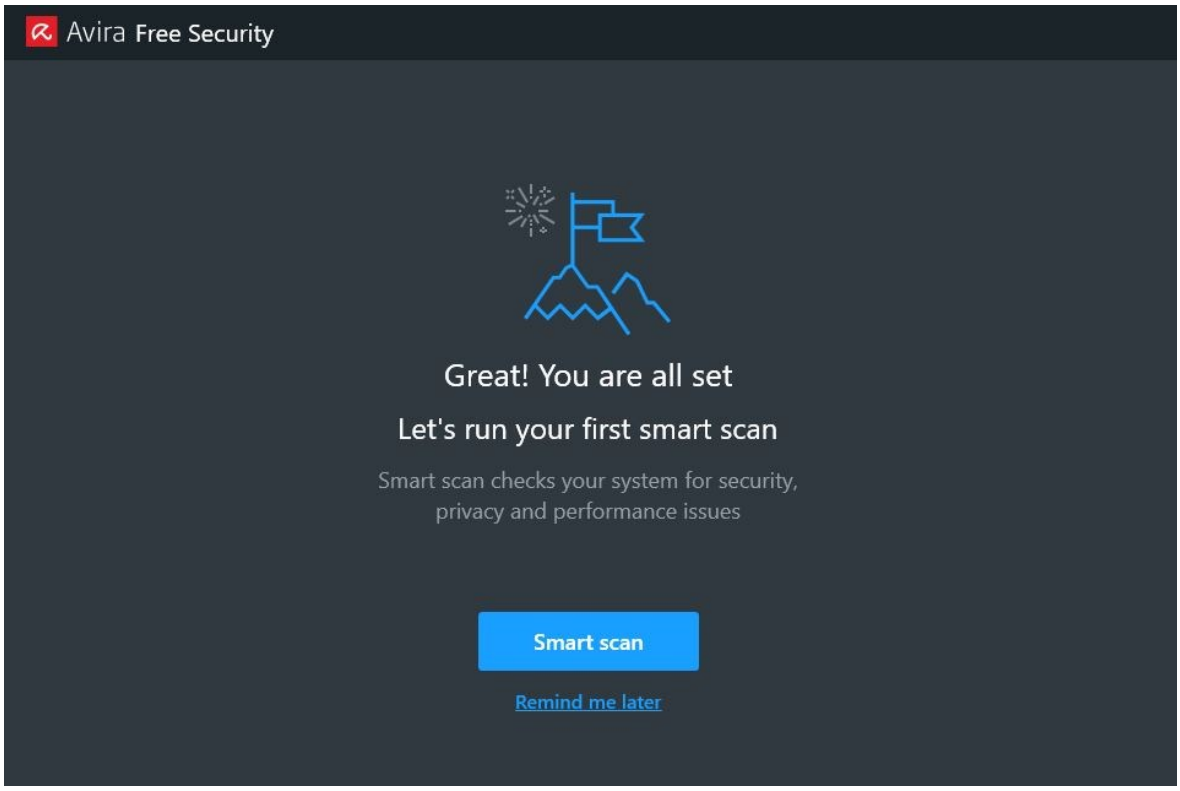
Avira Free Antivirus - návod

Vše začíná stažením souboru. Program jde stáhnout na oficiálních webových stránkách Aviry: https://www.avira.com/en/free-antivirus. Po stažení následuje instalace, která je velice jednoduchá a rychlá. Na obrázku č. 28 je vidět začátek instalace.



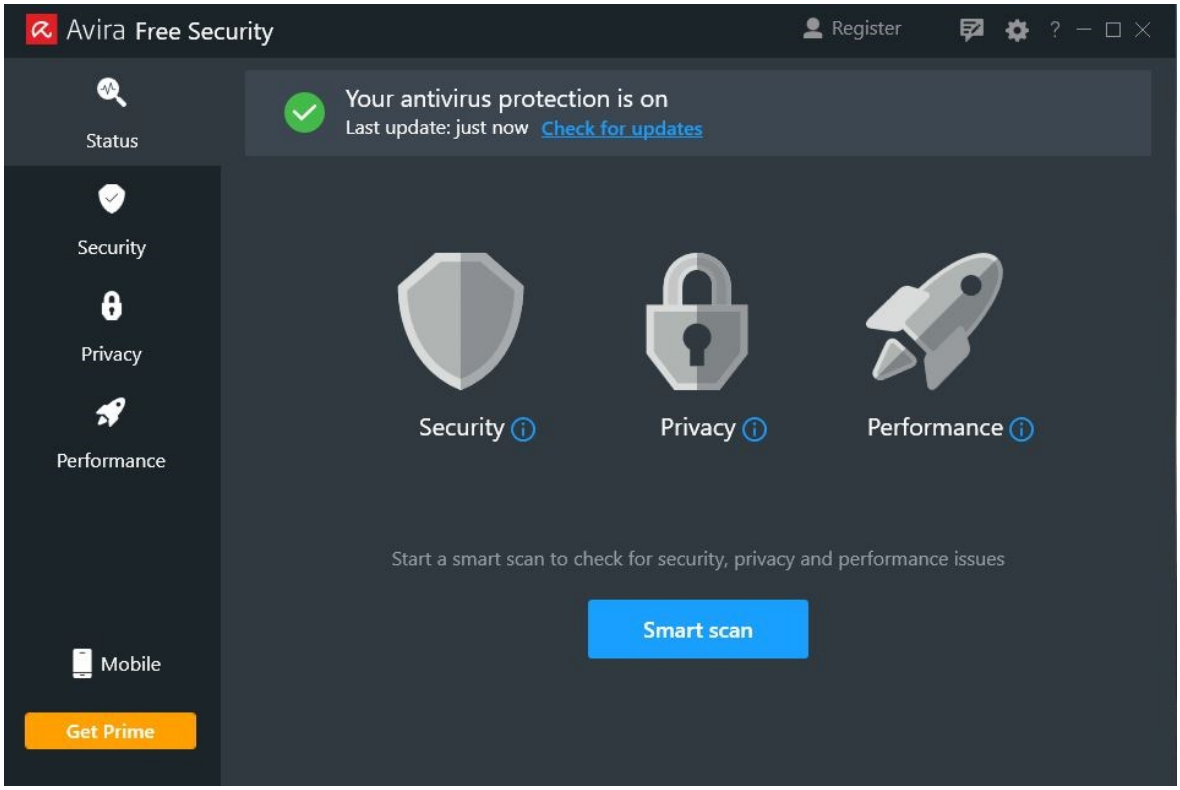
Obr. 28 – Instalační okno programu Avira (vlastní)

Po instalaci je uživatel vyzván k prvotnímu skenování počítače.



Obr. 29 – Nainstalovaný program s výzvou k prvotnímu skenování (vlastní)

Poté je již vše nastaveno a instalace je hotová. Kromě instalace samotného programu proběhne také instalace doplňků v prohlížeči jako správce hesel nebo doplněk pro upozorňování na nebezpečné webové stránky.



Obr. 30 – Úvodní okno programu Avira (vlastní)

ZÁVĚR

Diplomová práce se zabývala informační bezpečností z pohledu uživatele osobního počítače, což je velice aktuální téma, které je třeba dostat do podvědomí širšího okruhu obyvatel. Umět chránit svá data by měl každý bez ohledu na vzdělání či věk, proto je třeba toto téma šířit.

V první části práce byly vysvětleny pojmy z oblasti kybernetické a informační bezpečnosti jako kyberprostor, také rozdíl mezi kybernetickou a informační bezpečností či definice dat a informace. Další prostor byl věnován samotným kybernetickým útokům, které byly rozděleny podle dvou kritérií. Z nepřeberného množství útoků jsou zde zmíněny pouze ty, které jsou v této době asi nejčastějším problémem a také základní útoky, které je dobré znát. Právě pochopení podstaty kybernetických útoků je základem pro zvýšení informační bezpečnosti každého uživatele osobního počítače.

V praktické části práce jsou nejprve identifikovány hrozby pro informační bezpečnost. Tyto hrozby jsou rozděleny podle prostředí, ve kterém se mohou vyskytnout. Jsou u nich uvedeny také další skutečnosti včetně navrhovaných opatření. Na to poté navazuje analýza informační bezpečnosti uživatele osobního počítače, která je provedena formou dotazníkového šetření. Právě výsledky dotazníkového šetření měly ukázat, jak běžný uživatel řeší informační bezpečnost. Právě některé identifikované hrozby se podle výsledků dotazníku ukázaly jako nebezpečné. Celkové výsledky, ale nedopadly tak špatně. Dobrý výsledek je zejména u používání hesla pro přihlášení do počítače, kdy 112 respondentů (79,4 %) má heslo nastaveno a jen 29 (20,6 %) heslo nemá. Horší výsledek vykazovala otázka týkající se délky hesla, kterou má převážná většina v rozmezí od 6 do 10 znaků, což není bezpečná délka hesla. Další oblast, kterou mnoho respondentů nezná je šifrování. Také zálohování u většiny neprobíhá tak, aby zvýšili zabezpečení svých dat. Po vyhodnocení všech otázek došlo k návrhu ochranných opatření. Jednalo se o šifrování, zálohování, vytvoření silného hesla a používání anti-malwaru. Všechna tato ochranná opatření dohromady zvyšují informační bezpečnost a snižují riziko ztráty dat. Hlavním výstupem této diplomové práce je vytvořená „Příručka uživatele osobního počítače ke zvýšení bezpečnosti“. Tato příručka se zaměřuje na pět oblastí, u kterých uvádí různá doporučení ke zvýšení informační bezpečnosti. Při splnění těchto doporučení se riziko ztráty dat minimalizuje.

Tato diplomová práce je zaměřena na informační bezpečnost uživatele osobního počítače, ale jde spíše o obecnější zaměření. Detailnější rozebrání různých druhů ochrany dat a informací má potenciál při zpracování další absolventské práce. Věnování se informační bezpečnosti by mělo mít vysokou prioritu zejména v dnešní době, která je ovládána různými druhy informačních a komunikačních technologií.

SEZNAM POUŽITÉ LITERATURY

About NordLocker [online], © 2021. NordLocker [cit. 2021-7-26]. Dostupné z: https://nordlocker.com/about-us/

About the AV-TEST Institute [online], © 2021. Magdeburg: AV-TEST - The Independent IT-Security Institute [cit. 2021-7-27]. Dostupné z: https://www.av-test.org/en/about-the-institute/

Adware [online], © 1992 – 2021. Praha: ESET [cit. 2021-7-26]. Dostupné z: https://www.eset.com/cz/adware/

ANDERSON, Sophie. *Vyzkoušeno a testováno: 5 nejlepších softwarů proti malwaru* [online], 2019. Safety Detectives [cit. 2021-7-27]. Dostupné z: https://cs.safetydetectives.com/blog/vyzkouseno-a-testovano-nejlepsich-softwaru-proti-malwaru/#malwarebytes

Attack Vector [online], ©2021. Sumo Logic [cit. 2021-7-25]. Dostupné z: https://www.sumologic.com/glossary/attack-vector

AxCrypt Premium [online], c2021. Stockholm: AxCrypt [cit. 2021-7-26]. Dostupné z: https://www.axcrypt.net/axcrypt-premium/

BAKER, Kurt. *The 11 Most Common Types Of Malware* [online], 2021. Sunnyvale: Crowdstrike [cit. 2021-7-26]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

BARLOW, J. P. *A Declaration of the Independence of Cyberspace* [online], 1996. Davos [cit. 2021-7-23]. Dostupné z: https://www.eff.org/cyberspace-independence

BitLocker [online], 2018. Microsoft [cit. 2021-7-26]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview#bitlocker-overview

Botnet [online], © 2018. INTERNETEM BEZPEČNĚ [cit. 2021-7-26]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

BUSSELL, Jennifer. *Cyberspace* [online], 2013. Chicago: Encyclopædia Britannica [cit. 2021-7-23]. Dostupné z: https://www.britannica.com/topic/cyberspace

Co je IoT? [online], © 2021. IoT portál [cit. 2021-7-25]. Dostupné z: https://www.iot-portal.cz/co-je-iot/

Cryptainer PE [online], © 1999-2021. Cypherix [cit. 2021-7-26]. Dostupné z: https://www.cypherix.com/cryptainerpe/

CryptoExpert 8 - Secure Offline Storage for Windows 10. [online], c2016. InterCrypto Softwarfe [cit. 2021-7-26]. Dostupné z: https://www.cryptoexpert.com/

Datová média (CD, DVD, Blu-ray) [online], © 2021. Soft-Tech [cit. 2021-7-27]. Dostupné z: https://www.tonerdepot.cz/thumbs/400x150-resizeX-80/2b/bc/2bbc7213d8fb1fca90b1195b3310f69c-33-1772-cd-dvd-bluray.png

DE GUISE, Preston, 2020. *Data protection: ensuring data availability*. Second edition. New York: Taylor & Francis. ISBN 978-036-7256-777

DIOGENES, Yuri a Erdal OZKAYA. *Cybersecurity - attack and defense strategies: infrastructure security with Red Team and Blue Team tactics*. Birmingham: Packt, 2018, viii, 367 s. ISBN 9781788475297.

DiskCryptor [online], © 2021. Full Stack Technology FZCO [cit. 2021-7-26]. Dostupné z: https://www.filehorse.com/download-diskcryptor/

DiskStation DS220+ [online], © 2021. Synology [cit. 2021-7-27]. Dostupné z: https://www.synology.com/img/products/detail/DS220plus/heading.png

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

Downloads [online], c2021. [cit. 2021-7-26]. Dostupné z: https://www.veracrypt.fr/en/Downloads.html

DRAKE, Alexa. *Your Data Is at Risk: Why Backup Is So Important* [online], 2020. Chicago: G2 [cit. 2021-7-26]. Dostupné z: https://www.g2.com/articles/what-is-backup

Encryption Software [online], © 2001-2021. CryptoForge Encryption Software [cit. 2021-7-26]. Dostupné z: https://www.cryptoforge.com/

Encryption Software - File encryption, Secure File Transfer, Batch File Encryption and Encrypted Backups [online], c2014-1998. InterCrypto Software [cit. 2021-7-26]. Dostupné z: http://www.aeppro.com/file-encryption-software/aep-pro-features.shtml

EMPEY, Charlotte. *Jak si nastavit silné heslo* [online], 2019. Avast Software [cit. 2021-7-27]. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

FIŠER, Miloslav. *Experti varovali před útoky hackerů s předstihem. Bylo to ale marné* [online], 2021. Praha: Borgis [cit. 2021-7-25]. Dostupné z:

https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/experti-varovali-pred-utoky-hackeru-s-predstihem-bylo-to-ale-marne-40353115

Folder Lock [online], © 1997-2021. Softonic International [cit. 2021-7-26]. Dostupné z: https://folder-lock.en.softonic.com/

FRANKENFIELD, Jake. *Zero-Day Attack* [online], 2020. Investopedia [cit. 2021-7-26]. Dostupné z: https://www.investopedia.com/terms/z/zero-day-attack.asp

FRUHLINGER, Josh. *What is information security? Definition, principles, and jobs* [online], 2020. Needham: IDG Communications [cit. 2021-7-25]. Dostupné z: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

Generátor náhodných hesel [online], © 1988–2021. Avast Software [cit. 2021-7-27]. Dostupné z: https://www.avast.com/cs-cz/random-password-generator

Home [online], c2021. [cit. 2021-7-26]. Dostupné z: https://www.veracrypt.fr/en/Home.html

HOW SECURE IS MY PASSWORD? [online], © 2021. [cit. 2021-7-27]. Dostupné z: https://howsecureismypassword.net/

HRŮZA, Petr, 2013. *Kybernetická bezpečnost II* [online]. Brno: Univerzita obrany [cit. 2021-7-23]. ISBN 978-80-7231-931-2. Dostupné z: https://www.researchgate.net/publication/275029169_Kyberneticka_bezpecnost

Integrity in the Data LifeCycle [online], c2021. Waterford: Dataworks [cit. 2021-7-25]. Dostupné z: https://www.dataworks.ie/5-stages-in-the-data-management-lifecycle-process/

Interní pevný disk HDD 320GB 3,5" Western Digital WD3200AVVS [online], © 2021. Praha: Mámevšechno [cit. 2021-7-26]. Dostupné z: https://www.mamevsechno.cz/fotky102359/fotos/_vyr_2781.jpg

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada. ISBN 978-802-4715-612.

KOLOUCH, Jan, 2016. *CyberCrime*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-808-8168-157.

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

Malware [online], c2021. Cambridge: Cambridge University Press [cit. 2021-7-25]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/malware

March 17, 1948: William Gibson, Father of Cyberspace [online], 2009. New York: Condé Nast [cit. 2021-7-23]. Dostupné z: https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/

MARSHALL, Carrie, Brian TURNER a Mike WILLIAMS. *Best malware removal software 2021: free and paid anti-malware tools and services* [online], 2021. New York: Future US [cit. 2021-7-27]. Dostupné z: https://www.techradar.com/best/best-malware-removal

MASSCHELEIN, Jhon. *Episode 123 – Infrastructure and Data Lifecycle (part 2)* [online], 2019. Creative Commons Attribution-NoDerivatives 4.0 International License [cit. 2021-7-23]. Dostupné z: https://roaringelephant.org/2019/01/15/episode-123-infrastructure-and-data-lifecycle-part-2/

MILLS, Matt. *How Long Does it Take to Hack or Crack a Password* [online], 2020. ITIGIC [cit. 2021-7-27]. Dostupné z: https://itigic.com/how-long-does-it-take-to-hack-or-crack-a-password/

Nejlepší cloudové úložiště 2021 [online], © 2016 - 2021. 5nej [cit. 2021-7-26]. Dostupné z: https://www.5nej.cz/srovnani-cloudovych-ulozist/

Neuromancer [online], © 2008 - 2021. Praha: Databazeknih.cz [cit. 2021-7-23]. Dostupné z: https://www.databazeknih.cz/zajimavosti-knihy/neuromancer-423243

Password Manager [online], © 2021. Techopedia [cit. 2021-7-27]. Dostupné z: https://www.techopedia.com/definition/31435/password-manager

Počítačové viry, červi a trojské koně [online], © 2018. INTERNETEM BEZPEČNĚ [cit. 2021-7-26]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/virus/

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

RIPPL, Jan. *Bezpečnost v Linuxu: Aplikace a metody pro šifrování dat* [online], 2013. LinuxEXPRES [cit. 2021-7-26]. Dostupné z: https://www.linuxexpres.cz/praxe/bezpecnost-v-linuxu-aplikace-a-metody-pro-sifrovani-dat

ROSS, Ronald. *Guide for Conducting Risk Assessments* [online], 2012. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [cit. 2021-7-27] Dostupné z: https://doi.org/10.6028/NIST.SP.800-30r1

Secure IT [online], © 1999-2021. Cypherix [cit. 2021-7-26]. Dostupné z: https://www.cypherix.com/secureit2000/

SLÍŽEK, David. *Nepoužívejte produkty Kaspersky Lab, vyzvali europoslanci evropské instituce* [online], 2018. Praha: Internet Info [cit. 2021-7-27]. Dostupné z: https://www.lupa.cz/aktuality/nepouzivejte-produkty-kaspersky-lab-vyzvali-europoslanci-evropske-instituce/

Spyware [online], 2005, updated October 2008. Washington: US-Cert [cit. 2021-7-26]. Dostupné z: https://us-cert.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf

Steganos Safe 22 [online], c2021. Steganos [cit. 2021-7-26]. Dostupné z: https://www.steganos.com/en/products/steganos-safe-22

Šifrování startovacího disku Macu pomocí FileVaultu [online], © 2021. Apple [cit. 2021-7-26]. Dostupné z: https://support.apple.com/cs-cz/HT204837

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-807-3807-375.

TERRORISM [online], c2021. North Augusta: Connecting People and Government [cit. 2021-7-23]. Dostupné z: https://www.northaugusta.net/government/city-departments/public-safety/emergency-management/terrorism

The best Windows antivirus software for home users [online], © 2021. Magdeburg: AV-TEST - The Independent IT-Security Institute [cit. 2021-7-27]. Dostupné z: https://www.av-test.org/en/antivirus/home-windows/

The Online Hacker Jargon File, verze 5.0.1 [online], 2012. [cit. 2021-7-25]. Dostupné z: https://www.landley.net/history/mirror/jargon.html

The (Re)invention of Cyberspace [online], 2015. Oslo: Kunstkritikk Foundation [cit. 2021-7-23]. Dostupné z: https://kunstkritikk.com/the-reinvention-of-cyberspace/

Trojan Horse [online], © 2021. Radware [cit. 2021-7-26]. Dostupné z: https://www.radware.com/security/ddos-knowledge-center/ddospedia/trojan-horse

Trojan (trojský kůň) [online], c2018. Digitální pevnost [cit. 2021-7-26]. Dostupné z: https://www.digitalnipevnost.cz/viki/trojan-trojsky-kun

United States. Joint Chiefs of Staff. *DOD Cyberspace Operations Lexicon* [online]. In: . Washington, D. C., s. 16 [cit. 2021-7-29]. Dostupné z: https://www.hsdl.org/?view&did=734860

USB 3.0 - SATA3 adaptér s kabelem pro 2,5"/3,5"HDD [online], © 2021. SOFTCOM Group [cit. 2021-7-27]. Dostupné z: https://img1.softcom.cz/usb-3-0-sata3-adapter-s-kabelem-pro-2-5-3-5-hdd_i113733.jpg

USB flash disk 16GB [online], © 2010 - 2021. MIKROMARZ [cit. 2021-7-27]. Dostupné z: https://www.mikromarz.com/fotky28654/fotos/28654_424__vyr_423good_ram.jpg

What is Anti Malware? [online], © 2021. Comodo Group [cit. 2021-7-27]. Dostupné z: https://enterprise.comodo.com/what-is-anti-malware.php

What is a denial-of-service (DoS) attack? [online], © 2021. Cloudflare [cit. 2021-7-26]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

What is Cyber Security? Definition and Best Practices [online], © 2003-2021. Ely: IT Governance [cit. 2021-7-23]. Dostupné z: https://www.itgovernance.co.uk/what-is-cybersecurity

What is password management? [online], © 2021. Zoho Corporation [cit. 2021-7-27]. Dostupné z: https://www.zoho.com/vault/educational-content/what-is-password-management.html

What is Spyware? The 5 Examples You Need to Know [online], © 2014-2021. SoftwareLab [cit. 2021-7-26]. Dostupné z: https://softwarelab.org/what-is-spyware/

What is the CIA Triad? [online], © 2021. Forcepoint [cit. 2021-7-25]. Dostupné z: https://www.forcepoint.com/cyber-edu/cia-triad

YATZIV, Idan. *Five signs that you are part of a botnet attack* [online], 2020. Reblaze Technologies [cit. 2021-7-26]. Dostupné z: https://www.reblaze.com/blog/five-signs-part-botnet-attack/

ZAMORA, Wendy. *What's the difference between antivirus and anti-malware?* [online], 2015, updated 25 September 2019. Santa Clara: Malwarebytes [cit. 2021-7-27]. Dostupné z: https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/

Zálohování [online], © 2021. Praha: CZ.NIC [cit. 2021-7-26]. Dostupné z: https://www.jaknainternet.cz/page/1180/zalohovani/

ZIMA, Jiří. *Roční zkušenosti s šifrováním disku pomocí TrueCrypt* [online], 2011. CZECH NEWS CENTER [cit. 2021-7-26]. Dostupné z: https://www.zive.cz/clanky/rocni-zkusenosti-s-sifrovanim-disku-pomoci-truecrypt/sc-3-a-159188/default.aspx

ZORZ, Zeljka. *Flawed password managers allow malware to steal passwords from computer memory* [online], 2019. Kastav: Help Net Security [cit. 2021-7-27]. Dostupné z: https://www.helpnetsecurity.com/2019/02/20/flawed-password-managers-allow-malware-to-steal-passwords-from-computer-memory/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

.doc Document

AES Advanced Encryption Standard

CD Compact Disk

CIA Confidentiality Integrity Availability

CZK Česká koruna

DVD Digital Video Disk

FAT File Allocation Table

GB Gigabyte

ICT Information and Communication Technologies

MB Megabyte

MS Microsoft

NTFS New Technology File System

OS Operační systém

SHA Secure Hash Algorithm

TB Terabyte

TPM Trusted Platform Module

USB Universal Serial Bus

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: SCHÉMA DOTAZNÍKOVÉHO ŠETŘENÍ

Dotazníkové šetření informační bezpečnosti

Dobrý den,
jmenuji se Lukáš Navrátil a studuji 2. ročník navazujícího magisterského studia na FLKŘ UTB.
Tímto bych Vás chtěl poprosit o vyplnění dotazníkového šetření, jehož výstupy použiji jako podklady do mé diplomové práce, která je zaměřená na informační bezpečnost z pohledu uživatele osobního počítače.
Cílem dotazníku je zjištění, jak studenti FLKŘ UTB řeší informační bezpečnost na svém počítači a také jaké zabezpečení používají.
Moc Vám děkuji za vyplnění dotazníku a nezapomeňte chránit svoje data ☺.

Otázky

1. **Máte nastavené heslo pro přihlášení na počítač?**

Výběr z možností

   a. Ano.
   b. Ne.

2. **Máte v počítači vytvořeno více účtů?**

Výběr z možností

   a. Ano
   b. Ne

3. **(pokud ano) Máte vytvořeno více správcovských účtů?**

Výběr z možností

   a. Ano.
   b. Ne.

4. **Máte je zabezpečeny heslem?**

Výběr z možností

   a. Ano.
   b. Ne.

c. Pouze hlavní účet.
d. Pouze správcovské účty.

5. Zadáváte heslo k přihlášení do počítače v přítomnosti jiné osoby?

Výběr z možností

a. Ano.
b. Ano, ale pouze v přítomnosti rodiny.
c. Ne.

6. Dáváte si pozor, aby ho přítomná osoba neviděla?

Výběr z možností

a. Ano, požádám, aby se otočila.
b. Ano, ale zakryji jen klávesnici.
c. Ne, vyplňuji jako obvykle.

7. Nechal/a byste svůj notebook na veřejném místě (kavárna, vlak, lavička v parku apod.) chvíli bez dozoru či pozornosti?

Výběr z možností

a. Ano.
b. Ano, ale pouze za přítomnosti někoho z rodiny či přátel.
c. Ne.

8. Uzamykáte počítač v kontrolovaném prostředí (práce, škola) když od něj odcházíte?

Výběr z možností

a. Ano, vždy.
b. Ano, ale jen někdy.
c. Nikdy.

9. Uzamykáte počítač v nekontrolovaném prostředí (kavárna, restaurace apod.) když od něj odcházíte?

Výběr z možností

a. Ano, vždy.
b. Ano, ale jen někdy.
c. Nikdy.

10. Uzamykáte svůj počítač doma, když od něj odcházíte?

Výběr z možností

a. Ano, vždy.
b. Ano, ale jen někdy.
c. Nikdy.

11. Jak dlouhá hesla používáte?

Výběr z možností

a. Méně než 6 znaků.
b. 6 až 10 znaků.
c. 11 až 15 znaků.
d. 16 a více znaků.

12. Jak složitá hesla používáte?

Výběr z možností

a. Pouze malá písmena.
b. Malá i velká písmena.
c. Malá, velká písmena a čísla.
d. Malá, velká písmena, čísla a speciální znaky.

13. Používáte jedno heslo k více účtům (k počítači, emailu, Facebooku atd.) či k více zařízením?

Výběr z možností

a. Ano.
b. Ne.

14. Ke kolika účtům či zařízením používáte jedno heslo či PIN?

Výběr z možností

a. 2 účty či zařízení.
b. 3 až 5 účtů či zařízení.
c. 6 a více účtů či zařízení.

15. Jaký software pro správu hesel znáte nebo používáte?

Výběr z možností, více možných

a. KeePass.
b. Sticky Password.

c. 1Password.
d. LastPass.
e. Dashlane.
f. NordPass.
g. RoboForm.
h. Jiný…
i. Neznám ani jeden.

16. Používáte správce hesel v prohlížeči?

Výběr z možností

a. Ano.
b. Ne.
c. Nevím, že něco takového existuje.

17. Byl/a byste schopen/a prozradit heslo či jiné citlivé údaje člověku, který by vystupoval (v telefonu, SMS nebo emailu) jménem organizace (např. banky, sociálních sítí, pojišťovny apod.), kterou znáte, a uváděl by různé důvody, proč po Vás tyto informace chce?

Výběr z možností

a. Ano.
b. Ano, ale pouze pokud by mi dal kontakt.
c. Ne.

18. Zná nějaké Vaše heslo či PIN někdo jiný?

Výběr z možností, více možných

a. Příslušník rodiny.
b. Kamarád/ka.
c. Spolupracovník/spolupracovnice.
d. Nikdo jiný.

19. Máte šifrovaný disk v počítači?

Výběr z možností

a. Ano.
b. Ne.
c. Nevím.

20. Šifrujete cenná data ve svém počítači?

Výběr z možností

a. Ano.
b. Ne.

21. Jaký šifrovací software používáte?

Výběr z možností, více možných

a. Bitlocker.
b. AxCrypt.
c. Veracrypt.
d. Folder Lock.
e. NordLocker.
f. DiskCryptor.
g. TrueCrypt.
h. FileVault.
i. Ccrypt.
j. Jiný…

22. Znáte nějaký z uvedených šifrovacích programů?

Výběr z možností, více možných

a. Bitlocker.
b. AxCrypt.
c. Veracrypt.
d. Folder Lock.
e. NordLocker.
f. DiskCryptor.
g. TrueCrypt.
h. FileVault.
i. Ccrypt.
j. Jiný…
k. Žádný.

23. Zálohujete svá data?

Výběr z možností

a. Ano.
b. Ne.

24. Jak často zálohujete?

Výběr z možností

a. Každý den.
b. Každý týden.
c. Každý měsíc.
d. Jednou za několik měsíců.
e. Jednou za půl roku.
f. Jednou za rok.

25. Kam zálohujete?

Výběr z možností, více možných

a. Na pevný disk v počítači.
b. Na USB Flash disk nebo externí pevný disk.
c. Na optické úložiště (CD, DVD, Blu-Ray).
d. Na síťové úložiště.
e. Na cloudové úložiště.
f. Jinam…

26. Znáte nějaký z uvedených způsobů zálohování?

Výběr z možností, více možných

a. Na pevný disk v počítači.
b. Na USB Flash disk nebo externí pevný disk.
c. Na optické úložiště (CD, DVD, Blu-Ray).
d. Na síťové úložiště.
e. Na cloudové úložiště.

27. Máte v počítači nainstalovaný anti-malware/antivir?

Výběr z možností

a. Ano.
b. Ne.
c. Nevím.

28. Používáte placený nebo neplacený anti-malware/antivir?

Výběr z možností

a. Placený.
b. Neplacený.

29. Proč nemáte nainstalovaný anti-malware/antivir?

Výběr z možností

a. Neřeším to.
b. Nevím.
c. Nikdy jsem ho nepotřeboval.
d. Jiná…

30. Znáte některý z uvedených anti-malwarů?

Výběr z možností, více možných

a. Malwarebytes Anti-Malware.
b. Avast Antivirus.
c. Kaspersky Antivirus.
d. Avira Free Security Suite.
e. AVG AntiVirus Free.
f. ESET NOD32 Antivirus.
g. Jiný…

31. Jaký anti-malware/antivir používáte?

Výběr z možností, více možných

a. Malwarebytes Anti-Malware.
b. Avast Antivirus.
c. Kaspersky Antivirus.
d. Avira Free Security Suite.
e. AVG AntiVirus Free.
f. ESET NOD32 Antivirus.
g. Jiný…

32. Stahujete neznámé přílohy nebo klikáte na uvedené odkazy, když Vám přijde neznámý email?

Výběr z možností

a. Ano, dělám obojí.

b. Přílohy nestahuji, ale klikám na odkaz.
c. Stahuji přílohy, ale neklikám na odkaz.
d. Nedělám ani jedno.

33. Stahujete soubory z Vámi neznámých a podezřelých webových stránek?

Výběr z možností

a. Ano, často.
b. Ano, pokud soubor jinde nelze stáhnout.
c. Ne, nikdy.

PŘÍLOHA P II: PŘÍRUČKA UŽIVATELE OSOBNÍHO POČÍTAČE KE ZVÝŠENÍ BEZPEČNOSTI

PŘÍRUČKA UŽIVATELE OSOBNÍHO POČÍTAČE KE ZVÝŠENÍ BEZPEČNOSTI

Autor: Bc. Lukáš Navrátil

Úvod

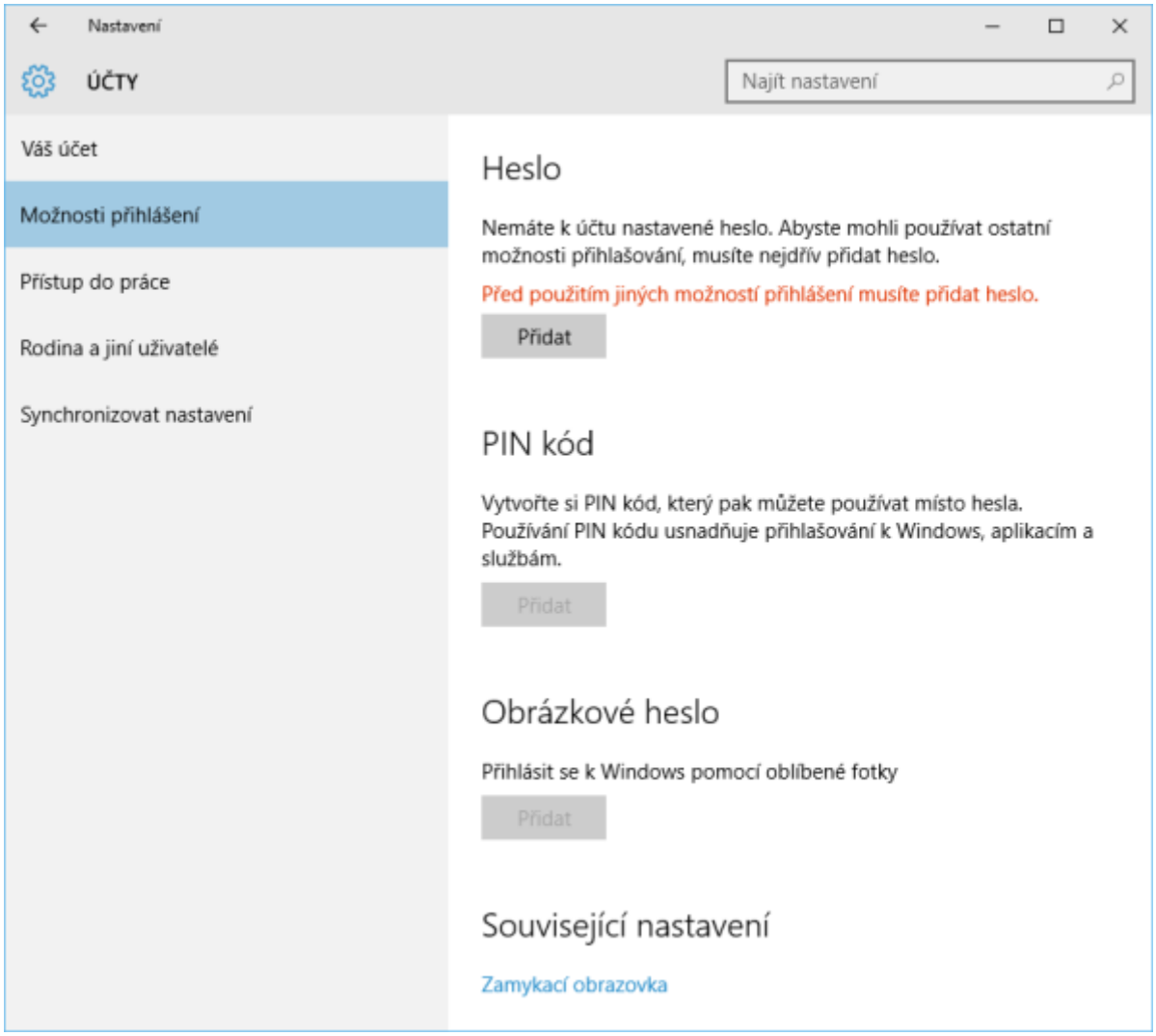
Tato příručka je zaměřena především na zajištění a zlepšení informační bezpečnosti běžného uživatele počítače. Informační bezpečnost je důležitou součástí každodenního života většiny lidí, protože kybernetický útok se může koneckonců týkat každého. Informační bezpečnost bývá ve většině případů podceňována a mnoho lidí to nebere vážně. Proto byla vytvořena tato příručka, která má ukázat, jaké kroky podniknout pro to, aby byli Vaše data v bezpečí.

1. Základní zabezpečení počítače

Základní zabezpečení lze pojmout jako úplně základní bezpečné zacházení s počítačem tak, aby se minimalizovalo riziko ztráty dat. Do této kapitoly patří zejména nastavení hesla pro přihlášení do počítače a uzamykání počítače při jeho opuštění.

Nastavení hesla

Základním zabezpečením je myšleno nastavení hesla od počítače. První krok ke zvýšení bezpečnosti tedy je nastavení hesla k účtu v počítači.



!!! POZOR !!!

Pro větší bezpečnost je dobré heslo nastavit pro každý uživatelský účet v počítači, protože existují možnosti, jak se z jednoho účtu dá dostat k datům z dalších.

Zadávání hesla

Zadávání hesla k jakémukoliv účtu je běžná věc a mnoho lidí ani nemyslí na to, že toto dělá, i když je kolem někdo cizí. Je důležité myslet na bezpečnost hesla, ať je zadáváno kdekoliv.

a) Kontrolované prostředí – práce, škola…

Rizika: lidé pohybující se na daném místě, návštěvníci.

Doporučení: zadávat heslo, tak aby na něj nikdo neviděl, protože se na místě může pohybovat někdo, kdo by mohl heslo zneužít a ukrást citlivá data uživatele nebo dané instituce.

b) Nekontrolované prostředí – restaurace, kavárna, nádraží,…

Rizika: všichni lidé, pohybující se kolem.

Doporučení: zadávat heslo, tak aby na něj nikdo neviděl. Zde je důvod zcela jasný, protože se kolem pohybují cizí lidé, kteří mohou mít nejrůznější úmysly.

c) Domácnost

Rizika: žádná.

Doporučení: doma nehrozí žádné riziko, protože se tam pohybuje jen rodina, proto není zcela nutné být při zadávání hesla opatrný. Jediný důvod k opatrnosti je to, že člověk nechce, aby se mu do počítače mohl podívat někdo z příbuzných.

Uzamykání počítače

Přihlašování do počítače je samozřejmě spojené s odhlašováním. Když je počítač zamčený, tak se do něj obyčejný člověk není schopen dostat, proto je uzamykání základním zabezpečením. I toto je důležité dodržovat. Doporučení pro různá prostředí jsou takováto:

a) Kontrolované – doporučuje se uzamykat počítač, když od něj uživatel odchází.
b) Nekontrolované – doporučuje se a je nezbytné uzamknout počítač, když od něj uživatel odchází z důvodu bezpečnosti dat. Navíc není doporučeno počítač (notebook) nechávat osamoceně na veřejných místech. Alespoň aby ho hlídala důvěrně známá osoba (rodina, přítel/přítelkyně, kamarád/kamarádka).
c) Domácnost – zde není nutné počítač uzamykat.

2. Heslová politika

Heslo je ta nejdůležitější informace, protože se jím uživatel přihlašuje k různým účtům. Heslo by mělo být silné, což znamená dostatečně dlouhé s dobrou kombinací znaků a složené tak, aby na to nepřišel nikdo jiný. Proto, aby bylo heslo dostatečně silné, je třeba dodržovat následující zásady:

1) Heslo musí být dostatečně dlouhé.

Délka hesla je jedním z nejzásadnějších parametrů. Hned poté je kombinace znaků. **Ideální je používat 15 a více znaků.** Pokud to jinak nejde, tak 10 znaků je nejkratší heslo, co se dá doporučit a to již není tak silné.

2) Heslo musí obsahovat kombinaci malých a velkých písmen, čísel a speciálních znaků.

Čím více druhů znaků se používá, tím více je heslo silné a těžší k prolomení. Proto je doporučeno používat všechny druhy znaků.

3) Nepoužívat běžné nahrazování znaků.

Útoky na prolomení hesla již znají toto nahrazování a není pro ně těžké heslo prolomit. Příkladem je např. BRNOJENEJ – **8RN0J3N3J**. Taková hesla už **NEPOUŽÍVAT**.

4) Nepoužívat po sobě jdoucí klávesy.

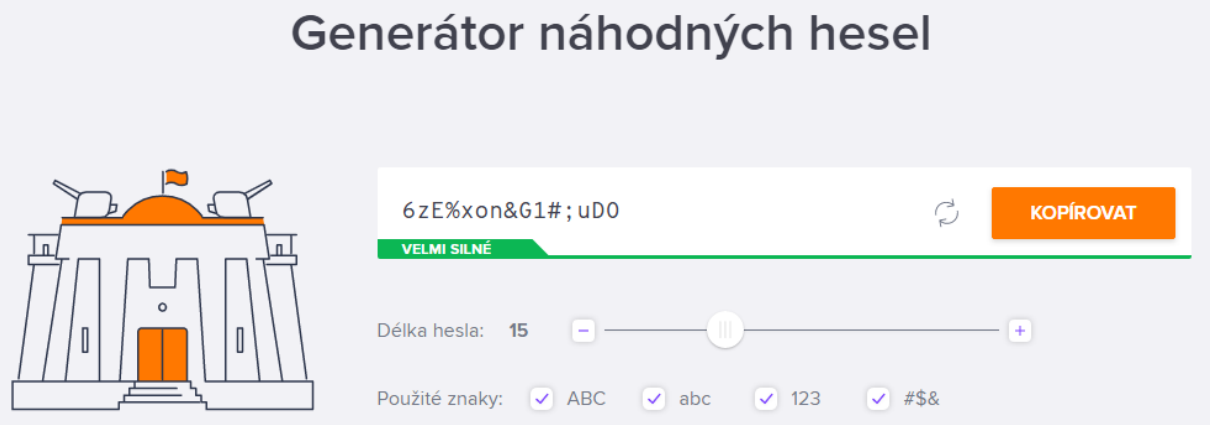
Toto je jeden z největších problémů, protože lidé si tvoří hesla tak, aby si je zapamatovali, a když chtějí jednoduché, tak použijí právě po sobě jdoucí klávesy (např. **qwerty** nebo **123456**). Toto také **NEPOUŽÍVAT**.
Pro zesílení hesla není špatné použít pasáže z knihy, filmu či seriálu. Pokud si to uživatel pamatuje a je to dost dlouhé většinou ani není třeba používat čísla či speciální znaky a heslo je dostatečně odolné proti útokům.

Příklad silného hesla:
UTB_flkr-ochrana2020

Pro představu jak dlouho trvá hackerovi prolomit heslo je následující tabulka, kde je ukázán počet znaků a použité typy znaků či jejich kombinace a délka trvání prolomení hesla.

Počet znaků	Pouze čísla	Malá písmena	Malá a velká písmena	Čísla, malá a velká písmena	Čísla, malá, velká písmena a speciální symboly
4	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
5	Okamžitě	Okamžitě	Okamžitě	Okamžitě	Okamžitě
6	Okamžitě	Okamžitě	Okamžitě	1 sekunda	5 sekund
7	Okamžitě	Okamžitě	25 sekund	1 minuta	6 minut
8	Okamžitě	5 sekund	22 minut	1 hodina	8 hodin
9	Okamžitě	2 minuty	19 hodin	3 dny	3 týdny
10	Okamžitě	58 minut	1 měsíc	7 měsíců	5 let
11	2 sekundy	1 den	5 let	41 let	400 let
12	25 sekund	3 týdny	300 let	2 tisíce let	34 tisíc let
13	4 minuty	1 rok	16 tisíc let	100 tisíc let	2 miliony let
14	41 minut	51 let	800 tisíc let	9 milionů let	200 milionů let
15	6 hodin	1 tisíc let	43 milionů let	600 milionů let	15 miliard let
16	2 dny	34 tisíc let	2 miliardy let	37 miliard let	1 bilion let
17	4 týdny	800 tisíc let	100 miliard let	2 biliony let	93 bilionů let
18	9 měsíců	23 milionů let	6 bilionů let	100 bilionů let	9 biliard let

Pokud uživatel není schopen vymyslet dostatečně odolné heslo je tu možnost použít generátor hesel. K tomuto účelu můžete využít například generátor náhodných hesel od Avastu (webové stránky: https://www.avast.com/cs-cz/random-password-generator). Heslo poté může vypadat jako na přiloženém obrázku.



K dalšímu zvýšení bezpečnosti přispívá i obměna hesla. Ideální je například jednou za měsíc případně za pár měsíců. Toto ovšem není zcela důležité, pokud je heslo samo o sobě dost silné, navíc mnoho lidí by to asi ani nebylo ochotno dělat. Je to tedy jen možná volba pro zabezpečení účtu.

Jedno heslo = jeden účet.

Tímto heslem by se měl řídit každý, protože se ukazuje, že jedno heslo mnoha lidem slouží k více účtům či zařízením a to v rozmezí od 2 do 6 či více účtům.

Správce hesel

Pokud je dodrženo vše výše uvedené, tak není od věci říci, že aby si uživatel nemusel pamatovat tolik složitých hesel je k dispozici tzv. správce hesel. Těchto softwarových pomocníků je mnoho a všechny fungují na principu toho, že si v nich uživatel uloží hesla. Ta jsou chráněna hlavním heslem, kterým se aplikace odemyká a poté se už jen heslo zkopíruje. Není tedy nutné si pamatovat mnoho hesel, ale v podstatě jen jedno, to od správce hesel.

Doporučit lze:

- KeePass.
- LastPass.
- 1Password.
- Dashlane.

Sociální inženýrství

Člověk je největším rizikem při ztrátě dat z počítače. Proto je důležité si hesla či další citlivá data a informace chránit a neprozrazovat je nikomu cizímu. Sociální inženýrství je i v dnešní době velice oblíbené a využívané, protože pokud je „útočník“ dostatečně charismatický a umí mluvit s lidmi, je mnohdy těžké takovémuto člověku neříct nic. Hlavní rada je **NEPROZRAZOVAT HESLA NEBO JINÁ CITLIVÁ DATA A INFORMACE NIKOMU, KOHO DOSTATEČNĚ DOBŘE NEZNÁTE.**

3. Pokročilé zabezpečení dat v počítači

Do pokročilého zabezpečení je zahrnuto šifrování dat, čímž se chrání data, pokud se útočník dostane do počítače, aby data nemohl přečíst a zneužít proti napadenému. Zálohování patří také do tohoto bodu. Zálohování je účinné zejména při poškození či ztrátě dat. Ztracená data se mohou bezpečně obnovit.

Šifrování

Šifrování je proces, kdy se data učiní nečitelnými pro všechny, kteří nemají klíč, tedy heslo k jejich dešifrování. Za tímto účelem existují šifrovací programy.

Doporučený šifrovací software:

a) OS X, Mac OS (operační systém od Applu)

Operační systém Apple zařízení má integrovaný software pro tento účel, který se nazývá FileVault. Proto je doporučeno využít tohoto nástroje.

b) OS Microsoft Windows

Microsoft Windows 10 má obdobně jako zařízení od Applu integrovaný software s názvem BitLocker. Uživatelům MS Windows 10 je proto doporučeno používat tento nástroj.

c) Jiné

Pokud se někomu nelíbí ani jeden ze zmíněných, tak autor doporučuje jeden z programů VeraCrypt nebo AxCrypt. Obě jsou zdarma a jsou ideální i k přenosu na přenosném úložišti.

Zálohování

Zálohováním se předchází ztrátě dat a v mnohých případech je velice užitečné i za cenu, že záloha zabírá místo na úložišti. Níže jsou uvedena doporučení na to KAM zálohovat a JAK ČASTO.

KAM?

Nejbezpečnější varianty jsou **cloudové úložiště**, které je spravováno jejím majitelem a ten ručí za bezpečnost dat. Dnes jsou již cloudová úložiště velmi dobře chráněna. Další variantou je **externí disk či USB Flash Disk.** Přenosné úložiště je bráno za bezpečné, ale je třeba si dávat pozor, aby si jej uživatel neopatrným zacházením nenakazil nějakým malwarem. Třetí možností, jež je také bezpečná, je **síťové datové úložiště**, tzv. NAS.

JAK ČASTO?

Ideální zálohování u běžného uživatele by mělo být **JEDNOU TÝDNĚ** až **JEDNOU MĚSÍČNĚ**, což je pravděpodobnější. Ucházející je také jednou za pár měsíců, ale to už není tak bezpečné.

4. Malware a zabezpečení

Pro pochopení je třeba povědět, že malware je škodlivý software, který má různou podobu a různý účinek. Jako ochranu proti malware je třeba mít nainstalovaný tzv anti-malware, v laické řeči nazývaný též antivir, který se stará o to, že se malware do počítače nedostane.
Doporučení anti-malwaru:

a) Neplacený

Protože v mnoha případech uživatel nechce investovat do ochrany, je skvělé, že je k dispozici i mnoho programů zdarma. Proto autor doporučuje **Aviru Free Antivirus**, který je dobrou volbou, obsahuje zásadní ochrany proti malwaru a je nenáročný na výkon počítače.

b) Placený

Pokud někdo chce za anti-malware utratit peníze, dostane mnohem více ochranných nástrojů. Zde autor doporučuje **ESET NOD32 Antivirus**, který bývá každoročně výborně hodnocen v mnoha bezpečnostních testech.

c) Integrovaný

V případě, že uživatel nechce nic řešit, nezbývá než využít integrovaný software. Příkladem je **Defender**, který se součástí MS Windows 10 a mívá také dobré výsledky v bezpečnostních testech.

5. Podvodné emaily a stahování souborů

Podvodné emaily nebo nevyžádaná pošta, která může být podvodným emailem, chodí snad každému, a proto je důležité si na ni dávat pozor. Pokud člověk není opatrný, může přijít o své přihlašovací údaje (např. pokud se přihlásí do internetového bankovnictví prostřednictvím uvedeného odkazu) nebo při stažení přílohy může nakazit počítač malwarem, který je skrytý v příloze. Stahování souborů z neznámých či podezřelých webových stránek je také velice nebezpečné, protože již při vstupu na neznámou stránku může být stažen malware, případně později jako součást stahovaného souboru.

Podvodné emaily

DOPORUČUJE SE NEZNÁMÉ EMAILY VŮBEC NEOTEVÍRAT. Případné smazání neuškodí, ovšem pouze pokud člověk ví, že to je někdo zcela neznámý a nesmaže si třeba email z práce apod.

Stahování souborů

Stahování souborů je dnes již normální, ale přesto by se měl uživatel držet několika zásad.

1) Stahovat nejlépe z oficiálních stránek.
2) Stahovat ze stránek, které jsou prověřené lidmi či někým známým.
3) Než vstoupí na webové stránky mít zapnutí anti-malware, který by měl upozornit, pokud je webová stránka nebezpečná (pokud program takovou funkci má).
4) Nevstupovat na stránky, jejichž název je podivný (může to být náznak, že se jedná o nebezpečné stránky).
5) Pokud je i přesto počítač nakažen, zanést ho k odborníkovi, který se na něj podívá.