Osobní počítače z pohledu bezpečnosti informací

Vít Charvát

Bakalářská práce
2020

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: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vít Charvát**
Osobní číslo:	**L17319**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Osobní počítače z pohledu bezpečnosti informací**

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k předmětné problematice.
2. Popište možnosti a principy ochrany dat u osobních počítačů a možné útoky na ně.
3. Proveďte analýzu úrovně zabezpečení dat uživatelů osobních počítačů.
4. Na základě předchozí analýzy navrhněte opatření pro zvýšení bezpečnosti dat uživatelů osobních počítačů.

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

Seznam doporučené literatury:

1. 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.
2. KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač.* Praha: Grada, 2015. ISBN 978-80-247-5453-6.
3. ŠULC, Vladimír. *Kybernetická bezpečnost.* Praha: Čeněk, 2018. ISBN 978-80-7380-737-5.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **1. listopadu 2019**
Termín odevzdání bakalářské práce: **15. května 2020**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2019

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 15. 5. 2020

Jméno a příjmení studenta: Vít Charvát

.....
podpis studenta

ABSTRAKT

Bakalářská práce je zaměřena na ochranou informací a dat u osobních počítačů. V teoretické části jsou vymezeny některé ze základních pojmů dané problematiky a také základní legislativa, která se k problematice vztahuje. V další kapitole teoretické části jsou základní možnosti ochrany počítače, tedy i informací a dat v něm. Následně jsou v práci popsány nejběžnější kybernetické útoky, se kterými se uživatelé můžou setkat. V první kapitole praktické části bakalářské práce je realizován slovníkový útok na dva testovací e-mailové účty. Další kapitola se zaměřuje na analýzu současného stavu zabezpečení dat uživateli v ČR.

Klíčová slova: Bezpečnost informací, kybernetické útoky, malware, slovníkový útok, heslo

ABSTRACT

The bachelor thesis aims to the protection of information and data in personal computers. The theoretical part defines some of the basic concepts of the issue and also the basic legislation that relates to the issue. In the next chapter of the theoretical part are the basic possibilities of computer protection, ie information and data in it. Subsequently, the work describes the most common cyber attacks that users may encounter. In the first chapter of the practical part of the bachelor's thesis, a dictionary attack on two test e-mail accounts is implemented. The next chapter focuses on the analysis of the current state of user data security in the Czech Republic.

Keywords: Information security, cyber attacks, malware, dictionary attack, password

Rád bych poděkoval svému vedoucímu panu Ing. Petru Svobodovi Ph. D. za odborné vedení, konzultace a cenné postřehy při zpracování mé bakalářské práce.

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

OBSAH

ÚVOD

Cílem teoretické části je zpracovat rešerši k problematice ochraně informací u osobních počítačů a vymezit některé ze základních pojmů. Dále popsat základní způsoby ochrany dat osobních počítačů a také nejčastější kybernetické útoky určené k získávání informací.

Cílem praktické části je za využití vybraného nástroje simulovat kybernetický útok na pracovní stanici – osobní počítač. A tím prokázat na důležitost heslové politiky, konkrétně volby silného hesla.

O době, v které právě žijeme můžeme hovořit jako o době informačních a komunikačních technologií. Počet počítačů a zařízení připojených k Internetu se neustále zvětšuje, tudíž se zvětšuje i počet jejich uživatelů, tedy i potencionálních obětí kybernetického útoku. Z počítače se stal pracovní nástroj spoustě lidí a většina domácností vlastní aspoň jeden osobní. V dnešní době umí se zařízením připojeným k internetu pracovat téměř každé dítě a ty o informační bezpečnosti neví skoro nic. Tito uživatelé často volí jednoduchá hesla nebo se na internetu nebojí sdílet informace, které můžou být následně zneužity. Dokonce ani firmy si neuvědomují rizika, protože si často myslí, že pro kybernetický útok nejsou nijak zajímaví. Ovšem počet útoků na velké, střední i malé firmy taktéž roste. V poslední době jsou kybernetické útoky čím dál více častější a řadí se dokonce mezi nejzávažnější rizika. Má bakalářská práce se zabývá ochranou počítače z pohledu bezpečnosti informací. V teoretické části je nejprve výčet důležitých základních pojmů týkajících se dané problematiky. Dále v práci popisuji základní a často velmi jednoduchá opatření, která by měl uživatel osobního počítače dodržovat, právě proto aby se nestal obětí kybernetického útoku a uchránil tak svá data. V další části se věnuji samotným kybernetickým útokům, které můžou být využity k získání informací a dat oběti, nebo k tomu jsou přímo určeny. Nejprve jejich základnímu rozdělení na útoky plošné a cílené, dále také vektorům, kterými jsou útoky vedeny. Poté blíže přibližuji problematiku sociálního inženýrství, které bývá velmi často využíváno k obelstění oběti. Dále se v práci věnuji druhům malware a následně útokům jako jsou například phishing, hacking, cracking nebo sniffing.

Hlavní kapitolou praktické části je realizace jedné z metod crackingu, konkrétně slovníkového útoku. Útok byl proveden pomocí operačního systému Kali Linux, ten byl totiž pro podobné účely vytvořen a obsahuje spoustu nástrojů na provedení penetračních testů. Útok byl cílen na dva testovací e-mailové účty. V následující kapitole jsou uvedeny různé následky, které mohou nastat pokud útočník heslo od e-mailového účtu prolomí.

Dále je také popsán návod pro vytvoření silného hesla, které slovníkovému útoku a také jiným odolá.

Součástí praktické části byla provedena analýza současného stavu zabezpečení dat uživatelů osobních počítačů. K té byly využity veřejné statistiky. Následně jsou definována bezpečnostní opatření a také tabulka, v které je znázorněno, jaká opatření jsou účinná proti daným útokům.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA KYBERNETICKÉ BEZPEČNOSTI

Úvodní kapitola bakalářské práce se zabývá základními pojmy, základní legislativou vztahující se k dané problematice a také mezinárodními normami ISO.

1.1 Základní pojmy

Cílem téhle podkapitoly není výčet všech základních pojmů, které se vztahují k problematice ICT bezpečnosti a ochrany informací. Vybral jsem pouze ty, které považuji za nejdůležitější.

Osobní počítač – Stroj sloužící ke zpracování dat, „*které probíhá podle předem vytvořeného programu uloženého v jeho paměti*“. [1]

Informace – Pojem informace je široký pojem. Jedna z definic je: „*Informace je každý znakový projev, který má smysl pro komunikátora i příjemce.*“ [1] O informacích lze tedy obecně hovořit jako o údajích reálného stavu a v něm probíhajících procesech. [2]

Kybernetická bezpečnost – Definici kybernetické bezpečnosti je obtížné definovat. Ustálených jich existuje již celá řada. Například „*Opatření přijatá k ochraně počítače nebo počítačového systému před neoprávněným přístupem nebo útokem*.“ [3] Někdo může kybernetickou bezpečnost chápat jako oblast, kterou se zabývají pouze odborníci a IT oddělení. Tato úvaha je ovšem chybná, neboť kybernetická bezpečnost se týká všech, kteří používají jakékoliv prvky ICT. [4]

Ochrana dat – Opatření, např. technická, administrativní nebo fyzická sloužící k zabránění neautorizovaného přístupu nebo k porušení integrity dat. [1]

Bezpečnost informací – Uplatnění obecných bezpečnostních opatření a postupů sloužících k ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, dostupnosti, spolehlivosti atd.). V případě tohoto zjištění přijetí nápravných opatření. [1]

Důvěrnost – Lze definovat jako zajištění, že informace jsou přístupné nebo jsou sděleny pouze oprávněným osobám. Pokud dojde k narušení důvěrnosti, tedy zpřístupnění informací, hovoříme o jejich úniku. [5]

Integrita – Zajištění správnosti a úplnosti informací. Pokud dojde k nežádoucí modifikaci, hovoříme o narušení integrity. [6]

Dostupnost – Nejčastěji definována jako zajištění přístupnosti informace oprávněnému uživateli v okamžiku jeho potřeby. [6]

Kybernetický útok – Úmyslné využití informačních technologií s cílem narušení dostupnosti, důvěrnosti a integrity dat. [4]

Zranitelnost – Můžeme charakterizovat jako slabé místo, určitou chybu v softwaru nebo také pochybení člověka. [1] Pokud je v některém programu nalezena, je potřeba ji pojmenovat a zaevidovat do databáze bezpečnostních chyb. Databáze se nazývá Common Vulnerabilities and Exposures (CVE) a obsahuje téměř 132 tisíc zranitelností. [7]

Zranitelnost nultého dne – Zranitelnost, která zatím není známá a neexistuje pro ni záplata. Doba od zjištění zranitelnosti po vytvoření a uvolnění záplaty se nazývá okno zranitelnosti.

Exploit – Nejčastěji jednoduchý kód, který zneužije určitou zranitelnost v systému. [8]

1.2 Legislativa a normy

Zde jsou uvedeny stručné obsahy zákonu o kybernetické bezpečnosti, směrnice Evropského parlamentu a Rady (EU) a také nařízení Evropského parlamentu o GDPR. Dále řada norem International Organization for Standardization (ISO), které nelze považovat za legislativu, ale v oblasti kybernetické bezpečnosti mají svůj význam.

1.2.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů upravuje práva a povinnosti osob a také pravomoci a působnost orgánů v oblasti kybernetické bezpečnosti. Zákon se zabývá kybernetickým prostorem a určuje systém, který kybernetickou bezpečnost zajišťuje. Určuje bezpečnostní opatření, což jsou úkony, jejichž cílem je zajištění bezpečnosti informací, dostupnost a spolehlivost sítí v kybernetickém prostoru. Vymezuje také pojem kybernetický bezpečnostní incident a zlepšuje jejich detekci. Déle také zavádí jejich hlášení a systém opatření k reakci na kybernetické bezpečnostní incidenty. [9]

1.2.2 Směrnice Evropského parlamentu a Rady (EU) 2016/1148

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS) má za cíl sladit právní předpisy členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti. Směrnice NIS také rozšiřuje skupinu subjektů, kteří podléhají povinnostem

v oblasti prevence a ochrany před kybernetickými bezpečnostními incidenty. Jedná se například o internetové vyhledávače. [10]

1.2.3 Nařízení Evropského parlamentu a Rady (EU) 2016/679

Obecné nařízení o ochraně osobních údajů neboli GDPR (General Data Protection Regulation) nabylo účinnosti v květnu 2018. Evropské nařízení nahrazuje zákon č. 101/2000 Sb., o ochraně osobních údajů. Cílem je jakési vylepšení a sjednocení právního rámce členských států EU a přizpůsobení dnešní době. Týká se všech subjektů, tedy firem i jednotlivců, kteří zpracovávají osobní údaje a ukládá jim povinnosti, jak s nimi zacházet. [11]

1.2.4 International Organization for Standardization (ISO)

V překladu Mezinárodní organizace pro standardizaci. Řada ISO 27000 je řadou norem, osvědčených postupů, které pomáhají organizacím zlepšit jejich informační bezpečnost. ISO publikovala normy společně s International Electrotechnical Commission (IEC), v překladu Mezinárodní elektrotechnická komise. Organizace spolu vysvětlují, jak realizovat systém řízení informační bezpečnosti. To je systematický přístup k řízení rizik, který se zaměřuje na lidi, procesy a technologie. Série se skládá ze 46 norem, první z nich, tedy ISO 27000 obsahuje definice a základní a klíčové pojmy. Jednotlivé normy cílí na různé aspekty informační bezpečnosti v organizacích

ISO 27001 a ISO 27002 jsou základními normami pro vytvoření bezpečného prostředí v informačních systémech. Lze je aplikovat na organizaci jakékoliv velikosti a v jakémkoliv sektoru. Poskytují ověření a kontrolu stavu bezpečnosti. [12]

2 MOŽNOSTI OCHRANY DAT A INFORMACÍ

V téhle kapitole jsou popsány některé ze základních opatření pro ochranu počítače a dat v něm. Opatření jsou seřazena od hardwarových po softwarové.

2.1 Fyzická ochrana

Jedním ze základních prvků ochrany dat je fyzická bezpečnost. Použití firewallu a antivirového programu je zbytečné, pokud se útočník dostane přímo k zařízení, použije například flash disk a zkopíruje z něj malware nebo ukradne pevný disk. Proto je vhodné zajistit bezpečnost v několika úrovních jako jsou perimetr. To je oblast, která obklopuje chráněná aktiva. V případě rodinného domu můžeme za perimetr považovat pozemek, plot atd.

Další úrovní je kontrola přístupu. Smysl téhle kontroly je zamezit průchodu perimetrem neoprávněným osobám.

Neméně důležitá je vnitřní ochrana, tedy ochrana samotného místa, kde je zařízení uloženo (místnost).

Mechanizmů fyzické bezpečnosti je celá řada, například různé zámky, instalace kamerového systému a elektronického zabezpečovacího systému připojeného na pult centralizované ochrany atd. [4]

2.2 Zálohování

Zálohování je vytvoření kopie dat a jejich uložení mimo médium, na kterém se data původně nacházela. Zálohování se provádí z důvodu ztráty dat, ať už kvůli poruše disku nebo nechtěném smazání, tak napadení zařízení malware, např. ransomware, který data zašifruje.

Typů médií, na které lze data zálohovat existuje několik. Jsou to například CD a DVD, na které data nelze zapisovat opakovaně. V dnešní době už se moc nepoužívají. Flash disky, které jsou malé, a tak se dají uložit prakticky kdekoliv. Externí disky, které jsou vhodné pro zálohování většího množství dat. Další formou jsou cloudové úložiště. Jejich výhodou je, že uživatel má k uloženým datům přístup na jakémkoliv zařízení, které je připojeno k internetu. [13]

2.3 Autentizace

Autentizace spočívá v tom, že daný subjekt musí prokázat, že je opravdu tím, za koho se vydává. Její metody můžou být založeny na několika způsobech:

- Uživatel něco ví – jedná se o nejpoužívanější metodu. Nejčastěji spočívá ve znalosti přihlašovacího jména a hesla.
- Uživatel něco je – tento typ analyzuje biometrické charakteristiky, (otisk prstu apod.). Uživatel se prokazuje tím, že prst přiloží ke snímači.
- Uživatel něco má – tato metoda spočívá ve vlastnictví určitého předmětu, (např. smart card, USB token). Uživatel se prokazuje tím, že předmět použije. Tento typ autentizace využívá kombinaci software a technického vybavení.

Uvedené metody autentizace se můžou kombinovat a tím se bezpečnost ještě zvýší. [5] [14]

„Uživatel něco ví“

Tato metoda je nejčastěji založena na znalosti přihlašovacího jména a hesla. „*Heslo je řetězec znaků, kterým uživatel potvrzuje svou identitu v rámci procesu autentizace*“. [5] Pokud se v řetězci nachází pouze čísla, heslo nazýváme PIN nebo passcode.

Po zadání hesla jej systém porovná s údaji, které má uložené v databázi. Nevýhodou této metody je, že si uživatel heslo musí pamatovat. To může vést k tomu, že si heslo zapíše. Dalším problémem může být volba hesla, které se bude sice dobře pamatovat, ale bude také snadné jej prolomit. Existují také výhody, a to například ta, že se uživatel může přihlásit kdekoliv, protože na počítači nemusí být nainstalován nějaký speciální hardware či software.

Základní kritéria bezpečného hesla jsou jeho délka. Dále by měly být použita velká i malá písmena v kombinaci s číslicemi a speciálními znaky. A ideálně by heslo nemělo mít nic společné s daným uživatelem. [5] [14] [15]

„Uživatel něco je“

Autentizaci založenou na biometrických charakteristikách můžeme rozdělit na tzv. fyziologické charakteristiky. Tam patří například otisk prstu a geometrie ruky. Druhá skupina jsou tzv. behaviorální charakteristiky. Tam patří například dynamika podpisu, rozpoznávání hlasu, atd. Velkou výhodou těchto metod je, že uživatel je nemůže zapomenout jako své heslo. Ovšem může se stát, že přijde o svůj hlas nebo prst.

Nevýhodou téhle autentizace je, že se musí pořídit speciální SW a HW. Další nevýhodou může být spolehlivost, kdy je oprávněnému uživateli přístup odepřen a on musí autentizaci opakovat. [5] [16]

„Uživatel něco má“

Jak bylo dříve zmíněno, princip tohoto typu autentizace spočívá ve vlastnictví určitého předmětu, kterým osoba prokáže, že se opravdu jedná o jeho vlastníka. Hlavní výhodou je, že daný předmět lze obtížně zkopírovat. Klíč na něm bývá většinou uložen a chráněn PINem. Po opakovaném zadání chybného PINu se předmět zablokuje. Je zde riziko, že uživatel může předmět ztratit nebo ho rozbít a také mu může být odcizen.

Tato metoda je náročnější a nákladnější než správa hesel a v běžném životě se s ní nejčastěji setkáme při placení kartou. [5] [14]

2.4 Aktualizace

Všechny programy, včetně operačních systémů nebo internetových prohlížečů, můžou obsahovat a většinou také obsahují chyby. To je důvodem, proč jsou aktualizace z pohledu bezpečnosti tak důležité. Po objevení dané zranitelnosti výrobce vydá aktualizaci, která obsahuje například záplaty nebo hotfixy, tedy opravy objevených zranitelností. Uživatelé by poté měli aktualizaci co nejdříve nainstalovat. Chybou je, pokud na ně zapomínají nebo je dokonce ignorují. [17]

Další problém může být užívání staršího produktu, na kterém se po čase objeví zranitelnost. Výrobce by měl vydat aktualizaci se záplatou, ale protože už vyrábí například nové generace daného zařízení, tak mu není věnována dostatečná pozornost a aktualizace vyjdou po delší době, nebo dokonce nevyjdou vůbec. [18]

2.5 Antivirový program

Jedna ze základních zásad ochrany počítače je užívání antivirových programů, tzv. antivir. Jeho primární úkol je najít viry, a to prohledáním počítače, jeho paměti i všech souborů na pevném disku. Nalezený vir se následně snaží odstranit bez poškození infikovaného souboru. Pokud je to nezbytné, tak smaže celý infikovaný soubor, nebo jej uloží do karantény. Poté již nepředstavuje riziko a nelze jej spustit. Antivirový program chrání počítač po celou dobu, kdy se s ním pracuje.

Jak už bylo řečeno, antivirový program prohledá a zkontroluje všechny spuštěné soubory, i takové, které do počítače přicházejí. Je třeba si uvědomit, že napadení počítače nějakým virem je něco jiného než hackerský útok, proti tomu vás antivir neochrání. Proto je vhodné používat také firewall.

Cena antivirového programu je v dnešní době několik stovek až tisíci korun za rok. [14] [17]

Virové databáze

Virová databáze je při používání antiviru velmi důležitá. Právě za ty se musí předplácet, protože se prakticky neustále aktualizují. Výrobci antivirových programů nabízejí různé balíčky, některé antiviry jsou dokonce zdarma a platí se jen za aktualizace virových databází.

Virové databáze a jejich aktualizace jsou velmi důležité, protože antivir rozpozná pouze ty viry, které zná a pouze ty dokáže odstranit. V případě agresivního viru, který se navíc stále vyvíjí, můžou výrobci antivirů zveřejňovat aktualizace jejich virových databází i každý den.

V případě že si uživatelé stáhnou antivirový program, ale neaktualizují již několikrát zmíněné virové databáze, může to nadělat více škody než užitku. Můžou si totiž myslet, že jejich počítač je dostatečně chráněn. Virus, který vzniknul později, ale antivir neobjeví a uživatelé jsou poté překvapeni, že byl jejich počítač infikován.

2.6 Firewall

Poskytnout bezpečné prostředí je obtížnější i z důvodu, že počítače jsou více vzájemně propojeny prostřednictvím sítí. Dá se říct, že firewall je kontrolní bod nebo vstupní brána pro komunikaci počítače se sítí. Je to tedy prostředek zabezpečení, který chrání interní síť před vnějšími hrozbami. Kontroluje, aby data, jdoucí z počítače, ale i do počítače, byla bezpečná. Jeho úkolem je zabránit neoprávněným průnikům do sítě a vymezit komunikaci, která je považována za bezpečnou a nutnou pro provoz. Naopak komunikace, která nesplňuje tyto „pravidla“, je zakázána. [14] [19]

3 KYBERNETICKÉ ÚTOKY

Tato kapitola se zabývá nejčastějšími kybernetickými útoky, které jsou využívány na získání dat a informací obětí. Je zde popsáno základní rozdělení na útoky plošné a cílené, dále technika, kterou se útočníci svou oběť snaží obelstít. V další podkapitole jsou vysvětleny cesty, kterými jsou kybernetické útoky vedeny, tzv. vektory útoku a poté samotné druhy útoků.

3.1 Plošné a cílené útoky

Většina útoků je v dnešní době vedeno plošně, najdou se ovšem i případy útoků cílených. U plošných útoků se útočníci obecně snaží o to, aby byl útok co nejméně náročný a co nejlevnější. Vědí totiž, že většina pokusů o útok neuspěje. Tím se ovšem nezdržují, protože také vědí, že se časem najde někdo, kdo bezpečnost příliš neřeší nebo je v téhle oblasti nezkušený a „chytne se do pasti“.

Většina útočníků nejsou žádní zkušení hackeři nebo experti na bezpečnost a používají exploity vytvořené někým schopnějším, a proto většinu útočníků odradí zavedení základních opatření. Pokud má útočník možnost využít např. zranitelnosti nultého dne, tak ji raději využije na útok cílený, protože z toho očekává větší výnos. Do cílených útoků na rozdíl od plošných útočníci investují mnohem více peněz a také času. U plošných útoků bývají výnosy zpravidla nižší a počet obětí může být i několik set. Cílené útoky nejsou sice tak časté jako plošné, ale obrana proti nim je složitější.

Následky útoků můžou být například:

- Krádež dat (kontakty, telefonní čísla, e-mailové adresy),
- karetní data (CVV, čísla karet),
- přihlašovací údaje,
- krádež finančních prostředků z účtu (např. pokud z daného počítače firma spravuje své finance). [5] [20]

3.2 Sociální inženýrství

Při kybernetických útocích, především cílených, je často využito technik sociálního inženýrství. Tato technika spočívá v manipulaci, ovlivňování a přesvědčování lidí. Útočník se pomocí metod sociálního inženýrství může snažit o to, aby oběť bez jejího vědomí sdělila nějaké informace, nebo aby udělala to co útočník chce. Osoba, která ovládá tyto

metody, se nazývá sociotechnik. Ten se snaží například vyvolat dojem časového presu a tvrdí, že určitou věc je potřeba provést co nejdříve, aby se snížily škody nebo se vydává za autoritu a snaží se vzbudit dojem důvěry.

Způsob, jakým osloví oběť, může být jakýkoliv, například e-mail nebo SMS. Často se jedná o tzv. spear phishing, tomu se věnuji v jedné z následujících kapitol. [5]

3.3 Vektory útoku

Vektor útoku představuje způsob, kterým dochází k napadení systému uživatele. Forma kompromitace může být za využití škodlivého kódu nebo sociálního inženýrství. [8]

Mezi nejčastější případy patří:

- SPAM a phishing – nevyžádaný e-mail ve kterém je obsažena škodlivá příloha nebo odkaz na její stažení. Může se zde také nacházet odkaz na stránky, které po uživateli vyžadují zadání přihlašovacích údajů.
- Infikované aplikace nacházející se na různých úložištích a marketech.
- Vyjímatelná média, které uživatel například najde nebo můžou být zaslány poštou.
- Webové stránky, na které škodlivý kód vložil jejich provozovatel nebo útočník. Kód bývá v reklamních bannerech nebo přímo na stránce. [5] [21]

3.4 Malware

Malware je název používaný pro škodlivý software. Jeho cíl může být různý a na napadeném zařízení se může různě projevovat. [22] Pro uživatele představuje velký problém z důvodu jeho rozmanitosti. Většina malware má společné to, že se na napadeném zařízení skrývá a snaží se o nějakou persistenci (tj. aby přežil restart počítače.) Existuje několik způsobů, kterými může být malware doručen na koncové zařízení. Říká se jim vektory útoku a většinou je potřebná aspoň minimální součinnost ze strany oběti. [14]

3.4.1 Rozdělení podle vektoru útoku

Drive – by download malware – při jeho stažení nemusí uživatel na nic klikat, stačí pouze návštěva infikované stránky.

Phishing – malware bývá doručen jako příloha e-mailu. Phishingové zprávy můžou vypadat jako zprávy od důvěryhodných organizací, ve skutečnosti se ale jedná o podvod.

Po kliknutí na odkaz v emailu budete přesměrováni na falešné stránky, kde se z vás útočníci budou snažit dostat citlivé informace, např. hesla.

Trojanizovaná aplikace – ta se může nacházet na oficiálním i neoficiálním marketu nebo na nějakém úložišti, i přenosném médiu. Jejich podstata jsou skryté funkce, s kterými uživatel nesouhlasí a neví o nich.

3.4.2 Rozdělení podle způsobu šíření

Virus – kód, který kopíruje sám sebe do spustitelného souboru. Šíří se při spuštění infikovaného souboru, a to tak že se zapíše do dalšího spustitelného souboru. Tuto operaci dokáže antivirus snadno detekovat, a proto v dnešní době virus představuje spíše menší hrozbu.

Macrovirus – kód napsaný v jazyce VBA, který kopíruje sám sebe do dalších souborů aplikace MS Office. Stejně jako virus může být snadno detekován antivirem, proto se s tímto typem viru často nesetkáváme. Macrovirus může být také využíván jako tzv. dropper, který slouží ke stažení dalšího malware.

Worm (červ) – program, který posílá sám sebe přes e-mail na další adresy nebo se šíří po síti tím, že vyhledává další stroje a zneužívá jejich zranitelnost, např. absenci nebo užití slabých hesel nebo neaktualizovaného SW a sám sebe tak kopíruje po síti.

Trojan horse (Trojský kůň) – tváří se jako aktualizace, např. prohlížeče, hry apod., nebo užitečná aplikace, která se do počítače dostává nejčastěji tak, že si ji uživatel sám stáhne a nainstaluje, ale na pozadí provádí škodlivou činnost. Jedná se například o dialery, které volají na zpoplatněná čísla, keyloggery, které odchytávají hesla, screengrabbery, které zaznamenávají dění na obrazovce.

3.4.3 Rozdělení podle projevů

Spyware – špionážní software, který přes internet odesílá informace o uživateli. Do počítače uživatele se nejčastěji dostává s jinou aplikací, která je trojským koněm. Časté jsou i případy, kdy je sbírání, odesílání a využití citlivých informací o uživateli zmíněno v licenčním ujednání, které při instalaci téměř nikdo nečte. Mezi spyware patří také keylogger, který snímá otisky kláves.

Scareware – falešný antivir. Doporučení na jeho stažení se zobrazí při surfování po webu v okamžiku, kdy navštíví infikovanou stránku.

Ransomware – vyděračský software, který zašifruje data na disku a heslo uživateli sdělí poté, co zaplatí výkupné.

Adware – reklamní software, který zobrazuje nežádoucí reklamu. Často legální způsob, jak může autor aplikace získat zpět aspoň část prostředků. Může být spojen například se spyware.

Backdoor – zadní vrátka do systému umožňující neoprávněný přístup. V systému jsou zanechány kvůli pozdějšímu přístupu.

Logical bomb (logická bomba) – aplikace, které čeká na splnění předem určitých podmínek.

Rootkit – malware skrývající se před detekcí, stává se součástí systému a umožní ho vzdáleně ovládat.

Banking malware (bankovní malware) – tento malware se rozšířil v posledních letech, kdy se více a více používá internetové bankovnictví. Malware krade přihlašovací údaje do internetového bankovnictví. [17] [5] [22]

Cryptominer – jedná se o relativně nový pojem. Cryptominer využívá výpočetního výkonu počítače k těžbě kryptoměny, aniž by o tom uživatel věděl. [23]

3.5 Spam

Nejčastěji se spam popisován jako jakýkoliv nevyžádaný e-mail. Tedy takový e-mail, u kterého se uživatel nepřihlásil k jeho odběru. [24] Spam může tvořit až 95 % přijaté pošty. Nejčastěji se jedná o nějaké reklamní nebo obchodní sdělení, může ale obsahovat i viry, trojské koně atd. [22] Většina spamu bývá zachycena nějakým antispamovým filtrem, na ten se ale nejde na 100 % spolehnout. Jako spam tak může být vyhodnocena nezávadná zpráva, nebo naopak filtr spam nepozná. Spam můžeme rozdělit na reklamní spam, HOAX a phishing. [5]

Reklamní spam

Nejčastější druh, obsahuje nějaké obchodní sdělení. Například propaguje určitý výrobek. Tento druh spamu může být spojen s další nelegální aktivitou, kdy příjemce na nabídku zareaguje a výrobek objedná, může mu být doručen padělek, nebo v případě platby předem bude okraden. [5] [25]

HOAX

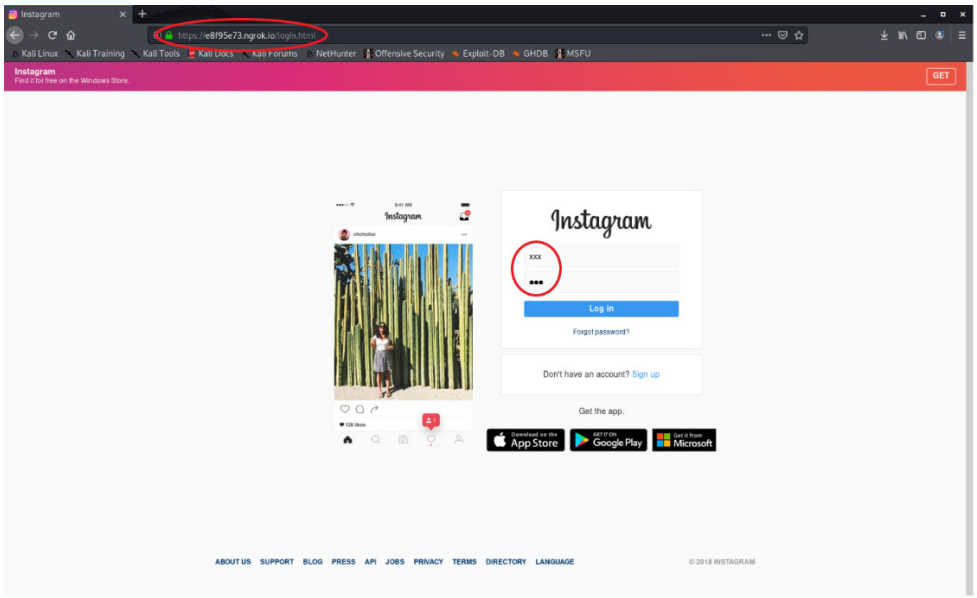
Jako HOAX jsou označovány nepravdivé a poplašné zprávy, k jejichž šíření napomáhají její příjemci, kteří je šíří dál. Takové zprávy nejčastěji varují před neexistující hrozbou. [26] Autoři se také často zaštiťují nějakou autoritou (např. Microsoft), která údajně vydala prohlášení o dané hrozbě. Šíření řetězových zpráv je škodlivé také proto, že dochází k přenášení seznamu aktivních e-mailových adres, které můžou být zneužity k šíření dalšího spamu. [5] [27]

3.6 Phishing

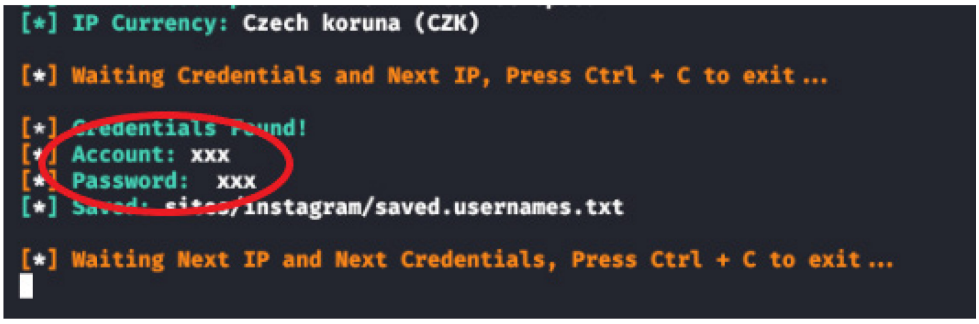
Dal by se přeložit jako rybaření. Útočník použije návnadu v podobě e-mailu, ve kterém se nachází příloha nebo odkaz. Ten obsahuje malware, nebo uživatele přesměruje na podvodné stránky, kde je požadováno vyplnění přihlašovacích údajů (např. internetové bankovnictví nebo sociální sítě). Návnada by měla vypadat natolik dobře, že na ni oběť klikne. Je zde využíváno technik sociálního inženýrství. [22] [25]

Phishing je velmi častý způsob, jak útočník dostává škodlivý kód do zařízení oběti nebo se z ní snaží vylákat informace, které může zneužít.

Na obrázku č. 1 je názorná ukázka, jak může vypadat podvodná stránka. Jedná se o falešnou stránku sociální sítě Instagram. Obrázek č. 2. ukazuje zaslané přihlašovací údaje útočníku poté, co se oběť pokusila přihlásit. K ukázce byl použit nástroj ShellPhish, určený pro vzdělávací účely.



Obrázek 1 – Podvodná stránka [Zdroj: vlastní]



Obrázek 2 – Přihlašovací údaje [Zdroj: vlastní]

V posledních letech se phishing natolik zlepšil, že ho i experti mají problém rozpoznat. V nedávné době proběhly phishingové kampaně a e-maily chodily od známých odesilatelů, měly bezchybnou češtinu a někdy byly dokonce příjemcem očekávány. Takhle sofistikovaná kampaň by se dala nazvat jako spear phishing.

E-Mail odeslaný konkrétní osobě bývá těžko zachycen antishipingových filtrem, protože se nerozesílá ve velkém množství jako je to u phishingu. [5] [28]

Rozdíly mezi phishingem a spear phishingem

Tabulka 1 – Rozdíly mezi phishingem a spear phishingem [5]

PHISHING	SPEAR PHISHING
Rozeslání e-mailu na větší počet adres.	Zaslání e-mailu jednomu příjemci.
V e-mailu se nachází internetový odkaz.	E-Mail neobsahuje internetový odkaz.
E-Mail přijde od osoby nebo firmy, kterou znáte.	E-Mail přijde od osoby nebo firmy, kterou znáte.
Je považováno zadání určitých údajů.	Není požadováno zadání žádných údajů.
Někdy obsahuje neúmyslné chyby.	E-Mail neobsahuje neúmyslné chyby.
E-Mail zpravidla neobsahuje přílohu.	E-Mail zpravidla obsahuje přílohu.
Cílem je získání přihlašovacích či osobních údajů.	Cílem je získání citlivých informací, které jsou předmětem duševního vlastnictví.

3.7 Pharming

Pharming je v podstatě sofistikovanější forma phishingu. Jedná se o podvodný útok, jehož cílem je oběť přesměrovat na falešné webové stránky, které jsou často k nerozeznání od originálních. Nejčastěji se jedná o stránky internetového bankovnictví uživatele. [29] Útok

spočívá v napadení DNS, kde dochází k přepsání domény na IP adresu. Oběť do internetového prohlížeče zadá adresu webové stránky, kterou chce navštívit, poté ale nedojde k propojení na IP adresu originálního webu, ale na webovou stránku podvrženou. V případě přihlášení do internetového bankovnictví na podvržených stránkách útočník získá citlivé informace, jako jsou právě přihlašovací údaje.

Dalším způsob pharmingu využívá malware a napadá počítač koncového uživatele. Malware změní soubor hostitelů a po zadání adresy cílené webové stránky odkloní přenos na stránky falešné. [22] [30]

3.8 Hacking

Hacking se dá obecně charakterizovat jako vstup do systému počítače nestandartní cestou. Forem nestandartní cesty je několik, může se jednat například o prolamování hesel, využití malware nebo sociálního inženýrství. Osoba, která tuhle činnost provádí se nazývá hacker. To je většinou někdo s dobrými znalostmi fungování informačních systému, často to jsou také dobří programátoři. Jejich činnost ovšem nemusí být vždy nelegální. Právě podle motivace je můžeme rozdělit do tří skupin. První skupinou jsou tzv. White hats. Tuto skupinu lze považovat za tu „hodnou“, protože nezpůsobují žádnou škodu, právě naopak. Jsou často placeni společnostmi, aby hledali slabá místa v jejich systému a následně provedli bezpečnostní opatření, aby k podobným útokům nedošlo. Druhou skupinou jsou tzv. Black hats, kteří jsou v podstatě opak White hats. Jejich motivací je jakékoliv poškození uživatele napadeného systému. Třetí skupinou jsou tzv. Gray hats. To je skupina, které je svým chováním mezi předešlými dvěma, občas poruší nějaký zákon, ale jejich motivací není prvoplánově někoho poškodit. [22] [31]

3.9 Cracking

Širokou veřejností bývá často zaměňován s hackingem. Jedná se o prolamování nebo obcházení bezpečnostních prvků počítačového systému, aplikací nebo programů. Motivací crackingu je jejich následné neoprávněné užití. Za crackcing považujeme také porušení autorských práv, tedy jednání, při kterém dochází k prolomení prvků zabraňujících vytváření kopií filmů, počítačových her atd. Další častá forma crackingu je „password cracking“, tedy zjišťování a prolamování hesla. To můžeme rozdělit do několika kategorií. [22] [32]

Odpozorování hesla – při zadávání hesla by měl být uživatel obezřetný. První a nejjednodušší způsob, jak odpozorování zabránit, je užívání zástupných znaků (nejčastěji hvězdičky). Ještě bezpečnější způsob ovšem je, aby se na obrazovce nezobrazovali znaky žádné. To útočníku zabrání vidět délku řetězce. V tomto případě útočníkovi nezbývá, než poslouchat kolik kláves bylo stisknuto nebo přímo odpozorovat na jaké klávesy uživatel kliknul. I pokud se ve vaší blízkosti nikdo nenachází, tak vaše heslo může být přesto odpozorováno například použitím kamery. Tomu lze zabránit zadáváním pouze některých znaků. Například když vás systém vyzve k zadání znaků, které jsou na první, čtvrté a osmé pozici hesla. Při dalším přihlášení by se jednalo o jiné pozice.

Zcizení hesla – dobré je se vyhnout zapisování hesel. Jsou případy, kdy si uživatelé svá hesla napíší na lísteček a ten přilepí například pod klávesnici nebo na obrazovku. Pokud je potřeba si heslo napsat, například z důvodu, že si jej nepamatujete, mělo by být uloženo na bezpečném místě (trezor).

Odchycení hesla na software úrovni – uživatel se může přihlásit na počítač, na kterém je nainstalován keylogger. Ke snížení rizika odchycení hesla lze užít například virtuální klávesnici, která se zobrazí na monitoru a uživatel na ni píše myší. Existují i speciální keyloggery, které jsou spojeny s obrazovkou a to tak, že z ní vyfotí screen i s pozicí kurzoru. Útočník tak vidí, na jaký znak uživatel myší kliknul.

Odchycení hesla na hardware úrovni – v tomto případě je potřeba aby měl útočník k danému zařízení fyzický přístup a umístil tak keylogger v podobě malého zařízení na klávesnici nebo na kabel vedoucí do počítače. Ochrana proti tomuto způsobu odchycení je snadná, ale otravná, a proto ji málo koho napadne provést. Vniknutí do počítače lze zabránit např. použitím zámku.

Uhádnutí hesla – uživatel by měl svá hesla volit taková, aby nešla lehce uhádnout. Existuje několik útoků, kterými se o to útočník může pokusit. Jedním z nich je slovníkový útok, kterým se zabývám v praktické části v kapitole 4. [5] [33]

3.10 Sniffing

Sniffing se dá popsat jako odposlech komunikace mezi počítači v lokální síti. Při využití téhle techniky dochází k odchytávání, ukládání a čtení paketů. Program, který odposlouchává síťovou komunikaci, se nazývá sniffer. Sniffing má využití při provádění diagnostiky sítě, lze ale využít i k nelegálním činnostem jako jsou například získání

uživatelských jmen a hesel nebo informací o používaných službách. Získané informace můžou být použity v realizaci dalšího útoku. Ke sniffingu může být využit také škodlivý kód, často se jedná o trojského koně. [32] [34]

3.11 Man in the middle

V překladu muž uprostřed. Jak název napovídá, jedná se o kybernetický útok, jehož podstatou je, že se útočník dostane mezi dvě zařízení, které spolu komunikují a komunikaci následně zachytí nebo upraví.

Častým cílem bývá komunikace mezi webovým prohlížečem a webovým serverem, ale útoky můžou být cíleny také například na e-mailovou komunikaci. Útočník může také získat uživatelovi přihlašovací údaje, pokud zacílí na komunikaci mezi uživatelem a webem, který chce navštívit. Toho lze dosáhnout zacílením na HTTP spojení mezi uživatelem a daným webem. „Únos“ tohoto spojení umožní útočníkovi jednat jako proxy, shromažďovat a upravovat informace odesílané mezi uživatelem a webem.

Útoky man in the middle mohou také cílit na servery DNS. Proces vyhledávání DNS je to, co umožňuje webovým prohlížečům najít webové stránky převedením doménových jmen na IP adresy. Útočník tedy může uživatele přesměrovat na weby, které obsahují malware. [35]

II. PRAKTICKÁ ČÁST

4 SLOVNÍKOVÝ ÚTOK

Slovníkový útok je jedna z nejjednodušších metod crackingu. Jeho cílem je uhádnutí hesla pomocí slovníku. To je jakýsi seznam možných hesel. Útočník může svůj slovník vytvořit mnoha způsoby. Jedním z nich je použít jako základ obyčejný slovník. Další variantou může být využitím seznamu nejčastěji používaných hesel. Tyto varianty může různě kombinovat, například vytvořit heslo z více slov, nebo ke slovům přidávat číslice a jiné znaky. Útočník může také sestavit svůj slovník podle zjištěných informací o uživateli (jméno, datum narození atd.), jehož heslo se snaží prolomit. Pro zvýšení pravděpodobnosti uhádnutá hesla se používají slovníky v mateřském jazyku oběti. Čím větší počet možných hesel útočník slovník obsahuje, tím se zvětšuje pravděpodobnost, že heslo uhádne. Tím se ale také zvyšuje čas potřebný pro zjištění hesla. [36]

4.1 Vybavení počítače

Realizace slovníkového útoku byla provedena na stolním počítači s následujícím hardwarovým a softwarovým vybavením.

Hardware

- Základová deska – GIGABYTE GA – H55M – S2H.
- Procesor – Intel Core i3 – 530. Disponuje dvojicí fyzických jader. Jejich pracovní frekvence je 2,93 GHz. Vyrovnávací paměti, 4 MB u procesoru a 256 kB u jader. Obsahuje integrované grafické jádro Intel GMA HD, které je taktováno na 733 MHz.
- Pracovní paměť (RAM) – DDR 2, 4096 MB.
- Grafická karta – Saphire HD 5770, 512 MB.

Software

- Operační systém – Kali Linux 2020.1, 64 bit, desktopové prostředí XFCE 4.14.2.

4.2 Realizace slovníkového útoku

Tato kapitola praktické části se bude zabývat uhádnutí hesla pomocí slovníkového útoku. K útoku byl použit jeden z mnoha penetračních nástrojů operačního systému Kali Linux nazvaný Hydra.

Byly uskutečněny 2 útoky na zjištění hesel. První z nich byl cílen na e-mailový účet se slabým heslem, zatímco druhý na účet se silným heslem. Oba útoky vycházely z předpokladu, že útočník znal e-mailové adresy obětí.

Pro provedení útoků jsem tedy vytvořil dvě e-mailové adresy na internetovém serveru Seznam. Pro první účet jsem zvolil adresu „kalitest1@seznam.cz“ s heslem „kalilinux1“. Pro účet druhý byla zvolena adresa „kalitest2@seznam.cz“ s heslem „kalilinux2“.

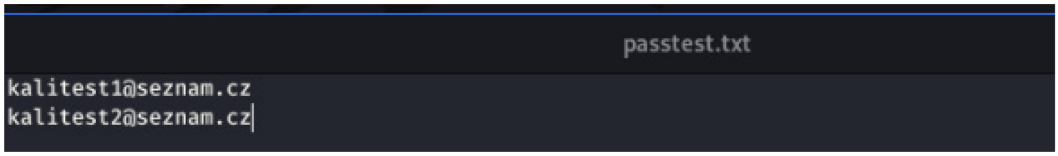
4.2.1 Kali Linux a penetrační nástroj Hydra

Kali je Linuxová distribuce založená na Debianu, vyvíjená a financovaná společností Offensive Security, které poskytuje školení v oblasti bezpečnosti informací. Byl vydán v březnu roku 2013 jako kompletně vylepšená obdoba systému BackTrack a je zcela zdarma. I to je důvodem, proč se stal tak oblíbeným. Kali Linux se zaměřuje na penetrační testy a bezpečnosti audit. Obsahuje spoustu nástrojů, které jsou zacíleny na úkoly související s bezpečností informací. Patří mezi ně například hardware hacking, sniffing a spoofing, útoky na heslo, ale také zátěžové testování, sběr informací, analýza zranitelností atd. Obsažených nástrojů je více než 600. [37]

Hydra je určená k prolamování přihlašovacích údajů. Je velmi rychlý, flexibilní a lze do něj přidat nové moduly. Nástroj Hydra je určený k výuce a umožňuje ukázat, jak snadné může být získání neoprávněného přístupu na dálku. Autory jsou Van Hauser a Roland Kessler. [38]

4.2.2 Příprava útoku

K provedení útoku pomocí nástroje Hydra je potřeba mít již zmíněné e-mailové adresy, které útočník může získat několika způsoby, například použitím nelegální databáze nebo jednoduchým prohledáním sociálních sítí a jiných internetových stránek. Mé dvě testovací e-mailové adresy jsem napsal do textového dokumentu a uložil (obr. 3).

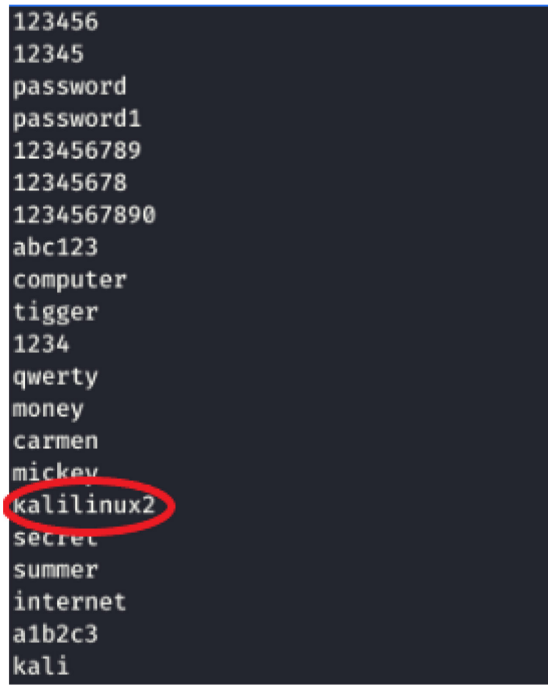


Obrázek 3 – E-mailové adresy [Zdroj: vlastní]

Potřeba je také databáze hesel (slovník). Ty se dají vytvořit nebo i volně stáhnout. Mohou obsahovat tisíce možných hesel. V mém případě jsem použil soubor s hesly, který již

v systému byl, právě pro podobné testovací účely. Jednalo se taktéž o obyčejný textový dokument.

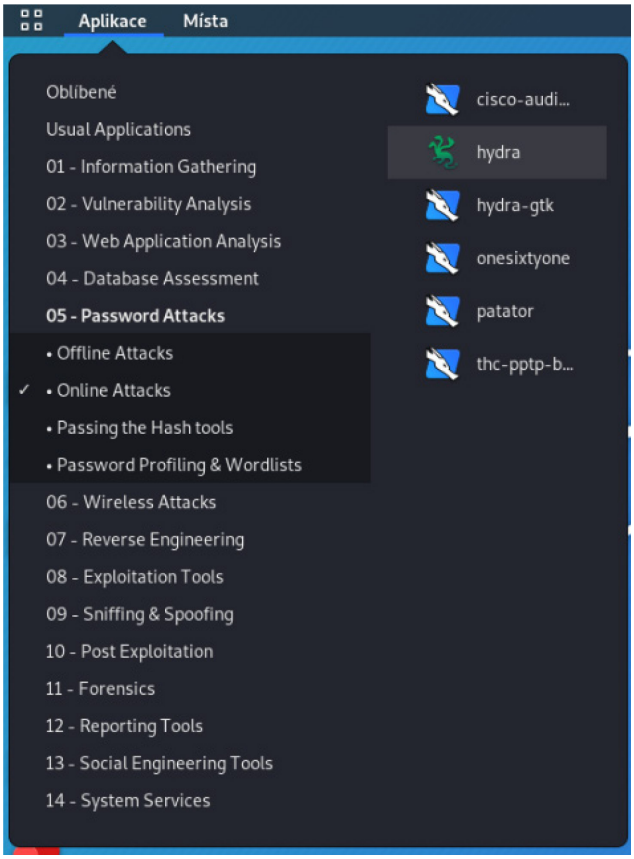
Pro oba e-mailové účty jsem zvolil podobná hesla, předpokládejme ovšem, že vlastník účtu „kalitest1@seznam.cz“ své heslo zvolil správně, tedy dostatečně silné. Vlastník účtu „kalitest2@seznam.cz“ naopak zvolil slabé heslo, které se nachází v útočníkovu seznamu častých hesel (obr. 4).



Obrázek 4 – Seznam hesel [Zdroj: vlastní]

4.2.3 Spuštění a nastavení penetračního nástroje Hydra

Hydra je v systému od samého začátku a k jejímu spuštění stačí rozkliknout menu „Aplikace“, poté položku číslo 5., která nese název „Password Attack“. Dále se zobrazí menu, ve kterém je potřeba vybrat „Online Attack“. To zobrazí nabídku několika nástrojů pro prolamování hesel (obr. 5).



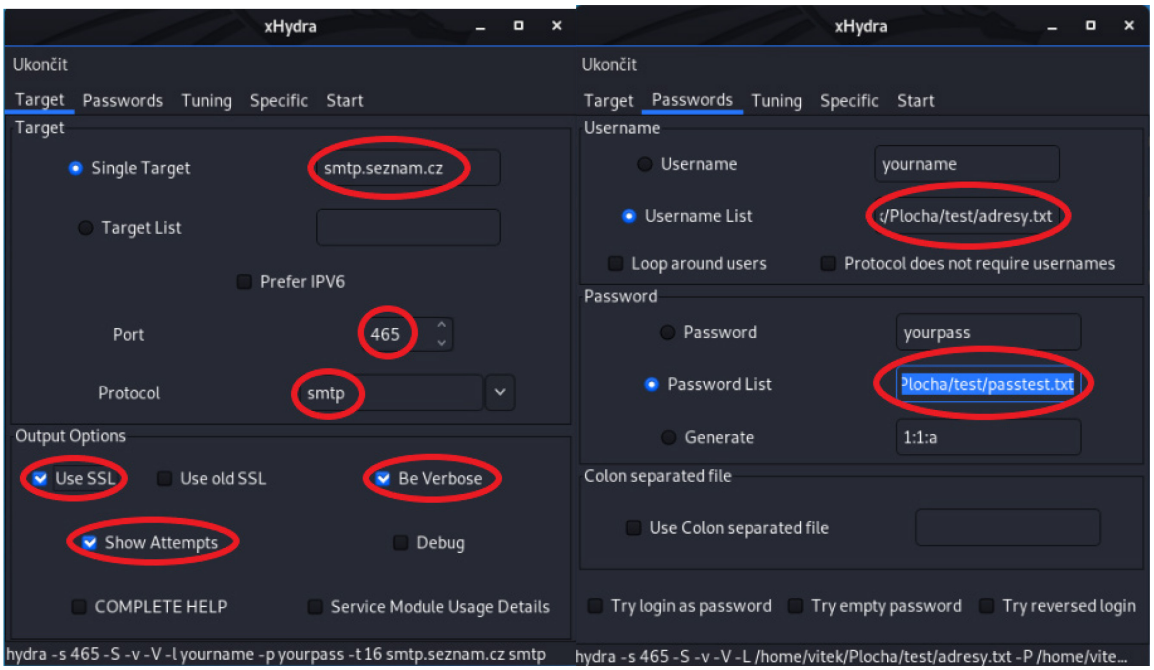
Obrázek 5 – Spuštění nástroje Hydra [Zdroj: vlastní]

Po kliknutí na ikonu s názvem „hydra – gtk“ se nástroj spustí a na obrazovce se otevře grafické rozhraní s jeho nastavením.

Dalším krokem bylo samotné nastavení nástroje Hydra, kde bylo nutné vyplnit údaje „Targer“ neboli cíl, dále port a také protokol. Po rozkliknutí možnosti výběru protokolu jsem zvolil „Simple Mail Transfer Protocol“ (SMTP). To je internetový protokol, který zajišťuje přenos elektronické pošty mezi odesilatelem a adresátem. [39] Číslo jeho portu je 465. Cílem byl server pro odchozí poštu, který má adresu „smtp.seznam.cz“. Všechny tyto údaje jsou dohledatelné na stránkách Seznamu. Vyžadováno bylo také zaškrtnutí „Use SSL“. SSL je protokol šifrující komunikaci mezi klientem a serverem. Také zaručuje identifikaci, klient i server má tedy jistotu, že komunikují opravdu spolu. To znemožňuje

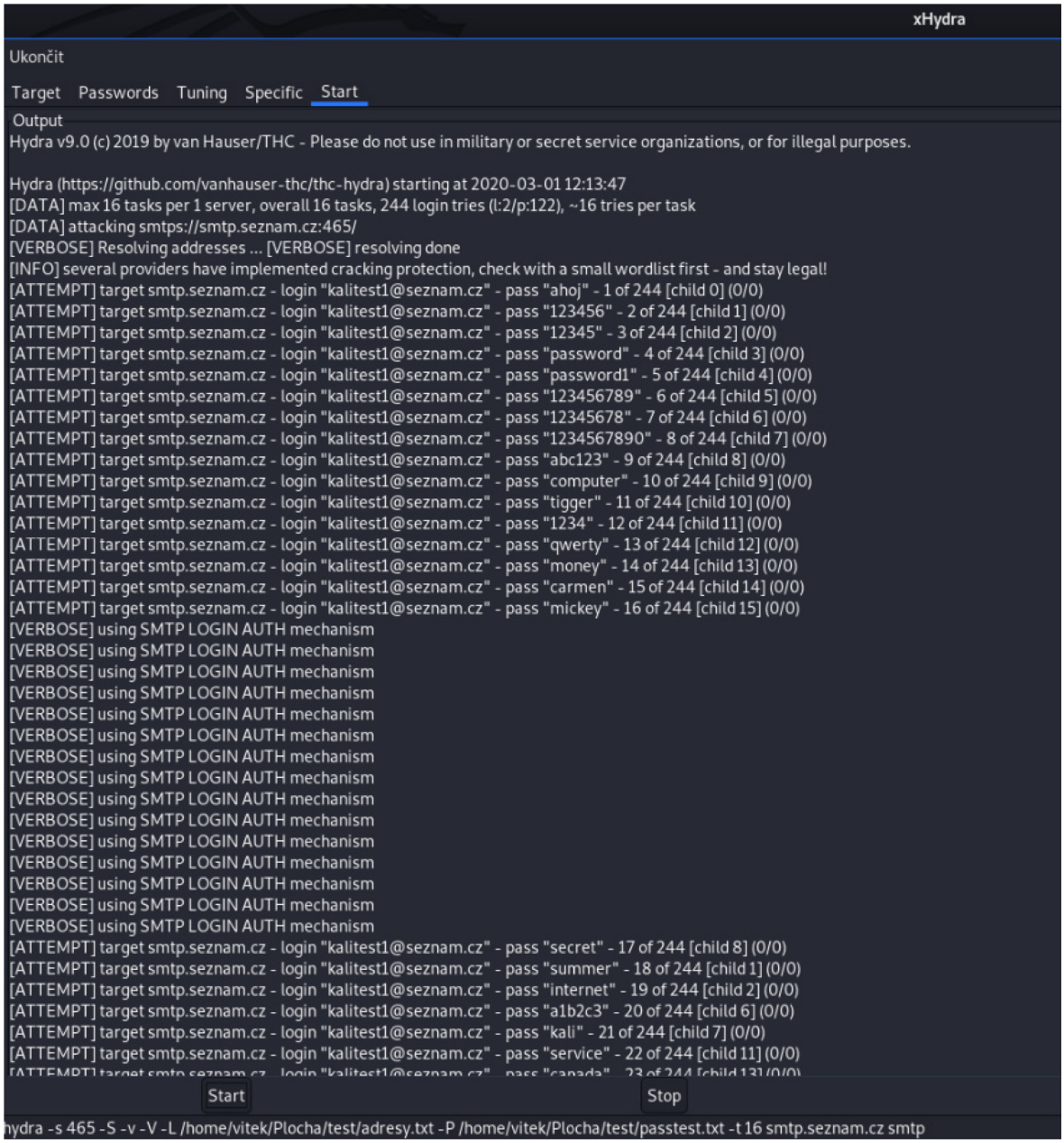
odposlouchávání komunikace a také to, že do ní nemůže nikdo vstoupit a vydávat se za jednoho z jejich původních účastníků. [40]

Zaškrtnutím „Be Verbose“ a „Show Attempts“ jsem aktivoval podrobný režim, kde Hydra zobrazí každý pokus uhádnutí hesla (obr. 7). Druhá část nastavení nese pojmenování „Passwords“. V tomto kroku si uživatel Hydry může vybrat, zda se pokusí prolomit přihlašovací údaje k jednomu, nebo více účtům. V případě útoku na jeden konkrétní cíl je do kolonky „Username“ potřeba napsat e-mailovou adresu oběti. Já jsem se ale rozhodl provést dva útoky najednou, a proto jsem zaškrtl „Username List“. Místo vepsání jedné adresy je nutné vložit cestu k adresáři, který jich obsahuje několik, v mém případě dvě. Dalším krokem bylo zaškrtnutí „Password List“ a vložení cesty k adresáři s hesly.



Obrázek 6 – Nastavení nástroje Hydra [Zdroj: vlastni]

Poté nezbývalo než samotný útok aktivovat tlačítkem „start“. Nejprve se objevilo upozornění, že penetrační nástroj nelze používat k nelegálním účelům a po pár sekundách program začal svou činnost. Zobrazil čas zahájení útoku a poté načetl první e-mailovou adresu z adresáře a postupně na ni začal zkoušet všechna hesla z načteného adresáře s hesly. Na obrázku č. 9 lze vidět, jak Hydra postupně zobrazuje jednotlivé pokusy uhádnutí hesla.

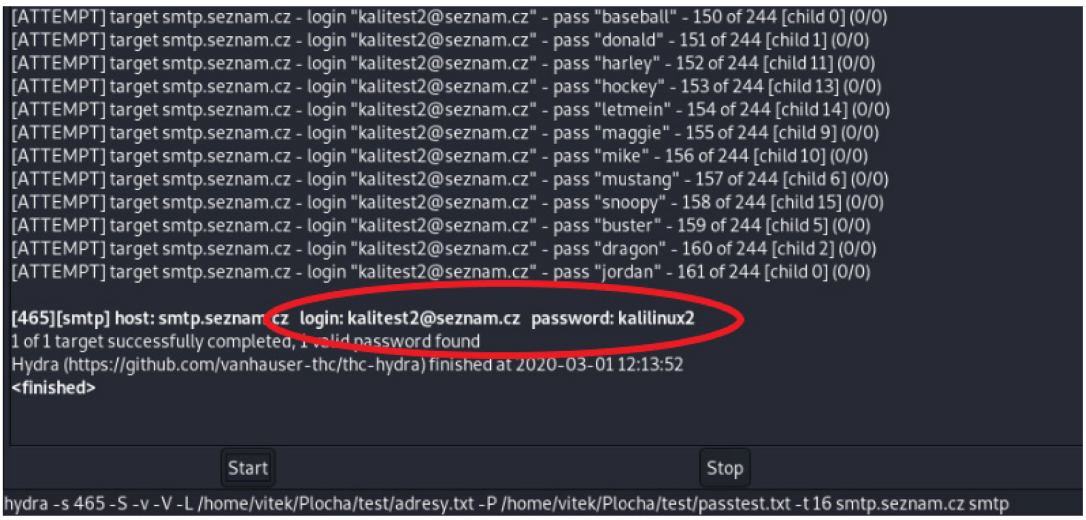


Obrázek 7 – Start činnosti nástroje Hydra [Zdroj: vlastní]

Hydra byla v počáteční fázi útoku neúspěšná, protože heslo pro login „kalitest1@seznam.cz“ se ve slovníku nenacházelo. Po vyzkoušení všech hesel a neúspěšném hledání, program automaticky načetl další e-mailovou adresu z vložené databáze, tedy „kalitest2@seznam.cz“ a začal opět zkoušet všechna hesla z adresáře viz. obr. 10.

Obrázek 8 – Změna adresy [Zdroj: vlastní]

Jelikož v databázi s e-mailovými adresami byly adresy pouze dvě, tak nástroj po vyzkoušení všech hesel ukončil svou činnost a zobrazil výsledek. A to takový, že bylo úspěšně nalezeno jedno heslo, a to k e-mailové adrese „kalitest2@seznam.cz“ (obr. 11).



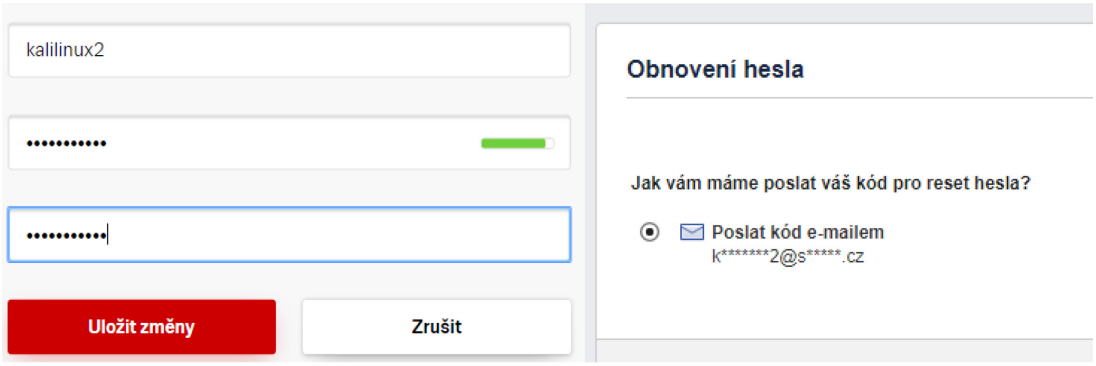
Obrázek 9 – Výsledek hledání hesel [Zdroj: vlastní]

Pokud takhle útočník zjistí heslo k e-mailové schránce u které si uživatel nenastavil dvoufázové ověření identity, tak k ní má plný přístup. Dvoufázové ověření je opatření, které chrání účet před neoprávněným přihlášením. Může mít několik podob. Například zasláním SMS s kódem. Podstatou je, aby každé ověření proběhlo jiným způsobem. K přihlášení tedy nestačí znát pouze heslo, ale je potřeba se prokázat dalším ověřením, kterým může být již zmíněný kód v SMS. [41]

4.3 Následky uhádnutí hesla

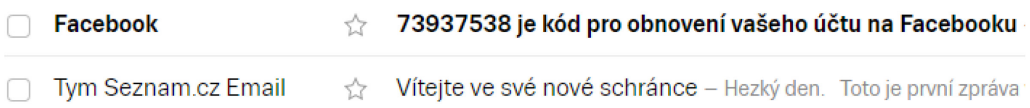
Problémů, které lze prostřednictvím e-mailového účtu způsobit je celá řada. Útočník po přihlášení do e-mailové schránky „kaliltest2@seznam.cz“ může změnit heslo a tím původnímu majiteli zabrání se později přihlásit. Změna hesla není nijak složitá, jelikož útočník zná původní heslo, stačí mu na to pár sekund, viz obr. 10. Poté má dostatek času na procházení a čtení e-mailů.

Prostřednictvím nabouraného e-mailu lze také změnit hesla k jiným účtům oběti. Může se jednat například o sociální sítě jako je Facebook. Útočník zadá e-mailovou adresu, na kterou se naboural a nechá si na ni zaslat kód, kterým prokáže, že se opravdu jedná o vlastníka účtu. (obr. 10).

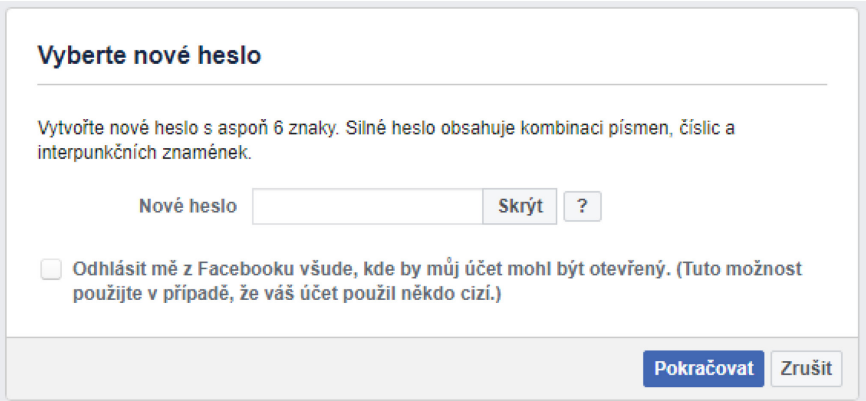


Obrázek 10 – Změna hesla [Zdroj: vlastní]

Po přijetí kódu do e-mailové schránky (obr. 11) jej útočník zadá a poté mu nezbývá nic jiného, než heslo změnit za své (obr. 12).



Obrázek 11 – Přijatý kód pro obnovení účtu [Zdroj: vlastní]



Obrázek 12 – Změna Facebookového hesla [Zdroj: vlastní]

Z prolomeného e-mailového, i Facebookového účtu lze odesílat zprávy se škodlivým kódem, odkazy na podvodné stránky atd. lidem, kteří můžou být přátelé oběti, a proto nejsou ostražití při otevírání přijatých příloh. Netuší totiž, že na účet jejich kamaráda se někdo naboural.

Původnímu vlastníkovi lze uškodit i dalšími způsoby. Představa, že se oběť například uchází o pracovní místo a útočník jejímu možnému budoucímu zaměstnavateli odepíše, že o pracovní pozici už nemá zájem, se někomu může zdát jako dobrý žert, ale dané osobě to může dost znepříjemnit život.

4.4 Volba silného hesla

Jak už bylo zmíněno, volba silného hesla je jedno ze základních bezpečnostních opatření a není dobré jej brát na lehkou váhu. V předchozí kapitole jste mohli vidět, jak snadné pro útočníka může být získání přihlašovacích údajů pomocí jednoho z nejjednodušších útoků a tím je slovníkový útok.

Prvním aspektem siného hesla je jeho délka. Dá se říct, že čím delší heslo, tím je složitější jeho prolomení. Dostatečně silné heslo by mělo mít alespoň 15 znaků. Počet znaků ovšem není jediné kritérium, které heslo dělá velmi obtížně prolomitelným. Velmi špatnou volbou jsou znaky, které jdou po sobě na klávesnici. Například „123456789“ nebo „qwertz“ jsou velmi dobře známe kombinace, a právě taková hesla se nachází na prvních místech v seznamech hesel útočníka. Heslo by se také nemělo skládat z obyčejných slov, které se nachází ve slovnících. Nejlépe když se heslo skládá z více slov, tím značně snížíte pravděpodobnost uhádnutí právě pomocí slovníkového útoku.

Pokud by se útočník zaměřil na konkrétní oběť, využil by všechny informace, které o ní zná. To je důvodem proč by heslo nemělo obsahovat uživatelovy osobní údaje, jako jsou např. jméno a datum narození.

Při volbě silného hesla je potřeba být kreativní a volit různé kombinace znaků. Tedy kombinaci velkých a malých písmen, číslic a jiných, například speciálních znaků. Opatrní musíme být také při používání běžných náhrad znaků, tj. záměny písmen za podobně vypadající číslice a naopak. Například ve slově „PROSIM“ lze následovně nahradit písmena O, S, I za číslice „PR051M“. S tímhle některé nástroje na crackování počítají a útočník vaše heslo tedy stejně prolomí. [42]

Dodržením všech popsaných kroků byste měli zvolit dostatečně silné heslo, které se útočníku pomocí slovníkového útoku nepodaří uhádnout.

Na internetové stránce nazvané „Have I Been Pwned?“ je možné porovnat své heslo s databází uniklých hesel. Stránku vytvořil bezpečnostní expert Troy Hunt a vydal databázi, která obsahuje hesla z většiny podstatných úniků dat. V té se nachází více než 555 milionů hesel. Po zadání svého hesla bude porovnáno s databází. Tak se dozvíte, zda se v některém z úniků nacházelo a pokud ano, je potřeba jej změnit. [43]

4.5 Správce hesel

V dnešní době uživatelé používají nejrůznější služby, ke kterým se musí přihlásit. Může se jednat například o e-mailovou schránku nebo sociální sítě. Pokud dodržují pravidla o správném nakládání s hesly, tedy pro každý účet používají jiné a volí je dostatečně silné, může být problém si je všechny pamatovat. Řešením může být správce hesel. To je program, který hesla uživatele uloží do bezpečné zašifrované databáze. Do přístupu k ní si zvolí jedno silné hlavní heslo. Funkce různých správců hesel se můžou lišit. Ty nejlepší dokážou analyzovat zvolená hesla a podávat informace o jejich síle. Dokážou také vygenerovat dostatečně silné a originální heslo a uživatel tak má o starost míň s jeho vymýšlením. Správce hesel po zadání hlavního hesla může automaticky vyplit formulář pro přihlášení. Podstatou správce hesel tedy je, že je nutné si pamatovat pouze jedno hlavní heslo, kterým získáte přístup ke svým ostatním. [44]

5 AKTUÁLNÍ STAV

Součástí praktické části je analyzování bezpečnostní úroveň zabezpečení dat uživateli osobních počítačů. Informace byly použity z veřejných statistik týkajících se bezpečnosti dat a obecně ICT.

5.1 Podnikatelský prostor

V dnešní době informačních a komunikačních technologií je k internetu připojeno velké procento firem s více než 10 zaměstnanci. V roce 2019 měla většina podniků (83 %) své webové stránky. V posledních letech také roste trend využívání sociálních sítí, jako jsou například Facebook, Instagram atd. Firem v České republice s více než 10 zaměstnanci, které vlastní účet na některé ze sociálních sítí je téměř polovina (45 %). Firmy se na sociálních sítích snaží prezentovat, ale i hledat nové zaměstnance. Velkých firem s profilem na sociálních sítí zde hledalo nové pracovníky až 90 %. S používáním těchto sítí a celkově s přesunutím své činnosti na internet samozřejmě stoupá riziko bezpečnostního incidentu.

V roce 2019 byla zjišťována bezpečnost ICT v podnikatelském sektoru. Bylo zjištěno, že za rok 2018 se alespoň s jedním bezpečnostním incidentem setkala pětina firem v Česku. Mezi nejčastější incidenty patřila nedostupnost služeb ICT, např. útoky typu ransomware a Denial of Service (DoS).

Mezi další bezpečnostní incidenty se řadilo poškození nebo zničení dat, ke kterému může dojít neoprávněným přístupem nebo infikováním malware. S tímto problémem se setkalo asi 10 % firem, největší podíl mají velké subjekty, těch bylo 17 %.

Mezi útoky, zaměřené nejčastěji na zaměstnance firmy můžeme zařadit phishing a pharming. Jejich cílem je zaměstnance oklamat a získat důvěrné informace. Tyto útoky byly poměrně vzácné, pouze 1 % malých firem a 5 % velkých přiznalo, že se s tímto incidentem setkalo.

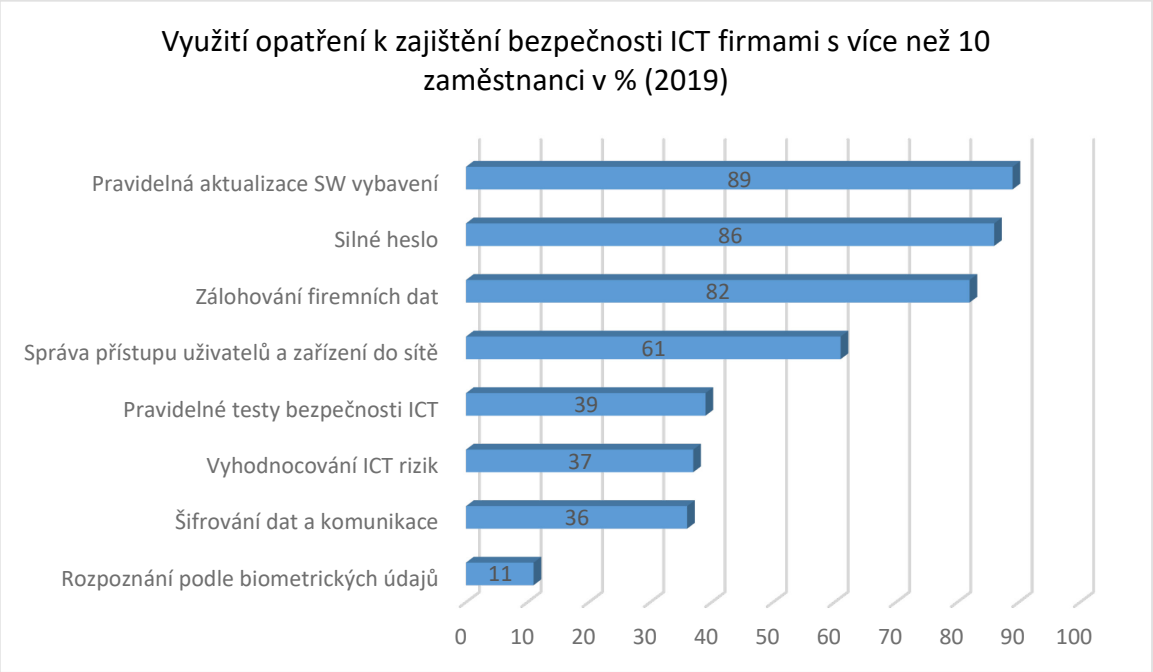
Zjišťovány byly také nejběžnější bezpečností opatření. Patřila mezi ně používání silných hesel, pravidelné aktualizace software a zálohování firemních dat. Tyto 3 opatření využilo 80 % firem s více než 10 zaměstnanci a velkých firem až 95 %. [45]

Pravidelné testy bezpečnosti provádí asi 35 % firem s více než 10 zaměstnanci. Nejlépe na tom jsou velké firmy, těch provádí pravidelné testy 64 %. Podíl firem, které rizika pravidelně vyhodnocují je podobný.

Řízení přístupu uživatelů a zařízení do podnikové sítě používá asi 60 % firem. Oprávnění přístupu k datům nebo do objektu kontroluje 55 % malých firem. V toto případě ovšem také s počtem zaměstnanců stoupají i procenta, protože velkých firem používá správu přístupu až 96 %.

Dalšími bezpečnostními opatřeními jsou šifrování dat nebo komunikace a rozpoznávání uživatelů na základě biometrických údajů. Šifrování komunikace využívá 30 % malých firem, středních 51 % a velkých subjektů 71 %. V České republice zatím není rozpoznávání uživatelů pomocí biometrických údajů příliš rozšířeno. Pouze 11 % firem jej v roce 2019 využívalo. [46]

Graf 1 – Zavedená bezpečnostní opatření ICT firmami [46]



5.2 Jednotlivci

Počet uživatelů internetu starších 16 let rok od roku stoupá. V roce 2019 se vyšplhal na asi 7,1 milionu, tedy 81 %. Drtivá většina uživatelů pak uvedla, že internet používají pravidelně. [47]

Zálohování je jedno nejčastějších bezpečnostních opatření. Podle průzkumu si 48 % Čechů starších 16 let své soubory zálohuje. O ukládání mimo původní zařízení se více zajímají muži než ženy, mužů asi 53 % zatímco žen asi o 10 % méně. Největší podíl na zálohování má mladší část populace, tedy osoby ve věku 16 – 24 let. 26 % osob uvedlo, že si svá data zálohují pouze na fyzickém nosiči, 18 % na fyzickém nosiči i internetovém úložišti

a pouze na internetu jen 3 %. Zajímavostí je, že v porovnání s ostatními státy Evropské unie se v používání internetových úložišť nacházíme pod průměrem.

Podle staršího průzkumu (2010) vyšlo najevo, že asi 65 % Čechů pro ochranu svého zařízení používá antivirový program. [48] V této době je procento výrazně vyšší. Jedním z důvodů je, že antivirový program je součástí operačního systému Windows, což je dlouhodobě nejpoužívanější systém. V roce 2019 odborníci otestovali několik programů chránících počítač a Microsoft Windows Defender se umístil mezi čtyřmi nejlépe ohodnocenými. Ovšem proti konkurenci má jednu velkou výhodu a to tu, že je zcela zdarma. [49]

V roce 2018 se v České republice rozšířily e-maily ve kterých se psalo, že uživatelé byli natočeni při sledování pornografie. Útočníci prostřednictvím těchto e-mailů uživatelům vyhrožovali, že pokud nezaplatí stanovenou částku, tak nahrávku zveřejní. Podle dostupných informací si útočníci přišli na téměř 130 tisíc korun. [50] V minulém roce 17 % Čechů starších 16 let obdrželo podvodný mail, ve kterém se požadovalo zaslání financí nebo osobních údajů. To z tohoto bezpečnostního incidentu dělá jeden z nejčastějších. Dalším incidentem bylo napadení e-mailového účtu nebo účtu na sociálních sítích, to postihlo 5,8 % lidí. Přesměrováno na falešnou webovou stránku bylo 3,3 % osob.

Bezpečnostní hrozbu představuje také malware. V posledních letech se v České republice rozšířil zejména ransomware a rostoucím trendem se staly také cryptominery. Častou internetovou hrozbu v roce 2018 představovala aplikace CoinMiner. Ta nelegálně těžila kryptoměnu za pomocí webové stránky, kterou oběť navštívila, nebo infikovala zranitelné zařízení. [50]

Šetření také ukázalo že osoby starší 50 let měli při používaní informačních technologií častěji obavu, že o své osobní údaje nebo peníze přijdou. Typickým příkladem je internetové bankovnictví. Mladších osob, které měli obavy s užíváním právě internetového bankovnictví bylo 13 %, zatímco osob starších 27 %. [51] Bankovnictví je pro kyberzločince lákavý cíl. Z pravidelných kontrol kybernetické bezpečnosti, které provádí Česká národní banka vyplývá, že Český bankovní sektor je poměrně dobře zabezpečený, protože se zde nevyskytují vážnější incidenty. Podle průzkumu v roce 2018 byli největší zranitelností právě uživatelé. Zvýšil se výskyt phishingových útoků na klienty. [50]

5.3 Bezpečnostní opatření

V této kapitole jsou v jednotlivých bodech vypsány některé z bezpečnostních opatření, které by měl uživatel dodržovat, aby snížil riziko ztráty svých dat.

Fyzická ochrana

Může se to zdát jako banální opatření, ovšem pokud má k zařízení někdo přístup, podstatně to zvyšuje riziko, že se dostane také k uloženým datům. Pokud zařízení dokonce odcizí, tak jsou například softwarová opatření k ničemu. [4]

- Zabránit fyzickému přístupu neoprávněných osob k vašemu zařízení.

Aktualizace

Výrobci na známe chyby v jejich programech a systémech vydávají aktualizace, které obsahují záplaty. Tím zabraňují využití daných zranitelností pro např. infikování malware. Vydaná aktualizace je k ničemu, pokud si nenainstalujeme. [14]

- Aktualizace operačního systému.
- Aktualizace antivirového programu.
- Aktualizace internetového prohlížeče a ostatních programů.

Antivirový program

Užíváním antivirového programu se značně zvyšujete ochrana zařízení proti malware. Virové testy odhalují přítomnost malwaru. Je ale potřeba zkontrolovat správné nastavení antiviru a ujistit se, zda některé důležité funkce nemá vypnuté. [17]

- Používání antivirového programu.
- Správné nastavení antivirového programu.
- Pravidelné virové testy celého počítače.

Firewall

Firewall kontroluje příchozí a odchozí komunikaci do vnitřní sítě. Tím chrání zařízení před různými útoky. V dnešní době je firewall součástí balíčku, které poskytují výrobci antivirových programů. [17]

- Používat firewall.

Nakládání s hesly

Základním bodem heslové politiky je mít silné heslo. O tom, jak zvolit správné heslo píši v kapitole 4.4. Další logickou zásadou je hesla nikomu nesdělovat, protože by se do Vašeho účtu mohl sám přihlásit, nebo heslo sdělit někomu dalšímu. V dnešní době většina lidí vlastní několik různých účtů ať už e-mailových, k sociálním sítím apod. Pokud se útočníkovi podaří zjistit heslo pouze k jednomu z nich a vy používáte pouze jedno heslo, tak může následně získat přístup ke všem vašim účtům. [42]

- Užívání silných hesel.
- Nikomu nesdělovat a nezapisovat hesla.
- Nepoužívat stejná hesla pro různá přihlášení.

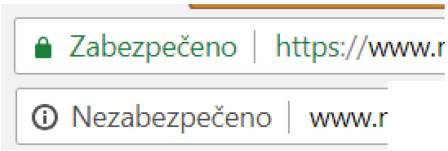
Zálohování

O svá data nemusíte přijít pouze z důvodu kybernetického útoku nebo malware. Pevný disk, na kterém jsou uloženy fotky a různé dokumenty může přestat fungovat ze spousta důvodů, kterými jsou výrobní vada, opotřebení materiálu, fyzický otřes atd. a vy tak o své data můžete nadobro přijít. [13]

- Zálohovat svá data, především ta důležitá.
- Pravidelné zálohování.

Návštěva webové stránky

Webové adresy by měli začínat „https“. To značí, že je komunikace šifrována. Pro stránky, které pracují s přihlašovacími údaji, platbami atd. je to nezbytné. Pokud je webová stránka nezabezpečena, její adresa začíná „http“ a prohlížeč na to upozorní. V případě stránky zabezpečené se vedle adresy nachází nejčastěji zelený zámeček. V opačném případě zámeček buďto chybí, nebo je červený, nebo se také objeví nápis „Nezabezpečeno“. [52]



Obrázek 13 – Rozdíl v URL zabezpečené a nezabezpečené stránky [53]

- Kontrola SSL certifikátu (https).

Elektronická pošta

U elektronické pošty je třeba dávat pozor zejména na přílohy. Odkazy můžou obsahovat malware nebo vás můžou přesměrovat na infikovanou stránku nebo stránky falešné. Je dobré na neznámé odkazy vůbec neklikat a zkontrolovat si kdo nám je posílá. U kontroly adresy odesilatele je potřeba se zaměřit, zda adresa neobsahuje chyby. Útočníci často využívají podobných adres, například jen přehodí nebo vynechají jedno písmeno. [28]

- Neklikat na neznáme odkazy.
- Kontrola e-mailové adresy odesilatele (hledání chyb).

Stahování

Stažený soubory může obsahovat malware. Je dobré se také vyhýbat cracknutým komerčním programům. Cracknuté programy lákají uživatele tím, že za ně nebudou muset platit, ale můžou také obsahovat malware. [53]

- Nestahovat neznáme soubory.
- Pozor na cracknuté programy.

Účinná opatření

Tabulka obsahuje bezpečnostní opatření a kybernetické útoky popisované v teoretické části. Popisuje, zda je dané opatření účinné proti danému útokem. Záloha dat byla vynechána, protože není přímo účinná proti zmíněným útokům. Její význam je v případě, kdy je některý z útoků úspěšný a uživatel by tak o svá data přišel.

Tabulka 2 – Účinná opatření proti daným kybernetickým útokům [Zdroj: vlastní]

	Fyzická ochrana	Autentizace	Aktualizace	Antivirový program	Firewall
Malware	Ano	Ano	Ano	Ano	Ano
Spam	Ne	Ne	Ano	Ano	Ne
Phishing	Ne	Ne	Ano	Ano	Ne
Pharming	Ne	Ne	Ano	Ano	Ne
Hacking	Ano	Ano	Ano	Ano	Ano
Cracking	Ano	Ano	Ano	Ne	Ne
Sniffing	Ano	Ano	Ano	Ano	Ano
MITM	Ne	Ne	Ne	Ne	Ne

Malware

Hlavní ochrana proti malware je samozřejmě antivirový program. Dalšími prvky jsou také fyzická ochrana a autentizace, ty totiž souvisí s přístupem k počítači. Pokud tomu zabráníme, nezbývá útočníkovi nic jiného než malware do počítače dostat jinou cestou.

Velmi důležité jsou také aktualizace operačního systému a ostatních programů včetně samotného antivirového programu. Tím například zabráníte útočníkovi využití zranitelnosti, kterou se může dostat do zařízení a infikovat jej. [5]

Spam

Přímo proti spamu se můžeme jen těžko bránit. Ani na antispamové filtry se nedá spolehnout na 100 %. Spam ovšem může obsahovat škodlivý kód proti kterému jsou účinné a také důležité aktualizace a antivirový program. Z tohoto pohledu jej není dobré podceňovat. [5]

Phishing

Phishing nejvíce ovlivňuje samotný uživatel. Ten se stává bezpečnostním opatřením, ale také slabým místem. Záleží na tom, zda útok odhalí nebo ne. Phishing je častým způsobem šíření malware. Pokud jej oběť neodhalí a klikne na obdržený odkaz, sehrávají zde roli opět aktualizovaný veškerý software a antivirový program. [5]

Pharming

Samotný pharimg a přesměrování na falešné webové stránky oběť jen těžko ovlivní. Pokud se tak stane a oběť je tedy přesměrována, může falešné stránky samozřejmě sama rozpoznat. K pharmingu lze využít také malware, který napadne koncové zařízení a pomocí něj oběť přesměruje na falešné stránky. V takovém případě se ovšem stává účinným antivirový program, který jej rozpozná. [22]

Hacking

Účinnou ochranou proti hackingu jsou všechna zmíněná opatření. Hackeři se totiž snaží využít všech dostupných možností, jak se do napadeného systému dostat. Mezi jejich typické aktivity patří sociální inženýrství přes prolamování hesel a phishing, až po odposlech komunikace. Záplatami vydaných v aktualizacích zabráníte zneužitím zranitelností. Důležitou roli zde hraje také firewall. [22]

Cracking

Základním opatřením proti útočníkovi, který se snaží prolomit bezpečnostní prvky, je fyzická ochrana a také autentizace. Právě tu se útočníci často snaží prolomit. Důležitý je také aktuální software, který neobsahuje známé zranitelnosti. [22]

Sniffing

Sniffing využívá odposlouchávací program. Proto je nutné útočníkovi zabránit v přístupu k počítači. V takovém případě je nutné vzdálené napadení, které může být úspěšné, pokud uživatel nemá aktuální svůj software jako je firewall a antivirový program. [32]

Man in the middle

MITM spočívá v zachycení komunikace mezi dvěma systémy. Žádný ze zmíněných bezpečnostních prvků proti tomuto druhu útoku není účinný. K zabránění zachytávání komunikace lze zamezit například kontrolou URL adresy navštěvované webové stránky a užívání pouze zabezpečené komunikace. Taková URL adresa začíná „https“. [35]

ZÁVĚR

Bakalářská práce se zabývala osobními počítači z pohledu bezpečností dat a informací. Cílem teoretické části bylo objasnit některé pojmy a také legislativu související s touhle problematikou a dále poukázat na základní bezpečnostní opatření, které by mě každý uživatel počítače dodržovat. Patří mezi ně fyzická ochrana, aktualizace, používání antivirového programu atd. Další část se zabývala nejčastějšími kybernetickými útoky, jako jsou například phishing, malware, nebo hacking.

Hlavním cílem praktické části byla realizace právě jednoho z útoků. Konkrétně se jednalo o metodu crackingu a to tzv. slovníkový útok. Útok byl proveden pomocí nástroje na prolamovaní hesel nazvaného Hydra. Ten je součástí operačního systému Kali Linux, který byl vytvořen pro testovací penetrační testy a bezpečnostní audit. Útok byl proveden na dva testovací e-mailové účty služby Seznam a vycházel z předpokladu, že jeden z účtů měl heslo silné, zatímco druhý měl heslo snadno uhodnutelné. Realizace útoku, kterým bylo uhádnuto heslo k jednomu z e-mailových účtů, poukázala na důležitost volby silného hesla. I v dnešní době, kdy má téměř každý z nás e-mailovou schránku, je uživatel sociálních sítí nebo jiné internetové služby, se najdou lidé, kteří volí velmi jednoduchá hesla, která útočníci dokážou prolomit za krátkou dobu. Součástí byla také podkapitola následky uhádnutí hesla. Tam jsem simuloval, jak je pro útočníka snadné se pomocí nabouraného e-mailu dostat na sítě, v mém konkrétním případě se jednalo o sociální síť Facebook.

Poslední kapitolou bakalářské práce byla statistika, jak uživatelé chrání svá zařízení a také s jakými bezpečnostními incidenty se setkali. Součástí této kapitoly bylo vytvoření tabulky s bezpečnostními opatřeními a kybernetickými útoky popisovanými v teoretické části. Významem tabulky bylo ukázat jaké konkrétní opatření je účinné proti danému útoku.

SEZNAM POUŽITÉ LITERATURY

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti* [online]. 3. Praha: Policejní akademie ČR, 2015 [cit. 2019-11-12]. ISBN 978-80-7251-436-6. Dostupné z: https://docplayer.cz/2694910-Vykladovy-slovnik-kyberneticke-bezpecnosti.html

[2] Informace. *ManagementMania: Sociální síť pro business* [online]. c2011-2016 [cit. 2020-02-15]. Dostupné z: https://managementmania.com/cs/informace

[3] Cybersecurity | Definition of Cybersecurity by Merriam-Webster. *Dictionary by Merriam-Webster: America's most-trusted online dictionary* [online]. Merriam-Webster, 2020 [cit. 2020-04-05]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity

[4] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. Praha: CZ.NIC, 2019 [cit. 2019-11-12]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[5] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 9788073807375.

[6] POŽÁR, Josef. *Informační bezpečnost*. Aleš Čeněk, 2005. ISBN 80-86898-38-5.

[7] ČÍŽEK, Jakub. Nejděravější firmy a programy roku 2019: Android, Debian a Windows. *Živě.cz – O počítačích, internetu, vědě a technice* [online]. CZECH NEWS CENTER a.s. a dodavatelé obsahu, 2019 [cit. 2020-03-06]. Dostupné z: https://www.zive.cz/clanky/nejderavejsi-firmy-a-programy-roku-2019-android-debian-a-windows/sc-3-a-202743/default.aspx

[8] ČERMÁK, Miroslav. Přečtěte si, co je to vektor útoku, zranitelnost, exploit a payload. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, 2008-2019 [cit. 2019-11-26]. Dostupné z: https://www.cleverandsmart.cz/prectete-si-co-je-to-vektor-utoku-zranitelnost-exploit-a-payload/

[9] 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi: Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. c2010-2020 [cit. 2020-02-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[10] Legislativa. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2020-02-15]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

[11] ŠKORNIČKOVÁ, Eva. Co je GDPR a jak bude aplikováno v Česku. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. [cit. 2020-04-01]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[12] IRWIN, Luke. What is the ISO 27000 series of standards?. *IT Governance: Governance, Risk Management and Compliance for Information Technology* [online]. c2003-2020 [cit. 2020-02-15]. Dostupné z: https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards

[13] Zálohování dat: věnujte mu pár desítek minut a budete mít klid na X let dopředu. *Bojujeme za bezpečnější on-line svět | Digitální pevnost* [online]. 2018 [cit. 2020-03-23]. Dostupné z: https://www.digitalnipevnost.cz/zpravodaj/detail/zalohovani-dat

[14] VACCA, John. *Computer and Information Security Handbook*. Burlington (Massachusetts): Morgan Kaufman Publishers, 2009. ISBN 978-0-12-374354-1.

[15] STAMP, Mark. *Information security: Principles and Practice*. 2. San Jose: Wiley, 2006. ISBN 978-0-471-73848-0.

[16] ČERMÁK, Miroslav. Autentizace: biometrické metody. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, c2008-2019 [cit. 2019-12-26]. Dostupné z: https://www.cleverandsmart.cz/autentizace-biometricke-metody/

[17] KRÁL, Mojmír. *Bezpečný internet: Chraňte sebe i svůj počítač*. Praha: Grada, 2015. ISBN 978-80-247-5453-6.

[18] HALLER, Martin. Útok na benešovskou nemocnici? Stačí jediná chyba, hackerům jde jen o peníze. *Aktuálně* [online]. Economia, 2005 [cit. 2019-12-19]. Dostupné z: https://video.aktualne.cz/dvtv/haller-utok-na-benesovskou-nemocnici-staci-jedina-chyba-hack/r~5e29cd6c1c3111ea858fac1f6b220ee8/

[19] KOCMAN, Rostislav a Jakub LOHNISKÝ. *Jak se bránit virům, spamu a spyware*. Brno: CP Books, 2005. ISBN 80-251-0793-0.

[20] ČERMÁK, Miroslav. Anatomie útoku: plošný útok a jak se mu bránit. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, 2008-2019 [cit. 2019-11-26]. Dostupné z: https://www.cleverandsmart.cz/anatomie-utoku-plosny-utok-a-jak-se-mu-branit/

[21] ČERMÁK, Miroslav. Attack surface, attack vector, threat landscape a threat horizon. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, 2008-2019 [cit. 2019-11-26]. Dostupné z: https://www.cleverandsmart.cz/attack-surface-attack-vector-threat-landscape-a-threat-horizon/

[22] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[23] STROUD, Forrest. What Is Cryptomining Malware? Webopedia Definition. *Webopedia: Online Tech Dictionary for IT Professionals* [online]. 2020 [cit. 2020-04-01]. Dostupné z: https://www.webopedia.com/TERM/C/cryptomining-malware.html

[24] Co je Spam. *Adaptic* [online]. Adaptic, c2005-2019 [cit. 2019-12-24]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/spam/

[25] ČERMÁK, Miroslav. Spam, scam, hoax nebo phishing?. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, 2008-2019 [cit. 2019-12-17]. Dostupné z: https://www.cleverandsmart.cz/spam-scam-hoax-nebo-phishing/

[26] Hoax. *ManagementMania: Sociální síť pro business* [online]. c2011-2016 [cit. 2019-12-24]. Dostupné z: https://managementmania.com/cs/hoax

[27] DŽUBÁK, Josef. Co je to HOAX. *HOAX* [online]. c2000-2020 [cit. 2020-01-09]. Dostupné z: https://www.hoax.cz/hoax/co-je-to-hoax

[28] DŽUBÁK, Josef. Co je to phishing. *HOAX | Phishing* [online]. c2000-2020 [cit. 2020-01-09]. Dostupné z: https://www.hoax.cz/phishing/co-je-to-phishing

[29] KANE, Artur. 7 kybernetických útoků, se kterými se setkáte. *SystemOnLine: ekonomické a informační systémy v praxi* [online]. CCB, c2001-2019 [cit. 2019-12-27]. Dostupné z: https://www.systemonline.cz/it-security/7-kybernetickych-utoku-se-kterymi-se-setkate.htm

[30] KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní aspekty phishingového útoku. *Trestní právo*. 2008, **13**(9), 5-12. ISSN 1211-2860.

[31] *Kyberterorismus: Úvod do problematiky, podoby a přehled aktů kybernetického terorismu, kybernetická bezpečnost, mezinárodní srovnání*. Praha: Kancelář Poslanecké sněmovny, 2019, (5383). ISSN 2533-4131. Dostupné z: http://www.psp.cz/sqw/ppi.sqw?d=1

[32] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[33] ČERMÁK, Miroslav. Autentizace: řekni mi své heslo. *CleverAndSmart Management Consulting* [online]. Miroslav Čermák, c2008-2019 [cit. 2019-12-26]. Dostupné z: https://www.cleverandsmart.cz/autentizace-neco-vi/

[34] Sniffing. *ManagementMania: Sociální síť pro business* [online]. c2011-2016 [cit. 2019-12-23]. Dostupné z: https://managementmania.com/cs/sniffing

[35] What is a Man-In-The-Middle Attack?. *Cloudflare: The Web Performance & Security Company* [online]. 2020 [cit. 2020-01-16]. Dostupné z: https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/

[36] Slovníkový útok. *>Sociální síť pro business - ManagementMania.com* [online]. c2011-2016 [cit. 2020-03-04]. Dostupné z: https://managementmania.com/cs/slovnikovy-utok

[37] What is Kali Linux?. *Kali Linux: Penetration Testing and Ethical Hacking Linux Distribution* [online]. 2020 [cit. 2020-02-21]. Dostupné z: https://www.kali.org/docs/introduction/what-is-kali-linux/

[38] THC-Hydra | Penetration Testing Tools. *Penetration Testing Tools - Kali Linux* [online]. 2020 [cit. 2020-02-26]. Dostupné z: https://tools.kali.org/password-attacks/hydra

[39] Co je to SMTP?. *Hosting, Registrace domény, Virtuální servery - VPS - BEST-HOSTING.cz* [online]. 2020 [cit. 2020-03-02]. Dostupné z: https://best-hosting.cz/cs/napoveda/co-je-to-smtp

[40] HANÁK, Jiří. Vysvětlení SSL certifikátů: Co jsou, jak fungují a proč je používat. *Master Internet* [online]. c1998-2020 [cit. 2020-03-01]. Dostupné z: https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

[41] Dvoufázové ověření. *Živě.cz – O počítačích, internetu, vědě a technice* [online]. CZECH NEWS CENTER a.s. a dodavatelé obsahu, 2019 [cit. 2020-04-02]. Dostupné z: https://www.zive.cz/dvoufazove-overeni/sc-679/default.aspx

[42] EMPEY, Charlotte. Jak si nastavit silné heslo. *Avast Blog* [online]. Avast Software, c1988-2020 [cit. 2020-03-15]. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

[43] Seznam hesel, která byste nikdy neměli použít. Je jich 320 milionů. *Živě.cz – O počítačích, internetu, vědě a technice* [online]. CZECH NEWS CENTER a.s. a dodavatelé obsahu, 2019 [cit. 2020-04-22]. Dostupné z: https://www.zive.cz/bleskovky/seznam-hesel-ktera-byste-nikdy-nemeli-pouzit-je-jich-320-milionu/sc-4-a-188881/default.aspx

[44] ANDERSON, Sophie. Nejlepší správci hesel roku 2020. *Safety Detectives* [online]. 2020 [cit. 2020-05-05]. Dostupné z: https://cs.safetydetectives.com/best-password-managers/

[45] S kybernetickým útokem se v roce 2018 setkaly dvě pětiny velkých firem v ČR. *Český statistický úřad | ČSÚ* [online]. [cit. 2020-02-21]. Dostupné z: https://www.czso.cz/csu/czso/s-kybernetickym-utokem-se-v-roce-2018-setkaly-dve-petiny-velkych-firem-v-cr

[46] Využívání informačních a komunikačních technologií v podnikatelském sektoru - rok 2018, leden 2019. *Český statistický úřad | ČSÚ* [online]. [cit. 2020-02-21]. Dostupné z: https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-podnikatelskem-sektoru-rok-2018-leden-2019

[47] Používání internetu jednotlivci. *Český statistický úřad | ČSÚ* [online]. [cit. 2020-02-

21]. Dostupné z: https://www.czso.cz/csu/czso/3-pouzivani-pocitace-a-jinych-zarizeni-k-pristupu-na-internet

[48] Internetová bezpečnost | ČSÚ. *Český statistický úřad | ČSÚ* [online]. [cit. 2020-03-09]. Dostupné z: https://www.czso.cz/csu/czso/1-9701-10--0305

[49] KILIÁN, Karel. Windows Defender je prý nejlepší antivirus, tvrdí AV-Test – Živě.cz. *Živě.cz – O počítačích, internetu, vědě a technice* [online]. CZECH NEWS CENTER a.s. a dodavatelé obsahu, 2019 [cit. 2020-03-09]. Dostupné z: https://www.zive.cz/clanky/windows-defender-je-pry-nejlepsi-antivirus-tvrdi-av-test/sc-3-a-199775/default.aspx

[50] Zpráva o stavu kybernetické bezpečnosti ČR za rok 2018. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-04-21]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1370-zprava-o-stavu-kyberneticke-bezpecnosti-cr-za-rok-2018/

[51] Bezpečnost na internetu. *Český statistický úřad | ČSÚ* [online]. [cit. 2020-02-22]. Dostupné z: https://www.czso.cz/csu/czso/18-pouzivani-informacnich-technologii-v-praci-lmahp64fx9

[52] Co to znamená, když prohlížeč označuje web jako nezabezpečený? Proč je https důležité a http musí skončit?. *@365tipu: Jeden tip denně (po-pá), starší často aktualizované.* [online]. 2020 [cit. 2020-04-07]. Dostupné z: https://365tipu.cz/2018/07/25/co-to-znamena-kdyz-prohlizec-oznacuje-web-jako-nezabezpecny-proc-je-https-dulezite-a-http-musi-skoncit/

[53] Jak na HTTPS aneb jak se zbavit nálepky nezabezpečeného webu. *Martin Domes | webdesignér, lektor, autor knih* [online]. [cit. 2020-05-25]. Dostupné z: https://www.martindomes.cz/jak-na-https-aneb-jak-se-zbavit-nalepky-nezabezpeceneho-webu/

[54] KOPECKÝ, Matěj. Zásady bezpečného chování na internetu. *Křivonet* [online]. [cit. 2020-05-09]. Dostupné z: https://krivonet.cz/o-nas/zasady-bezpecneho-chovani-na-internetu/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CVE Common Vulnerabilities and Exposures

CVV Card Verification Value

DDOS Distributed Denial of Service

DNS Domain Name System

DOS Denial of Service

DVD Digital Versatile Dics

EU Evropská unie

GDPR General Data Protection Regulation

HTTP Hypertext Transfer Protocol

HW Hardware

ICT Informační a komunikační technologie

IEC International Electrotechnical Commission

IP Internet Protocol

ISO International Organization for Standardization

MITM Man in the Middle

PIN Personal Identification Number

SMS Short Message Service

SMTP Simple Mail Transfer Protocol

SSL Secure Sockets Layer

SW Software

URL Uniform Resource Locator

USB Universal Seriál Bus

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ