Informační technologie jako prostředek šíření kriminality

Ing. Radka Procházková

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ing. Radka Procházková**
Osobní číslo:	**A18631**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Informační technologie jako prostředek šíření kriminality**
Téma práce anglicky:	**Information Technology as a Means Of Spreading Crime**

Zásady pro vypracování

1. Zpracujte rešerši literatury a pramenů k tématu.
2. Vymezte etiologické a fenomenologické otázky daného tématu.
3. Analyzujte a kvantifikujte podíl informačních technologií v oblasti šíření a prezentace kriminality.
4. Analyzujte nejčastější formy kriminality, šířené prostřednictvím informačních technologií.
5. Výstupy a výsledky anylitické části vyhodnoťte a prezentujte v grafické podobě.

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

Seznam doporučené literatury:

1. VESECKÁ, Renáta. Kriminalita, veřejnost a média. Praha : Linde Praha, 2009. ISBN – 9788072017720.
2. DAVIDSON, Alan. Social media and electronic commerce law. Cambridge, 2016. ISBN – 9781107500532.
3. SMART, Carol. Women, crime, and criminology: feminist critique. Routledge, 2013. ISBN – 9780415644174.
4. KOLOUCH, Jan. CyberCrimme. Praha : CZ.NIC, z.s.p.o., 2016. ISBN – 9788088168157.
5. HAYDEN, Carol. Childern in trouble: the role of families, schols and... New York, 2007. ISBN – 9781403994868.
6. VÁLKOVÁ, Helena a KUCHTA, Josef a HULMÁKOVÁ, Jana. Základy kriminologie a trestní politiky. Praha, C.H. Beck, 2019. ISBN – 9788074007323.

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

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

Ve Zlíně, dne 13.8.2020

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá vlivem informačních technologií na šíření kriminality. Teoretická část se zaměřuje na informační technologie, počítačovou bezpečnost, počítačovou kriminalitu a co je to kyberprostor, jednotlivé útoky APT. Praktická část se zaměřuje na jednotlivé druhy kriminality šířené prostřednictvím informačních technologií s provedeným kvantitativným výzkumem.

Klíčová slova: infomační technologie, bezpečnost, kyberprostor, útoky APT, kriminalita pomocí počítačových sítí

ABSTRACT

The diploma thesis deals with the influence of information technologies on the spread of crime. The theoretical part focuses on information technology, computer security, computer crime and what cyberspace is, individual APT attacks. The practical part focuses on individual types of crime disseminated through information technology with quantitative research.

Keywords: information technology, security, cyberspace, APT attacks, crime using computer networks

Tímto bych chtěla poděkovat vedoucímu mé práce PhDr. Mgr. Stanislavu Zelinkovi za odborné vedení, cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování diplomové práce.

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

OBSAH

ÚVOD

V diplomové práci se zabývám problematikou šíření kriminality prostřednictvím informační technologie. Informační technologie, počítačová bezpečnost, kyberprostor, chytré telefony, elektronická data, útoky na počítače, chytré přístroje jsou v dnešní době každodenní součástí života.

Snad každý z nás se setkal s nějakým informačním systémem a využívá ho ke své práci nebo v soukromém životě. Počítače, chytré telefony, tablety atd. jsou součástí každodenního života. Dnes jsou všechna data digitalizována, většina dat se uchovává pouze v elektronické podobě, což může být výhodou, ale i nevýhodou. V případě, že data nejsou dostatečně ochráněna, může dojít k jejich ztrátě a následnému zneužití.

Data začínají být dnes to nejcennější co máme, a to nejen ty naše osobní, ale i data firemní. S daty se již delší dobu obchoduje, zneužívají se k obohacení, konkurence si ráda zakoupí data o firmě, kterou chce na trhnu atakovat, nebo alespoň získat převahu na trhu nad ní. Proto je dnes není nutno chránit pouze před jejich ztrátou, ale hlavně před jejich zneužitím.

Již s rozvojem počítačů docházelo k tomu, že chtěli někteří lidé převzít kontrolu nad počítači a stále je vylepšovat, ale bohužel ne vždy v tom dobrém. Chtěli je využívat ve svůj prospěch, aby mohli získat cizí data, které použijí k získání cenných informací, peněžních prostředků nebo ovládnout určitou část businessu. S rozvojem internetu docházelo i k rozvoji kyberkriminality, vznikaly malware, spamy, útočníci se nabourávali do počítačů nejen jedinců, ale celých firem. Proto je potřeba neustále chránit a zlepšovat ochranu dat, aby nemohlo dojít k jejich zneužití. Nejedná se pouze o krádež peněžních prostředků, ale hlavně citlivých dat a v dnešní době o ovlivnění státního zřízení protivníka a ovládnutí jeho vojenské síly.

V praktické části jsou uvedeny způsoby ochrany identifikačních karet, které se ve světě masově využívají, a proto je důležité, aby i tyto data byla chráněna. O průkaz totožnosti můžeme přijít snadno a pak se divíme, že máme někde půjčku, o které nevíme, dlužíme peníze, které jsme si nepůjčili, vlastníme nemovitost, kterou jsme nekoupili, ale ani ji nesplácíme nebo se můžeme jednoduše dostat do nějakého trestného činu, aniž bychom o tom vůbec věděli. Proto je důležité chránit nejen elektronická data, ale i naše osobní průkazy a doklady.

Protože dnes je mnoho způsobů, jak se šíří kybernetická kriminalita, jak útočníci získávají data, které pak využívají, nebo spíše zneužívají, je nutná i velká osvěta obyvatelstva, aby

věděli, co jim hrozí, pokud nebudou opatrní a nebudou chránit svoje data. A není to pouze o tom, abychom si správně chránili naše data, ale i o tom, že si svoje počítače, telefony nebo tablety musíme chránit proti tomu, aby se nám pachatelé nedostali do našich prostorů a nepáchali kriminalitu prostřednictvím našeho počítače nebo telefonu.

V praktické části se zabývám průzkumem, ke kterému jsem měla k dispozici 80 respondentů níže uvedené firmy. Respondentů jsem se tázala, zdali aktivně využívají antivirové a bezpečnostní produkty na svých počítačích a elektronických zařízeních, zajímala jsem se o to, jak mají zabezpečeny tyto zařízení, co se týká útoků na jejich počítače. Průzkum byl veden dotazníkovou formou a následně ještě probíhala komunikace s pracovníky na přátelské bázi formou rozhovoru.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ TECHNOLOGIE

1.1 Informační technologie

Informační technologie je dnes snad nejrychleji rostoucí obor. To, co je dnes nejmodernější technologií, bude za nedlouho zastaralé a nahrazené daleko modernější technologií. V počátcích vývoje informačních technologií byl vývoj pomalý a každý nový objev byl velkým krokem vpřed. V současnosti je vývoj technologií velice rychlý a žádný nový vynález již dávno není vynálezem převratným.

Co jsou tedy informační technologie? Pod informační technologie můžeme zařadit veškeré elektronické přístroje, které jsou schopny zpracovat informace. Aby bylo možno přístroj zařadit do informačních technologií, musí umět přijmout vstupní data, které samostatně zpracuje a vytvoří z nich výstupní data.

Informační technologie jako vědní obor, je obor velice široký a můžeme sem zařadit počítače, mobilní telefony, internet, tablety a jiné elektronické chytré přístroje.

1.1.1 Historie

Na začátku celého pokroku informačních technologií, již před několika tisíci lety, byla různá počítadla, která byla určená pro sčítání a odečítání. Používal se systém korálků nebo kuliček na drátech nad sebou, tomuto systému se říkalo Abakus a je to vlastně systém dnešního počítadla, se kterým se učí děti počítat ve škole. Okolo roku 1642 vznikl první mechanický stroj na sčítání a odečítání a byl navržen francouzským fyzikem Blaise Pascalem. Následně byl stroj zdokonalen německým matematikem Wilhelmem von Liebnitzem, takže dokázal dělit, násobit a spočítat druhou odmocninu. Následovaly mechanické kalkulačky, které se využívaly až do 70 let minulého století. Děrné štítky byly dalším krokem ve vývoji, byly řízeny programy počítacích strojů. Po roce 1900, kdy byla vynalezena elektronka, se urychlil vývoj počítačů a začal rozvoj výpočetní techniky. První počítač byl v roce 1945 sestrojen v USA a byl přes celý velký sál. Tento počítač pracoval na systému jedniček a nul. Po vynalezení mikroprocesoru, v roce 1971, nastal prudký rozvoj počítačů a informační technologie. Počítače dostaly čím dál menší rozměr a neustále se zmenšovaly, a staly se dostupné pro širokou veřejnost.

Díky tlaku veřejnosti se vývoj informačních technologií posouvá neustále dopředu.

1.1.2 Dopady na společnost

Rozvoj informačních technologií přispívá i k tomu, že se mění lidská společnost. Bohužel to není jen v tom dobrém, ale přichází i hrozby, jako jsou například ztráta soukromí, ztráta špatně zabezpečených dat, mládež nechce trávit čas jinak než s počítačem nebo mobilním telefonem. Díky sociálním sítím se náš život stává čím dál tím více izolovaný, ale i lehce napadnutelný a z neuživatelný. V neposlední řadě se informační technologie využívají při páchání trestné činnosti.

1.2 Počítačová bezpečnost

„Počítačová bezpečnost je stav, kdy je dosaženo dostupnosti, integrity, důvěrnosti, odpovědnosti.“ [4]

Počítačová bezpečnost je v dnešní době obor informatiky, který se zabývá zabezpečením dat v počítačích a na úložištích. V dnešní době se jedná o velice důležitý obor, protože data mohou být zneužita.

K počítačové bezpečnosti patří:

- síťová bezpečnost
- bezpečnost koncových zařízení
- internetová bezpečnost
- e-podpisy, e-archivace a jiné speciální prostředky

Počítačová bezpečnost má zajistit ochranu dat před kybernetickými útoky, a zajistit bezpečný provoz informačních technologií před útoky.

2 POČÍTAČOVÁ KRIMINALITA

2.1 Počítačová kriminalita

Počítačová kriminalita jako pojem se těžko specifikuje, neexistuje přesná definice. Počítačová kriminalita je veškerá trestná činnost, kdy jsou jako nástroj nebo cíl kriminality využíván počítač nebo jakékoliv elektronické zařízení. Pro spáchání trestného činu není důležité elektronické zařízení, ale síť, kterou jsou elektronická zařízená propojena a informačním systémem. Mnohdy napadený neví hned, že byl proti němu spáchán trestný čin.

Podle bukurešťské úmluvy je rozdělení trestných činů následující:

- „Neoprávněný přístup – za neoprávněný přistup je považován průnik do počítačového systému a dat bez souhlasu nebo vědomí oprávněné osoby. Takový průnik může být jen příprava pro další čin. Příkladem je zničení nebo poškození informací. V tomto případě je objektem ochrana bezpečnosti počítačového systému a dat, přístup do systému je objektivní stránkou.
- Neoprávněné zachycení informací – Bezpečnost soukromé datové komunikace je objektem, objektivní stránkou je zaznamenání neveřejných přenosů dat. Komunikace zaměstnanců ve firmě má také znaky neveřejných přenosů a je chráněna.
- Zásah do dat – Ochrana počítačových programů a dat před způsobením škody je objektem, jedná se o porušování integrity nebo neoprávněné užívání počítačových dat. Objektivní stránkou zde je změna, poškození a vymazání dat. Tuto činnost představují viry a jiné zásahy, například trojský kůň.
- Zásah do systému – Hlavním smyslem je ochrana uživatelů a operátorů telekomunikačních a informačních systému, toto se dá také označit jako počítačová sabotáž. Spadá sem narušování nebo zničení počítačových dat. Jedná se o narušení systému takovým způsobem, že způsobuje uživateli problémy. Pomocí škodlivých virů a odepření služby dochází k narušení nebo zpomalení chodu systému a zablokování komunikačních cest
- Zneužití zařízení – Toto jednání působí v materiální povaze jako přípravná činnost pro páchání dalšího trestního činu v kyberprostoru. Ohrožení zájmu společnosti a jednotlivce vychází z nekontrolovatelné výroby, prodeje a distribuce, které napomáhají trestné činnosti v kyberprostoru.

- Falšování údajů spojené s počítači – Jde o ochranu elektronických dat, které můžou způsobit důsledky v právních vztazích. Falešné údaje vznikají v důsledku vymazání, změny nebo vložení dat. Obdobou falšování údajů je padělání hmotných dokumentů.
- Podvody spojené s počítači – Nepatřičná manipulace a zpracování dat s cílem nezákonně získat cizí vlastnictví
- Trestné činy spojené s dětskou pornografií – Ochrana dětí před podněcováním ke skutečnému sexuálnímu zneužívání. Rovněž i tvorba a zasílání odkazů s dětskou pornografií.
- Trestné činy spojené s porušením autorského práva a práv jemu příbuzných – Jedná se o porušení autorského práva a práv příbuzných autorskému právu, pokud k tomuto jednání došlo díky počítačovému systému“ [1]

2.2 Kybernetická kriminalita

„Kybernetická kriminalita představuje trestnou činnost, která zahrnuje počítač nebo síťové zařízení. Patří zde i zločiny prováděné prostřednictvím internetu, jako podvody, krádež osobních údajů a identity nebo kreditní karty. Velké množství útoků je prováděno za účelem získání peněžních prostředků.“ [2]

2.2.1 Kyberprostor

„Kyberprostor. Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky …. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světa seřazené v neprostoru mysli, shluky souhvězdí dat. Jako světla města, ustupující …“ [3]

Toto je definice podle Gibsona, na svou dobu vzniku docela přesná, ovšem pro naši představu hůře zhmotnitelná.

Kyberprostor je virtuální prostředí, on-line prostředí nebo internet jsou v dnešním světě běžné věci, které neodlučitelně patří k našemu životu a zná je každý. Díky internetu můžeme komunikovat on-line s ostatními lidmi nebo získávat informace z informačních zdrojů. V dnešní době si většina z nás již nedovede ani představit být „off-line“ (neboli nepřipojen k internetu) jako tomu bylo v 80 letech, kdy se Internet teprve rozvíjel.

Současné virtuální prostředí nám umožňuje být kdykoliv potřebujeme propojeni na sociálních sítích, můžeme kdykoliv číst a reagovat na e-mailové zprávy, jsme odkudkoliv připojeni do banky. Všechno připojení a veškerá data, která jsou o nás uložena na sítí, sebou ale přináší větší možnosti jejich zneužití dat.

Základní stavební jednotnou kyberprostoru jsou informace, které jsou vlastně v dnešní době to nejcennější a jsou velice lehce zneužitelné, pokud nejsou dobře ochráněny.

2.2.2 Kybernetický útok

Kybernetický útok je útok zahájený kybernetickými zločinci, kteří používají jeden nebo více počítačů proti jednomu nebo více počítačům nebo sítím. Počítačový útok může nebezpečně deaktivovat počítače, ukrást data nebo použít poškozený počítač jako startovací bod pro jiné útoky. Počítačoví zločinci používají k zahájení kybernetického útoku řadu metod, mezi které patří malware, phishing, ransomware nebo jiný útok.

2.2.3 Kyberšikana

Kyberšikana je velmi nebezpečným činem, který má mnoho podob a forem. Může se jednat o pronásledování, obtěžování, zesměšňování, týrání a ponižování oběti, týrání. Útočník je na rozdíl od fyzické formy šikany anonymní, a proto je pro oběť mnohokrát tento způsob šikany ještě horší. Většinou se jedná o skupinové jednání, kdy i neprůbojný jedinec se může díky kolektivu a jeho podpory nebo hecování, dostat do toho, že bude šikanovat přes kyberprostor silnější oběť, než je on sám.

2.3 Druhy počítačové kriminality

Počítačovou kriminalitu dělíme ze dvou hledisek, a to z hlediska pozice, ve které je počítač při páchání trestné činnosti a podle typu činu.

Podle postavení počítače při páchání trestné činnosti se dělí na:

- protiprávní jednání, kdy je počítač terčem útoku
- protiprávní jednání, které je spácháno s daným počítačem

Podle typu činu:

- protiprávní jednání tradiční
- protiprávní jednání nová, která přichází s rozvojem moderních informačních technologii

2.3.1 Pachatelé na internetu

Pachatelé, kteří páchají trestný čin na internetu se dělí na dvě skupiny a to:

- profesionály, kteří se pácháním trestné činnosti živí, trestnou činnost páchají cíleně ať už na objednávku nebo pro sebe. Patří sem např. softwarový piráti, specialisté informatici, teroristé atd.
- amatéry, kteří do počítačových sítí pronikají náhodně, hledají zranitelná místa. Cíle jejich motivace jsou rozdílné. Jedná se o hackery, crackery, atd.

2.2.1.1. Crackeři

Jsou osoby, které jsou schopny prolomit kód SW, daný software zkopírovat nebo poškodit. Do systému pronikají slabinami v systému, které nebyly administrátory opraveny. Většinou pracují ve skupinách, každý má ve skupině přidělenou svoji roli ve skupině.

Cracking je vlastně softwarové pirátství, kdy je nelegálně využívána kopie bez autorských práv. Jedná se o nedodržení ochranných prvků, formou stahování nelegálních kopií, využívání nelegálních počítačových programů, stahování filmů nebo hudebních produktů.

2.2.1.2. Hackeři

Tito lidé jsou počítačový specialisté nebo programátoři, kteří systém znají a umí ho požívat. Sytém si upraví podle svých potřeb, tak aby sloužil jejich cíli.

2.3.2 Způsoby napadání

2.3.2.1 Virus

Virus je neznámější způsob napadení počítače. Viry jsou malé softwarové programy, které se šíří po síti pomocí mailu a mají poškodit nebo smazat data v počítači, někdy mají za úkol vymazání celého pevného disku počítače.

Viry mohou být vytvořeny cíleně na šíření spamů z vícero počítačů najednou nebo je mohou vytvářet začínající programátoři, kteří si chtějí vyzkoušet, že toto zvládnou naprogramovat a rozeslat.

2.3.2.2 Červ

Červ je naprogramován tak, aby se sám kopíroval a šířil z jednoho počítače do druhého a následně převzal kontrolu nad některými funkcemi počítače, aby mohl následně přenášet informace a data.

2.3.2.3 Trojský kůň

Trojský kůň se tváří zcela nevině a mnohdy si ho sami naistalujeme při instalaci nového softwaru. Ovšem později začne páchat škody v počítači, kopíruje soubory, ničí soubory atd.

2.3.2.4 Spyreware

Spyreware byl vytvořen na kradení hesel z počítače, historii návštěvnosti stránek, čísel kreditních karet. Následně data odešle zadanému uživateli, který získaná data následně zneužije.

Každý útok APT má určité fáze, které začínají přípravou samotného útoku, pokračují přes napadení až po dosažení cíle útoku.

- Příprava – jedná se o počáteční fázi útoku, která se také označuje jako external reconnaissance. Útočník se snaží zjistit co nejvíce informací o objektu, který má být napaden. Analyzuje veškerá dostupná data z internetu jako jsou profily na sociálních sítích, webové stránky společnosti a jiné možné dostupné informace z internetu a hledá zranitelnost. Útočník se snaží zjistit, co nejvíce informací a pokud není možné zjistit požadované informace, jedná i tak, že se nechá zaměstnat v dané organizaci, aby mohl danou organizaci sledovat a zjistit slabá místa pro úspěšný útok. Útočník používá často falešnou identitu nebo si něčí identitu přivlastní. Následně je vyvinut

sofistikovaný malware a začne příprava na útok, připravují se e-maily, ze kterých se bude malware rozesílat, webové stránky, se kterými bude malware komunikovat, server, na který se budou zjištěná data zasílat.

- Průnik – je druhou fázi APT útoku. V této fázi dochází k doručení a spuštění škodlivého viru na jednom napadeném počítači. Následně dochází k průniku do sítě a napadení dalších počítačů v organizaci. Nejčastěji je malware rozesílán jako škodlivá příloha e-mailu s odkazem na stránky, které spustí škodlivý malware. Problémem bývá a pro útočníka je to výhodou, že nejsou na koncových stanicích dostatečně často prováděné aktualizace systémů. Jiným způsobem zaslání škodlivého malware do společnosti je, že útočník zjistí, na které stránky chodí často zaměstnanci firmy a malwate umístí přímo na ně. Zaměstnanci se pak připojí na tyto stránky a počítač je přesměrován na server, který mu vnutí falešnou aktualizaci software a následné nainstalování malware. Dalším způsobem je, že je malware šířen přes paměťová média, USB disky a CD disky. Poslední možností infikování společnosti škodlivým malware je, že je malware umístěn přímo na hardware, který organizace kupuje od třetí strany a využívá na svých počítačích.
- Kompromitace – útočník v této fázi útoku z napadeného počítače vyhledává a napadá další systémy v síti organizace a snaží se zajistit trvalý vzdálený přístup do těchto systémů. Útočník sbírá informace, snaží se důmyslně ukrýt malware v napadeném systému tak, aby ho nebylo možno odhalit. Velice důležité pro útok je zmapování

Spyreware se dělí do několika skupin:

- Malware je software, který slouží k narušení činnosti počítače, získá z něj informace a využije přístupu do daného počítače. Malware umí plnit více funkcí, může se šířit e-mailem dále nebo může získávat adresy z napadeného počítače.

- Carbanak je název malware, který funguje jako sofistikovaný verzatilní systémový backdoor odesílající uživatelská data organizované kriminální skupině, která je využívala k útokům na bankovní sítě. Malware byl aktivní od roku 2013. Od roku 2013 bylo napadeno zhruba 100 bank ve více než 40 zemích na celém světě a bylo

odcizeno 1,2 miliardy dolarů. Na aktivitu tohoto malware upozornila po dvou letech fungování bezpečnostní společnost Group-IB a Fox-IT.

Cílem Carbanaku bylo cílení na infrastrukturu finančních institucí. „Systém fungoval tak, že se škodlivý kód skrze spear-phishingové e-maily dostal do počítačů zaměstnanců bank, odkud se pak dostal do infrastruktury.“ [1] Útočníci si převáděli peníze na jiné účty, zvyšovali zůstatky účtů, na dálku zasílali příkazy bankomatům, aby bankomaty vydávaly peníze neoprávněným lidem. Peníze z bankomatů pro ně vybírali takzvaní „money mules“.

Carbanak útočil na počítače s operačním systémem Windows.

Následně bylo zjištěno, že ve fázi průzkumu byla shromažďována data ohledně bankovní infrastruktury, tento průzkum dělali útočníci hlavně po pracovní době ve finančních institucích nebo o víkendu.

Samotné útoky probíhaly tak, že zaměstnanec obdržel e-mail, který vypadal velmi přesvědčivě a obsahoval škodlivou přílohu. Po otevření této přílohy došlo ke stažení a aktivaci trojského koně, následně začala být sledována a ukládána potenciálně citlivá data v napadeném počítači. Po shromáždění potřebných dat byla data odeslána na zvolenou adresu. Z jednotlivých počítačů zaměstnanců banky se malware následně dostal do infrastruktury celé finanční instituce. Tímto získali útočníci kontrolu nad kamerami, získávali jména a hesla, která klienti používali pro přihlášení do bankovního systému. Díky malware bylo nahráváno, co se děje na obrazovce počítače. Na dálku bylo možno připojení k napadenému počítači a bylo možno jeho ovládání na dálku.

Bankovní systém byl útočníky ovládnut a následně docházelo k převodům finančních prostředků na účty útočníků. Pomocí malware si útočníci na napadeném počítači nahráli způsob, jakým bankovní zaměstnanec realizuje převod peněz. Jiný způsob, jak se útočníci dostávali k finančním prostředkům byl, že ovládli bankomat, který na základě pokynu útočníků vydal daný obnos finančních prostředků v danou dobu bez platební karty. U bankomat čekal jeden z útočníků, který bankovky z bankomatu vybral. Jiný způsob, kterým útočníci získávali finanční prostředky z bankomatu byl, že byl odstraněn limit pro výběr z bankomatu a bankomat následně vyplácel stejnou částku peněz, aniž by byl vydán zákaz transakce.

Útočníkům nechyběla trpělivost, konečný úder byl vždy pečlivě připraven a jeho příprava trvala i několik měsíců. Útočníci si vybrali zaměstnance, který měl dostatečná oprávnění pro přesun peněz mezi účty, mohl schvalovat půjčky, obsluhovat bankomaty a měl oprávnění k mezinárodním transakcím.

Kyberzločinci začali působit v srpnu 2013, kdy malware Carbanak byl testován. První spolehlivě ověřený důkaz o aktivitě tohoto malware byl v dubnu 2014.

současné době je malware Carbanak stále aktivní, avšak ne v prostředí finančních institucí, ale útočníci se zaměřili na hotely a restaurace.

- Desert Falcons je první arabská kyberšpionážní skupina s vybranými cíli. V překladu skupina znamená pouštní sokoli. Kyberútočníci mluví arabsky a sídlo mají v Palestině, Turecku a Egyptě. Před každým útokem důkladně prověří svůj cíl a po útoku pečlivě sledují svůj cíl. Většina obětí jejich útoků je ze Středního východu – Egypt, Izrael, Jordánsko, Saúdská Arábie, Palestina, ale útočí i mimo toto území, další napadené země jsou např. USA, Maroko, Katar nebo Jižní Korea.

  Skupina začala působit v roce 2011, kdy docházelo k testování tohoto malware. První napadení počítačů viry tohoto malware bylo zaregistrováno o dva roky později, tzn. v únoru 2013. Nejvyšší aktivita skupiny byla v roce 2015. V dnešní době je skupina stále aktivní, vyvíjí trojské koně a jiné pokročilé techniky, aby svoje účinnost jejích útoků byla vyšší.

  Tímto malware bylo napadeno 3 000 obětí z více jak 50 zemí, ukradeno více než 1 milion souborů z počítačů a mobilních zařízení. Byly napadeny počítače se systémem Windows a mobilní telefony s Androidem.

  K rozšíření malware útočníci používali falešné webové stránky, phishingové maily, sociální sítě, kde pomocí zpráv šířili škodlivé soubory. Po tom, co se do napadeného zařízení dostal malware, byly pořizovány snímky z obrazovky, zaznamenával se stisk na klávesnici, nahrávaly se a stahovaly soubory, o všech souborech Word a Excel na disku napadeného počítače byly shromažďovány informace, rovněž byly shromažďovány informace o připojených externích zařízeních. Útočníci ukradli hesla, které byly následně zneužita. U mobilních telefonů se systémem Android mohl malware pořizovat zvukové nahrávky, informace o hovorech a spravovat SMS.

Skupina byla nejvíce aktivní na začátku roku 2015, kdy byly zaznamenány nejméně tři škodlivé útoky, které byly zaměřeny na různé skupiny obětí v různých zemích. Napadeny byly státní organizace, vojenské organizace. Největší část útoků byla vedena na státní úředníky, kteří se zabývali bojem proti praní špinavých peněz a financování terorismu. Před útoky nebyly uchráněny ani nemocnice, výzkumné instituce, energetické společnosti, finanční instituce, politici.

Cílem útoků je získání citlivých informací, vojenských plánů a dokumentů, finančních dokumentů, seznam kontaktů, různých citlivých souborů, které útočníci mohou použít na následné vydírání obětí, aby jim byli nápomocni při jejich dalších operacích a nekalé činnosti.

- Flame byl objeven v počítačových systémech na Středním východě a jednalo se o trojský kůň s charakteristikami, které má počítačový červ. Cílem bylo získávání citlivých dat z napadených systémů a velice dlouhou dobu nebyl objeven. Jeho velikost byla několik MB.

  Malware Flame útočil na počítače s operačním systémem Microsoft Windows. „Malware Flame infikoval tisíce počítačů zejména v Izraeli, Iránu a Středním východě. Útok byl podle odborníků sponzorován dosud neznámým státem.“ [2]

  Software byl aktivní od března 2010, aniž by byl detekován antivirovým programem. Podnět k jeho hledání dala Mezinárodní telekomunikační unie Spojených národů, protože měla podezření na to, že existuje vir, který útočí na počítačovou síť íránského ministerstva ropného průmyslu. Malware sloužil ke špionáži v zemích Blízkého východu, především v Iránu, Izraeli, Súdánu, Sýrii, Palestině, Saudské Arábii a Egyptě.

  Malware Flame byl napsán ve skriptovacím jazyce Lua a zkompilovaném C++. Program zjistil používaný antivirový program a podle toho upravil své chování, aby mohl napadnout daný počítač. Tím, že měnil své chování, bylo jeho dopadení značně ztíženo. V květnu 2012 však byl odhalen. Malware byl velmi složitý, mohl se šířit po místní síti (LAN). Měl za úkol sbírat citlivé informace z napadených počítačů a posílat je útočníkům. Sbíral informace o různých souborech, dokumentech, nahrával zvuk pomocí mikrofonu v počítači, snímal fotografie, zaznamenával psaní na klávesnici, snímal obrazovku, síťový provoz. Pomocí tohoto malware bylo možno zaznamenávat konverzaci přes Skype, přes Bluetooth v napadeném počítači bylo

možno se připojit k okolním mobilním zařízením a z nich stahovat další informace a data. Všechna získaná data byla posílána na asi 80 serverů uložených po celém světě.

Malware Flame v napadeném počítači dokázal hledat soubory s konkrétním obsahem nebo konkrétní příponou.

Jakmile došlo k jeho objevení, byl spuštěn samo destruktivní proces a malware sám sebe zničil.

Takto bylo infikováno více jak 1 000 počítačů na úřadech vlády, školách, domácnostech, firmách, nemocnicích a ostatních organizacích.

Flame je neaktivní od roku 2013.

- WannaCry útočí na sítě protokolu SMB, který zajišťuje komunikaci počítačů s tiskárnami a jinými koncovými zařízeními.

  „Před rokem, v polovině května, se uskutečnil jeden z největších kybernetických útoků současnosti. Kvůli vyděračskému viru WannaCry totiž zkolabovaly systém drah, benzínek i nemocnic. Jediný škodlivý kód tak ukázal, jak zranitelný je moderní svět, který je závislý na počítačích a internetu.“ [4]

  Jedná se o vyděračský počítačový program, který infikoval již více jak 300 000 zařízení na celém světě. Jsou napadány počítače s operačním systémem Microsoft Windows.

  WannaCry v napadeném počítači zašifruje soubory různých typů, včetně kancelářských dokumentů, obrázků, videí, archivů, programátorských projektů a dalších formátů souborů, takže k nim znemožní přístup a po uživateli pak vyžaduje, aby to třech dnů zaplatil výkupné v bitcoinech v hodnotě 300 USD. Pokud napadený nezaplatí, cena výkupného se zdvojnásobuje. Přípony šifrovaných souborů jsou přejmenovány, aby byly soubory pro vlastníky zcela nepřístupné. Malware změní tapetu plochy napadeného počítače na obrázek, kde jsou informace o tom, že daný počítač byl napaden a jsou na něm podrobné informace o tom, co má napadený uživatel provést, aby byly jeho soubory znovu zpřístupněny.

  Malware je šířen e-mailem, který obsahuje přílohu, tvářící se jako ZIP archiv a když napadený otevře tuto přílohu, virus se naistaluje do počítače. V lokální síti se virus šíří skrz nezáplatované systémy nebo skrz vlastní botnetovou síť. Virus skenuje další

dostupné IP adresy, vyhledává počítače, které může díky nízkému zabezpečení napadnout.

Poprvé byl detekován tento virus v únoru 2017.

Největší rozmach tohoto malware byl v květnu 2017, kdy bylo během jediného dne zaznamenáno více jak 100 000 útoků. Do cca poloviny května bylo vybráno jako výkupné 41 bitcoinů, což je asi 70 000 USD. Celková škoda byla mnohonásobně vyšší. Největší množství zaznamenaných útoků bylo v Rusku, v Číně, na Ukrajině, v Indii, na Tchaj-wanu a v Brazilii. Útoky byly mířeny na státní organizace, univerzity, nemocnice, železniční společnosti, technologické firmy, telekomunikační firmy, ale i jednotlivce. Útoky byly zaznamenány ve více jak 150 zemích světa. Mezi nejznámější napadené firmy patří Deutsche Bahn, španělská Telefonica, FedEx nebo Hitachi.

V současné době je tento malware stále aktivní a infikuje počítače, míra jeho útoků je však menší než v roce 2017. Ovšem i v dnešní době dokáže způsobit značné škody a problémy napadeným uživatelům. Napadení uživatelé však i po uhrazení výkupného své soubory zpět již nedostanou.

Virus je možno odstranit antivirovým softwarem, ovšem již napadené a zaheslováné soubory nelze zachránit.

V roce 2018 bylo napadeno virovou nákazou velké množství továren, po důkladném zjištění bylo zjištěno, že šlo o ransomwate WannaCry, který tou dobou neměl být podle odborníků již aktivní. Zřejmě se jednalo o novou variantu, kdy počítače ani nemusí být připojeny na internet. Tento útok přinesl výrobcům značné škody, protože byla odstavena výroba čipů pro mobilní telefony, kdy nejzávažnější následek byl odstavení výroby čipů pro nový IPhone.

„Předpokládá se, že to celé bude společnost stát okolo 250 milionů USD, o což se jí sníží příjmy. Původní předpoklad příjmů za toto čtvrtletí se pohyboval mezi 8,45 až 8,55 miliardami dolarů, takže infekce nejspíš ukrojí nemalá 3 procenta.“ [6]

- Dialery přemísťuje telefonní linky na drahé telefonní linky, aniž by to volající věděli, že nevolají za normální tarif, ale na drahou placenou linku.
- Adwate obtěžuje uživatele internetu nevyžádanou reklamou**.**
- Hijacker dokáže změnit domovskou stránku uživatele.

2.3.2.5 Phishing

Podvodníci se snaží pomocí podvodných e-mailů snaží z uživatelů internetového bankovnictví snaží vylákat jejich přístupové údaje a heslo do bankovnictví, aby jim následně mohli odcizit finanční prostředky na účtu.

Většinou mail obsahuje formulář, pomocí kterého se majitel účtu má přihlásit do banky. Do svého internetového bankovnictví se však nepřihlásí, protože se jedná o podvodný formulář, kdy podvodníci získají přístupové údaje, které následně zneužijí.

První útok u nás na české klienty byl v roce 2006 na klienty banky CITIBANK.

2.3.2.6 Spam

Spam je odesílání nevyžádaného sdělení, reklam, komentářů, jsou to e-maily, které nechceme dostávat, které zaplňují naši stránku a obtěžují nás.

Mezi typický spam patří:

- nabídky s provizemi
- reklamní nabídky zboží, které jsme si neobjednali
- reklamy na hubnutí, levné mobilní telefony

Tyto e-maily jsou spamery rozesílány ve velkých množstvích z neznámé adresy, která není dohledatelná, na adresy lidí, na které vůbec tato reklama necílí.

Spam škodí protože:

- mezi spamy můžeme přehlédnout důležitý e-mail
- zaplňují nám zbytečně schránku, při stahování berou data
- ztrácíme čas při jejich třídění, rozlišování a mazání
- zatěžuji poštovní servery svým velkým množstvím odeslaných e-mailů

2.3.2.7 HOAX

Jedná se o rozesílání nepravdivé informace o tom, že je rozesílán vir, který ani neexistuje.

Tyto zprávy mají za úkol vytvořit zmatek ves společnosti. Zprávy nejsou škodlivé, ale jsou obtěžující.

3 INFORMAČNÍ TECHNOLOGIE A ORGANIZOVANÝ ZLOČIN

3.1 IT a organizovaný zločin

Výzkum kriminální situace a studium jejich zvláštností a tendencí v 21. století je nemožné bez vědeckého a technického jevu jako je obecného využití informačních technologií.

Existují tři aspekty daného problému:

- informační technologie používané orgány činnými v trestním řízení v boji proti zločincům,
- vědecký a technický pokrok uplatňovaný zločinci, zločineckými skupinami a komunitami,
- zákonná kontrola procesů souvisejících s trestním používáním počítačových technologií

3.2 IT je prostředek boje proti zločincům

Tradičním způsobem využití IT v donucovacích agenturách a zvláštních službách je výroba různých elektronických karetních souborů, databází, automatizovaných databází bank, informačních a vyhledávacích systémů na regionální, národní a mezinárodní úrovni (Interpol a další mezinárodní policejní organizace, zejména). Tento přístup byl doslova realizován od prvních dnů vzniku počítačů a má jednoznačný pozitivní účinek, nevyčerpává však zdroje moderních informačních technologií.

Skutečností je, že nové informační technologie umožňují dynamicky sledovat aktivitu delikventních komunit na zásadně nové úrovni. Podle našeho názoru je značně zajímavá americká speciální zkušenost s vývojem a používáním systémů „Oasis“ (CIA) a „Magic Lantern“ (FBI), které umožňují nejen kontrolu zločineckých komunit? výměna informací, ale také „rozbíjení“ počítačů podezřelých osob, včleňování „trojských koní“ (programové viry, které umožňují v daném počítači následující informace) atd.

Úřad pokročilých informačních technologií (AIT), který patří do CIA Science and Technology Administration, používá „Oasis“ k převodu televizního a rozhlasového vysílání na text. Tento program umožňuje rozpoznávat řeč a hlasy různých mužů a žen. V konečném textu jsou takové poznámky jako „Man 1“, „Woman 1“ a „Man 2“ atd. Pokud počítač jednou identifikoval hlas, bude jej dále znát a označit správným způsobem. Kromě toho „Oasis“ v textu vyhledává „nebezpečná“ slova (například „terorismus“, „bomba“) a jejich synonyma.

Technologie „Oasis“ zpracovává pouze anglickou řeč, ale brzy bude podporována arabština a čínština.

„Plynulá“ technologie hledá informace v dokumentech psaných v několika cizích jazycích, přičemž znalost těchto jazyků není povinná. Uživatel může do vyhledávacího pole zadat například výraz „jaderné zbraně“ a odškrtnout jazyky, které je třeba prozkoumat. Systém vyhledá dokumenty s požadovanými slovy a přeloží je do angličtiny.

Nyní může systém „Fluent“ překládat z čínštiny, korejštiny, portugalštiny, ruštiny a ukrajinštiny. Pokud je dokument považován za „užitečný“ pro další revizi, učiní osoba přesnější překlad.

Důstojníci FBI mohou číst kodifikované informace z počítačů pomocí programu „Magic Lantern“. Doposud měla FBI pouze program „masožravec“, který se zdál být bezmocný proti těm zločincům, kteří byli rychle svědky, že si své soubory zašifrovali.

Software „Magic Lantern“ nainstaluje počítačový program, který registruje všechny stisky kláves, čímž vytváří informace zadané do počítače, i když jsou kodifikovány.

Program „Magic Lantern“ odesílá virům podezřelé osobě e-mailem. Pokud to není možné, může být provedeno jménem jeho příbuzného nebo dobrého přítele. „Kouzelná lucerna“ používá také známé díry v rozprostřeném softwaru, které mají být zavedeny do počítače.

Není zcela jasné, jak „Magic Lantern“ pošle shromážděné informace zpět FBI - přes internet nebo FBI důstojník přijde a vezme je z počítače osobně. V každém případě současný „Key Logger System“ vyžaduje osobní návštěvu důstojníka.

FBI prohlašuje, že použití „magické lucerny“ bude v souladu se všemi ústavními normami a neporuší právo na soukromý život a obchodní tajemství. Toto tvrzení vyvolává určité pochybnosti, ale je to další problém.

Scotland Yard navrhl zajímavý přístup k využívání informačních technologií proti trestným činům. Posílá e-mail obyvatelům Londýna s podrobným popisem zločinců působících v jejich okresu. Policie tedy chce chránit obyvatele Londýna před kapsáři, zloději a únosci. Nyní tento systém prošel testem v jedné z londýnských čtvrtí, kde žije 40 tisíc lidí. Pokud to odůvodní naděje, budou takové zprávy zaslány obyvatelům jiných londýnských čtvrtí.

Scotland Yard počítá s tím, že tento projekt, který stojí jen dva tisíce liber, drasticky změní trestní situaci ve městě. Podle názoru policistů budou měšťané dostávat informace o zločincích e-mailem rychleji než noviny nebo pouliční plakáty.

Scotland Yard počítá s tím, že tento projekt, který stojí jen dva tisíce liber, drasticky změní trestní situaci ve městě. Podle názoru policistů budou měšťané dostávat informace o zločincích e-mailem rychleji než noviny nebo pouliční plakáty.

Pokud jde o počítačové sítě a databáze samotných donucovacích orgánů, je třeba poznamenat, že je třeba nezapomenout na zlepšení bezpečnosti správných informací (4), protože zločinecké komunity disponují moderním hardwarem a někdy najímají vysoce kvalifikované hackery.

3.2.1 Informační technologie jako nástroj trestné činnosti

První problém spočívá v tom, že nejnovější technologie stimulovaly nejen volný obchod a hospodářskou činnost, ale také delikventní. Modernizace a integrace různých komunikačních a telekomunikačních prostředků usnadnila navazování kontaktů mezi zločineckými skupinami a komunitami z mnoha zemí a kontinentů. Moderní bankovní podnikání, které široce používá různé prostředky výpočetní techniky a nové informační technologie, upřednostňuje uzavření mezinárodních delikventních transakcí. Revoluce v oblasti elektroniky poskytla zločineckým skupinám přístup k novým technickým prostředkům, které jim umožňují zneužívat obrovské finanční prostředky, vyhýbat se zdanění a praní špinavých peněz.

Druhým problémem je samotná „počítačová kriminalita“, nejmladší a nejdynamičtěji se rozvíjející oblast trestné činnosti.

Podle Institutu počítačové bezpečnosti bylo v roce 2002 asi 90 % amerických společností vystaveno počítačovým útokům a přibližně 80 % z nich utrpělo škodu v důsledku činnosti hackerů.

V roce 2002 bylo na světě opraveno více než 80 tisíc případů nezákonného proniknutí do počítačových sítí (útoky hackerů, pokusy o krádež informací atd.). Jejich počet se náhle zvýšil ve srovnání s rokem 2001, kdy bylo zaznamenáno asi 58 tisíc takových porušení (téměř 20 tisíc v roce 2000). Úmyslní zločinci se častěji zaměřují na americké sítě. V roce 2002 bylo opraveno téměř 27 tisíc počítačových útoků. Britské počítačové sítě byly vystaveny méně než 5 000 útokům, německé – asi 4,6 tisíc.

Členové organizovaných delikventních komunit – hackerů mafie, se dopouštějí zhruba 10 % počítačových útoků. Odborníci FBI se domnívají, že nejaktivnější jsou „gangsteři“ z bývalého SSSR a zemí východní Evropy.

Jediným cílem těchto hackerů je získat zisky. Jejich cílem jsou proto banky, finanční a obchodní společnosti. Teroristé také používají služby hackerů mafie. Například teroristická organizace „Republikánská armáda Irska“ (RAI) vytvořila speciální skupiny hackerských sympatizantů, kteří ukradli peníze RAI a shromažďovali informace pro budoucí teroristické činy.

Existují podezření, že speciální služby a teroristické organizace někdy používají hackery k nalezení slabých míst v počítačových systémech jiných zemí. Například v roce 2001 čínští hackeři tvrdě zaútočili na řadu amerických webů, včetně webů amerického ministerstva obrany.

Existuje mnoho analytických materiálů tohoto druhu. Například podle americké společnosti pro průmyslovou bezpečnost a Price Waterhouse Coopers Company, právě v roce 1999, ztratily korporace patřící do žebříčku Fortune Top-1000 45 miliard dolarů kvůli krádežím informací. Rostoucí zranitelnost se stává systémem bezhotovostních vypořádání. Účty více než 5 milionů držitelů karet Visa a MasterCard v USA byly nedávno zlomeny v důsledku útoku hackerů na centrum zpracovávající platby obchodních organizací.

Někteří analytici se domnívají, že kybernetičtí teroristé ohrožují ekonomiku USA jako celek (8). Ronald L.Dick, nový ředitel amerického Národního centra pro ochranu infrastruktury (NIPC), uvedl, že on-line terorismus a další druhy počítačových zločinů by mohly negativně ovlivnit ekonomiku USA, pokud by federální agentury a korporace v tomto směru pracovaly těsněji.

Pan Dick řekl, že mnoho částí země s „kritickou infrastrukturou“, včetně elektráren, kanceláří federálních organizací a životně důležitých center počítačových systémů, může být vystaveno útokům ze strany kohokoli – od zástupců vyhnanců národů po uraženou společnost. úředníci. Ve svém projevu s kolegy, kteří byli bývalými důstojníky ministerstva obrany FBI a USA, pan Dick uvedl, že právě v současné době bylo vyšetřováno asi 1400 případů trestných činů v počítačových sítích a jejich počet neustále rostl, v průměru se objevilo až 50 počítačových virů s různými ničivými silami. každý týden.

Je zřejmé, že „kriminální zdroje“ informačních technologií nejsou vyčerpány tím, co bylo zmíněno. Tato oblast je charakterizována širokým porušováním autorských práv a souvisejících softwarových práv (zejména v Rusku). Profesionální hackeři jsou přitahováni k rozbití informačních systémů bank a společností. Často se setkáváme s obchodními fakty a „virovou“ špionáží. Existuje mnoho pokusů proniknout do databází státních orgánů, včetně

automatizovaných hlasovacích systémů. Důvěrné informace jsou odcizeny (například z databází NASA). Mnoho dalších trestných činů je spácháno pomocí informačních technologií. Lze konstatovat, že blok problémů spojených s IT je nejzákladnější při vyšetřování organizované trestné činnosti a korupce.

3.2.2 IT a právo

S přihlédnutím k nebezpečí trestných činů v oblasti IT světová praxe vždy vylepšuje zákony, zpřísňuje tresty za tyto trestné činy a schvaluje odpovídající mezinárodní dohody.

V roce 2001 přijal Výbor pro trestnou činnost, který byl vytvořen v rámci Evropské rady, konečnou verzi Mezinárodní dohody o boji proti počítačové trestné činnosti. Na práci Výboru se jako zástupci podíleli zástupci ministerstva práva USA.

ZD-Net informuje, že dohoda je předložena k posouzení Radě Evropy. Dne 29. června bude její konečné znění zveřejněno na zvláštních stránkách Rady. Pokud je dokument v tomto případě schválen, obdrží jej vysoké státní orgány zemí zastoupených v Radě. Očekává se, že kromě 43 evropských zemí bude dohoda podepsána USA a státy, které patří do Evropské rady jako diváci: Mexiko, Kanada, Japonsko a Vatikán.

Před přijetím konečné verze zvážil výbor 27 variant. Vše, co očekávali, že země tento dokument podepsaly, by na místní úrovni zavedly určité minimum zákonů proti takovým počítačovým zločinům, jako je neoprávněný přístup k počítačovým sítím, zachycování dat, internetové podvody, dětská pornografie a počítačové pirátství.

Mezitímní varianty byly vystaveny této kritice, protože věnovaly malou pozornost ochraně důvěrnosti uživatelů. Bylo také zjištěno, že většina variant dohody vyvolala zásah státu do osobních věcí občanů.

USA zpřísňují trest za počítačové zločiny. Společnost Reuters informovala, že právní výbor zastupitelské komory USA schválil právní předpisy o zpřísňování trestů za počítačové zločiny. Zákon zároveň rozšiřuje práva poskytovatelů na stínování jejich uživatelů.

Podle současné právní úpravy soud volí trest pro hackery, virové spisovatele a jiné počítačové chuligány v závislosti na ekonomických škodách způsobených jejich činy. V důsledku toho většina odsouzených vystoupí s malými pokutami a pouze několik z nich má vězení, což je také malé. Například autor viru Melissa, který způsobil škodu 1,2 miliardy dolarů, byl odsouzen k 20měsíčnímu uvěznění a pokutě 5 000 $.

Podle nového návrhu budou zohledněny i další faktory. Hackerovi, který zlomil počítač s důležitými informacemi o státě, bude hrozit vážnějším trestem, než který proniká do domácích počítačů jeho sousedů.

Pokud jde o poskytovatele, budou nyní moci informovat orgány činné v trestním řízení nejen o incidentech ohrožujících život a zdraví osob, ale také o podezřelých případech s menší závažností. Současně nový zákon ruší předpisy umožňující podat žalobu proti porušení soukromí uživatelů v takových případech. Pokud prezident navíc podepíše tento zákon, budou poskytovatelé povinni uchovávat veškeré elektronické poznámky, zejména elektronickou korespondenci svých klientů, alespoň po dobu 90 dnů. Jinak jim bude hrozit vážná pokuta. Je třeba poznamenat, že položka zajišťující náhradu nákladů na zavedení stínového systému byla z právních předpisů vyloučena.

Není to však konec. Amerika jde dál. Kongres USA schválil návrh na doživotí za rozbití počítačových systémů.

Reprezentativní komora Kongresu USA schválila drtivou většinou návrh na zvýšení počítačové bezpečnosti, který dříve navrhovala vláda prezidenta. Tři sta osmdesát pět zástupců kongresu hlasovalo pro schválení tohoto návrhu, zatímco pouze tři členové - proti. Návrh zákona byl připraven v administrativě prezidenta USA před zářijovými teroristickými činy ^; truchlivé události v New Yorku a Washingtonu urychlily práci na tom a vedly k téměř jednomyslnému schválení zákona v reprezentativní komoře.

Návrh stanoví doživotní trest odnětí svobody za rozbití počítačových systémů. Rozšiřuje také práva policistů na zachycování dat. Podle návrhu zákona lze poklepáním na telefonní konverzaci a odposlouchávaním elektronických zpráv provádět bez souhlasu soudu. Jakmile bude návrh přijat v reprezentativní komoře, bude předložen k posouzení Senátu USA. Pravděpodobně tato fáze nebude mít žádné potíže.

Analogický proces hrozícího trestu se odehrává v Argentině, Číně (kde je za tyto zločiny stanoven trest smrti), Malajsii (doživotní vězení), Austrálii (až na deset let vězení) a v ostatní země. Ve Velké Británii je „Zákon o terorismu - 2000“ definován jako „terorismus“, který nejprve zahrnuje kybernetický prostor. Jak to vypadá? Je problém potrestání těchto zločinů vyřešen ruským trestním zákoníkem?

Je třeba učinit výhradu (tato otázka není nová), že ruské zákony úspěšně upravují informační vztahy. Objevila se nová oblast práva – informační právo – která se účinně rozvíjí. Až dosud bylo přijato a je v současné době více než deset zvláštních federálních zákonů. Mezi tyto

zákony patří informace, informatizace a ochrana informací, účast na mezinárodní výměně informací, státní tajemství, povinné kopírování dokumentů, soubor normativních zákonů o archivech a archivních rezervách, masmédiích atd.

Podle mého názoru zůstává závažným problémem kriminalizace akcí spojených s počítačovými technologiemi. Zavedení kapitoly 28 do trestního zákoníku Ruské federace – Trestné činy v oblasti počítačových informací – problém nevyřeší. Zdá se, že to bylo vyřešeno.

Je třeba poznamenat, že právě takový přístup byl vytvořen od samého počátku činnosti ruských zákonodárců v této oblasti. Od roku 1991 se u nás začala trestněprávní regulace v oblasti počítačových informací. V prosinci 1991 byl předložen k posouzení návrh zákona Ruské federace „Odpovědnost za delikvence při práci s informacemi“. Předpokládalo zavedení celé sady nových deliktů korpusů spojených s informacemi o počítači. Stanovisko uvedené v návrhu bylo schváleno. Část 5 vyhlášky Nejvyššího sovětu Ruské federace (RF) „Právní ochrana programů pro výpočetní techniku a databáze“ se provádí: „Vláda RF by se měla do 1. října 1992 podrobit návrhu RF Nejvyššího sovětu ve stanovených návrzích návrhů RF zákonů o zavedení změny a dodatky občanského zákoníku RF, trestního zákoníku RF a dalších souvisejících legislativních aktů “. Tento krok prokázal nutnost trestněprávní regulace právních vztahů souvisejících s informacemi.

Práce provedené tímto směrem přinesly v roce 1994 návrh zavedení dodatků do trestního zákoníku RF, který stanovil následující delikty korpusu:

- nelegální držení programů pro počítače, soubory s databázemi;

- falšování a ničení informací v automatizovaném systému;

- nezákonné proniknutí do automatizovaného informačního systému (AIS) nezákonným získáním údajů o hesle, narušení přístupu nebo obcházení mechanismu ochrany informací za účelem jejich neoprávněného kopírování, změny nebo zničení;

- vkládání nebo šíření „počítačových virů“;

- Porušení pravidel zajišťujících bezpečnost AIS.

II. PRAKTICKÁ ČÁST

4 KRIMINALITA NA INTERNETU

Kybernetická kriminalita a počet trestných činů na internetu s rozšiřujícím se internetovým dostupným připojením neustále roste.

V roce 2011 bylo evidováno 1502 trestných činů na internetu, v roce 2019 bylo těchto trestných činů 8417. Kyberkriminalita za posledních 8 let vzrostla více jak o 460 %. Tyto čísla jsou více než varující, a proto je potřeba dbát na vysoké zabezpečení našich dat, a to nejen na internetu, ale chránit si i svoje osobní data. Stále velká část lidí nevyužívá ani dvoufázové zabezpečení při přihlašování do internetového bankovnictví a pak jsou překvapeni, když jim někdo zcizí přihlašovací údaje a odcizí peněžní prostředky z bankovního účtu.

Mezi nejrozšířenější kybernetickou kriminalitu patří útoky na internetové bankovnictví, na druhém místě je ztráta osobních dat a jejich zneužití při podvodných činnostech.

Internetové bankovnictví je nejrozšířenější forma přímého přístupu jak k firemním, tak k osobním financím v bance. Přes internetové bankovnictví je možno kompletně spravovat bankovní účty, tzn. zadávat platební příkazy, zjistit zůstatek na účtu, zažádat o platební kartu nebo úvěr.

S rostoucí kriminalitou na internetu je nutno stále více více zabezpečovat svoje data, a hlavně být obezřetný, které stránky člověk navštěvuje, kam vkládá svoje osobní údaje nebo kde si ukládá v prohlížeči svoje přístupová hesla.

4.1 Kriminalita ve virtuálním prostoru

Počítačová kriminalita patří k dnešní době. Většina z nás tráví spoustu času na internetu, hledá různé informace a data, provádí nákupy na internetu, vkládá svoje osobní údaje, údaje o platebních kartách atd., takže při neopatrné manipulaci lehce dojde ke ztrátě dat a následně jejich zneužití.

Jednotlivé druhy počítačové kriminality jsou různé a čím dál tím více promyšlené.

Mezi nejznámější útoky na počítače patří:

4.1.1 Spam

Spam je nejrozšířenější způsob útoků na počítače. Nejedná se však o škodlivé útoky, jedná se o rozesílání nabídek zboží nebo služeb bez vyžádání konkrétní nabídky.

K rozesílání spamu se využívají infikované počítače, které jsou spojené do botnetové sítě a navzájem komunikují. Tyto počítače jsou pod plnou kontrolou útočníka.

První spam byl rozeslán v roce 1978. V dnešní době umí antivirové programy z velké části tyto zprávy eliminovat a při příchodu do pošty dát do složky nevyžádaná pošta.

Přesto, že nejsou tyto e-maily škodlivé, je důležité neotevírat tyto zprávy.

4.1.2 Phishing

Tento druh počítačové kriminality je zaměřen na získání PIN kódu ke kartám nebo přístupové údaje do internetového bankovnictví.

Celý princip tohoto útoku funguje tak, že pachatelé rozesílají podvodné e-maily, které vypadají jako oficiální emaily z bankovních institucí. Tyto e-maily mají za cíl získat přihlašovací údaje a heslo do internetového bankovnictví, aby se pachatelé mohli přihlásit do cizího bankovnictví a získat finanční prostředky.

Při tomto útoku je využíváno základních kódů HTML a PHP. Phishing sada je uložena na kompromitovaném serveru, kde je okolo 36 hodin a pak dojde k jejímu automatickému vymazání, aby útočník nebyl dohledatelný.

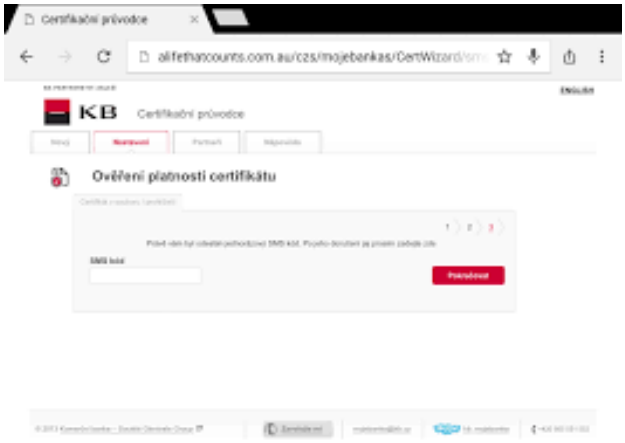
Jaká je praxe, že stále velké množství lidí se nechá takovýmto způsobem okrást? Je to velice jednoduché, do mailu přijde přihlašovací stránka internetového bankovnictví, která je na první pohled stejná s „pravou“ stránkou. Napadený je vyzvaný k tomu, aby zadal přihlašovací jméno a heslo, ovšem po zadání těchto údajů není přesměrován do svého internetového bankovnictví, ale na podvodnou internetovou stránku, kde dojde ke zkopírování jeho údajů a následně ke zneužití přihlašovacích údajů.

Jedinou možnou ochranou je dvoufázové ověření, kdy kromě zadaného přihlašovacího jména a hesla musí být přihlášení potvrzeno ještě ve spárovaném telefonu.

Vlastně nejlepší ochrana je, na takové e-maily vůbec nereagovat, protože banka tímto způsobem se svými klienty nekomunikuje.

Největší pishingové útoky zaznamenala Komerční banka v roce 2015 a bojuje s těmito útoky na své klienty do dnešní doby. Proto radí svým klientům, aby:

- nikdy neotevírali podezřelé e-maily
- nikdy nesdělovali nikomu svoje hesla a přístupové údaje
- měli dobře zabezpečený počítač
- nikdy nenakupovali na podezřelých internetových stránkách
- instalované aplikace do počítače nebo telefonu pocházely vždy od důvěryhodného zdroje



Obrázek 1 Přihlášení do internetového bankovnictví [12]

Obrázek 2 Podvodný email [12]

Po těchto útocích dala Komerční banka svým klientům k dispozici specializovaný software pro přihlašování do internetového bankovnictví Trusteer Rapport a ve velice krátké době došlo k tomu, že se se o více jak 90 % snížilo přihlašování do internetového bankovnictví ze zavirovaných počítačů.

4.1.3 Carding

Tento druh útoku je zaměřený na odcizení platební karty, získání čísla platební karty, zjištění PIN kódu a následně její využití v prospěch pachatele při internetových nákupech.

Novým způsobem získání karty podvodným způsobem je tzv. skimming. Tento druh útoku je prováděný přímo na bankomatu banky, na zařízení bankomatu je nainstalované čtecí zařízení, které má za úkol kartu zkopírovat, a kamera, která je naistalována na bankomat nelegálně, získá informace o PIN kódu ke kartě. A následně pachatelé začnou využívat podvodně získaná data z platební karty na svoje nákupy na internetu.

Obrázek 3 Skimming [13]

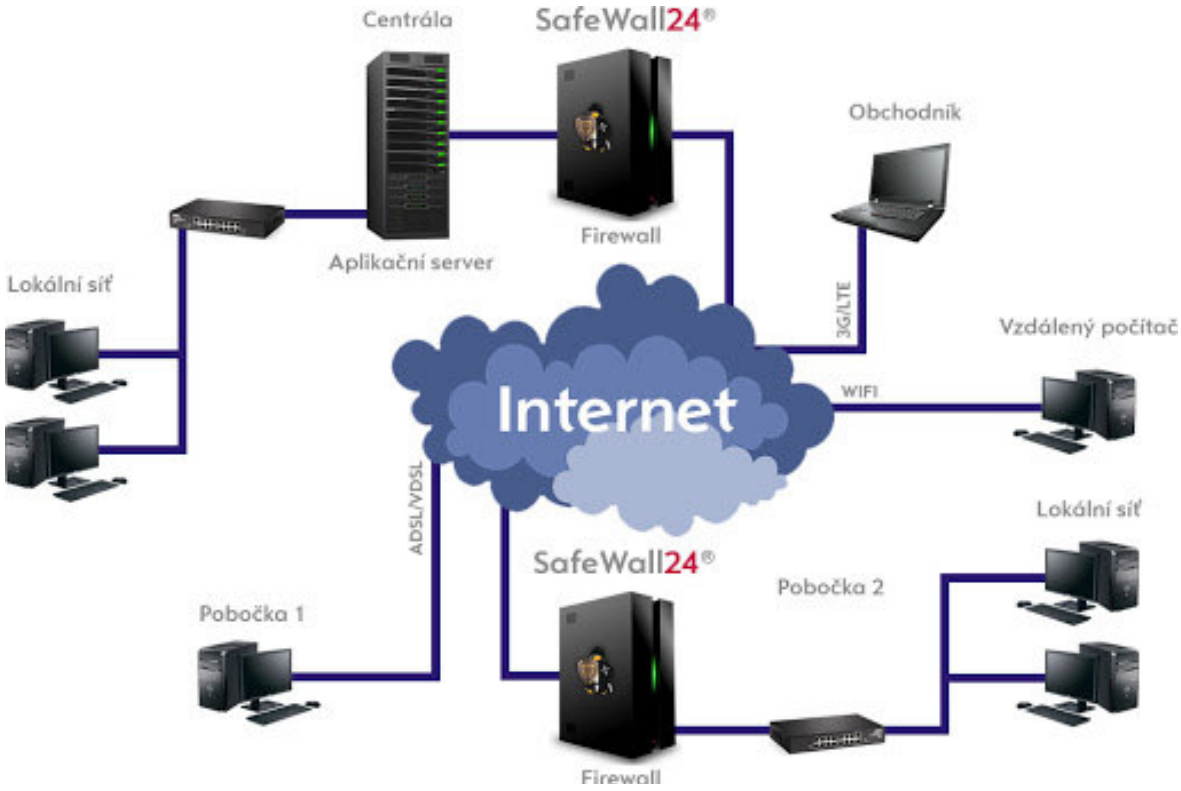
4.1.4 Sniffing

Sniffing je speciální technika, která umožňuje odposlouchávat počítače v síti v místní síti. Mohou být odposlouchávány např. informace, které se nemají dostat ke konkurenci (např. výrobní postupu, plán nových výrobků) a sniffer, pokud je získá, je může konkurenci prodat.

Fyzicky k tomu dochází tak, že je ukládán TCP paket, který je následně čten a jsou získána potřebná data. K odposlechu je potřeba zařízení sniffer a softwarové vybavení, které umožňuje odposlouchávání. Sniffing může dělat správce sítě, který má neomezený přístup k firemním počítačům, snifferem může být i uklízečka, která vyslechne rozhovor dvou kolegů, který mají poradu na citlivé téma. Siffera je velice těžko najít a usvědčit.

Jediná bezpečná cesta proti sniffingu je, odesílat zabezpečená data přes SSL certifikát a určitě nejednat o důležitých věcech, novinkách atd. před nikým dalším, byť se jedná o dlouholetého pracovníka firmy. Firemní síť by měla být zabezpečena heslem a neměl by být

dovolenou přístup cizímu návštěvníkovi připojení ani na chvíli za účelem např. prezentace připojení do firemní sítě.



Obrázek 4 Ochrana vnitřní sítě [14]

5 FYZICKÉ PODVODY

Krádeže identit nebo citlivých údajů prostřednictvím informačních technologií neustále v posledních letech roste. Obětmi se stávají jednotliví lidé, ale také i firmy.

Ke zneužití našich osobních dat dochází každý den a různými způsoby, proto je nutno chránit nejen veškerá osobní data na internetu, ale i ID doklady, které jsou pro nás průkazem naší totožnosti. ID doklad může být velice lehce zneužit při internetové kriminalitě nebo při finančních podvodech. Ztráta našeho osobního dokladu, ať naší vinou nebo nechtěným zkopírováním neoprávněnou osobou nás může stát spousty peněz, problémů a nepříjemností. Dnes existují i internetové stránky, kde jsou ID karty nebo řidičské průkazy z různých zemí nabízené na internetu k prodeji za malou částku. Samozřejmě se jedná o padělky, ale padělky vysoce vydařené. Protože k jejich výrobě se využívají moderní informační technologie, jsou na první pohled nerozeznatelné od originálu, obzvláště pro lidské oko. Proto je nutno doklady chránit bezpečnostními prvky.

Jednou z největších firem, které v České republice zajišťují výrobu ID dokladů a platebních karet, je firma Eltrax v Havířově. Firma používá k výrobě ID dokladů a platebních karet vysoké bezpečnostní zabezpečovací prvky a některé z nich jsou unikátní a firma je má celosvětově patentované pro výrobu ID dokladů. Samozřejmostí je, že výroba probíhá nejmodernějšími výrobními informačními technologiemi.

5.1 Bezpečnostní prvky na ID dokladech

Je bezpodmínečně nutné, aby se padělatelům co nejvíce znemožnilo padělání osobních dokladů, aby výroba těchto padělaných dokladů byla tak vysoce drahá a náročná pro padělatele, aby se jim nevyplatilo ID karty vůbec padělat.

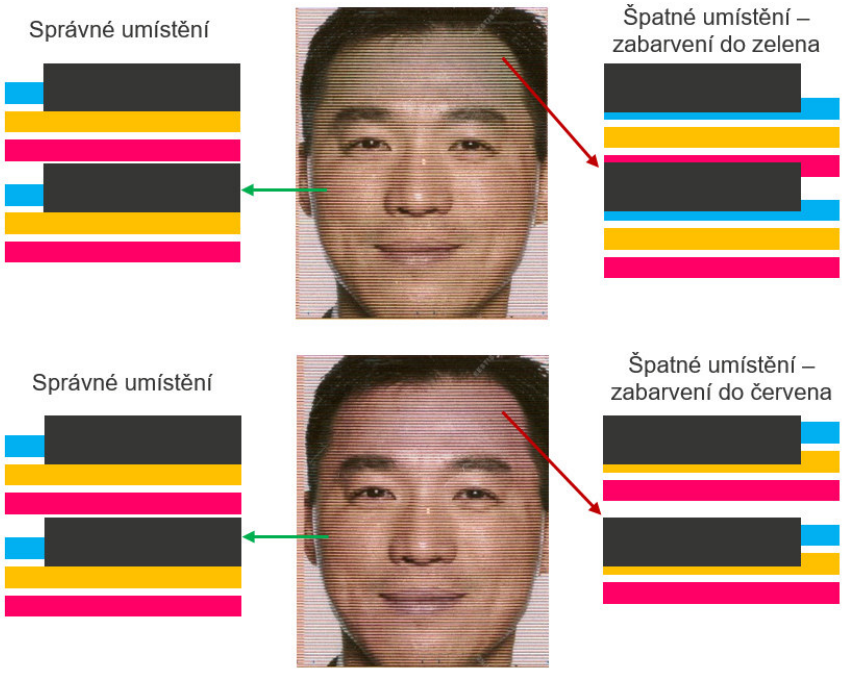
V následujících bodech se budu zabývat ochrannými prvky na ID dokladech.

Způsoby zabezpečení dokladů:

5.1.1 Lasing technologie

Jedná se o světový unikát, pro ochranu fotografií na osobních dokladech. Firma Eltrax má patent na tuto technologii a celosvětově je touto technologií pokryto 34 % trhnu výroby všech ID dokladů.

Na každém dokladu jsou tři proužky – červený, žlutý a tyrkysový. Speciální výrobní metodou jsou jako miniaturní černé tečky se vyrobí na ID doklad fotografie. Takto vzniklá fotografie je barevná a jedinečná. Tento způsob výroby fotografie na doklad umožňuje i to, že např. do horního koutku oka se natiskne speciální znak, nápis nebo cokoliv, co není běžným okem viditelné. Policista nebo úředník, který následně provádí kontrolu občana a kontroluje jeho doklad, má u sebe malou plastovou kartičku, která se přiloží k fotografii na dokladu a ihned policista zjistí, zda je doklad pravý nebo padělaný, protože přes tuto speciální folii, je vidět, jak vyražený nápis v oku, tak i fotografie, když je vidět správně, má své ochranné prvky při výrobě.



Obrázek 5 Tisk fotografie [15]

Na obrázku je vidět, že vlivem laminace dochází k deformaci Lasingu (barvy), Při personalizaci dokladu se tiskne pouze černou barvou. V případě deformace Lasingu dochází k nesprávnému umístění neboli spasování černé barvy a výsledný obraz personalizace má neshodnou barevnost.

5.1.2 Bezdrátová anténa s čipem

V každém vyrobeném dokladu, který je chráněn touto technologií, je zabudován čip s anténou, kdy v každém čipu je nahrané sériové číslo dokladu. Toto sériové číslo musí být shodné s číslem dokladu, které je čitelně vypálené na ID kartě jako číslo dokladu. Tato technologie se využívá například na ID dokladech v Maroku, kde je číslo dokladu propojené s národní databází občanů, kde je nahraná fotografie každého občana a jeho rodné číslo. Takže, když dojde např. ke kontrole občana policií Maroka, policejní úředník ihned při kontrole vidí v databázi občanů, zda ID doklad je uveden v databázi nebo zda je doklad nepravý. Provede kontrolu čísla, fotografie a rodného čísla občana.

5.1.3 Čáry na dokladu

V dokladech jsou barevné čáry – žlutá, modrá, tyrkysová – vzdálenost čar od sebe je v desítkách mikronů, tloušťka čáry je 60 mikronů. Technologii laiser se vpalují černé tečky a vzniká na dokladu barevné fotografie pro identifikaci občana. Rozlišení tisku fotografií na dokladech je 12.000 dpi. Pro porovnání, pokud tiskneme kvalitní kancelářský dokument, je rozlišení 300 dpi.

Obrázek 6 Ochranné čáry [15]

Pod speciální folii na kontrolu pravosti dokladu jsou opět vidět tyto čáry, které okem nejsou viditelné a mají zabránit padělání ID dokladů.

Tuto ochranu využívá při výrobě svých dokladů například Litva.

5.1.4 Tiskové efekty

Tiskové efekty jsou další součástí ochrany osobních dokladů, kdy tyto speciálně vytištěné efekty jsou viditelné pouze pod mikroskopem. Například u výroby dokladů pro Litvu se využívá efekt OVI. Na doklad je vyroben speciální tiskovou technologií zeleno-zlatý lístek. Tento lístek je viditelný z různých úhlů pohledu na doklad různými barvami. Při kontrole pravosti dokladů se pak hodnotí, zda vytištěný lístek je opravdu z různých úhlů různě barevný. Pokud by byl pouze jednobarevný, je doklad padělaný.

5.1.5 UV ochrana

UV ochrana se využívá jako další ochranný bezpečnostní prvek. Na doklad je vytištěn speciální obrázek, většinou na zadní stranu dokladu, který pod UV světlem vypadá jako fotografie. Většinou se u této technologie využívá pro tisk ochranného obrázku 2–3 barvy, kterým je obrázek vytištěn. Tato technologie se považuje za důležitou a velice složitou ochranu dokladů. Doklady pro Taiwan jsou tištěny s nejvyšším možným počtem použitých barev a mají v tomto směru nejvyšší možnou ochranu. Doklady pro Maroko jsou chráněny 2 barvami, kterými je na zadní straně vytištěn obrázek mešity, který je viditelný pouze pod UV světlem. Barvy musí být při výrobě dobře promíchané, aby byla barevná škála vždy stejná a výsledný obrázek měl odpovídající barevné rozlišení.

5.1.6 Punch window

Punch window je moderní technologie, kterou využívá například Litva. Jedná se o další bezpečnostní prvek proti padělání dokladů. V dokladu je lisovaná díra, kdy zapadají části do sebe

5.1.7 Tiskové efekty

Tiskové barvy na ID doklady mají speciální vlastnosti, aby bylo padělání dokladů co nejvíce padělatelům ztíženo. Speciální vlastnosti barev jsou viditelné pouze pod mikroskopem, kdy např. modré barvě jsou miniaturní stříbrné třpytky. Tyto barvy jsou několikanásobně dražší než normální barvy (3 litry této barvy stojí okolo 2.000 €). To, že se využívají speciální

barvy, které jsou drahé a mají speciální vlastnosti, je pro padělatele problém, že by se výroba padělaných dokladů velice prodražila.

5.1.8 Speciální materiál

ID karty jsou lisované ze speciálních plechů. Každá karta je z 5–7 vrstev plechů, které jsou určitou teplotou a tlakem lisované k sobě. Výsledná ID karta má tloušťku 0,83 mm a má speciální gravírovací znaky, které brání snadnému kopírování dokladů. Vygravírované znaky jsou pozitivní – po přejetí karty rukou, jsou cítit vystouplé znaky, nebo negativní, kdy po přejetí jsou cítit vygravírované znaky jako „prohlubeň“.

5.1.9 Matový efekt

Matový efekt je viditelný pouhým okem, celá ID karta je lesklá a obrázek je matný. Tento ochranný prvek je cítit pouhým přejetím prstu.

5.2 Bezpečnostní prvky na platebních kartách

Platební kartu v dnešní době používáme všichni. Platební karta je nástroj sloužící k bezhotovostní úhradě zboží, služeb nebo k výběru hotovosti z bankomatu. Výroba a používání platebních karet se řídí zákonem č.124/2002 Sb. o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku).

Platební karta je plastová karta, která je jednoznačně vydaná pro svého uživatele k jeho peněžnímu účtu a musí mít určité vlastnosti a ochranné prostředky.

I když mají karty svoje ochranné prvky, nejsou tak zabezpečené jako jsou ID doklady. Hologramy, které jsou na každé platební kartě jsou lehce padělatelné, a proto výrobci karet vždy za určitý čas vzhled těchto hologramů aktualizují.

Výrobci karet se snaží výrobní náklady na platební karty minimalizovat, protože se jedná o soukromé organizace, které mají jeden z předních svých cílů maximalizovat zisk. Oproti tomu výroba ID dokladů je hrazena státem, kdy na prvním místě je bezpečnost a zabezpečení dat a nemožnost padělání a kopírovaní dokladů.

V porovnání náklady na výrobu platební karty s čipem je 17,50 Kč a oproti tomu ID karta pro Taiwan, která má nejvyšší zabezpečení, jsou výrobní náklady 150 Kč za kus.

Při výrobě karet se využívá tzv. metoda roztrženého dolaru. Firma, která vyrábí plastové karty, zamkne polovinu čipu inicializačním klíčem (program na PC, který aktivuje kartu). Inicializátor u příjemce karet má druhou polovinu inicializačního klíče, pokud klíče navzájem do sebe pasují, je karta inicializovaná a může být personalizovaná pro konkrétní osobou ke konkrétnímu číslu účtu. Protože karty nelze jinak při převozu elektronicky chránit proti krádeži, je tohle nejbezpečnější způsob zabezpečení převozu karet z výroby k inicializátorovi karet.

Bezpečnostní prvky na platebních kartách:

5.2.1 Hologram

Hologram není v dnešní době žádná ochrana karty, protože v Číně umí tento hologram velice lehce padělat na počítači a vyrobit za velice nízkou částku

5.2.2 Hologram

Magnetická páska neobsahuje žádné informace, protože její kopírování je velice lehké. V dnešní době je hlavní funkcí této pásky otevírání dveří banky při přístupu k bankomatu, když jsou dveře mimo otevírací dobu uzavřené.

5.2.3 Čip

Na čipu karty, který je spojen s anténou v kartě jsou uložené veškeré informace o majiteli karty, včetně čísla účtu, ke kterému je karta vydaná. Na čipu je uložen i bezpečnostní prvek karty – PIN. PIN slouží k přístupu ke kartě a možnosti platby kartou. Každá karta je spojená s PINem. Nejčastější útoky jsou na bankomaty, kdy je na čtecím zařízení falešné zařízení, které si „přečte“ veškeré informace uložené na kartě. Na jiném místě na bankomatu je kamera, která snímá PIN. Ve chvíli, kdy padělatelé získají data o platební kartě včetně PINu, začnou nakupovat na internetu na tuto „zcizenou“ platební kartu dokud majitel karty nezjistí, že mu odchází finanční prostředky z účtu, ke kterým nezadal sám žádný příkaz. Všechny banky nabízí pojištění ke kartám, které kryje i tyto nenadálé případy krádeží na internetu.

Obrázek 7 Stroj na kontrolu bezpečnostních prvků [15]

6 KRIMINALITA ŠÍŘENÁ PROSTŘEDNICTVÍM INFORMAČNÍCH TECHNOLOGIÍ

Mezi útoky, které směřují ke zneužití počítačů, dat a jiných informací, kdy je počítač prostředek k páchání trestné činy můžeme zařadit počítačové, finanční a investiční podvody, finanční hry, hry hazardního charakteru. Nejjednodušší způsob získání finančních prostředků pomocí informačních technologií, je manipulace s daty, jejich úprava k tomu, aby pachateli přinesly požadovaný výsledek.

V 90.-tých letech se daly trestné činy v kyberkriminalitě dělit na

- Trestné činy páchané proti počítačům
- Tresné činy páchané pomocí počítači

Dnes již toto jednoduché členění nestačí, protože se dá říčí, že pomocí infomačních technologií lze páchat jakoukoliv trestnou činnost, kde není nutná přítomnost pachatele na místě. Samozřejmě, že trestný čin nemusí být přímo proveden pomocí informačních technologií, ale pachatelé se mohou pomocí informačních technologií domlouvat na podrobnostech spáchání trestného činu, který jinak musí provést fyzicky.

Členění trestné činnosti podle Úmluvy o počítačové kriminalitě dělí trestné činy do čtyř základních oblastí:

- Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a počítačových systémů – neoprávněný přístup, neoprávněné odposlouchávání, narušování dat
- Trestné činy se vztahem k počítači – počítačové padělání, počítačový obchod
- Trestné činy se vztahem k obsahu počítače – dětská pornografie
- Trestné činy související s porušováním autorského práva a práv s ním souvisejících

6.1 Trestné činy, při níž jsou informační technologie prostředek jejich páchání

Nejčastějším trestným činem, kdy je prostřednictvím počítače nebo jiné informační technologie proveden zločin, je neoprávněný převod finančních prostředků na účet. Za účelem převodu peněz pachatelé již předem založí účet, který není dohledatelný. Většinou jsou terčem těchto útoků velké finanční ústavy, telekomunikační ústavy a další velké firmy. 70 % všech těchto trestných činů souvisí se zaměstnanci dané instituce nebo bývalí zaměstnanci.

Sociální inženýrství – jedná se o jednoduchý a velice dostupný nástroj, kdy se využije lidský faktor a jeho zvídavost a důvěřivost. Na tento jednoduchý trik, kdy pachatelé získávají prostřednictvím falešných internetových stránek a e-mailů čísla bankovních účtů, přístupové údaje do internetového bankovnictví nebo čísla karet, každý rok doplatí 5–10 % z celkově zaslaných falešných zpráv.

Nejčastější způsoby kyberiminality šířené pomocí počítače jsou:

- phishing
- cyberstalking, kyberšikana
- hoaex
- carding
- pornografie
- extremismus
- vydírání a elektronické výpalné
- podvody a zpronevěra

6.2 Nejčastější formy kriminality

Nejčastější způsoby páchání trestné činnosti v oblasti kyberkriminality jsou:

- útoky směřující na uživatele sociálních sítí, tzn. sexting, kyberšikana, kybergrooming, kyberstalking, hatecrime, hacking. Podpora propagace hnutí podporující potlačování svobody člověka

- dětská pornografie
- pornografie při níž se projevuje neúcta k člověku nebo pornografie člověka se zvířetem, její šíření a výroba
- neoprávněné útoky do počítačového systému s cílem zcizit data, útoky ransomware, DDoS, malware
- legalizace výnosů z trestné činnosti – placení virtuálními měnami
- páchání trestné činnosti pomocí prostředí darknetu
- podvodné prodeje na podvodných serverech, podvodné e-shopy
- útoky na elektronickou komunikaci – phishing, spam, pharming, spear phishing
- nelegální šíření hudby, filmu nebo softwaru bez autorských práv (neoprávněné kopírování hudby, filmů, softwaru)
- napadení systému IOT

6.2.1 Útoky na uživatele sociálních sítí

Sociální sítě jsou určené na seznamování, kontakt s novými i stávajícími kamarády, rychlou komunikaci, sdělování informací většímu počtu lidí najednou. Ovšem naše informace, které zveřejňujeme na sociálních sítích jsou zveřejněné pro všechny naše kontakty a podle nastavení pak i pro kontakty našich kontaktů. Proto je nutné velice obezřetně zveřejňovat na internetu informace o sobě, protože informace jednou zveřejněné, nejdou vzít zpět. Pro případné útočníky jsou pak všechny informace dobré – jaké má člověk koníčky, zda jede na dovolenou a kam. Pak se jednodušeji jim pracuje a ví, kam člověka nalákat, jaká jsou jeho slabá místa. Zejména pak děti jsou lehkým terčem a může docházet ke kyberšikaně nebo sextingu.

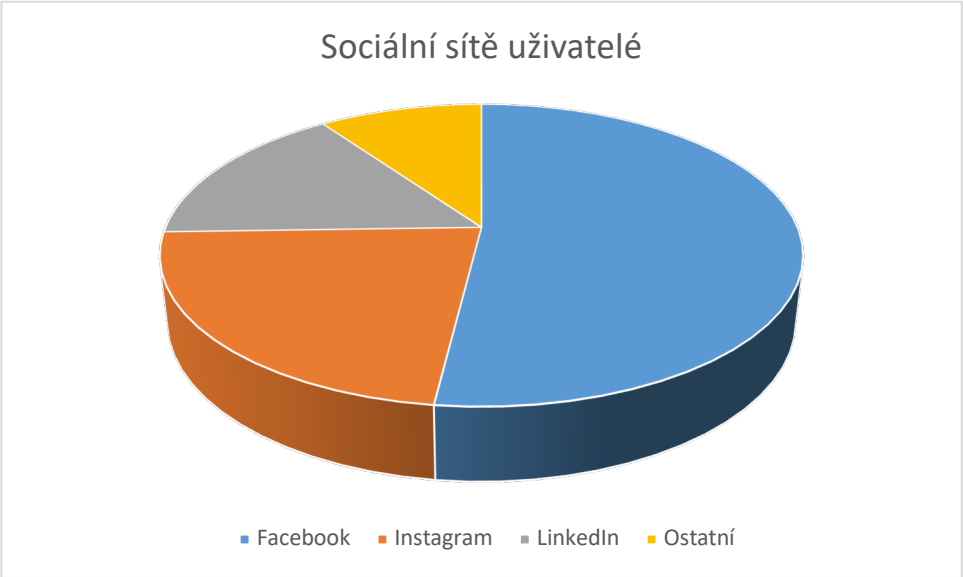
V současné době existuje celá řada sociálních sítí, které jsou využívány mnoha uživateli. Mezi nejznámější patří: Facebook, YouTube, Whatsapp, Wecha, Google+, Shazam, Linkedin, Dropbox, iCloud, Skype, Twitter, iMessage, Facebook Messenger, Instagram, Badoo, Viber, Snapchat atd.

Počet uživatelů internetu v České republice v roce 2010 bylo 7 milionů. Denní počet uživatelů internetu bylo 6,1 milionu obyvatel.

Počet lidí na sociálních sítích 5,7 milionu, počet uživatelů přes mobilní telefon 4,8 milionu.

Sociální síť	Počet uživatelů
Facebook	5,3 milionů
Instagram	2,3 milionů
LinkedIn	1,6 milionů
Twitter	389 tisíc
Snapchat	615 tisíc

Tabulka 1 Počet uživatelů sociálních sítí



Graf 1 Počet uživatelů sociálních sítí

Celkově využívá sociální sítě 52,6 % žen a 49,4 % mužů.

Ženy nejvíce využívají Instagram 54 %, muži jsou nejaktivnější na Twitter 74 %

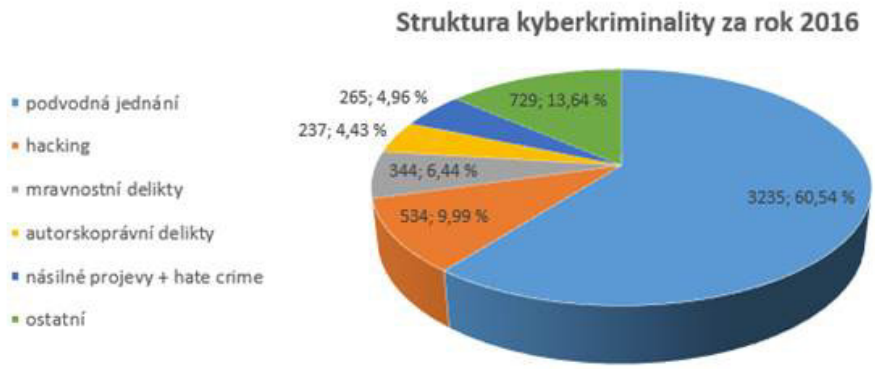
Při kyberšikaně jsou většinu zakládány nepravé profily na sociálních sítích a na těch jsou zveřejňovány informace, fotografie vedené proti poškozenému.

Projevy kyberšikany:

- vydávání se za někoho jiného
- vyloučení a ostrakizace – dnešní mládež tráví většinu volného času na internetu a sociálních sítích, proto je pro ně velice důležité, zda je jejich kamarádi přizvou do

svojí skupiny na sociálních sítích či nikoliv. Pokud jsou ze skupiny vyloučeni, dochází velice často k frustraci.

- Flaming – tento výraz se využívá pro hádku na sociálních sítích. Velice často v různých skupinách dochází k tomu, že je hádka vyvolána úmyslně za účelem toho, aby pak oběť mohla být urážena vulgárními výrazy, urážkami nebo ji mohlo být vyhrožováno.
- kyberharašení, kyberstalking – agresor zasílá oběti velké množství obrázků, které oběť bere jako nepříjemné, urážlivé.
- pomlouvání – jedná se o šíření nepravdivých informací o oběti za účelem poškození oběti
- odhalení a podvádění – agresor šíří po sociálních sítích informace o oběti, které nejsou pravdivé a mají za cíl oběti ublížit
- sexting – jedná se o rozesílání obrázků nebo zpráv se sexuálním podtextem, které mají za cíl kompromitovat oběť, ublížit jí a někdy i vydírat.



Graf 2 Struktura kyberkriminality v roce 2016 [11]

Velice častým jevem na sociálních sítích je tzv. hoax, kdy dochází k šíření nepravdivé poplašné zprávy. V roce 2019 více jak polovina Čechů naletěla na hoax zprávu.

6.2.2 Dětská pornografie

Dětská pornografie na internetu je nelegální a trestná. Za šíření dětské pornografie se považují fotografie dětí se zvýrazněnými pohlavními orgány.

Policie stále bojuje s touto formou kriminality na internetu.

6.2.3 Podvodné e-shopy

On-line nákupy se těší čím dál tím větší oblibě, ovšem s rostoucím zájmem kupujících o nákupy na internetu roste i množství podvodů v oblasti prodeje na intertnetu. V současné době má 65 % české populace zkušenosti s nákupem na internetu. Podle statistik České policie stouply podvody v kyberprostoru v této oblasti za posledních sedm let více jak o 241 %.

Je potřeba u neznámých e-shopů se zaměřit na maličkosti, které mohou napovědět, že se jedná o podvodný e-shop, jako jsou např. nízké ceny, není uveřejněna adresa sídla, jediná platební možnost je platba předem na bankovní účet nebo platba kartou.

E-shopy, které jsou založeny s cílem získaní peněz neoprávněně, většinou obdrží peníze od zákazníka, ale zboží zákazníkovi nedoručí, následně přestane reagovat na maily, nezvedá telefony a vlastně se vytratí z trhnu.

U podvodných e-shopů při platbě předem na bankovní účet nebo platbě kartou platba většinou míří do nějaké banky v cizí zemi, jako je například Brazílie nebo Kypr. Pachatelé vždy peníze převedou přes několik bank tak, aby platba nebyla vystopovatelná.

Každý rok ČOI obdrží přes 6 tis udání na podezřelé e-shopy, které vybraly peníze od zákazníků a nedoručily zboží.

Na černé listině ČOI je přes 600 nebezpečných webů.

Rok	Počet nebezpečných e-shopů
2015	4
2016	4
2017	131
2018	365
2019	425

Tabulka 2 Počet nezabezpečených e-shopů

Graf 3 Počet nezabezpečených e-shopů

6.2.4 Útoky na elektronickou komunikaci

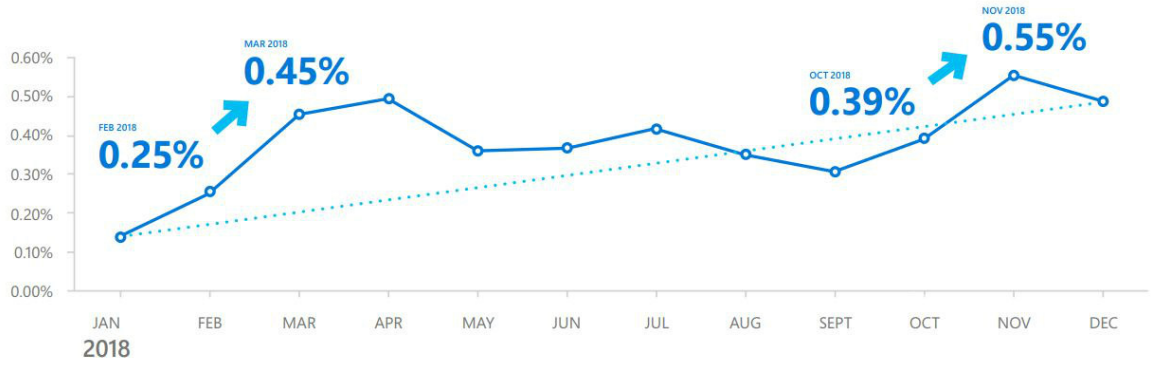
Jeden z druhů útoků na elektronickou komunikaci je spam. Spam je hromadně rozesílaná elektronická pošta. Nejedná se o žádnou reklamu, která by cílila na konkrétní okruh lidí, jedná se o hromadné rozesílání zpráv na obrovské množství e-mailových adres. Adresa odesílatele není skutečná, odesílatel je neexitující adresa. Kdyby spammeři rozesílali spamy ze své skutečné dresy, byli by lehce dohledatelní a mohli by být trestáni, protože rozesílání spamu se bere za obtěžující nevyžádané zprávy.

Poměr počtu poslaných mailů a rozeslaných spamů je 93 % spamů a pouze 7 % e-mailových zpráv. Každý den je rozesláno přes 107 miliard spamu.

V roce 2019 patřilo Česko mezi největší rozesilatele spamu, každý stošedesátý spam byl odeslán z České republiky.

Dalším druhem útoku na elektronickou komunikaci je phishing, v překladu rybaření. Útočníci se snaží získat citlivá data napadených, jejich hesla, přístup do banky, osobní údaje, čísla účtu. Tento druh zpráv se říší podvodnými e-maily nebo přesměrováním na podvodné webové stránky.

Kybernetiční útočníci používají velkou škálu metod a stále je mění. V roce 2018 narostl počet rozeslaných phishingových e-mailů celosvětově o 250 %.



Graf 4 Podíl phishingových e-mailů na počtu celkově odeslaných e-mailů [16]

6.2.5 Porušení autorských práv

Porušování autorských práv je nelegální kopírování software, hudby, filmů, programů aj. bez souhlasu nositelů autorských práv a šíření těchto souborů dále mezi ostatní uživatele.

Jedná se o duševní vlastnictví, které nesmí být nelegálně šířeno dále.

Největším nelegálním úložištěm filmů, hudby atd. je Uloz.to. Počet návštěv v prosinci 2019 byl přes 20 milionů návštěvníků tohoto serveru. Přes 132 tisíc odkazů je na tomto serveru.

Internetové stránky Filmydokapsy.cz zveřejnily návštěvnost serverů s nelegálním obsahem:

Úložiště	Počet návštěv
uloz.to	20 160 000
sledujserialy.to	12 840 000
freefilm.to	6 920 000
bombuj.tv	5 910 000
najserialy.to	5 330 000
websharte.cz	2 790 000
fastshare.cz	2 320 000
prehrajto.cz	1 800 000
freeserial,to	1 540 000
halispy.cz	1 230 000

Tabulka 3 Návštěvnost úložišť

Graf 5 Podíl návštěv úložišť

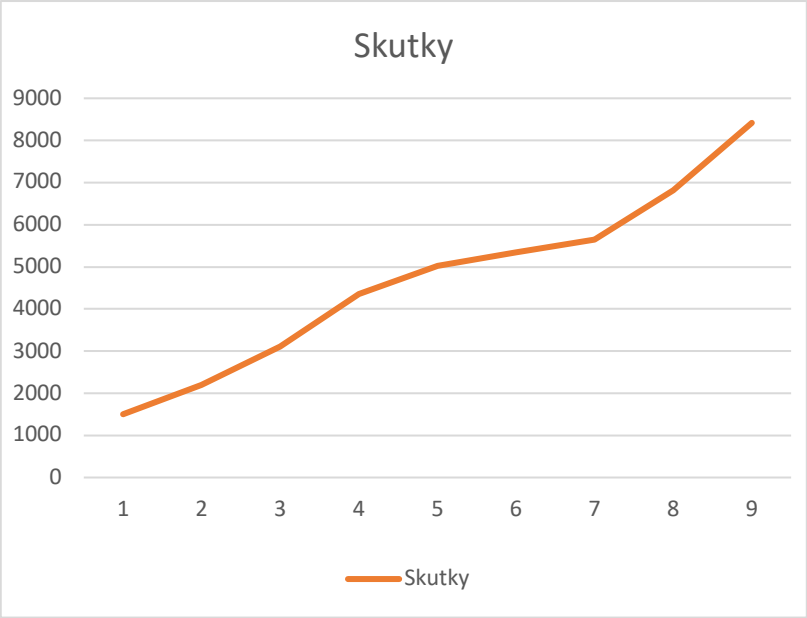
Proč lidé vůbec stahují tento nelegální obsah? Důvodem je cena, pokud si stáhnout film z některého serveru s nelegálním obsahem, platí pouze za to, pokud chce, aby byl obsah stažen rychleji, a to cca 1 Kč až 10 Kč. Pokud si zaplatí film legální cestou, je cena 100 až 400 Kč za film.

6.3 Kyberkriminalita v České republice

Vývoj kybernetické kriminality má v posledních letech stoupající tendenci a velmi silný dynamický vývoj. V roce 2019 bylo 8 417 trestných skutků, v roce 2018 bylo zaznamenáno 6 815 skutků, což je 23,8 % nárůst.

Rok	2011	2012	2013	2014	2015	2016	2017	2018	2019
Skutky	1 502	2 195	3 108	4 348	5 023	5 344	5 654	6 815	8 417

Tabulka 4 Kriminalita v České republice



Graf 6 Skutky kriminality

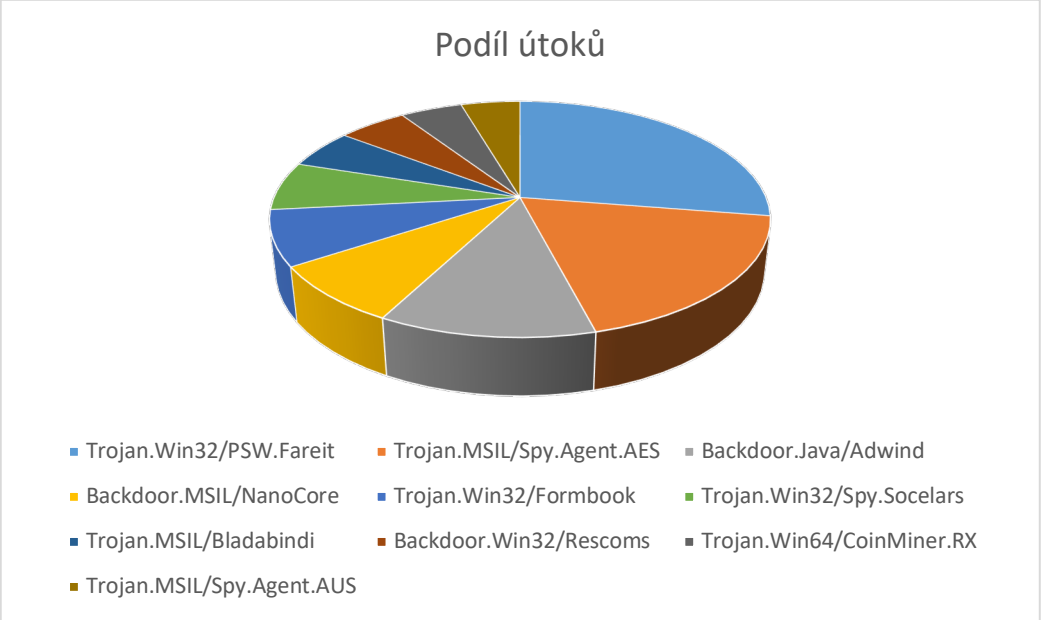
6.4 Nejčastější kybernetické hrozby v České republice v roce 2019

Každý rok jsou nové a nové hrozby, kterými data napadána a počítače a chytré telefony musí být proti nim chráněny.

V roce 2019 byly zaznamenány tyto nejčastější kybernetické útoky:

Druh útoku	podíl v %
Trojan.Win32/PSW.Fareit	7,67
Trojan.MSIL/Spy.Agent.AES	5,14
Backdoor.Java/Adwind	3,29
Backdoor.MSIL/NanoCore	2,24
Trojan.Win32/Formbook	2,11
Trojan.Win32/Spy.Socelars	1,86
Trojan.MSIL/Bladabindi	1,5
Backdoor.Win32/Rescoms	1,48
Trojan.Win64/CoinMiner.RX	1,33
Trojan.MSIL/Spy.Agent.AUS	1,27

Tabulka 5 Kybernetické útoky



Graf 7 Podíl útoků

7 PREVENCE KYBERKRIMINALITY

V poslední době je kyberkriminalita neustále na vzestupu a je nutno zavádět stále nová a nová opatření proti kriminalitě, ministerstvo vnitra se rozhodlo, že více bude dělat osvětu toho, jak má bezpečné chování na internetu vypadat. V rámci Dne bezpečného internetu uveřejnilo Ministerstvo vnitra 10 nových video spotů „Pozor na kyberprostor“, kde jsou uvedeny jednotlivé druhy kybernetické kriminality a také to, jak se proti ní bránit a jak se na internetu chovat bezpečně.

Nejčastějším kriminálním činem na internetu je podvodné jednání. V roce 2019 o třetinu vzrostl hacking, kdy je využíváno tzv. děr v různých aplikacích a hrách a počítač v tu chvíli není dostatečně ochráněn, pachatelé získají z počítače potřebné údaje a data.

V České republice upravuje trestné činy v kyberprostoru zákon č. 40/2009 Sb., kdy trestným činem je:

- neoprávněný přístup k počítači nebo nosiči informací
- poškození záznamu v počítači nebo na nosiči informací
- získání a přechovávání přístupového zařízení a uchování hesla k počítačovému systému jiné osoby nebo firmy
- šíření pornografie
- výroba a šíření dětské pornografie
- porušení autorského práva
- hanobení

7.1 Tvoje cesta onlinem

Ministerstvo vnitra spustilo nový projekt určen pro děti a mládež, který má ukázat, jak se pohybovat na internetu bezpečně, jak se chránit. Především ukazuje na příkladech, jak se útočníci snaží získat data, jaké nebezpečí hrozní dětem na sociálních sítích a jak se mají děti na internetu chovat a jaké dodržovat bezpečnostní zásady a pravidla.

Hlavním partnerem tohoto projektu je ČSOB, která pomáhá šířit osvětu po školách po celé České republice.

Problémem je, že děti a mládež v dnešní době na sociálních sítích tráví většinu svého volného času, není to jako dříve, kdy nebyl internet a mobilní telefony k dispozici vůbec nebo v takové míře, děti si hrály navzájem spolu venku, znaly se a problém s neznámými útočníky nebyl. V dnešní době tím, že tráví čas na sociálních sítí, komunikují s lidmi, které ani kolikrát neznají, se velice snadno může stát, že je dítě napadeno tzv. predátorem, který se snaží od nich získat citlivá data nebo je jinak zatáhnout do trestné činnosti.

Je potřeba, aby se rodiče aktivně podíleli na výchově svých dětí a vysvětlili jim případná rizika, která je mohou na internetu ohrozit. Tento projekt České policie a ČSOB banky má pomoci, ale hlavní roli stále hraje výchova v rodině.

8 DOTAZNÍKOVÉ ŠETŘENÍ

V praktické části jsem nejprve stanovila jasné cíle svojí práce. Na jejich základě jsem připravila otázky a zvolila metodu dotazníkového šetření. K dotazování bylo vybrán vzorek 50 lidí s různými pracovními pozicemi.

8.1 Cíl práce

1. Zjistit, zda běžný občan byl v minulosti max. 3 let cílem hackerských útoků
2. Zjistit, zda útok byl na počítači, mobilním telefonu nebo tabletu
3. Jaký typ útoku – útok hrubou silou nebo spam

8.2 Dotazníkové šetření

Dotazník měl 18 otázek a směřoval k různým věkovým kategoriím a různým profesím. Výzkum probíhal v měsíci květen a červen 2020 v jedné středně velké firmě v Kolíně. Průzkum byl zcela anonymní a zúčastnilo se ho 70 lidí. Dotazník je součástí Přílohy 1.

V dotazníku jsem zjišťovala, jaké jsou používána zařízení informačních technologií mezi běžnými zaměstnanci, zda mají svoje zařízení chráněno antivirem, dostatečně dlouhým heslem, využití dvoufázového věření a zda se sami setkali s útokem hrubou silou na vlastním zařízení – počítači, telefonu nebo tabletu a jak často a jaké množství dostávají spamu.

8.3 Výsledky výzkumu a jeho zpracování

Celkový počet rozdaných dotazníků byl 80 kusů a návratnost byla 70 kusů z důvodu čerpání dovolených a neplánovaných dlouhodobých pracovních neschopností. Dotazníky jsem rozdala ve městě Kolín v jedné středně velké firmě a výsledky jsem zpracovala do přehledných tabulek a grafů.

Otázka číslo 1 – Vaše pohlaví?

pohlaví	počet	procenta
žena	48	68,57 %
muž	22	31,43 %
celkem respondentů	70	100,00 %

Tabulka 6 Pohlaví

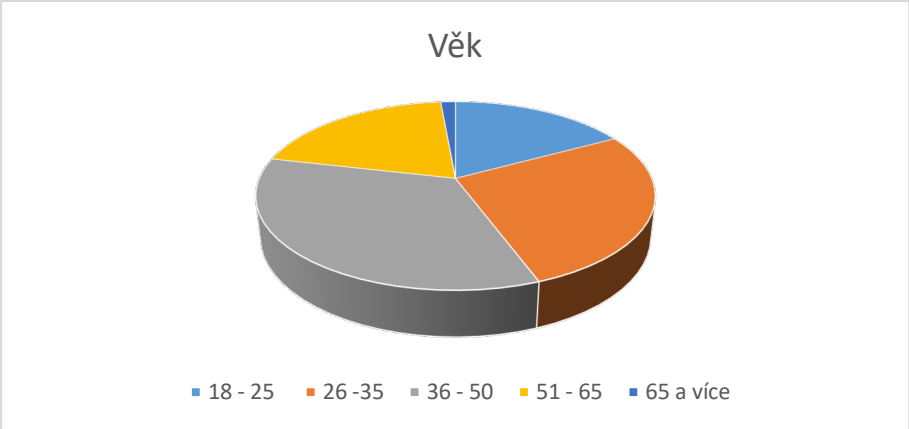
Graf 8 Pohlaví

Výzkumu se ve větší míře zúčastnily ženy – přes 68 %.

Otázka číslo 2 – Vaše věková kategorie?

Věková kategorie	Počet	Procenta
18–25	12	17,14 %
26–35	19	27,14 %
36–50	24	34,29 %
51–65	14	20,00 %
65 a více	1	1,43 %
celkem	70	100,00 %

Tabulka 7 Věk



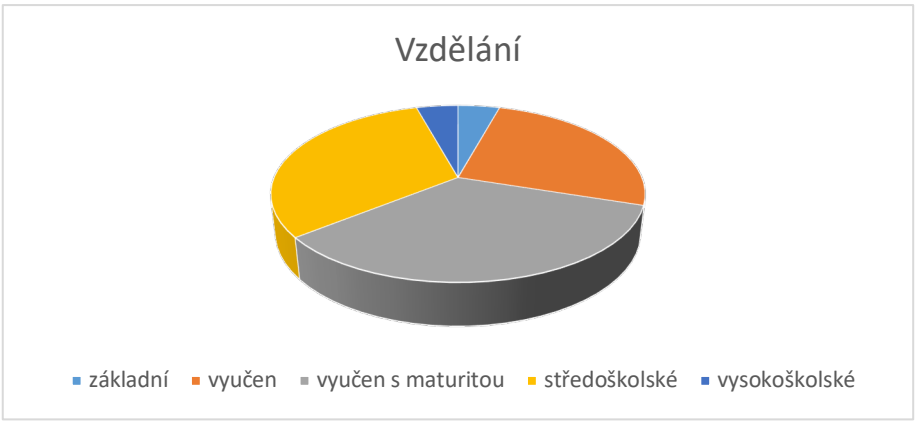
Graf 9 Věková kategorie

Z provedeného průzkumu vyplývá, že věkové kategorie jsou hodně vyrovnané, kromě jedné kategorie, proto počítačová gramotnost by mohla být vysoká mezi pracovníky této firmy.

Otázka číslo 3 – Jaké je Vaše vzdělání?

Vzdělání	Počet	Procenta
základní	3	4,29 %
vyučen	18	25,71 %
vyučen s maturitou	24	34,29 %
středoškolské	22	31,43 %
vysokoškolské	3	4,29 %
celkem	70	100,00 %

Tabulka 8 Vzdělání



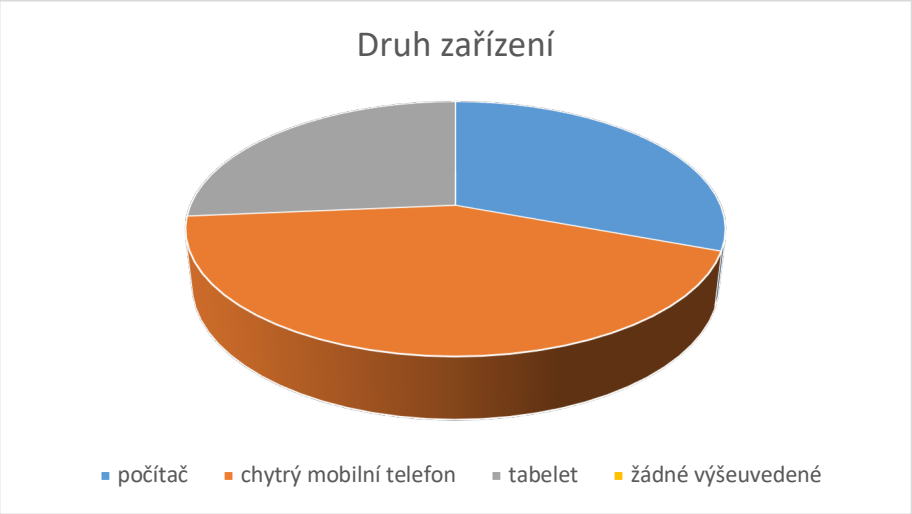
Graf 10 Vzdělání

Ve firmě převládá vyučen s maturitou, středoškolské vzdělání a vyučen, což předpokládá, že téměř všichni pracovníci se ve škole setkali s výukou počítačové gramotnosti a jejich znalosti zabezpečení počítačů by měly být dostatečné na to, aby svoje data dokázali ochránit.

Otázka číslo 4 – Jaké používáte informační technologie?

otázka	počet	procenta
počítač	50	30,67 %
chytrý mobilní telefon	70	42,94 %
tablet	43	26,38 %
žádné výše uvedené	0	0,00 %
celkem	163	100,00 %

Tabulka 9 Druh zařízení



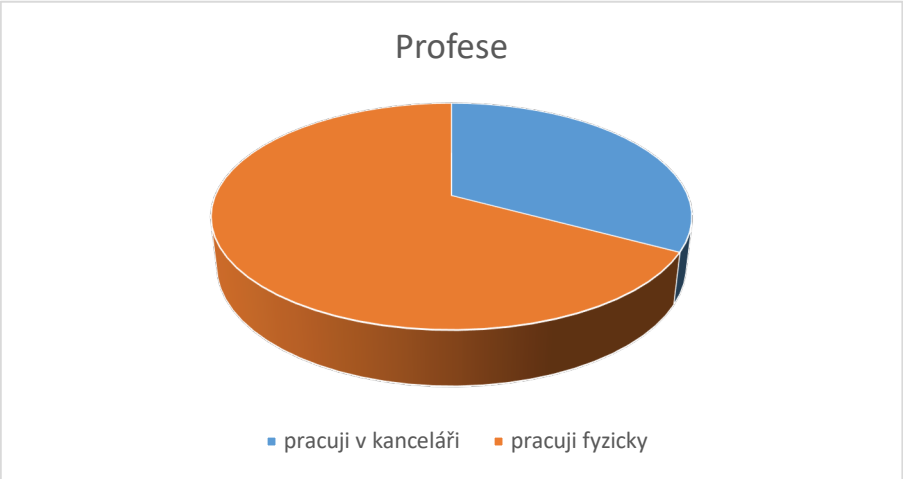
Graf 11 Druh zařízení

Z výše uvedených výsledků je patrné, že každý korespondent používá chytrý mobilní telefon, z celkového počtu využívaných informačních technologií představuje využívání mobilních telefonů více jak 42 %, počítač je využíván u více jak poloviny respondentů a jeho využití představuje přes 30 % využití informačních technologií.

Otázka číslo 5 – Vaše profese?

Vaše profese	Počet	Procenta
pracuji v kanceláři	23	32,86 %
pracuji manuálně	47	67,14 %
celkem	70	100,00 %

Tabulka 10 Profese



Graf 12 Profese

Z provedeného průzkumu vyplývá, že větší část respondentů - 67 % pracuje manuálně, v této firmě to znamená ve skladu jako skladník, ve výrobní části jako montér drobných dílů, expedient nebo na příjmu zboží.

Otázka číslo 6 – Máte na vašem zařízení aktivovaný antivir?

Antivir	Počet	Procenta
ano	65	92,86 %
ne	5	7,14 %
nevím	1	1,43 %
celkem	70	100,00 %

Tabulka 11 Antivir

Graf 13 Antivir

Z průzkumu je patrné, že kromě 8 % respondentů mají všichni aktivovaný na svých zařízeních antiviry proti ochraně nežádoucích napadení jejich zařízení.

Otázka číslo 7 – Víte, co to znamená, když Vám někdo ve Vašem zařízení (počítač, tablet, chytrý telefon) napadne Vaše data hrubou silou?

Útok hrubou silou	Počet	Procenta
ano	51	72,86 %
ne	15	21,43 %
nevím	4	5,71 %
celkem	70	100,00 %

Tabulka 12 Útok hrubou silou

Graf 14 Útok hrubou silou

Z provedeného průzkumu vyplývá, že většina lidí, ví, co znamená útok hrubou silou na jejich data – necelých 73 % respondentů.

Otázka číslo 8 – Setkali jste se v posledních 5 letech na Vašem zařízení (počítač, tablet, chytrý telefon) s útokem hrubou silou na Vaše data nebo zařízení?

Setkali jste se s útokem	Počet	Procenta
ano	41	58,57 %
ne	26	37,14 %
nevím	3	4,29 %
celkem	70	100,00 %

Tabulka 13 Útok na data

Graf 15 Počet útoků

Většina respondentů – přes 58 % se za posledních 5 let setkalo s hrubým útokem na svoje data, což je poměrně dost vysoké číslo.

Otázka číslo 9 – Byl Váš počítač, tablet, chytrý mobilní telefon napaden útokem hrubou silou – byla Vaše data zneužita?

Napadení zařízení	Počet	Procenta
ano	27	38,57 %
ne	34	48,57 %
nevím	9	12,86 %
celkem	70	100,00 %

Tabulka 14 Napadení počítače

Graf 16 Počet napadení zařízení

U vybraného vzorku lidí bylo téměř 30 % zařízení napadena útokem hrubou silou, to je docela vysoké číslo na to, že se snaží banky dělat osvětu na to, abychom nedávali nikomu svoje přístupové údaje, neklikali na neznámé e-maily atd.

Otázka číslo 10 – Používáte dostatečně zabezpečená hesla aplikací, kde máte důležité osobní údaje?

Bezpečná hesla	Počet	Procenta
ano	43	61,43 %
ne	23	32,86 %
nevím	4	5,71 %
celkem	70	100,00 %

Tabulka 15 Hesla

Graf 17 Bezpečnost hesla

U vybraných korespondentů bylo zjištěno, že lidé moc nedbají na dostatečně zabezpečená hesla. Podle slovního zjištění u dodatečného slovního průzkumu bylo zjištěno, že používají hesla rodná čísla, přezdívky nebo zcela jednoduchá hesla posloupné číselné řady. Většinou využívají jedno heslo do více aplikací a na přihlášení na více internetových stránek.

Otázka číslo 11 – Používáte dvoufázové ověření u aplikací, kde máte osobní data nebo jiné osobní údaje?

Dvoufázové ověření	Počet	Procenta
ano	16	22,86 %
ne	51	72,86 %
nevím	3	4,29 %
celkem	70	100,00 %

Tabulka 16 Dvoufázové ověření

Graf 18 Dvoufázové ověření

Dvoufázové ověření používá pouze 16 % respondentů, což je velice malé a přímo alarmující číslo, protože data nejsou chráněna a lidé si to vůbec neuvědomují.

Otázka číslo 12 – Píšete si svoje hesla do aplikací na papírek?

Hesla na papírku	Počet	Procenta
ano	31	44,29 %
ne	39	55,71 %
celkem	70	100,00 %

Tabulka 17 Hesla a papírek

Graf 19 Hesla na papírku

31 % napsaných hesel na papírku je hrozivě vysoké číslo, protože data pak nejsou vůbec chráněna a mohou být velice lehce zneužita.

Otázka číslo 13 – Ukládáte svoje hesla do aplikací do klíčenky na Claudu?

Hesla na Claudu	Počet	Procenta
ano	39	55,71 %
ne	31	44,29 %
celkem	70	100,00 %

Tabulka 18 Hesla na Claudu

Graf 20 Hesla na Claudu

Claudy v dnešní době mají zabezpečení a neměl by být problém, že většina lidí si ukládá hesla do Claudu, ale je potřeba mít dvoufázové zabezpečení, což většina uživatelů informačních technologií nemá, a hlavně by neměli na Claud ukládat přístupová data k nejcitlivějším údajům, jako je např. vstup do banky.

Otázka číslo 14 – Dostáváte spamy ve Vaší e-mailové komunikaci?

Spamy	Počet	Procenta
ano	66	94,29 %
ne	1	1,43 %
nevím	3	4,29 %
celkem	70	100,00 %

Tabulka 19 Spam

Graf 21 Spam

66 % respondentů dostává spam, které jsou obtěžující a reklamní sdělení, které si nikdo z nás neobjednal, a přesto nám zahlcují naší e-mailovou schránku.

Otázka číslo 15 – Pokud dostáváte v e-mailové komunikaci spamy, jak často je dostáváte?

Četnost spamů	Počet	Procenta
každý den	58	84,06 %
párkrát za týden	11	15,94 %
celkem	69	100,00 %

Tabulka 20 Četnost spam

Graf 22 Četnost spam

84 % respondentů dostává nějaký spam každý den, což je vysoké a varující číslo před kybernetickým obtěžováním nevyžádanými maily.

Otázka číslo 16 – Pokud dostáváte v e-mailové komunikaci spamy, kolik jich obdržíte denně v průměru?

Počet spamů za den	Počet	Procenta
1-5	50	86,21 %
5 a více	8	13,79 %
celkem	58	100,00 %

Tabulka 21 Počet spamů za den

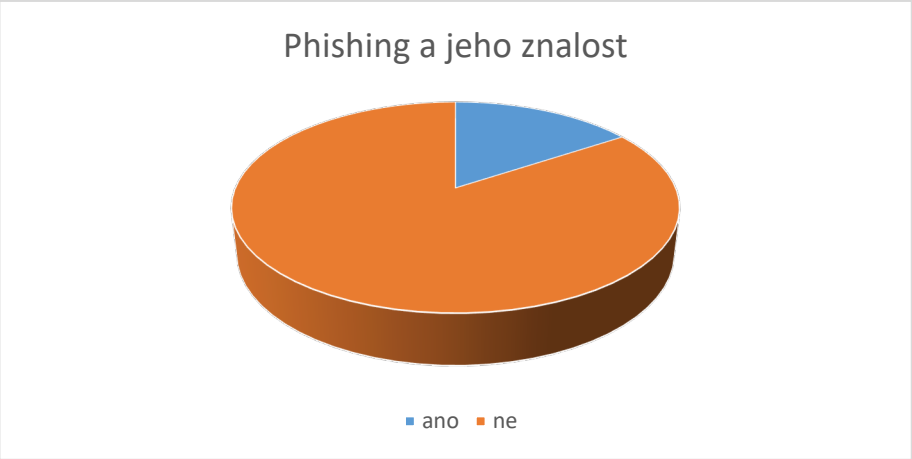
Graf 23 Počet spamů za den

Denně je nejvíce rozesíláno mezi 1–5 spamy, toto číslo bylo zjištěno u 86 % respondentů.

Otázka číslo 16 – Víte, co je o phishing v počítačovém slangu?

Phishing znalost	Počet	Procenta
ano	11	15,71 %
ne	59	84,29 %
celkem	70	100,00 %

Tabulka 22 Phishing



Graf 24 Phishing a jeho znalost

Podle průzkumu by bylo potřeba provést větší informovanost obyvatelstva o možných kybernetických útocích, které mohou ohrozit jejich data.

Otázka číslo 17 – Setkali jste se s phishingem osobně?

Osobní zkušenost phishing	Počet	Procenta
ano	5	7,14 %
ne	65	92,86 %
celkem	70	100,00 %

Tabulka 23 Phishing osobní zkušenost

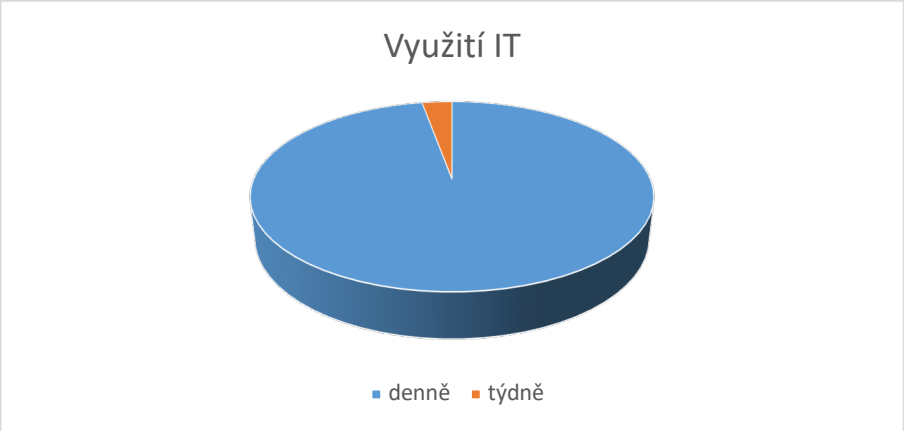
Graf 25 Osobní zkušenost

Pouze 5 % respondentů se potkalo s útokem na svůj počítač ve formě phishing, což je velice uspokojivý výsledek.

Otázka číslo 18 – Používáte informační technologie – telefon, počítač, tablet, denně?

Využití IT	Počet	Procenta
denně	68	97,14 %
týdně	2	2,86 %
celkem	70	100,00 %

Tabulka 24 Využití IT



Graf 26 Využití IT

Informační technologie – počítače, tablety nebo chytré telefony lidé využívají každý den, a to ať ke svojí práci nebo při hledání věcí k jejich koníčkům nebo jen pro čtení zpráv. Proto je nutno, aby se zvýšila informovanost o možných kybernetických útocích mezi obyvateli.

ZÁVĚR

S rozvojem internetu, ale i dalších informačních technologií dochází samozřejmě i k rozvoji kriminality v kybernetickém prostoru. Útočníci jsou stále jeden krok před námi uživateli, a proto si musíme dávat hodně velký pozor na to, komu sdělujeme svoje data, jaká hesla používáme, z jakého počítače a jakého internetového připojení se připojujeme ke stránkám, kde využíváme naše citlivá nebo osobní data. Nemusí být zcizena pouze naše data, ale náš počítač, chytrý telefon nebo tablet mohou být využity útočníky na páchání trestných činů, aniž bychom to věděli. Je důležité neustále aktualizovat antivirové programy, využívat dvojí zabezpečení na všech aplikací, kde je to možné, nesdělovat nikomu naše hesla ani jiné údaje.

Z průzkumu bylo zjištěno, že lidé si svoje data moc nechrání, používají jednoduchá hesla, heslo použijí ke vstupu do více aplikací, nevyužívají dvojí zabezpečení vstupu a nejsou téměř vůbec informováni o tom, že i když jim nikdo neukradne fyzicky počítač nebo telefon, může být jejich počítač prostředkem k páchání trestného činu. Lidé věří tomu, že se jim nikdo nepokusí nabourat do počítače, telefonu nebo tabletu, a proto nevěnují dostatečnou pozornost jejich zabezpečení.

Je nutno dělat daleko větší osvětu kybernetické kriminality mezi lidmi, ukázat jim, co vše se může stát, jak lehce se mohou stát cílem útočníků a jak jednoduše mohou přijít o svoje data nebo finanční prostředky. Že ani nemusí vědět, že prostřednictvím jejich počítače je páchán trestný čin, o kterém oni nevědí. Hlavně je nutno šířit osvětu, jak se chránit a ochranu dat, že není vůbec možno podceňovat.

Kromě osobních údajů a hesel, si musíme chránit samozřejmě i svoje platební karty, které se stávají často terčem zločinců, proto se rozvíjí stále více systému k placení na internetu PayPal a to hlavně z toho důvodu, že každý den na internetu vnikají nové a nové e-shopy, které jsou bez historie a člověk neví, zda se jedná o seriózní obchod nebo je to jeden z mnoha podvodných e-shopů, které mají pouze vylákat peníze za zboží od lidí. Mnohdy není objednané zboží ani zaslané, nebo je zaslané v jiné kvalitě nebo zcela jiné zboží, které nemá žádnou hodnotu. Bylo mnoho případů, kdy místo objednaného zboží lidé v balíčku obdrželi zákazníci např. cihlu a následně při reklamaci u e-shopu, kde si zboží objednali, se reklamace nedočkali, protože daný e-shop již neexistoval.

Aby k tomuto problému nedocházelo, společnost PayPal má takový systém placení, kdy zákazník za zboží zaplatí této společnosti a ta následně zaplatí danému e-shopu. Společnost PayPal před uzavřením smlouvy s e-shopem, který o to požádá, daný obchod prověří, zjistí

jeho korektnost a pravost údajů, aby nemohlo dojít k tomu, že koncový zákazník si objedná zboží, zaplatí a žádné nedostane.

Toto je jedna z možností, jak předcházet podvodům s nepravými e-shopy.

Budoucnost nákupu v prodejnách se bude ubírat s největší pravděpodobností tak, že každé zboží bude mít v sobě čip a při východu z prodejny bude tento čip přečten speciální technologií a dojde k zaplacení zboží např. okem. Tímto způsobem by se eliminovaly z procesu platební karty, které se lehce zkopírují a mohou být zneužity. Tento způsob platby se již testuje.

V současné době se snaží banky přicházet se stále novějšími technologiemi placení, aby platební karty, které nejsou tak zabezpečeny, byly z procesu placení vynechány, a tak je možno platit např. chytrým telefonem nebo hodinkami, kdy oba tyto přístroje jsou více zabezpečeny než samotná platební karta.

SEZNAM POUŽITÉ LITERATURY

podle použité citační normy

[1] ZAVRŠIK, Aleš. Kyberkriminalita. Praha - Wolters Kluwer ČR, 2017, 148 s. ISBN 978-80-7552-758-5.

[2] Kybernetická bezpečnost (Cyber Security). CyberSecurity [online]. [cit. 2019-02-13]. Dostupné z: https://www.cybersecurity.cz/basic.html

[3] GIBSON, William. Neuromancer. Vyd. 1. Plzeň: Laser, 1992, 234 s. ISBN 8085601273.

[4] ČECH, Pavel a Josef ZELENKA. Ochrana dat: informační bezpečnost – výkladový slovník. Vyd. 1. Hradec Králové: Gaudeamus, 2002. ISBN 80-7041-197-X.

[5] Šéf hackerské skupiny byl dopaden. *Lupa.cz* [online]. 29.3.2018 [cit. 2020-26-02]. Dostupné z: https://www.lupa.cz/aktuality/sef-hackerske-skupiny-byl-dopaden-carbanak-zcizil-miliardu-eur-byl-i-v-cesku/

[6] Nový velký cyber útok cílil na Írán a Izrael. Virus Flame řádil pět let. *Idnes.cz* [online]. 28.5.2012 [cit. 2020-26-02]. Dostupné z: https://www.idnes.cz/technet/internet/byl-odhalen-nejvetsi-cyber-utok-v-historii-virus-flame-radil-pet-let-v-iranu-a-izraelu.A120528_143110_sw_internet_vse

[7] Pozor na malware v RAR souborech. *Computerworld.cz* [online]. 12.12.2019 [cit. 2020-26-02]. Dostupné z: https://computerworld.cz/securityworld/pozor-na-malware-v-rar-souborech-55762

[8] Zkolabovaly dráhy i nemocnice. Virus WannaCry ochromil před rokem počítačový svět. *Novinky.cz* [online]. 15.5.2018 [cit. 2020-27-02]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/zkolabovaly-drahy-i-nemocnice-virus-wannacry-ochromil-pred-rokem-pocitacovy-svet-14725

[9] Nenápadné cílené útoky. Jak se proti nim bránit? *Systemonline.cz*. [online]. 2014 [cit. 2020-27-02]. Dostupné z: https://www.systemonline.cz/it-security/nenapadne-cilene-utoky.htm

[10] TMSC identifikovala virus, jde o ransomware WannaCry. *Světhardware.cz* [online]. 7.8.2018 [cit. 2020-27-02]. Dostupné z: https://www.svethardware.cz/tsmc-identifikovala-virus-jde-o-ransomware-wannacry/47227

[11] Jednotlivé druhy kriminality. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[12] Podklady z Komerční banky

[13]Engangend.com dostupné z https://www.engadget.com/2014-07-28-credit-card-skimming-explainer.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmN6Lw&guce_referrer_sig=AQAAACeME8xxuJmrEnP0xlDCBxHxnjm3llOA1Qbw5IhxgHUFtxN

uQL3U1mVMQ9n8FVEujeKiXgG-uJ7WNyGqRu9HjjqowGEymJyv-xnraU-ak8doQRUxljofvMuwES56liigaozbCjaPaUG3Bf5r4R0ni65zyIBI0oPRLXb8jWK_Fjp0

[14] PC-centrum.cz – komplexní řešení pro bezpečné provozování internetových technologií. Dostupné na: http://www.pc-centrum.cz/

[15] Interní doklady firmy Eltrax v Havířově

[16] Microsoft.com – Spear Phishing campaigns – they're sharper thank you thing – dostupné z https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/

Ostatní tabulky a grafy jsou moje vlastní práce

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT Informační technologie

ID Identifikační karta

SMS Short message service

APT Advanced Persisten Thrath

SMB Server Message Block

RAI Republikánská armáda Irska

AIS Automatizovaný informační systém

TCP Transmission Control Protocol

PIN Personal Identification Number

USB Universal Seriál Bus

CD Candela

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK K PRŮZKUMU

Informační technologie jako prostředek šíření kriminality

Dobrý den,
na úvod mi dovolte, abych se představila. Jmenuji se Radka Procházková a jsem posluchačem závěrečného ročníku magisterského studia Fakulty aplikované informatiky na Univerzitě Tomáše Bati ve Zlíně, oboru Bezpečnostní technologie, systémy a management.
Projekt "Infomační technologie jako prostředek šíření kriminality." realizovaný formou dotazníkového výzkumu veřejného mínění slouží pro účely diplomové práce a jeho výsledky budou publikovány výhradně v praktické části této práce, nikoliv veřejně, ani nebudou předány třetím stranám.
Vyplnění dotazníku je zcela anonymní a nemělo by Vám zabrat více než 5 minut. Jedinými vstupními podmínkami k dotazování je dosažení hranice 18 let a česká státní příslušnost.
Dotazník je pouze v papírové formě.
Za vyplnění dotazníku Vám upřímně mnohokrát děkuji. V případě jakýchkoliv dotazů, námětů a připomínek, mě neváhejte kontaktovat prostřednictvím e-mailu na: radkap@volny.cz
S pozdravem,
Ing. Radka Procházková

1. OBECNÉ

Nyní prosím zodpovězte několik obecných otázek.
Pohlaví *

- Muž
- Žena

Věk * Vyberte z příslušné nabídky věkovou kategorii, která Vám náleží.

- 18 - 25
- 26 - 35
- 36 - 50
- 51 - 65
- 65 a více

Vzdělání *Vyberte ze seznamu Vaše dosud nejvyšší ukončené vzdělání

- Základní
- Vyučen
- Vyučen s maturitou
- středoškolské
- vysokoškolské.

2. INFORMAČNÍ TECHNOLOGIE

Následující otázky se budou týkat Vaší práce s IT

Jaké používáte informační technologie? *

- Počítač
- Tablet
- Chytrý mobilní telefon
- Žádné výše uvedené

Vaše profese? *

- Pracuji v kanceláři
- Pracuji manuálně

Máte na Vašem zařízení aktivovaný antivir? *

- Ano
- Ne
- Nevím

Víte, co to znamená, když Vám někdo ve Vašem zařízení (počítač, tablet, chytrý telefon) napadne Vaše data hrubou silou? *

- Ano
- Ne
- Nevím

Setkali jste se v posledních 5 letech na Vašem zařízení (počítač, tablet, chytrý telefon) s útokem hrubou silou na Vaše data nebo zařízení? *

- Ano
- Ne
- Nevím

Byl Váš počítač, tablet, chytrý mobilní telefon napaden útokem hrubou silou – byla Vaše data zneužita? *

- Ano
- Ne
- Nevím

Používáte dostatečně zabezpečená hesla aplikací, kde mát důležité osobní údaje? *

- Ano
- Ne
- Nevím

Používáte dvoufázové ověření u aplikací, kde máte osobní data nebo jiné osobní údaje? *

- Ano
- Ne
- Nevím

Píšete si svoje hesla do aplikací na papírek? *

- Ano
- Ne

Ukládáte svoje hesla do aplikací do aplikace klíčenka na Claudu? *

- Ano
- Ne
- Nevím

Dostáváte spamy ve Vaší e-mailové komunikaci? *

- Ano
- Ne
- Nevím

Pokud dostáváte v e-mailové komunikaci spamy, jak často je dostáváte? *

- Každý den
- Párkrát za týden

Pokud dostáváte v e-mailové komunikaci spamy, kolik jich obdržíte denně v průměru? *

- 1-5
- 5 a více
- Nevím

Víte, co je to phishing v počítačovém slangu? *

- Ano
- Ne
- Nevím

Setkali jste se s phishingem osobně? *

- Ano
- Ne
- Nevím

Používáte informační technologie (počítač, tablet, chytrý mobilní telefon) denně? *

- Ano
- Ne