UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2016-2017

BAKALÁŘSKÁ PRÁCE

Tomáš Nestroj

Počítačová bezpečnost a ochrana dat u Policie České republiky

Praha 2017

Vedoucí bakalářské práce: Ing. Michaela Melicharová

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED (PART TIME) STUDIES

2016-2017

BACHELOR THESIS THESIS

Tomáš Nestroj

Cybersecurity and data protection in the Czech Republic Police

Prague 2017

The Bachelor Thesis Work Supervisor: Ing. Michaela Melicharová

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 28.1.2017 Tomáš Nestroj .....

Poděkování

Chtěl bych poděkovat vedoucí mé bakalářské práce paní Ing. Michaele Melicharové za odborné vedení a cenné připomínky při zpracování práce.

Anotace

Tato bakalářská práce se zabývá problematikou počítačové bezpečnosti a ochranou dat u Policie České republiky. Cílem teoretické části je definovat negativní aktivity v kyberprostoru se zaměřením na útoky hackerů a kybernetickou válku. V práci chci popsat bezpečnou manipulaci s výpočetní technikou u Policie České republiky a povinnosti zaměstnanců. Práce se zabývá taktéž problematikou zpracování osobních údajů v informačních systémech, které využívá Policie České republiky.

Náplní praktické části je dotazníkový průzkumu mezi policisty, kteří jsou uživateli koncových počítačových stanic s cílem zjistit, zda dodržují bezpečnostní požadavky, které jsou od nich vyžadovány. Dotazníkový průzkum je východiskem k návrhu optimálního doporučení pro zvýšení bezpečnosti počítačových systémů. V rámci výzkumu byly stanoveny čtyři hypotézy a cílem práce je hypotézy potvrdit nebo je vyvrátit.

Závěr bakalářské práce se již zabývá shrnutím získaných poznatků a zhodnocením. V této práci je použita odborná literatura, legislativní normy, články z časopisů a internetové zdroje.

Klíčová slova

Bezpečnostní hrozby, informační systém, ochrana dat, počítačová bezpečnost, Policie České republiky, škodlivý software, zabezpečení

Annotation

This thesis deals with computer security and data protection by the Police of the Czech Republic. The aim is to define negative activities in cyberspace with a focus on hackers and cyber war. At work I want to describe the safe handling of computer technology in the Czech Republic Police and obligations of employees. Work also addresses the issue of the processing of personal data in information systems used by the Police of the Czech Republic.

In the practical part of the questionnaire survey among police officers, who are the users end workstations to determine their compliance with safety requirements that are required from them. The questionnaire survey is the starting point for designing the optimum recommendations for increasing the security of computer systems. The research was four hypothesis and the objective is to confirm the hypothesis or disprove.

Conclusion The work is already dealing with a summary of lessons learned and evaluation. In this work, using professional literature, legislative standards, magazine articles and Internet resources.

Keywords

Computer security, Data protection, Information System, malware, Security threats, Police of the Czech Republic, Security,

ÚVOD

Vzhledem ke své dlouholeté profesi policisty, jsem si zvolil jako téma bakalářské práce: Počítačová bezpečnost a ochrana dat u Policie České republiky. Jedná se o velmi důležité téma, které se neustále dostává do popředí v souvislosti s bezpečností. Používání informačních systémů má mnoho výhod, ale také mnoho rizik. Bakalářská práce je rozdělena na dvě části.

Teoretická část se nejprve zaměřuje na vymezení základních pojmů a legislativních předpisů v oblasti kybernetické bezpečnosti. Další část popisuje činnost a postavení Policie české republiky, která užívá ke komunikaci intranetovou síť a popisuje nejpoužívanější základní informační systémy. Vzhledem ke skutečnostem, že počítačová síť Ministerstva vnitra patří mezi kritickou infrastrukturu, je potřeba dodržovat nejpřísnější bezpečnostní předpisy, které jsou stanoveny v interních aktech řízení. V další kapitole se nachází výčet těchto požadavků na pracovníky a administrátory. V práci popisuji nejen postup zabezpečení výpočetní techniky a dodržování bezpečnostních pravidel, ale pro lepší pochopení odkrývám i principy a metody, kterými se hackeři do sytému dostávají nebo mohou dostat. Další kapitoly poskytují cenné rady a doporučení jak průnikům zabránit.

Empirická část práce se zaměřuje na výzkum uskutečněný pomocí dotazníkového šetření mezi policisty Územního odboru Opava. V rámci této části práce je sestaven dotazník zaměřující se na problematiku bezpečné manipulace s výpočetní technikou. Získaná fakta jsou následně vyhodnocena a jsou navrhnuta doporučení. V rámci výzkumu jsou stanoveny čtyři hypotézy a cílem práce je potvrdit je nebo je vyvrátit. Závěr bakalářské práce se již zabývá shrnutím získaných poznatků s vyvozením výsledků a zhodnocení. V této práci je použitá odborná literatura, legislativní normy, články z odborných časopisů a internetové zdroje. V rámci elektronických zdrojů to bude vedle sítě Internet především datová síť Intranet Ministerstva vnitra Hermes, která je zřízená pro plnění úkolů Policie České republiky a provozovaná v působnosti Ministerstva vnitra.

1 POČÍTAČOVÁ BEZPEČNOST U POLICIE ČESKÉ REPUBLIKY

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích. Počítačová bezpečnost obsahuje ochranu před neoprávněnou manipulací s daty, zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému, ochranu informací před krádeží, nelegální tvorbu kopií dat nebo poškození, bezpečnou komunikaci a přenos dat, bezpečné uložení dat a dostupnost, celistvost.[1]

Policie České republiky je jednotný ozbrojený bezpečnostní sbor, který slouží veřejnosti a působí na celém území České republiky a je povolán k ochraně bezpečnosti osob, majetku a veřejného pořádku. K zajištění plnění úkolů státní správy, vnitřního pořádku a bezpečnosti ve věcech společnosti. Policie České republiky (dále jen PČR) zajišťuje veřejný pořádek a v případech, kdy byl narušen, činí úkony k jeho obnovení. Vyšetřuje a odhaluje protiprávní jednání, které mohou naplňovat skutkovou podstatu trestného činu nebo přestupku. Dohlíží a kontroluje bezpečnost a plynulost silničního provozu, zajišťuje pohotovostní ochranu jaderných zařízení a jaderného materiálu, vede boj proti terorismu a zajišťuje ochranu státních hranic ve vymezeném rozsahu. Policie ČR spolupracuje se zahraničními bezpečnostními sbory (např. Interpol, Europol), zpracovává informace o osobních údajích a vede evidenci cizinců. V neposlední řadě spolupracuje a koordinuje činnost útvarů obecní policie.

Základním právním předpisem Policie České republiky je zákon č. 278/2008 Sb., o Policii České republiky. Tento zákon říká, že policie slouží veřejnosti, definuje její úkoly a stanovuje místo její působnosti, tedy Českou republiku, není-li jiným právním předpisem stanoveno jinak.

Úkolem PČR je ochrana bezpečnosti osob, majetku a veřejného pořádku. Činností PČR je rovněž předcházení trestné činnosti, plnění úkolů dle trestního řádu a úkolů vnitřního pořádku.

Policie České republiky je podřízena Ministerstvu vnitra ČR, které vytváří podmínky pro činnost policie. Nejvyšší řídící orgán PČR je policejní prezidium v čele s policejním ředitelem. Policejnímu prezidiu jsou podřízena krajská ředitelství a celostátní útvary PČR. V ČR je 14 krajských ředitelství, v jejichž čele stojí krajský ředitel PČR. Krajská ředitelství jsou organizační složkou státu a účetní jednotkou, jehož příjmy a výdaje jsou součástí rozpočtu ministerstva vnitra.

[1] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 85. ISBN 978-80-7251-436-6.

Útvary zřízené krajským ředitelstvím jsou vnitřními organizačními jednotkami krajského ředitelství. Tyto útvary zřizuje policejní prezident na návrh krajského ředitele PČR.

Obrázek 1: Operační středisko Policie ČR v Ostravě

Zdroj[2]

Policie pro svou činnost a dokumentaci využívá výpočetní techniku a informační systémy, které tvoří funkční celek, určený k zajištění činnosti a k plnění úkolů jednotlivých útvarů a složek policie. Výpočetní technika zabezpečuje shromažďování, zpracování, přenos dat mezi jednotlivými systémy. Veškerá činnost informačních systémů se děje v souladu s obecně platnými a interními právními i předpisy. Na základě těchto norem PČR zpracovává ve svých systémech získané informace včetně osobních údajů. Výpočetní technika PČR není přímo připojena do sítě Internet, čímž se zvyšuje stupeň bezpečnosti a snižuje stupeň infiltrace.

1.1 CHARAKTERISTIKA ZÁKLADNÍCH POJMŮ

Níže jsou uvedeny definice pojmů, které se budou v textu dále opakovaně vyskytovat. Uvedené pojmy jsou z Výkladového slovníku kybernetické bezpečnosti, který vydala Policejní akademie České republiky.

Bezpečnostní hrozba

Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.[3]

[2] Integrované bezpečnostní centrum Moravskoslezského kraje [online]. s. 23 [cit. 2017-01-01]. Dostupné z: http://www.hzscr.cz/soubor/2015-04-ibc-msk-cz-pdf.aspx

[3] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 25. ISBN 978-80-7251-436-6.

Kritická informační infrastruktura

Komplex informačních a komunikačních systémů, jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.[4]

Kritická infrastruktura

Systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva.[5]

Kritická komunikační infrastruktura (státu)

Komplex komunikačních systémů, služeb nebo sítí elektronických komunikací (naplňující stanovená průřezová kritéria a odvětvová kritéria v oblasti kybernetické bezpečnosti), jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.[6]

Kybernetická bezpečnost

Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.[7]

Kybernetický útok

Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.[8]

[4] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 65-66. ISBN 978-80-7251-436-6.
[5] Tamtéž, s. 66.
[6] Tamtéž, s. 66.
[7] Tamtéž, s. 69.
[8] Tamtéž, s. 71.

1.2 LEGISLATIVNÍ PŘEDPISY V OBLASTI KYBERBEZPEČNOSTI

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon nabyl platnosti vyhlášením ve Sbírce zákonů dne 29. 8. 2014 a účinný je od 1. 1. 2015, žádná novelizace doposud neproběhla. Upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Nevztahuje se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Výjimka zohledňující specifika činnosti zpravodajských služeb a Policie České republiky.[9]

Cílem zákona je zavést do praxe soubor oprávnění a povinností se zaměřením zvýšit bezpečnost kybernetického prostoru a nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou. Účelem je vyšší efektivita řešení kybernetických bezpečnostních incidentů a v případě stavu kybernetického nebezpečí provozovatelé musí provádět reaktivní opatření vydaná Národním bezpečnostním úřadem. Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.

Právní úprava ukládá vybraným skupinám orgánů a osob, tj. správcům kritické informační infrastruktury a správcům významných informačních systémů, definovat a aplikovat systém opatření a postupů pro případ narušení či ohrožení kybernetického prostoru. Jedná se zejména o zavedení přístupových práv, logovacích a kryptografických nástrojů, zavádění nových technologií, krizové řízení lidských zdrojů nebo zvládání specifických organizačních postupů při řešení mimořádných událostí, tvorba funkčního systému ochrany a zajištění včasnou detekcí kybernetických bezpečnostních událostí a hlášení kybernetických bezpečnostních incidentů v kritické informační infrastruktuře a ve významných informačních systémech.

[9] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Sbírka zákonů České republiky. 2014. § 33. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací mají povinnost hlásit kontaktní údaje národnímu CERT. Národní CERT (Computer emergency response team – skupina pro reakci na počítačové hrozby) je provozována vybraná právnická osoba na základě veřejnoprávní smlouvy s Národním bezpečnostním úřadem.[10]

Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti.

Touto vyhláškou se určí obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu.[11]

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

Stanoví práva a povinnosti správců informačních systémů veřejné správy (dále ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Stanoví povinnosti v oblasti řízení životního cyklu ISVS, povinné náležitostí informačních systémů. V rámci zákona je působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Vytváří podmínky, aby kvalitní informační systémy byly dobrým nástrojem pro výkon veřejné správy. Zákon dále upravuje atestace a postavení atestačních středisek, doručování zpráv orgánům veřejné moci prostřednictvím portálu veřejné správy a poskytování ověřených výstupů z ISVS.

- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

- Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432 /2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

- Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.

[10] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Sbírka zákonů České republiky. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181.

[11] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316

1.3 INTRANETOVÁ SÍŤ HERMES

Počítačová síť s názvem HERMES je jednou z intranetových datových sítí zřízených a provozovaných v působnosti Ministerstva vnitra. Slouží Policii ČR k zajištění vnitroresortní komunikace a sdílení technických prostředků, programů a dat. Síť intranet mohou využívat pro plnění úkolů podle zvláštních právních předpisů oprávnění příslušníci a zaměstnanci policie a v případech upravených meziresortními dohodami a interními akty řízení též mimorezortní subjekty.

Využívání datové sítě Intranet Ministerstva vnitra Hermes upravuje závazný pokyn policejního prezidenta číslo 80 ze dne 9. srpna 2005. Síť Intranet mohou v rámci působnosti policie využívat pro plnění služebních úkolů oprávnění příslušníci a zaměstnanci policie.

Na intranetu jsou pravidelně zveřejňovány všechny interní akty Policejního prezidia či Ministerstva vnitra, informace o jednotlivých službách v rámci policie či různé informace pro samotný výkon služby, publikovány metodické postupy a doporučení. Na intranetu je v provozu rovněž vyhledávací server, který podobně jako na internetu umožňuje provádět vyhledávání konkrétní informace pomocí klíčových slov. Intranet slouží taktéž pro přístup do informačních systémů, kterých policie využívá celkově okolo 50. Na úrovni centra jsou servery celorepublikových služeb, dále pak síť tvoří krajské servery a dále servery jednotlivých územních odborů. K intranetové síti jsou kromě počítačů připojené periferní zařízení, jako jsou skenery, multifunkční zařízení, tiskárny.

1.4 BEZPEČNOSTNÍ PŘEDPISY PRO PRÁCI S VÝPOČETNÍ TECHNIKOU

Zařízení výpočetní techniky se dělí na:

- **pracovní stanice**, kterými jsou počítačové sestavy sloužící jednomu nebo více uživatelům ke komunikaci s ostatními uživateli nebo využívání sdílených technických prostředků, programů, dat a datových služeb poskytovaných v síti Intranet. Pracovní stanice může poskytovat v rámci lokální sítě datové služby, sdílení technických prostředků, sdílení adresářů a souborů,
- **lokální servery**, kterými jsou počítačové sestavy, na nichž jsou uloženy sdílené programy, data a technické prostředky a které poskytují v rámci sítě Intranet datové služby zejména provoz elektronické pošty, informační služby (web), databázové služby, FTP přenos souborů, provoz diskusních skupin, sdílení technických prostředků, programů a dat,
- **jiná zařízení výpočetní techniky** jako jsou síťové tiskárny, skenery, která poskytují uživatelům v rámci lokální sítě vymezené datové služby.

Počítačová sestava připojená do sítě Intranet :

- musí být vybavena antivirovým programem spouštěným po startu operačního systému, který průběžně zajišťuje automatickou kontrolu všech programů a dalších souborů spouštěných, otevíraných nebo zapisovaných při práci na počítačové sestavě,
- musí být vybavena aktuální verzí souboru známých definic (signatur) virů,
- musí mít nainstalovány všechny důležité opravné a bezpečnostní aktualizace, které jsou k operačnímu systému a použitým programům k dispozici např. na serveru věcného gestora nebo provozního gestora v síti Intranet,
- musí mít vytvořena uživatelská konta jednotlivých uživatelů,
- nesmí být propojována propojovacími prvky k jiné počítačové sestavě, která je nebo bude připojena do jiné datové sítě,
- nesmí být jakýmkoli způsobem připojena současně ani následně do jiné datové sítě bez provedení kompletního zformátování všech pevně instalovaných i přepisovatelných výměnných paměťových médií a reinstalace veškerého programového vybavení.

Na pevně instalovaných i přepisovatelných výměnných paměťových médiích počítačové sestavy připojené do sítě intranet nesmějí být uloženy nebo zpracovávány utajované informace.[12] Pokud dochází ke zpracování osobních údajů, postupuje se podle právních předpisů a interního aktu řízení.[13]

Počítačová sestava, která byla připojena do jakékoli jiné datové sítě, nesmí být připojena do sítě intranet bez provedení kompletního zformátování všech pevně instalovaných i přepisovatelných výměnných paměťových médií a reinstalace veškerého programového vybavení.

Přepisovatelná výměnná paměťová média nebo externí paměťová zařízení, která slouží pro přenos dat z jiné datové sítě nebo z jiné počítačové sestavy musí být před použitím v počítačové sestavě připojené do sítě Intranet podrobena antivirové kontrole.[14]

1.5 POVINNOSTI ADMINISTRÁTORA LOKÁLNÍ SÍTĚ

Administrátoři lokální sítě, administrátoři lokálních serverů, správci uživatelských kont a správci počítačových programů neprodleně informují službu „hot line" odboru systémového řízení a informatiky:

- skutečnosti, které by mohly způsobit ohrožení bezpečnosti, funkčnosti nebo dostupnosti centrálních serverů, centrálních částí celostátních aplikací nebo datových služeb v síti Intranet,
- zjištění poruchy lokální nebo centrální části některé celostátní aplikace,
- zjištění virového napadení pracovních stanic nebo lokálních serverů,
- provádí kontroly a nastavení komunikačních parametrů a parametrů síťového zabezpečení u zařízení připojených do lokální sítě a provádí změny v nastavení technických a programových prostředků lokální sítě,
- realizuje připojení pracovních stanic do lokální sítě,
- oznamuje v předstihu vedoucím pracovníkům plánované změny, omezení nebo přerušení provozu lokální sítě,

12 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
13 Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
14 Závazný pokyn policejního prezidenta č. 80/2005 ze dne 9. srpna 2005, kterým se upravuje využívání datové sítě Intranet Ministerstva vnitra „Hermes"

- provádí instalace, konfigurace, údržbu a aktualizace programového vybavení lokálních serverů a aplikací na nich provozovaných,
- zajišťuje pravidelné aktualizace souboru známých definic virů na lokálních serverech v souladu s postupy a návody,
- na základě požadavků vedoucích pracovníků zajišťuje instalace, konfigurace, a aktualizace programového vybavení na pracovních stanicích.

1.6 POVINNOSTI UŽIVATELE PRACOVNÍ STANICE

Každý policista pracující s výpočetní technikou je povinen se seznámit s interními bezpečnostními předpisy, které se týkají práce s prostředky výpočetní techniky a práce v síti a naučit se tyto předpisy respektovat. Mezi základní povinnosti patří:

- uživatel využívá pracovních stanic a lokálních serverů v síti Intranet pouze v rozsahu stanovených oprávnění a v rozsahu nutném pro plnění služebních nebo pracovních úkolů,
- vytváření, ukládání, zveřejňování, přenos, získávání a využívání dat v síti Intranet pouze v rozsahu nutném pro plnění služebních nebo pracovních úkolů,
- používat přidělené uživatelské konto pro přístup k těm serverům nebo datovým službám serverů, u kterých je vyžadována identifikace uživatele,
- chránit své uživatelské heslo před možným zneužitím,
- neumožnit ostatním pracovníkům použití svého uživatelského konta při práci v síti Intranet,
- po skončení práce v síti Intranet provést odhlášení uživatele ze sítě Intranet ukončením aplikace Microsoft Internet Explorer,
- znát ovládáni antivirových programů a provádět jejich pravidelnou aktualizaci,
- paměťová media, která byla vložena do jiného počítače, před použitím prověřit na přítomnost počítačových virů,
- pracovní data a dokumenty ukládat na určené sdílené síťové úložiště, na pevném disku pracovní stanice smějí být ukládány pouze kopie,
- zajištění pravidelné aktualizace souboru známých definic virů na přidělených pracovních stanicích v souladu s postupy a návody, které zpracoval správce počítačových programů (jestliže není možné nastavit automatické provádění aktualizací); aktualizace souboru

známých definic virů není považována za aktualizaci počítačového programu ve smyslu interního aktu řízení.[15]

- uživatel je povinen po skončení práce na pracovní stanici
    - provést odhlášení uživatele,
    - pracovní stanici vypnout nebo ji zajistit proti neoprávněnému použití jiným způsobem,
- neprodleně vypnout pracovní stanici při zjištění závady na pracovní stanici, která by mohla ohrozit bezpečnost nebo funkčnost sítě Intranet (např. napadení virem),
- informovat administrátora lokální sítě
    - skutečnosti, které by mohly způsobit ohrožení bezpečnosti nebo funkčnosti sítě Intranet,
    - zjištění poruchy některé služby sítě Intranet.

Uživatel nesmí na pracovních stanicích:

- provádět změny v konfiguraci technického a programového vybavení komunikačních prostředků a měnit připojení a přidělenou identifikaci (IP adresu) pracovní stanice vůči počítačové síti, není-li administrátorem lokální sítě nebo správcem počítačových programů,
- instalovat počítačové programy a aplikace, není-li správcem počítačových programů,
- spouštět a provozovat datové služby, které z pracovní stanice vytvoří server, pokud tak nebylo stanoveno interním aktem řízení lokálního provozovatele,
- zpracovávat, ukládat, odesílat nebo zpřístupňovat materiály, obsahující utajované informace,
- připojovat do lokální sítě jiné počítačové sestavy, než které byly připojeny administrátorem lokální sítě,
- žádnými prostředky se pokoušet získat v síti Intranet přístupová práva, která mu nebyla přidělena; pokud chybou získá jemu nepříslušející přístupová práva, je povinen tuto skutečnost neprodleně ohlásit správci uživatelských kont,
- vykonávat takové úkony, které vedou k dlouhodobému zpomalování nebo časovému omezování práce ostatních uživatelů sítě Intranet (například přenášení rozsáhlých datových souborů) mimo dobu, kterou pro tento účel vymezil lokální provozovatel na základě dohody s provozním gestorem, s výjimkou mimořádných případů, kdy je to nezbytně nutné pro plnění

[15)] Nařízení Ministerstva vnitra č. 21/2004, kterým se stanoví pravidla a způsob zabezpečování kontroly užívání počítačových programů v působnosti Ministerstva vnitra. Čl. 2 písm. d).

služebních nebo pracovních úkolů a hrozí nebezpečí z prodlení; v takovém případě je osoba povinná informovat vedoucího pracovníka lokálního provozovatele.[16]

1.7 ZÁSADA TVORBY KVALITNÍHO HESLA

Zásady tvorby a používání hesel je upraveno v interních pokynech vydaných k jednotlivým informačním systémům, které pracují s osobními údaji. Mezi základní pravidla při použití hesel patří:

- délka minimálně 8 znaků (15 u privilegovaných účtů),
- nesmí se shodovat s uživatelským jménem, ani se jménem či příjmením uživatele,
- liší se od předchozího hesla minimálně ve třech znacích,
- nesmí být částí textu popisu uživatele,
- nesmí být povolena hesla s dvěma a více za sebou jdoucími shodnými znaky,
- obsahuje alespoň 3 ze 4 požadavků komplexity (velké písmeno; malé písmeno; číslice; speciální znak),
- nejvýše 6 neplatných pokusů o přihlášení, poté dojde k blokaci účtu,
- platnost hesla v systémech je 3 měsíce,
- nepoužívat stejné heslo do různých služeb a sítí,
- heslo nesmí být snadno dostupné a nesmí být sdělováno jiným osobám.

[16] Závazný pokyn policejního prezidenta č. 80/2005 ze dne 9. srpna 2005, kterým se upravuje využívání datové sítě Intranet Ministerstva vnitra „Hermes“, článek 6.

2 OCHRANA DAT

2.1 ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ

V České republice existuje ústavní garance práva na informace. V článku 17 Listiny základních práv a svobod je zaručeno právo na informace. Každý má právo svobodné se vyjadřovat slovem, písmem, tiskem, obrazem jakož i jinými způsoby a také svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu. Výslovně je zakázána cenzura. Tato práva mohou být omezena jen tehdy, jestliže se jedná o opatření nezbytná v demokratické společnosti pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu zdraví a mravnosti. Zákon může uložit např. povinnost mlčenlivosti, označit určitou informaci za utajovanou nebo zakázat její šíření proto, že odporuje právním normám. Základní právní normou na úseku ochrany osobních údajů v České republice je zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

2.2 ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Úřad je nezávislým orgánem, který nepodléhá žádnému ministerstvu ani jinému státnímu orgánu. Jsou mu však svěřeny kompetence ústředního správního úřadu pro oblasti ochrany osobních údajů v rozsahu, který stanoví zákon o ochraně osobních údajů.

Základní pojmy

Osobním údajem se rozumí jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjektem údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.[17]

Citlivým údajem se rozumí osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství

[17] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů, § 4 písm. a).

a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů.[18]

Zveřejněným osobním údajem se rozumí osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.[19]

Utajovanou informací se rozumí informace zaznamenaná na jakémkoliv nosiči, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací. Seznam utajovaných informací vydá vláda svým nařízením. Utajovaná informace se klasifikuje stupněm utajení: vyhrazené, důvěrné, tajné, přísně tajné.[20]

2.3 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ U POLICIE ČESKÉ REPUBLIKY

Zákon o ochraně osobních údajů představuje obecnou právní úpravu, přičemž zákon předpokládá, že další právní úprava bude rozpracována ve zvláštních zákonech. Zvláštní zákon předpokládá tento zákon pro zpracování údajů pro účely statistické a archívní, stejně tak je tornu u zpracovávání osobních údajů zpravodajskými službami.

Rozsáhlou zvláštní právní úpravu zpracování osobních údajů má Policie České republiky v zákoně č. 273/2008 Sb., ve znění pozdějších předpisů.

Jedná se o ustanovení hlavy desáté Práce s informacemi,

§ 60 Obecná ustanovení o zpracování informací policií,

§ 62 Pořizování záznamů,

§ 63 Prokázání totožnosti,

§ 65 Získávání osobních údajů pro účely budoucí identifikace,

§ 66 Získávání informací z evidenci,

[18] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů, § 4 písm. b).
[19] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů, § 4 písm. l).
[20] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

§ 67 Získávání informací v souvislosti s odhalováním a šetřením přestupků,

§ 79 Zvláštní ustanovení o zpracovávání osobních údajů policií,

§ 80 Předávání nebo zpřístupňování osobních údajů,

§ 81 Zveřejňování osobních údajů,

§ 82 Prověřování potřebnosti dalšího zpracovávání osobních údajů,

§ 83 Informování o osobních údajích a oprava nepravdivých nebo nepřesných osobních údajů,

§ 84 Zpracování osobních údajů v Schengenském informačním systému,

§ 85 Zpracovávání osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti.

V rozsahu nezbytně nutném může policie zveřejňovat osobní údaje, a to v souvislosti s trestním řízením nebo pátráním po osobách. Zveřejnění se provádí zejména v hromadných sdělovacích prostředcích. Policie je oprávněna požadovat z evidencí provozovaných na základě zvláštního zákona potřebné údaje včetně osobních (např. z evidenci identifikačních dokladů). U některých těchto databází musí být dostupnost zajištěna způsobem umožňujícím dálkový a nepřetržitý přístup, tj . zejména prostřednictvím internetu a intranetu.

Informace může policista žádat pouze v míře nezbytné k provedení služebního úkonu a musí se tak dít způsobem, který umožňuje identifikovat policistu, který informaci žádá, účel, k němuž byla vyžádána, a to nejméně po dobu pěti let.

Povinnost mlčenlivosti

Povinnost mlčenlivosti podle zákona č. 101/2000 Sb., o ochraně osobních údajů, je definována:

Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních

opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.[21]

Pracovník je povinen zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Porušení této povinnosti je přestupkem podle § 44 odst. 1 zákona č. 101/2000 Sb.

2.4 OCHRANA DAT V INFORMAČNÍCH SYSTÉMECH

Právo na ochranu osobních údajů v informačních systémech je právem jednotlivce a vychází především z čl. 10 Listiny základních práv a svobod, ve kterém je uvedeno, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Toto právo musí být zajištěno nejen povahou vlastních informačních systémů, ale také způsobem obsluhy a ovládání těchto systémů. Informační systémy provozované policií pro plnění jejích úkolů obsahující osobní údaje podléhají režimu zákona číslo 101/2000 Sb., o ochraně osobních údajů. Tento zákon upravuje ochranu osobních údajů fyzických osob, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států. Uvedený zákon je ve vztahu k ochraně osobních údajů obecným předpisem, z něhož existuje řada výjimek upravených zvláštními zákony. Jedním z těchto zákonů je i zákon 273/2008 Sb., o Policii ČR, především hlava desátá - Práce s informacemi. V této části zákona jsou stanovena i pravidla pro likvidaci osobních údajů § 82 odst. 1. Policie nejméně jednou za tři roky prověřuje, jsou-li zpracovávané osobní údaje nadále potřebné pro plnění jejích úkolů. Je-li zjištěna nepotřebnost dalšího zpracování osobních údajů, jediným řešením této situace je jejich likvidace, a to bez zbytečného odkladu. Zpracování osobních údajů prováděná v rámci policie pochopitelně řeší i interní předpis - jedná se o závazný pokyn policejního prezidenta č. 215/2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů.

[21] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů, § 15.

2.5 OCHRANA OSOBNÍCH ÚDAJŮ PŘED JEJICH ZNEUŽITÍM

Každý uživatel si musí uvědomit svoji osobní odpovědnost za svěřená přístupová práva do informačního systému, zejména ve vztahu k jejich potenciálnímu zneužití. Veškerý přístup do informačních systémů je monitorován a pravidelně vyhodnocován. Dotazy do systémů by se měly provádět jen v souvislosti s plněním přidělených pracovních úkolů. V případě neoprávněného nakládání s osobními údaji pracovníkem Policie ČR je taková skutečnost posuzována jako porušení služební kázně[22], popřípadě naplnění skutkové podstaty trestného činu neoprávněné nakládání s osobními údaji.[23]

2.6 ZÁKLADNÍ INFORMAČNÍ SYSTÉMY PČR

Informační systémy Policie České republiky tvoří funkční celek, určený k zajištění činnosti a k plnění úkolů jednotlivých útvarů a složek policie. Na bázi výpočetní techniky zabezpečují shromažďování, zpracování, přenos a zpřístupnění informací oprávněným pracovníkům včetně ochrany dat.

Veškerá činnost informačních systémů se děje v souladu s obecně platnými a interními právními předpisy. Na základě těchto norem PČR zpracovává ve svých systémech získané informace včetně osobních údajů. Tyto údaje shromažďuje v rozsahu jen nezbytně nutném pro plnění svých úkolů. Základními právními předpisy jsou zákon č. 273/2008 Sb., o Policii České republiky, hlava X a zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Jednotlivé policejní informační systémy jsou vzájemně propojené a to následně umožňuje na základě jediného dotazu získat informace z více systémů.

Policie České republiky užívá více než 50 informačních systémů. Mezi základní a nejdůležitější informační systémy, které jsou užívány a mají klíčovou roli, patří Evidence trestního řízení (ETŘ), Ekonomický informační systém Ministerstva vnitra ČR (EKIS), informační systém Dotaz.

[22] Zákon č. 361/2003 Sb., o služebním poměru příslušníků PČR, § 46.
[23] Zákon č. 40/2009 Sb., trestní zákoník, § 180.

2.6.1 EVIDENCE TRESTNÍHO ŘÍZENÍ

Jeho účelem je dokumentování průběhu trestního, přestupkového a správního řízení na krajské úrovni a postupná elektronizace spisových materiálů. Systém je provozován na krajských serverech fyzicky umístěných na režimových pracovištích, na která mají přístup pouze oprávněné osoby. Do systému se každý uživatel přihlašuje přiděleným jménem a voleným heslem. Přístup ke spisům je určen pomocí tzv. rolí uživatele v systému a dále tím, zda spis již má přiděleného zpracovatele, zda je zpracovatel na základním útvaru nebo na útvary služby kriminální policie a vyšetřování.

Mezi základní funkce patří evidence dokumentů a vedení spisové služby, odesílání uložených dat do systému Kriminalisticky sledovaná událost, Události, P-Zbraně, IS-Banka, SVI. V systému je zakomponován export/import dat na jiný kraj, zpracování a uchovávání formulářů, vytváření statistických výstupů, evidence blokového řízení, přístup do rejstříku trestů a do databází pátrání po osobách, věcech a motorových vozidlech. Systémem ETŘ lze rovněž přijímat a odesílat datové zprávy fyzickým, právnickým osobám a orgánům veřejné moci, kdy zadaného příjemce datové zprávy systém vždy ověřuje. Systém dále umožnuje vytvářet elektronické podpisy k dokumentům a disponuje datovým prostorem pro ukládání multimediálních souborů k jednotlivým elektronickým spisům.

2.6.2 EKONOMICKÝ INFORMAČNÍ SYSTÉM MINISTERSTVA VNITRA ČR

Jedná se o komplexní modulární systém, který je určen k vedení ekonomických, mzdových a personálních agend. Mezi základní funkce systému EKIS (elektronický informační systém) patří řízení ekonomických procesů a lidských zdrojů, což umožnuje vedoucím pracovníkům efektivní řízení výdajů, osob a jejich odměňování.

Systém kromě dalších funkcí umožňuje účtování po účetních jednotkách, vedení podvojného účetnictví, sledování nákladů dle různých volitelných hledisek, evidenci dlouhodobého a hmotného majetku, evidenci zásob, včetně objednávek a inventur. Přičemž využívá čárového kódu, dále umožňuje spravovat osobní konta policistů dle jim přidělených výstrojních norem, vede katalogy prací a profesí, evidenci volných míst dle organizační struktury Policie. Sytém EKIS je určen pro ekonomické zajištění činnosti Policie ČR.

2.6.3 SCHENGENSKÝ INFORMAČNÍ SYSTÉM

SIS slouží zejména pro pátrání po osobách a věcech. Do systému přispívají všechny členské státy přímo ze svých národních pátracích databází.

2.6.4 INFORMAČNÍ SYSTÉM DOTAZ

Dotazy do informačních systémů je základním prostředkem pro získávání informací z informačních systémů Policie ČR a z informačních systémů státní správy. Přístup do programu je povolen příslušníkům a zaměstnancům policie a inspekce ministra vnitra, kteří přístup nezbytně potřebují k plnění svých služebních úkolů. Přístup je možný jen přes přidělené uživatelské konto, které je tvořeno uživatelským jménem a heslem. K práci s programem je vydán závazný pokyn policejního prezidenta č. 168/2009, kterým se upravuje jednotný postup při jeho provozování a využívání. Program umožňuje uživatelům zadávat z pracovní stanice dotazy do informačních systémů ve 3. úrovních:

Základní dotaz s přesným zadáním, kdy při dotazu musí být přesně zadány stanovené identifikační údaje konkrétní osoby nebo věci; úroveň umožňuje na základě jediného zadání dotazu získat informace ze zvolených informačních systémů v rámci přidělených oprávnění. Systémy, ve kterých bude dotaz proveden, je nutné označit zatržením. Pro vyhledání osoby zadejte příjmení, jméno a datum narození. Pro vyhledání vozidla je třeba zadat kompletní registrační značku.

Komplexní dotaz s neúplným zadáním, kdy při dotazu stačí zadat jen část identifikačních údajů jako je například část jména, příjmení nebo rozsah data narození. Komplexní dotaz se zadává vždy do jednoho konkrétního informačního systému.

Full Textový dotaz umožňuje vyhledávání podle jednotlivých slov, jejich částí a jejich kombinací spojených logickými operátory; odpověď na dotaz obsahuje všechny záznamy ze zvolených informačních systémů (v rámci přidělených oprávnění), v nichž se zadané slovo nebo logická kombinace slov vyskytuje. Při každém dotazu je uživatel povinen dle závazného pokynu policejního prezidenta č. 215/2008 kterým se stanoví podmínky a postupy pro zpracování osobních údajů při plnění úkolů Policie České republiky vyplnit důvod dotazu. V evidenci dotazů se informace o každém provedeném dotazu uchovává po dobu 5 let.

3 BEZPEČNOSTNÍ HROZBY

Informační technologie pronikají do všech oblastí života a fungování společnosti. Závislost České republiky na informačních technologiích do budoucna bude nadále narůstat. Agendy v rámci státní správy přecházejí z fyzické podoby dokumentů do digitální podoby, která pak umožnuje efektivnější komunikaci a rychlejší využití dokumentů a přístupu do informačních systémů. Tyto výhody jsou zároveň zranitelnější vůči hrozbám a útokům, které přicházejí do anonymního kyberprostoru, která představuje pro stát a občany bezpečnostní hrozby, kterým je nutno předcházet. Zapotřebí bylo vytvoření jednotného a pevně stanoveného zákonného rámce, kterým se stal v roce 2014 **zákon o kybernetické bezpečnosti** a s ním související prováděcí předpisy. Informační technologie poskytují stále nové funkce a možnosti pro rychlejší výměnu dat, zvyšuje se datová propustnost síťových linek. Zároveň poskytují výhodu těm, kteří mají záměr tyto data zneužit ve svůj prospěch. Výhoda anonymity v počítačových sítí způsobuje, že se rozšiřují kriminální aktivity, které se přesouvají do kyberprostoru, který umožnuje útočníkům rychlé získání požadovaného cíle s minimálním rizikem odhalení a bez nutnosti fyzické přítomnosti, kdy útok může byt proveden z kteréhokoliv kontinentu. Aktuální kybernetické hrozby lze rozdělit do několika forem útoku. Nejzávažnější skupinu tvoří špionáže cizích států, sabotáže, DDoS útoky na servery, hackerství. Tyto útoky vedou často ke krádeži osobních a přístupových údajů a následného vyřazení bezpečnostního systému. Příčinou útoku může být kolaps informačních systémů. Častým ziskem útočníků je prodej získaných důvěrných dat, přístupových údajů a hesel, které jsou prodány zájemcům. Při získání těchto údajů dochází k ohrožení internetového bankovnictví, kritické infrastruktury. Další formou nežádoucích aktivit je šíření dětské pornografie, anonymní prodej drog a přeměna nelegálně získaných peněz na přeměnu s pomocí virtuálních měn na legální, internetová šikana, šíření spamu. Kybernetický prostor je rovněž ve velké míře využíván k projevu extrémismu a k šíření propagaci teroristických aktivit. Boj proti uvedených aktivitám je stále náročnější z důvodu sofistikovanějšího způsobu útoku a schopnostech útočníků zůstat v anonymitě.[24] Bezpečnostní hrozby lze z obecného pohledu rozdělit na rizika **vnější** a **vnitřní.**

[24] Bezpečnostní hrozby: Kybernetické hrozby. *Ministerstvo vnitra České republiky* [online]. [cit. 2017-01-20]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

3.1 VNITŘNÍ RIZIKA

Představují nebezpečí, které ohrožuje samotný chod počítače, sítě.

- **Poškození technického zařízení:** spočívá v selhání hardwarových komponentů a následnou jejich nefunkčnost.
- **Výpadek elektrického proudu:** výpočetní technika se bez dostatečného přísunu elektrické energie neobejde.
- **Programové chyby:** každý naprogramovaný systém obsahuje chyby.
- **Kolize technického či programového vybavení:** ke správné funkčnosti systému, je potřeba mít sladěné hardwarové a softwarové vybavení.
- **Chyba uživatele:** značná část problémů a ztrát informací je způsobena samotným uživatelem, který buď úmyslně, nebo svojí neznalosti poškodí potřebné data nebo technické vybavení.

3.1.1 PREVENTIVNÍ OPATŘENÍ PRO VNITŘNÍ RIZIKA

Pravidelná záloha vybraných dat, které uložíme na jiné médium. Při zálohování je nutné dodržovat pravidelnost a ověřovat zpětnou čitelnost. Rovněž je nutná kontrola stavu hardwarových komponentů a sledování případné změny, jako je například přehřívání hardwaru. Nutné je rovněž sledovat dobu pořízení a vytíženost užívaného zařízení. Dále je potřeba v datových centrech a servrovnách zajistit dostatečný odvod tepla, které produkují. Většinou je tento problém vyřešen umístěním klimatizační jednotky. Strategicky důležitá zařízení je nutné napojit na zdroj nepřerušovaného napájení, často označovaný zkratkou UPS[25]. Jedná se o zařízení, které zajišťuje nepřetržitou dodávku elektrického proudu pro výpočetní techniku, která nesmí být neočekávaně vypnuta. Každý naprogramovaný systém obsahuje chyby, které je třeba odstranit testováním. Zjištěné chyby se opravují v podobě aktualizací, případně vychází kompletně nová verze aplikace. Zde rovněž platí pravidelná záloha dat. K zabránění technické kolize je nutné volit vhodný hardware komponenty v kombinaci se softwarovým vybavením. Není například možné užívat nejnovější operační systém na počítačové sestavě z roku 2000. K minimalizování chyb uživatelů při práci je důkladné proškolení a vzdělávání zaměstnanců a upozornění na chyby, kterých se dopouštějí.[26]

Obrázek 2: Záložní zdroj elektrické energie v budově IBC Ostrava
Obrázek 3: Záložní zdroj elektrické energie v budově IBC Ostrava

[25] Uninterruptible Power Sumpply - zdroj nepřerušovaného napájení.
[26] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada, 2015, s. 13. Průvodce (Grada). ISBN 978-80-247-5453-6.

Obrázek 4: Záložní zdroj elektrické energie v budově IBC Ostrava

Zdroj[27]

3.2 VNĚJŠÍ RIZIKA

Je soubor rizik, která ohrožují cenné informace z vnějšího prostředí a představují nebezpečí ztráty dat, pozměnění souborů nebo odcizení datových souborů. Z uvedeného důvodu je nutno nastavit opatření k minimalizaci těchto rizik a dodržovat bezpečnostní zásady.

- **Krádež zařízení**
  Data jsou ložena na pevných discích v počítači nebo na discích na datovém uložišti. Je nutné zabránit fyzickému odcizení těchto datových nosičů.
- **Neoprávněný přístup k zařízení**
  Pro přihlášení je potřeba použít dostatečně silné heslo.
- **Počítačová infiltrace**
  Infiltrace pomocí malware - škodlivé programy. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software.[28]

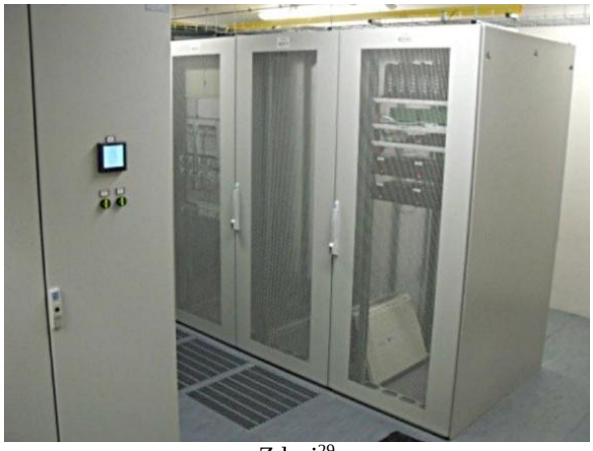
3.2.1 PREVENTIVNÍ OPATŘENÍ PRO VNĚJŠÍ RIZIKA

Výpočetní techniku situovat na místa, kde je riziko odcizení zařízení minimální. Jedná se o uzamčené prostory, které jsou v nepřítomnosti uživatele elektronicky chráněny s napojením na pult centrální ochrany. PC skříň opatřit bezpečnostní samolepící plombou. V případě ochrany datových center, je nutná fyzická ostraha objektu a nastavení přísných podmínek pro přístup

[27] Integrované bezpečnostní centrum Moravskoslezského kraje [online]. s. 31 [cit. 2017-01-01]. Dostupné z: http://www.hzscr.cz/soubor/2015-04-ibc-msk-cz-pdf/
[28] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 115. ISBN 978-80-7251-436-6.

k samotným severům, kde se nacházejí datové nosiče. Vstup do uvedeného prostoru je možný pouze přes bezpečnostní dveře, prostor elektronicky zabezpečit a prostor monitorovat kamerovým systémem. Nutné je rovněž prostor zabezpečit plynovou protipožární ochranou. Pro neoprávněný přístup k zřízení je nutné volit dostatečné silné heslo. Více informací v kapitole 1.7 a 3.6. Nutností je rovněž při každém odchodu od počítače použít systémový zámek, který lze vyvolat v operačním systému Microsoft Windows kombinace kláves Win+L.

Obrázek 5: Datové centrum v IBC Ostrava



Zdroj[29]

3.3 POČÍTAČOVÁ INFILTRACE

Počítačová infiltrace je provedený útok v podobě malware (z anglického MALicocius softWARE – zlomyslný program).

Základní rozdělení škodlivosti jednotlivých druhů malware:

- **Adware**
  Typ softwarové licence, jejíž užívání je zdarma, v programu se objevuje reklama, ze které je financován jeho vývoj.[30]
- **Backdoor (zadní vrátka)**
  Skrytý softwarový nebo hardwarový mechanizmus obvykle vytvořený pro testování a odstraňování chyb, který může být použít k obejití počítačové bezpečnosti. Metoda v počítačovém systému nebo v algoritmu, která útočníkovi umožňuje obejít běžnou

[29] Integrované bezpečnostní centrum Moravskoslezského kraje [online]. s. 29 [cit. 2017-01-01]. Dostupné z: http://www.hzscr.cz/soubor/2015-04-ibc-msk-cz-pdf/
[30] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 15. ISBN 978-80-7251-436-6.

autentizaci uživatele při vstupu do programu nebo systému a zároveň mu umožňuje zachovat tento přístup skrytý před běžnou kontrolou. Pro vniknutí do operačního systému mohou obejít firewall například tím, že se vydávají za webový prohlížeč. Tento kód může mít formu samostatně instalovaného programu nebo se jedná o modifikaci stávajícího systému. Samotný vstup do systému pak mívá formu zadání fiktivního uživatelského jména a hesla, které napadený systém kontroly přijme a přidělí uživateli administrátorská práva.[31]Zadní vrátka obsahují taktéž jako trojský kůň serverovou a klientskou část.[32]

- **Keylogger**

  Software, který snímá stisky jednotlivých kláves, bývá však antivirem považován za virus, v případě softwaru se jedná o určitou formu spyware, ale existují i hardwarové keyloggery. Často se používá pro utajený monitoring všech aktivit na PC, jenž je pro ostatní uživatele neviditelný a chráněný heslem. Umožňuje automatické zaznamenávání všech stisků kláves (psaný text, hesla apod.), navštívených www stránek, chatů a diskuzí přes ICQ, MSN apod., spouštěných aplikací, screenshotů práce s počítačem, práce uživatele se soubory a další. Zaznamenaná data mohou být skrytě odesílána emailem.[33]

- **Ransomware**

  Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného.[34] Následná komunikace mezi poškozeným a hackerem probíhá po síti Tor, která byla vytvořená s cílem zůstat v anonymní a sdílet informace, návody, prodej nelegálního zboží. Výkupní chtějí obvykle v podobě měny Bitcon, kdy tato měna nepodléhá kontrole ze strany úřadů, bank.

- **Spyware**

  Spyware jsou programy, které sledují vaší činnost a poté data odesílají z počítače bez vědomí uživatele. Přítomnost spyware často vede k instalaci dalšího škodlivého softwaru, který následně provede nastavení internetového prohlížeče, instaluje další škodlivý software a zobrazuje cílené reklamy.

---

[31] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 131. ISBN 978-80-7251-436-6.
[32] KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně*. Praha: Grada, 2006, s. 334. Průvodce (Grada). ISBN 80-247-1408-6.
[33] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 62-63. ISBN 978-80-7251-436-6.
[34] *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, s. 97. ISBN 978-80-7251-436-6.

3.4 ZÁKLADNÍ DRUHY MALWARU PODLE ZPŮSOBU INFILTRACE

- **Trojan hors (trojský kůň)**

Jedná se o nejoblíbenější a nejrozšířenější hackerský nástroj současnosti. Trojský kůň jakožto funkční celek se skládá ze dvou částí, serveru a klienta. Server program běžící na počítači oběti, obvykle bez jeho vědomí a otvírá přístup k ovládání počítače. Skrze otevřený přístup je běžící server ovládán útočníkem. Podle množství funkcí, které server nabízí, může útočník s počítačem oběti provádět tomu adekvátní úkony. Server se spouští na infikovaném počítači, anebo je k tomuto účelu užita slabina softwarového vybavení počítače jako je chyba v e-mailovém klientovi nebo internetovém prohlížeči.[35] Trojské koně se používají na nejrůznější účely, jako jsou monitorování činnosti napadeného počítače až po zneužití počítače pro DoS útok. Trojský kůň se často jeví jako užitečný software, ale místo užitku naruší zabezpečit celé sítě.

- **Virus**

Virus se v oblasti počítačové bezpečnosti označuje jako nežádoucí program, který se dokáže sám šířit a infikuje bez vědomí uživatele další počítače. Má podobné vlastnosti jako biologický virus. Pro množení využívá zejména spustitelných souborů nebo makra dokumentů. Oblíbeným médiem pro přenos viru jsou USB flash disky.

- **Worms (červ)**

Je program rozšiřující se pomocí počítačové sítě. K šíření může používat sdílené disky nebo jiné komunikační kanály, nejčastěji způsobem šíření je prostřednictvím elektronické pošty.36

[35] *Slabá místa Windows, aneb, Jak se bránit hackerům*. Kralice na Hané: Computer Media, 2004, s. 112. Vzdělávání, které baví. ISBN 80-86686-11-6.
[36] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada, 2015, s. 15. Průvodce (Grada). ISBN 978-80-247-5453-6.

Ochrana a prevence před malware:

Skutečná ochrana před trojskými koňmi a backdoor spočívá, stejně tak jako v případě virů, v prevenci. Základem je kvalitní antivirový program, který je pravidelně aktualizován. Antivirový program dovede vyřešit řadu problému a odhalit hrozící nebezpečí. Součásti prevence není jen instalace antivirového programů, ale také znalost prostředí, v kterém pracujete. Není vhodné spouštět a instalovat neznámé aplikace a otevírat e-mailovou přílohu, kterou neočekáváte, a neznáte přesný obsah přiloženého souboru. Je rovněž důležité znát počet spuštěných procesů v pozadí operačního systému. Aby mohl server trojského koně s klientem vzájemně komunikovat, musí být pro tuto komunikaci vyhrazeny určité porty. Server na daném portu vyčkává na připojení klienta. Tímto způsobem pracují nejenom trojské koně, ale také všechny ostatní sítové aplikace.[37] Je důležité sledovat aktivitu všech síťových portů. Je nutné sledovat, zda se v počítači neděje něco podezřelého, nestandardního, jako je například neobvyklý nárůst přenosu dat, zvýšená činnost disku. V případě rozsáhlých systému provádět penetrační testování, kdy se zkoumá funkce počítačového systémů a sítí s cílem detekovat slabá místa a slabou bezpečnost a tyto slabiny ochránit.

Ochrana a prevence před sypware:

Ochrana spočívá v neinstalování aplikace, o kterých je veřejně známo, že spyware obsahuji. Při volbě programů nespoléhat na bezplatné aplikace freeware, protože i tito autoři chtějí mít příjem peněz, který si často získávají informacemi o uživatelích jejích programů. Nejedná se o virus, ale podstatnou skutečností je, že se spyware rozšiřuje společně s řadou volně šiřitelných programů, jako jsou video kodeky, videopřehrávače.

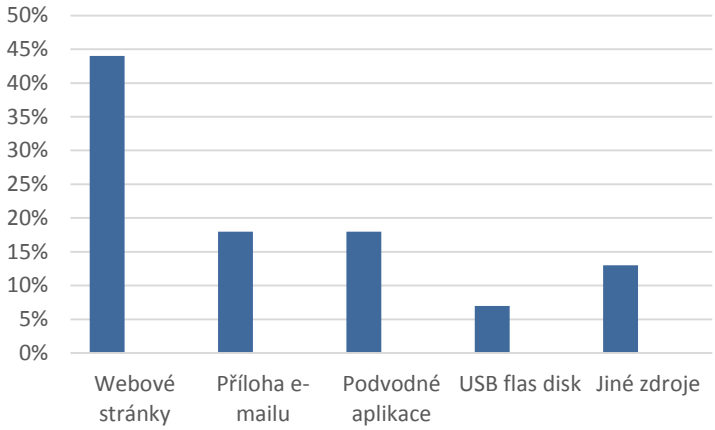
3.5 NEJČASTĚJŠÍ ZDROJE INFIKOVÁNÍ MALWAREM

Průzkum společnosti Kaspersky Lab potvrdil, že malware představuje nejběžnější bezpečnostní hrozbu, které uživatelé čelí. 41 % dotázaných také k vyřešení problému způsobeného malwarových útoku muselo zaplatit za svá data, přičemž průměrná částka za jednu opravu přesáhla částku 3000,- Kč. Zajímavosti je, že podstatná část uživatelů (33 %) neví, jak se

[37] *Slabá místa Windows, aneb, Jak se bránit hackerům*. Kralice na Hané: Computer Media, 2004, s. 121. Vzdělávání, které baví. ISBN 80-86686-11-6.

malware do jejich zařízení dostal. V ostatních případech jsou nejčastějším zdrojem infekce webové stránky.[38]

Graf 1: Nejčastější zdroje infikování malwarem



Zdroj[39]

Z pohledu hackerů jsou USB disky ideálními branami do počítačů. Zcela bezpečné už nejsou izolované sítě, které nejsou připojeny k internetu – pro jejich infikovaní mohou hackeři bez problému využít například USB flesh disk. Už se také objevily viry, které byly nainstalovány v klávesnicích, ze kterých později infikovaly celou sít. Hackeři jsou zkrátka stále vynalézavější a téměř žádný komponent už nemusí být v bezpečí.[40]Ochrana jak předejít infikování hardwarového zařízení je neinstalovat jiné verze firmwaru, než který pochází od výrobce a volit známé a prověřené výrobce hardwaru.

3.6 HESLA A JEJICH ZABEZPEČENÍ

Hesla se dají přirovnat k základům zabezpečení systému, a pokud je heslo prolomeno a odhaleno, základ systému je narušen a je jen otázka času, kdy následuje zhroucení veškeré bezpečnosti. Je proto na místě, že se hesla snažíme co nejvíce chránit, abychom podobným

[38] Nejčastější zdroje infikování malwarem. *CHIP Magazín o digitálních technologiích*. Praha: BURDA Praha, spol. s r.o., 2017, č.1 , s. 27, ISSN 1210-0684.
[39] Nejčastější zdroje infikování malwarem. *CHIP Magazín o digitálních technologiích*. Praha: BURDA Praha, spol. s r.o., 2017, č.1 , s. 27, ISSN 1210-0684.
[40] *CHIP Magazín o digitálních technologiích*, 10/2015, Praha: BURDA Praha, spol. s r.o., 2015, č. 10, s. 15, ISSN 1210-0684.

nehodám předešli. Pokud naše přihlašovací údaje budou veřejně známé, nemá žádné bezpečnostní opatření smysl.

Operační systém Microsoft Windows se během své evoluce značně polepšil, ale stále obsahuje mnoho vad, které bezpečnost značně odkrývají.[41] Uvedený operační systém je užíván na většině pracovních stanic u Police České republiky.

3.6.1 ZOBRAZENÍ ULOŽENÝCH HESEL

V průběhu práce na PC jsme nuceni zadávat hesla pro přístup do informačních systémů, internetového prohlížeče, e-mailového klienta. Mezi nejčastější údaje, které vyplňujeme, je správcem přidělené uživatelské jméno a následně heslo, které si po prvním přihlášení pozměníme. Operační systém Windows si tyto údaje ukládá do takzvaného chráněného úložiště v nijak nezměněné a nezašifrované podobě, bez vědomí uživatele. Přihlašovací údaje se ukládají na pracovní stanici, na které pracujeme. Je celá řada programů, které zobrazení informací uložených v takzvaně chráněném uložišti umožnují. Jedná se například o programy PasswdFinder, Cain & Abel.

PasswdFinder je aplikace určená k získávání hesel uložených v e-mailových klientech, FTP klientech, internetových prohlížečích, správcích vzdáleného přístupu či dalších typech softwaru. Po spuštění aplikace se provede sken všech podporovaných programů, následně se zobrazí přístupové údaje (uživatelská jména a hesla) používané v těchto programech. Nástroj si poradí se zobrazením uložených údajů z: Mozilla Firefox, Google Chrome, Safari, Opera, Outlook, Yahoo Messenger, MSN Messenger, CamFrog, Google Talk, ICQ, Mozilla Thunderbird a v desítkách dalších jiných programů.

Cain & Abel je aplikace, která umožňuje obnovu hesel z většiny populárních protokolů včetně FTP klientů, SMTP, HTTP, mySQL, POP3, ICQ, Telnetu a dalších. Zobrazit lze i hesla skrytá za hvězdičkami, které jsou uložená ve Virtual Network Computing profilech. Jedná se o grafický program, který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní pomocí počítačové sítě.

[41] *Slabá místa Windows, aneb, Jak se bránit hackerům*. Kralice na Hané: Computer Media, 2004, s. 14. Vzdělávání, které baví. ISBN 80-86686-11-6.

Výše uvedené aplikace jsou bezplatné a volně přístupné na Internetu. Je třeba vycházet z faktu, že většina uživatelů volí shodné hesla k přístupům, tudíž lze předpokládat, že v případě odhalení hesla např. k emailové schránce, shodné heslo je využito i k služně internetové bankovnictví, sociální sítí Facebook, informačním systémům atd.

Ochrana

U počítačů v síti, ke kterým je volný přístup a často se u nich střídají uživatelé, je podstatné, aby správce sítě vypnul funkce, jako je automatické dokončování textu či ukládání hesel. Obzvlášť pak v programu internetových prohlížečů, které jsou vstupní bránou do informačních systémů. Pro uživatele tato funkce může představovat jisté pohodlí, ale z bezpečnostního hlediska se jedná o velkou slabinu operačního systému Microsoft Windows.[42] Základem bezpečnosti je zamezit možnosti instalace jakýchkoliv aplikací, které jsou určeny k získání hesla a umožnují k nim přístup.

3.6.2 PROLAMOVAČE HESEL

Tento druh útoku spočívá v postupném zkoušení všech možných kombinací zadaných znaků, dokud není správná kombinace – heslo. Jedná se o jeden z nejstarších nástrojů používaných hackery. Cílem je prolomení ochrany nebo autorizace, která je prováděna statickým heslem. Princip prolomení hesla spočívá v generování nejrůznějších kombinací znaků, a pokud autorizace bude pozitivní, následuje odeslání správného hesla hackerovi. Jsou dva základní druhy útoků realizovány prolamovači hesel:

- **Slovníkové útoky**, hesla jsou zadávána z databáze slov, která obsahuje nejpoužívanější hesla a slova,
- **Útok hrubou silou**, aplikace postupně generuje všechny možné kombinace potřebné délky a znaků, zda nevyhovuje zadanému heslu.

[42] *Slabá místa Windows, aneb, Jak se bránit hackerům*. Kralice na Hané: Computer Media, 2004, s. 16. Vzdělávání, které baví. ISBN 80-86686-11-6.

3.6.3 ZÍSKÁNÍ HESLA HRUBOU SILOU

Tato forma útoku se nejčastěji užívá v případech, kdy není pro ověření korektnosti zadaného hesla použito správné heslo. Nedochází tedy k přímému porovnání zadaného správného hesla. Místo toho je využita jeho zašifrovaná podoba. Zašifrované heslo nelze zpět dešifrovat, a proto při útoku hrubou silou postupuje program stejným způsobem jako algoritmus pro ověřování platnosti hesla, kdy program proto vygeneruje nějaké heslo (heslo je tvořeno systematicky, aby nedocházelo výskytu duplicitních záznamů), zašifruje ho a porovná s uloženou zašifrovanou hodnotou. Pokud se obě hodnoty shodují, bylo nalezeno správné heslo. Pokud ne, celý postup se opakuje.[43] V dnešní době je volně k dispozici množství prolamovačů, které lze volně stáhnout a užívat. Pro názornost jak rychle lze zjistit heslo, uvádím tabulku s kombinaci pro použité heslo a přehled odhadované doby pro prolomení hesla.

Tabulka 1: Odhady doby práce prolomení hesla podle kombinace hesla

Kombinace použitá pro heslo	Odhad doby práce prolamovače hesel
4 velká nebo malá písmena	několik sekund
4 velká a malá písmena, libovolná kombinace	několik sekund
4 velká a malá písmena a číslice v libovolné kombinaci	několik sekund
5 velkých nebo malých písmen	méně než 1 minuta
5 velkých a malých písmen v libovolné kombinaci	cca 6 minut
5 velkých a malých písmen a číslic v libovolné kombinaci	cca 15 minut
8 velkých nebo malých písmen	cca 58 hodin
8 velkých a malých písmen a číslic v libovolné kombinaci	cca 7 let
10 velkých nebo malých písmen	cca 5 let
10 velkých a malých písmen v libovolné kombinaci	cca 4648 let
10 velkých a malých písmen a číslic v libovolné kombinaci	cca 26984 let

Zdroj[44]

[43] *Slabá místa Windows, aneb, Jak se bránit hackerům*. Kralice na Hané: Computer Media, 2004, s. 18. Vzdělávání, které baví. ISBN 80-86686-11-6.
[44] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007. s. 63. ISBN 978-80-2471561-2.

Rychlost prolamovačů na odhalení hesel k zakódovaným souborům např. Microsoft Word nebo Acrobat se pohybuje zhruba od 50 000 hesel za sekundu na běžném počítači. K nejvýznamnějším faktorům, které ovlivňuji rychlost prolamovače patří:

- rychlost počítače,
- typ prolamovaných dat, typ souboru,
- umístění dat nebo souboru (zda se soubor nachází na lokálním disku, v síti apod.),
- struktura zakódovaného souboru.

Ochrana

Ochrana proti tomuto druhu útoku prolomení hesla je velmi obtížná. Základem je, aby administrátoři sítí nenechávali počítače, kde se přihlašují, bez dozoru. Tím mohou útočníkovi značně usnadnit práci. Dalším důležitým opatřením je volba hesla, aby bylo co nejobtížnější ho odhalit. Pro větší bezpečnost je nejlepší heslo pravidelně měnit a volit kombinaci s opravdu obtížným heslem. Vhodné je zvolit jako první znak hesla písmeno z, neboť při útoku hrubou silou většina aplikací volí přednastavené znakové sady a – z, a program se dostane k heslům začínajícím písmenem Z až úplně na závěr.[45]

Nejpoužívanější hesla v roce 2016

Internetový portál Letem světem Applem zveřejnil informaci, že v roce 2016 byla provedená analýza na více než 10 milionech heslech, která za uplynulý rok pronikla na veřejnost při narušení bezpečnosti několika služeb. Keeper tým zjistil, že přibližně 17% uživatelů stále používá nejprimitivnější heslo "123456" a to už několik let v řadě. Nejčastější a zároveň ta nejjednodušší hesla se za poslední roky vůbec nezměnila. Uživatelé se i přes neustálá upozornění na nutnost zvolení kvalitního hesla stále nemají k tomu, nastavit si alespoň o něco složitější heslo, než právě čísla od 1 do 6. [46] Níže uvedený výčet 10. nejpoužívanějších hesel v roce 2016 má upozorňovat na skutečnost, že uživatelé i přesto, že jsou upozorňování na hrozby a časté případy prolomení hesel, nerespektují toto varování a volí jednoduché heslo, které si lze lehce zapamatovat.

[45] Slabá místa Windows, aneb, Jak se bránit hackerům. Kralice na Hané: Computer Media, 2004, s. 23. Vzdělávání, které baví. ISBN 80-86686-11-6.
[46] Letem světem Applem: Tohle jsou nejpoužívanější hesla roku 2016. Horší už to být asi nemohlo. [online]. [cit. 2017-01-01]. Dostupné z: https://www.letemsvetemapplem.eu/2017/01/19/nejpouzivanejsi-hesla-roku-2016/

Tabulka 2: 10 nejpoužívanějších hesel roku 2016

10 nejpoužívanějších hesel roku 2016	
1	123456
2	123456789
3	Qwerty
4	12345678
5	111111
6	1234567890
7	1234567
8	Password
9	123123
10	987654321

Zdroj [47]

Další způsobem, jak lze heslo získat, je instalace softwarového nebo fyzického keyloggeru.

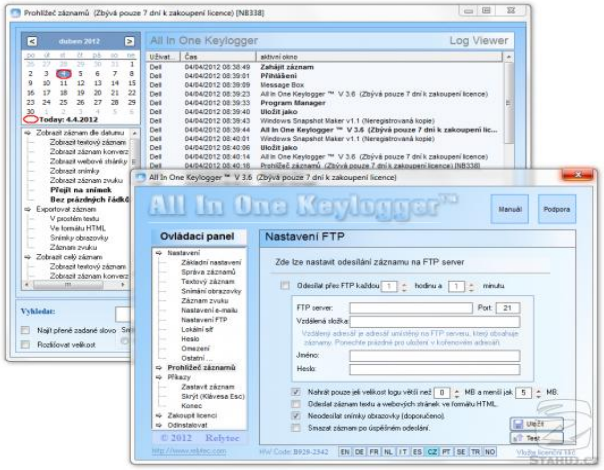
3.6.4 SOFTWAROVÝ KEYLOGGER

Heslo a další komunikaci lze získat od uživatele instalací aplikace, které jsou označeny jako tzv. key-loggery, které monitorují klávesové stisky, které si zapisují. Aplikace se skrytě instaluje do počítače a následně monitoruje uživatele, kdy veškeré klávesové stisky ukládá do logovacího souboru, který je zakódován a přístupný po zadání hesla. Jeden z nejznámějších keyloggerů je : All In One Keylogger. Tento program nejen zaznamenává stisknuté klávesy, ale dokáže také nahrávat zvuky z interních mikrofonů zabudovaných v zařízení, získávat snímky obrazovky v různých intervalech a ty poté ukládat a případně odesílat.

Logy, které program získá, následně uloží na předem určené místo na pevném disku, případně je odešle na FTP server. All In One Keylogger má ale také pokročilé bezpečnostní funkce, které zabraňují jeho zobrazení v seznamu běžících procesů, či znemožňují blokování různým anti-keyloggerům. Tento program není virus, i když jeho funkce tomu napovídají. Je nespočet firem, kde je tato aplikace instalována záměrně z důvodu větší kontroly nad zaměstnanci.

[47] Letem světem Applem: Tohle jsou nejpoužívanější hesla roku 2016. Horší už to být asi nemohlo. [online]. [cit. 2017-01-01]. Dostupné z: https://www.letemsvetemapplem.eu/2017/01/19/nejpouzivanejsi-hesla-roku-2016/

Obrázek 6: Uživatelské prostředí programu All In One Keylogger



Zdroj[48]

Ochrana

Ochrana proti spuštěné aplikaci, která zapisuje klávesové stisky, spočívá hlavně v kontrole seznamu běžících procesů/služeb. Každý administrátor by měl pravidelně kontrolovat, jaké procesy na počítačích a sítí běží.

3.6.5 FYZICKÝ KEYLOGGER

Jedná se o poměrně malé zařízení, které propojuje klávesnici a počítač. Keylogger začne po propojení automaticky evidovat veškeré úhozy provedené na klávesnici. Data lze z fyzického keylogeru získat pomocí dodané aplikace společně se zařízením. Nejmodernější fyzické keylogerry jsou již vybaveny bezdrátovým přenosem WIFI a samotný přístup k počítači není nutný.

Obrázek 7: USB Keylogger

Zdroj [49]

[48] All In One Keylogger. In: *Stahuj.cz* [online]. [cit. 2017-01-01]. Dostupné z: http://www.stahuj.centrum.cz/direct/iR/all-in-one-keylogger/_detail--300x.png.
[49] USB keylogger PROFI. In: *SPY OBCHOD* [online]. [cit. 2017-01-01]. Dostupné z: http://www.spyobchod.cz/galerie/2_171/usb-keylogger-pro-original.jpg.

Ochrana: Uvedené zařízení nelze dálkově detekovat jako nové hardwarové zařízení a jediná účinná ochrana spočívá ve fyzické kontrole kabelu po celé jeho délce od klávesnice až k připojení do počítače. Zařízení lze zakoupit v českých internetových e-shopech.

3.7 AKTUÁLNÍ VIROVÉ HROZBY

Společnost ESET software spol. s r.o. na portálu http://www.virovyradar.cz. Nabízí aktuální přehled detekovaných virů na konkrétním území a časové ose. Níže uvedená tabulka č. 3 zobrazuje virový radar v České republice k lednu 2017. [50]

Tabulka 3: 10 nejrozšířenějších viru k lednu 2017 na území České republiky

Virový radar České republiky		
Pořadí	Název	četnost
1	JS/Danger.ScriptAttachment	20,1 %
2	JS/TrojanDownloader.Nemucod	18.5 %
3	JS/ProxyChanger	3,9 %
4	Java/Adwind	3,2 %
5	VBA/TrojanDownloader.Agent.CJQ	2,9 %
6	JS/TrojanDownloader.Iframe	2,7 %
7	VBA/TrojanDownloader.Agent.CIY	2,6 %
8	JS/Kryptik.RE	2,3 %
9	JS/Danger.DoubleExtension	2,2 %
10	Win32/Adware.ELEX	1,9 %

Zdroj[51]

Pro pochopení škodlivosti je zde charakteristika dvou vybraných virů, které zaujímají celkově 38,6 % napadených počítačů. Jedná se o údaj z ledna 2017 na území České republiky.

- **JS/Danger.ScriptAttachment**
  Jedná se o vyděračské viry z typu ransomware, který zašifruje obsah počítače a poté uživateli zobrazí oznámení, že za dešifrování počítače musí zaplatit v Bitcoinech, v opačném případě dojde k nenávratnému smazání dat. Je spousta uživatelů, kterým se i po zaplacení výkupného v anonymní měně, zakódovaná data neobnovila. Virus je nutné

[50] *ESET Virus radar* [online]. [cit. 2017-01-01]. Dostupné z: http://www.virovyradar.cz
[51] *ESET Virus radar* [online]. [cit. 2017-01-01]. Dostupné z: http://www.virovyradar.cz.

z počítače odinstalovat speciálním softwarem a data zálohovat. Zachránit data tímto způsobem se povedlo jen malé části uživatelů.[52]

- **JS/TrojanDownloader.Nemucod**
  Trojan Nemucod je škodlivý software, který se maskuje jako bezpečný soubor. Soubor se šíří pomocí emailové komunikace a často se jeví jako dokument. Tento škodlivý soubor obsahuje Java Script kód, který následně stáhne a aktivuje spustitelný soubor viru Nemucod, který poté běží na pozadí systému, tiše infikuje počítače dalšími viry, včetně červů, trojských koní. Virus JS.Nemucod je také známý jako TrojanDownloader: JS / Nemucod.H. Jakmile získá přístup k počítači oběti, způsobí zmatek v celém systému: zničí důležité soubory, poškodí registr systému Windows, ukradne osobní údaje a také nainstaluje další malware. Údajně virus Nemucod šíří viry typu ransomware, včetně těch nejvíce známých, jako je TeslaCrypt, Crypted a Locky virus. Ransomware je pravděpodobně jedním z nejhorších počítačových virů, který napadá počítač, blokuje k němu přístup nebo šifruje veškerá data na něm uložená. Pak žádá zaplatit výkupné a vydírá oběť, aby tak učinila co nejdříve. [53]

Sofistikované viry

Nejmodernější a sofistikované viry zřejmě vytvářejí vlády, armády a týmy specialistů v dané problematice. Těmto skupinám nejde o dokumenty a hudbu uloženou v počítači, ale sbírají informace a ohrožují kritickou infrastrukturu vybraných zemí. Tyto viry jsou natolik propracované, že je zcela vyloučené, že autory je malá skupina programátorů. Viry se do sítě dostávají pomocí připojení hardwarového zařízení, případně připojením periferních zařízení jako jsou tiskárny, skenery. Například virus Stuxnet byl údajně instalován do sítě jaderné elektrárny pomocí tiskárny a způsobil milionové dolarové škody a zpomalil vývoj atomových zbraní, což byl jeho záměr.

[52] *NOVINKY CZ: Nejrozšířenějším škodlivým kódem v Česku je virus Danger* [online]. [cit. 2017-01-10]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/423462-nejrozsirenejsim-skodlivym-kodem-v-cesku-je-virus-danger.html
[53] *Odstranit virus: JS.Nemucod. Jak ho odstranit?* [online]. [cit. 2017-01-10]. Dostupné z: https://odstranitvirus.cz/js-nemucod/

- **Virus Flame**
  Jedná se o nejsofistikovanější virus, který byl doposud vytvořen. Při aktivaci se promění ve špionážní nástroj, který umí nahrávat video z webové kamery a zvuk z vestavěných mikrofonů. Průběžně vytváří a zaznamenává do souborů printscreen obrazovky, loguje síťový provoz, ukládá výstup z klávesnice. Virus skrytě pomocí Bluetooth rozhraní komunikuje s okolími zařízeními jako jsou tablety, mobilní telefony a zkouší stáhnou požadované informace. Všechny nelegálně získané informace zašifruje a odešle na řídící server a poté čeká na další pokyny. Jedná z hypotéz je, že virus byl vytvořen CIA, NSA nebo izraelskou armádou. Není totiž zvláštností, že nejvíce nakažených počítačů se nachází v zemích středního východu.[54]
- **Červ Stuxnet**
  Jedná se o první červ pro průmyslové systémy SCADA[55], který dokázal napadnout, přeprogramovat řídící jednotky a zamést za sebou stopy. Cílem byla elektrická distribuční síť, dopravní infrastruktura a další klíčové prvky. Největší škoda byla způsobena na jaderné elektrárně Búšehr v Iránu a v jaderném závodu na obohacování uranu v Natzanu, kde nenávratně poškodil centrifugy a vyrobené uranové produkty. Experti zabývající se detekcí viru se shodují, že Stuxnet vytvořil tým profesionálních programátorů.[56]

Denně vznikají nové a dokonalejší viry, které zůstávají neodhalené a jejích cílem jsou konkrétní instituce, společnosti. Někdy se může jednat o pouze jediného cíleného adresáta, kdy virus nedetekují žádné ochranné systémy a odhalení je minimální, neboť je určen jedinému příjemci. Zde nepomůžou antivirové systémy.

3.8 KYBERNETICKÁ VÁLKA

V současnosti stoupá ve světe napětí v podobě politických změn, ekonomických krizí, nově vzniklých ohnisek válek a konfliktů. Tyto konflikty se neodehrávají pouze v reálném světě, ale i

[54] *TECHNET CZ: 15+1 NEJ virů světa: mažou disky, kradou hesla a ohrožují elektrárny* [online]. [cit. 2017-01-10]. Dostupné z: http://technet.idnes.cz/15-nej-viru-sveta-0ja-/software.aspx?c=A120716_110329_software_nyv.

[55] SCADA je zkratka pro dispečerské řízení a sběr dat. Pojem užívaný v souvislosti pro software, který z centrálního pracoviště monitoruje průmyslová a jiná technická zařízení a procesy a umožňuje jejich ovládání.

[56] *TECHNET CZ: 15+1 NEJ virů světa: mažou disky, kradou hesla a ohrožují elektrárny* [online]. [cit. 2017-01-10]. Dostupné z: http://technet.idnes.cz/15-nej-viru-sveta-0ja-/software.aspx?c=A120716_110329_software_nyv.

v tom nehmatatelném, virtuálním. Dnešní svět je natolik propojen, že představa, že celosvětová sít zkolabuje, je stejně katastrofický scénář, jako žít bez elektrické energie.

Způsobů, jakým pachatelé vnikají pomocí škodlivých programů do systému, je nespočet, stejná je různorodost účelu těchto útoků. Jsou skupiny programátorů, kterým jde hlavně co nejrychleji a anonymně vydělat peníze, kdy se jedná převážně o tvůrce viru typu ramsorware. Tito pachatelé si uvědomují cenu dat a za vaše zakódované data si nechají zaplatit. Představa, že tento druh viru napadne intranetovou sít užívanou Ministerstvem vnitra, kde se bude skrytě šířit a následně zakóduje datová centra, je noční můrou všech administrátorů sítě. I přesto, že počítačové stanice jsou vybaveny antiviry a probíhá zde pravidelná aktualizace, je nutné vir detekovat z databáze viru. Ale co když tento vir je cíleně naprogramován na konkrétní systém s konkrétním cílem?

Viry jsou tvořeny nadšenci, ale také profesionálně vedenými týmy. V současné době probíhá mezí velmocí USA a Ruskou federací konflikt v oblasti cílených kybernetických útoků při ovlivňování politiky v zemi. Koncem roku 2016 došlo k útokům hackerů na server americké Demokratické strany, z kterého byly odcizeny citlivé data. Také USA obviňují protistranu, že pomocí počítačů a cílených úkorů ovlivňovala výsledky voleb v USA. Ruská federace toto tvrzení samozřejmě popírá a odmítá. Možná je to jen nesmíření se s prohrou ve volbách, ale co když opravdu výsledek voleb rozhodl útok hackerů?

V České republice se v lednu 2017 podařilo neznámým pachatelům získat přístup k e-mailovýcm systémům ministerstva zahraničních věcí. Experti na kybernetickou bezpečnost označili prolomení e-mailových účtů ministerstva za mimořádný bezpečnostní incident. Informace naznačují, že útok byl vedený ze zahraničí a že nese shodné znaky jako útoky hackerů na e-mailové účty americké Demokratické strany před tamními loňskými prezidentskými volbami. Šetřením se nyní podařilo zjistit, že podobnost tkví v IP adresách, ze kterých hackeři útočili.[57]

Rovněž počítačová síť Ministerstva vnitra se může napříště stát cíleným místem útoků hackerů. Následky můžou mít nevyčíslitelnou hodnotu a hlavně velký vliv na bezpečnost v zemi. Z uvedeného důvodu je nutné dodržovat stanovené bezpečnostní předpisy a nepodceňovat, že antivirové programy vše odhalí. Hackeři jsou vždy krok před námi a ohrožují náš reálný svět.

[57] Hackeři při útoku na Černínský palác stáhli přes sedm tisíc záznamů. *Novinky.cz* [online]. [cit. 2017-02-01]. Dostupné z: https://www.novinky.cz/domaci/428172-hackeri-pri-utoku-na-cerninsky-palac-stahli-pres-sedm-tisic-zaznamu.html.

4 EMPIRICKÝ PRŮZKUM

Empirickou část bakalářské práce tvoří kvalitativní výzkum provedený formou dotazníkového šetření. Dotazníkového šetření se celkově účastnilo 45 policistů České republiky z územního odboru Opava.

4.1 PRŮBĚH VÝZKUMU

Dotazník byl sestaven konkrétními otázkami ke shromáždění dat, které jsem chtěl od dotazovaných osob získat k následnému vyhodnocení. Dotazník byl po dohodě s vedoucím obvodního oddělení Policie České republiky v Kravařích konzultován a v tištěné podobě předán policistům územního odboru Opava k vyplnění. Jednalo se o dotazník, který byl anonymní a rovněž dobrovolný. Celkově jsem distribuoval 90 dotazníků a obdržel jsem 45 vyplněných dotazníků zpět k vyhodnocení.

4.1.1 STRUKTURA DOTAZNÍKU

Dotazník obsahuje 16 otázek zaměřených na problematiku v oblasti výpočetní techniky. Všechny otázky jsou uzavřené, neboť se jedná o jednodušší formu odpovědí a respondent pouze volí z daných možností. Dotazník je součásti přílohy č. 1.

4.1.2 CÍLE VÝZKUMU

Cílem výzkumné části bakalářské práce je zmapování problematiky bezpečné manipulace s výpočetní technikou ze strany uživatelů, která je součásti struktury sítě Ministerstva vnitra.

Na základě kvalitativní analýzy je nutné odhalit, jaký mají respondenti k dané problematice přístup a zda dodržují stanovené bezpečnostní zásady, kterými jsou vázáni. K této analýze bylo využito výzkumné metody formou dotazníku, který má za cíl zjistit případné nedostatky v oblasti bezpečnosti. Provedenou analýzou jsem chtěl nejen zjistit nedostatky, ale poté i nalézt vhodné řešení pro snížení rizik úniku informací a zvýšení bezpečnosti na pracovišti.

4.2 HYPOTÉZY

Výzkumná část bakalářské práce se skládá z hypotéz.

„ Hypotéza není jakýkoliv předpoklad, hledání, střílení do prázdna. Musí důsledně vycházet z poznatků, které jsou o zkoumaném jevu známý, nebo z praktických zkušenosti výzkumníka.“[58]

Seznam jednotlivých hypotéz:

Hypotéza č. 1: Lze předpokládat, že 85 % policistů dodržují základní bezpečnostní zásady, které jsou stanovené interními akty řízení.

Domnívám se, že vzhledem k pravidelným školením a všeobecného povědomí o bezpečnosti škodlivých aplikací a možných útoků, policisté dodržují bezpečnostní opatření při práci na služebním PC.

Hypotéza č. 2: Lze předpokládat, že 90 % policistů své osobní přihlašovací údaje do informačních systémů nikdy nesdělují dalším osobám.

Přihlašovací uživatelské jméno a heslo jsou klíčové údaje, které není možné sdělovat, nikde zapisovat, a proto se domnívám, že tuto základní zásadu dodržují všichni uživatelé.

Hypotéza č. 3: Lze předpokládat, že 80 % policistů je seznámen s postupem, jak reagovat na nestandardní chování PC a mají povědomí o možných hrozbách.

V současné době již každý policista vlastní osobní počítač doma a nestandardní chování je schopen rozlišit. V případě zjištění, že počítač začne vykazovat nestandardní chování, jistě bude vědět, že je potřeba kontaktovat administrátory sítě při územním odboru Policie České republiky.

Hypotéza č. 4: Lze předpokládat, že 80% policistů vědí, že je nepřípustné instalovat neznámé aplikace do služebních počítačů a v případě dodaných souborů je nutné provést antivirovou kontrolu médií, na kterém je soubor nahrán.

Každý policista je opakovaně seznámen, že instalovat aplikace na služební počítač není povoleno. Každý služební počítač je vybaven antivirovým programem, který policisté využívají.

[58] GAVORA, Petr. *Úvod do pedagogického výzkumu*. 2., rozš. české vyd. Brno: Paido, 2010, s. 50. ISBN 978-80-7315-185-0.

4.3 DOTAZNÍKOVÉ ŠETŘENÍ

Dotazníkové šetření je následně rozpracováno do grafického zobrazení.

Otázka číslo 1, 2 : Pohlaví a věk respondentů.

Tabulka 4: Pohlaví a věk

		Počet respondentů	podíl
Pohlaví	muž	40	89 %
	žena	5	11 %
Věk	do 20 let	0	0 %
	21-30 let	20	44 %
	31-40 let	19	43 %
	41let a více	6	13 %

Zdroj[59]

Otázka číslo 3: Jak dlouho pracujete (počet let) u Policie České republiky.

Cílem statistického dotazu bylo zjistit počet odsloužených let u respondentů. Z celkových 45 odpovědi byla zjištěna průměrná hodnota 8 odsloužených let u Policie České republiky. Z výsledku vyplývá, že respondenti jsou již zapracovaní policisté se zkušenostmi.

Tabulka 5: Počet let v pracovního poměru u PČR

		počet	podíl
Počet let	1-3	4	9 %
	3-6	8	18 %
	6-10	20	45 %
	10-15	6	13 %
	15-20	5	11 %
	Více než 20	2	4 %

Zdroj[60]

Otázka číslo 4 : Kolik hodin v průměru pracujete na služebním PC během jednoho pracovního dne?

Tímto dotazem jsem chtěl zjistit, kolik času v průměru pracuje policista na služebním počítači během jednoho pracovního dne.

[59] Autor práce, 2017 (vlastní šetření)
[60] Autor práce, 2017 (vlastní šetření)

Tabulka 6: Průměrný počet hodin práce na služebním PC během dne

		Počet odpovědí	podíl
Počet hodin/den	1	1	2%
	2	8	18 %
	3	8	18 %
	4	7	16 %
	5	5	11 %
	6	8	18 %
	7	4	9 %
	8	3	7 %
	9	1	2 %

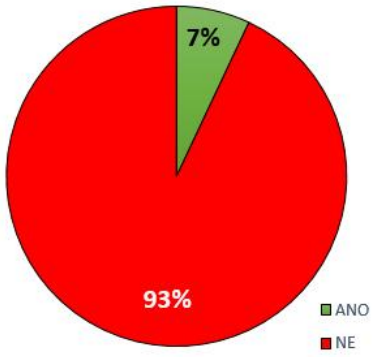
Zdroj[61]

Provedeným šetřením bylo zjištěno, že průměrná doba práce na počítači je mezi respondenty 4,5 hodiny, což představuje celkově 37% pracovní doby v případě 12. hodinové směny.

Otázka číslo 5 : Necháváte Vaše pracovní PC bez dohledu, pokud jste přihlášeni svým přihlašovacím jménem a heslem?

Otázka byla položena s cílem zjistit, zda uživatelé dodržují zásadu takzvaného "prázdného stolu", tj. zda při vzdálení se od pracovního počítače se odhlásí, případně uzamknou počítač. Tato povinnost je uvedená v závazný pokyn policejního prezidenta č. 80/2005 ze dne 9. srpna 2005, kterým se upravuje využívání datové sítě Intranet Ministerstva vnitra. Otázka ověřuje hypotézu č. 1, 2.

Graf 2: Necháváte Vaše pracovní PC bez dohledu, pokud jste přihlášeni svým přihlašovacím jménem a heslem?



Zdroj[62]

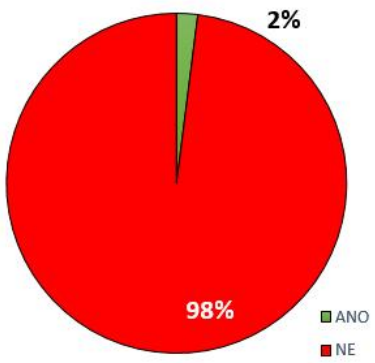
[61] Autor práce, 2017 (vlastní šetření)
[62] Autor práce, 2017 (vlastní šetření)

Na předmětnou otázku odpovědělo **42** (93 %) dotázaných, že při odchodu od služebního PC počítač uzamknou. Pouze **3** respondenti (7 %) uvedli, že tuto zásadu nedodržují a počítač nechávají bez dohledu.

Otázka číslo č. 6: Předal/a jste vaše přihlašovací údaje k informačním systému jiné osobě?

Cílem dotazu bylo zjistit, zda dochází k předání přihlašovacích údajů jiným osobám, čímž dochází k nerespektování Nařízení Ministerstva vnitra č. 21/2004, kterým se stanoví pravidla a způsob zabezpečování kontroly užívání počítačových programů v působnosti Ministerstva vnitra. Otázka ověřuje hypotézu č. 2.

Graf 3: Předal/a jste vaše přihlašovací údaje k informačnímu systému jiné osobě?



Zdroj[63]

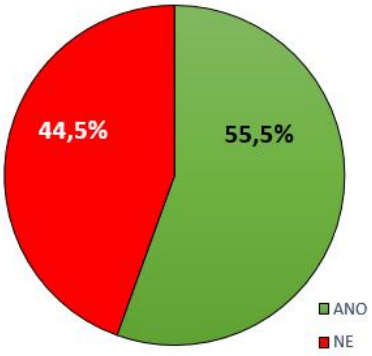
Na výše uvedený dotaz odpovědělo **44** (97,7 %) dotázaných, že přihlašovací údaje k informačním systémům nepředalo cizím osobám. Pouze jeden respondent uvedl, že ano, což představuje pouhá 2 % z dotázaných osob.

Otázka číslo 7: Znáte softwarové a hardwarové vybavení své pracovní stanice?

Dotaz směřoval na respondenty, zda jsou seznámení s vybavením své pracovní stanice jak po stránce hardwarové, tak také programového vybavení. Tento dotaz nemá zásadní vliv na bezpečnost, ale poukazuje na povědomí a schopnost pracovat s výpočetní technikou a orientaci v oblasti výpočetní techniky. Otázka ověřuje hypotézu č. 3.

[63] Autor práce, 2017 (vlastní šetření)

Graf 4: Znáte softwarové a hardwarové vybavení své pracovní stanice?



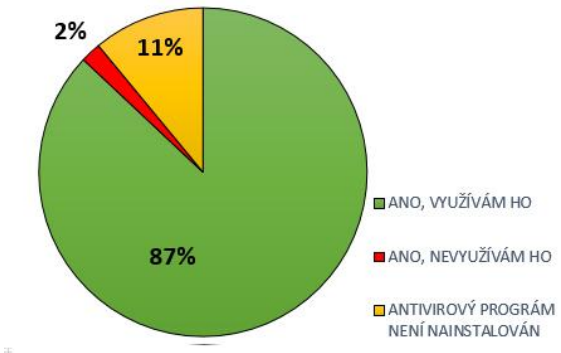
Zdroj[64]

Celkově odpovědělo 25 (55,5 %) dotázaných, že znají hardwarové a softwarové vybavení své pracovní stanice. 20 dotázaných (44,5 %) osob uvedlo, že neznají softwarové a hardwarové vybavení své pracovní stanice.

Otázka číslo 8: Je instalován ve služebním PC antivirový program?

Každá počítačová sestava je vybavena aktuálním antivirovým programem. Cílem bylo zjistit, zda tento antivirový program respondenti užívají a vědí o přítomnosti softwaru. Otázka ověřuje hypotézu č. 4.

Graf 5: Je instalován ve služebním PC antivirový program?



Zdroj[65]

[64] Autor práce, 2017 (vlastní šetření)
[65] Autor práce, 2017 (vlastní šetření)

Z oslovených policistů 39 (87 %) osob o přítomnosti antivirového programu ví a využívá ho. Jedna osoba (2%) o existenci antiviru ví, ale program nevyužívá a 5 osob se domnívá, že antivirový program není nainstalován.

Otázka číslo 9: S jakou formou narušení bezpečnosti jste se setkal na vašem služebním PC?

Otázka byla položena za účelem zjištění, zda se respondent již setkal s formou narušení bezpečnosti a zda jí dovede pojmenovat, případně se doposud s narušením bezpečnosti nesetkal. Otázka ověřuje hypotézu č. 3.

Tabulka 7: Forma narušení bezpečnosti, se kterou se setkal respondent

		Počet	Podíl
Detekována forma narušení	Doposud se nesetkal	40	89 %
	Malware	1	2 %
	Spyware	0	0 %
	Phishing	0	0 %
	Viry	2	4 %
	Hacking	0	0 %
	Nedokáži odpovědět, krom virů neví, co výše uvedené pojmy znamenají	2	4 %

Zdroj[66]

Provedeným dotazníkovým šetřením bylo zjištěno, že 40 (89 %) dotázaných odpovědělo, že se doposud na služebním PC nesetkalo s formou narušení bezpečnosti. Dva policisté (4 %) uvedli, že již zaznamenali počítačový vir a jeden respondent (2 %) zaznamenal Malware. Dva respondenti (2 %) nedokáží na otázku odpovědět z důvodu, že neznají výše uvedené pojmy.

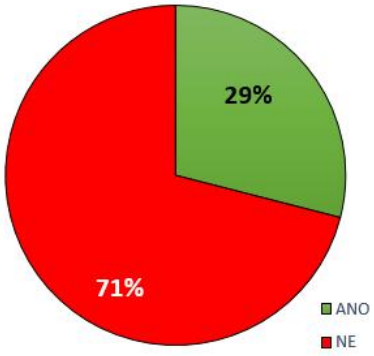
Otázka číslo 10: Instalujete nebo spouštíte na služební pracovním PC vlastní software? (např. dodaný videopřehrávač s videem z bezpečnostních kamer apod.)

Tímto dotazem jsem chtěl zjistit, zda dochází k instalaci neautorizovaného softwaru a tudíž se jedná o vážnou hrozbu v oblasti bezpečnosti sítě. Velmi často dodaný videozáznam z bezpečnostních kamer vyžaduje spuštění své aplikace, která podporuje daný videosoubor.

[66] Autor práce, 2017 (vlastní šetření)

Nikdy nelze vyloučit, že dodaný přehrávač neobsahuje škodlivý kód. Otázka ověřuje hypotézu č. 4.

Graf 6: Instalujete nebo spouštíte na služební pracovním PC vlastní software?



Zdroj[67]

Na otázku č. 10 odpovědělo 13 (29 %) dotázaných, že neznámý software již na služební PC instalovalo a 32 (71 %) dotázaných uvedlo, že nikoliv.

Otázka číslo 11: Pokud se setkáte s nevyžádanou poštou na služebním PC, jak se zachováte?

Nevyžádaná pošta, takzvaný spam, neobtěžuje pouze běžné majitele e-mailových schránek, ale také služební počítače. Cílem bylo zjistit, zda vědí policisté jak reagovat na nevyžádanou poštou. Otázka ověřuje hypotézu č. 3.

Tabulka 8: Reakce na nevyžádanou poštu

		počet	podíl
Reakce na nevyžádanou elektronickou poštu	Email ihned odstraní	12	27 %
	Email označí jako nevyžádaná pošta a neotevře	33	73 %
	Přečte obsah, včetně příloh	0	0 %

Zdroj[68]

[67] Autor práce, 2017 (vlastní šetření)
[68] Autor práce, 2017 (vlastní šetření)

Na nevyžádanou poštu v dotazníku uvedlo 33 osob (73%), že e-mail označí jako spam a obsah a přílohy neotevře. Zbývajících 12 dotazovaných (27%) uvedlo, že email ihned odstraní. Žádný z respondentů obsah nevyžádané pošty nečte a neotvírá přílohy.

Otázka číslo 12: Otevíráte přílohy, které jsou součásti přílohy v e-mailu?

Častým zdrojem infiltrace počítače jsou příchozí soubory, které jsou součásti přílohy v e-mailové zprávě. Cílem dotazu bylo zjistit, jak policisté reagují, pokud obdrží e-mailovou zprávu s přílohou. Otázka ověřuje hypotézu č. 1.

Tabulka 9: Otevření přílohy v e-mailu

		počet	podíl
Otevření přílohy v e-mailu	Přílohy před otevřením zkontroluji antivirovým programem	44	98 %
	Přílohu otevře bez antivirové kontroly	0	0 %
	Přílohu neotvírám	1	2 %
	E-mail s přílohou ihned smažu	0	0 %

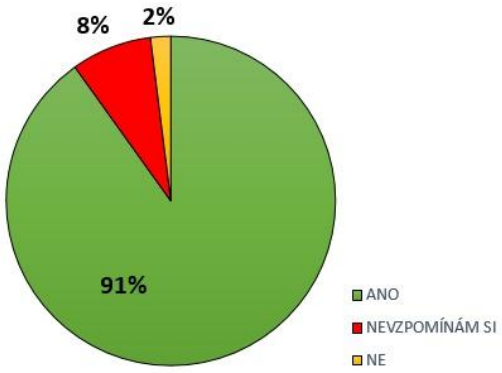
Zdroj[69]

Přílohy před otevřením kontroluje antivirovou ochranou 44 osob, což představuje 98% podíl. Pouze jeden respondent uvedl, že neotvírá přílohy, které jsou součásti e-mailu, což představuje podíl 2 %.

Otázka číslo 13: Byl/a jste seznámen/a s bezpečnostními pravidly používání pracovního počítače dle nařízení Ministerstva vnitra č. 21/2004 a ZPPP č. 80/2005?

Dotazem jsem chtěl zjistit, zda jsou policisté seznámení s interními akty řízení a s pravidly bezpečné manipulace s výpočetní technikou. Otázka ověřuje hypotézu č. 1, 2.

Graf 7: Seznámení s bezpečnostními pravidly používání pracovního počítače?



Zdroj[70]

[69] Autor práce, 2017 (vlastní šetření)
[70] Autor práce, 2017 (vlastní šetření)

Z celkového počtu 45 osob odpovědělo 40, že jsou seznámení s interními pravidly, což představuje 91 % respondentů a 4 osoby, což představuje 27 %, si nevzpomíná, zda byli seznámeni. Jedena osoba odpověděla, že nebyla seznámena, což představují podíl 2 % z celkového počtu dotázaných osob.

Otázka číslo 14: Jak se zachováte a budete reagovat při nestandardním chování PC?

V případě nestandardního chodu počítače je potřeba správně reagovat. Tímto dotazem jsem chtěl zjistit, zda jsou respondenti schopni reagovat, když zjistí, že se PC chová nestandardně. Otázka ověřuje hypotézu č. 3.

Tabulka 10: Reakce na nestandardní chování PC

		počet	podíl
Reakce na nestandardní chování PC	Událost oznámí dozorčí službě	6	13 %
	Informuje administrátora lokální sítě	39	87 %
	Pokusí se sám závadu odstranit	0	0 %

Zdroj[71]

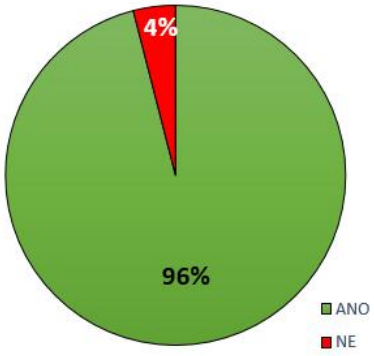
Celkově 39 respondentů odpovědělo, že v případě nestandardního chování PC budou informovat administrátora sítě, což je 87 % podíl. Událost oznámí 6 (13 %) osob dozorčí službě. Žádný z dotazovaných by se nepokusil odstranit závadu sám.

Otázka číslo č. 15 : Provádíte kontrolu antivirovým programem při vložení USB disku, CD?

Dotazem jsem chtěl zjistit, zda provádí respondent kontrolu antivirovým programem při vložení USB disku nebo CD. Otázka ověřuje hypotézu č. 4.

[71] Autor práce, 2017 (vlastní šetření)

Graf 8: Provádíte kontrolu antivirovým programem při vložení USB disku, CD?



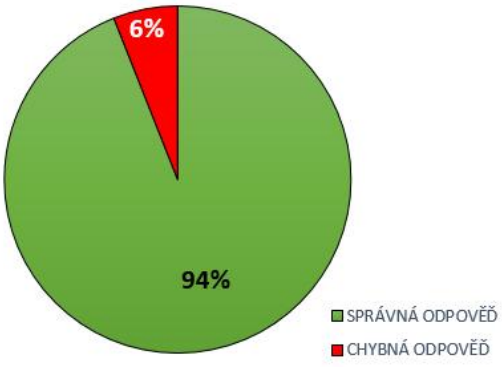
Zdroj[72]

Z celkového počtu 43 (96 %) dotázaných odpovědělo, že antivirus užívají a pouze 2 (4%) uživatelé antivirus nepoužívají.

Otázka číslo 16 : Počítačová síť Ministerstva vnitra je součásti kritické komunikační infrastrukturu České republiky. Co tento pojem znamená?

Poslední otázka je vědomostí s cílem zjistit, zda respondenti znají pojem kritická komunikační infrastruktura. Respondenti mají na výběr ze třech možných odpovědí, kde je pouze jedna správná varianta.

Graf 9: Znalost pojmu kritická komunikační infrastruktura



Zdroj[73]

Na tento poslední dotaz odpovědělo 43 osob (94 %) správně. Chybně odpověděli 3 respondenti, což je 6 % podíl z celkového počtu.

[72] Autor práce, 2017 (vlastní šetření)
[73] Autor práce, 2017 (vlastní šetření)

4.4 SHRNUTÍ DOTAZNÍKOVÉHO ŠETŘENÍ

Cílem bakalářské práce bylo provést a vyhodnotit empirické šetření pro počítačové oblasti bezpečnosti a navrhnout výhodná doporučení pro jejich prevenci. Vyhodnocením výsledků dotazníkového šetření vyplynulo, že policisté mají o bezpečnostních systémech PČR dobrý přehled a dodržují stanovené zásady. Cílem výzkumu bylo potvrdit nebo vyvrátit vytvořené hypotézy, které jsou níže uvedené. V rámci výzkumu byly stanoveny 4 hypotézy, které se potvrdily.

4.5 VERIFIKACE HYPOTÉZ

Hypotéza číslo 1: Lze předpokládat, že 85 % policistů dodržují základní bezpečnostní zásady, které jsou stanovené interními akty řízení.

Z celkového počtu 45 oslovených respondentů odpovědělo 40 osob, což představuje 91 % respondentů, že jsou seznámení s bezpečnostními pravidly používání pracovního počítače dle Nařízení Ministerstva vnitra č. 21/2004, kterým se stanoví pravidla a způsob zabezpečování kontroly užívání počítačových programů v působnosti Ministerstva vnitra a jsou seznámeny se Závazný pokynem policejního prezidenta číslo 80 ze dne 9. srpna 2005 o využívání datové sítě Intranet Ministerstva vnitra Hermes. Z provedeného dotazníkového šetření vyplývá, že 42 osob (93 %) při odchodu od služebního PC počítač uzamknou a 39 (87%) respondentů odpovědělo, že v případě nestandardního chování PC budou informovat administrátora sítě, což je standardní postup v případě zjištění ohrožení PC. V příchozí poště přílohy před otevřením kontroluje 44 osob, což představuje 98% podíl. Antivirový program užívá celkově 43 osob, což představuje 96 % podíl. Hypotéza č. 1. byla potvrzena.

Hypotéza číslo 2: Lze předpokládat, že 90 % policistů své osobní přihlašovací údaje do informačních systémů nikdy nesdělují dalším osobám.

Tato hypotéza se potvrdila, neboť 44 (97,7 %) dotázaných přihlašovací údaje k informačním systémům nepředalo cizím osobám a pouze jeden respondent uvedl, že ano, což představuje pouhá 2 % z dotázaných osob. Šetřením bylo dále zjištěno, že 42 (93 %) dotázaných uvedlo, že při odchodu od služebního PC počítač softwarově uzamknou a znemožní tímto přístup do informačních systémů neoprávněným osobám. Pouze 3 respondenti (7 %) uvedli, že tuto zásadu nedodržují.

Hypotéza číslo 3: Lze předpokládat, že 85 % policistů jsou seznámeni s postupem, jak reagovat na nestandardní chování PC a mají povědomí o možných hrozbách.

Z oslovených policistů 39 odpovědělo, že v případě nestandardního chování PC budou informovat administrátora sítě, což je 87 % podíl. Událost oznámí 6 (13 %) osob dozorčí službě, což nepředstavuje správný postup. Žádný z dotazovaných by se nepokusil odstranit závadu sám.

Celkově 40 osob potvrdilo, což představuje podíl 91 % respondentů, že jsou seznámení s bezpečnostními pravidly dle Nařízení Ministerstva vnitra č. 21/2004, kterým se stanoví pravidla a způsob zabezpečování kontroly užívání počítačových programů v působnosti Ministerstva vnitra a Závazným pokynem policejního prezidenta číslo 80 o využívání datové sítě Intranet Ministerstva vnitra Hermes.

Na nevyžádanou elektronickou poštu v dotazníku uvedlo 33 osob (73%), že e-mail následně označí jako spam a obsah a přílohy neotevřou. Zbývajících 12 dotazovaných (27%) uvedlo, že email ihned odstraní. Uvedené varianty jsou u nevyžádané pošty přípustné. Déle bylo dotazníkem zjištěno, že 40 (89 %) osob se doposud na služebním PC nesetkalo s formou narušení bezpečnosti. Dva policisté (4 %) uvedli, že již zaznamenali počítačový vir a jeden respondent (2 %) zaznamenal Malware. Tato hypotéza se rovněž potvrdila.

Hypotéza číslo 4: Lze předpokládat, že 85% policistů vědí, že je nepřípustné instalovat neznámé aplikace do služebních počítačů a v případě dodaných souborů je nutné provést antivirovou kontrolu médií, na kterém je soubor nahrán.

Z oslovených policistů 39 (87 %) osob o přítomnosti antivirového programu ví a antivir využívá. Jedna osoba (2%) o existenci antiviru ví, ale program nevyužívá a 5 osob se domnívá, že antivirový program není na každém služebním PC nainstalován.

Na otázku, zda instalují nebo spouštějí na služební pracovním PC respondenti vlastní software dodaný například s videosouborem z bezpečnostních kamer, odpovědělo celkově 13 (29 %) dotázaných, že neznámý software již na služební PC instalovalo a 32 (71 %) dotázaných osob uvedlo, že nikoliv.

Antivirusový program celkově využívá 43 (96 %) dotázaných. Pouze 2 osoby (4%) antivirus nepoužívají. Při práci s elektronickou poštou přílohy před otevřením kontroluje antivirovou ochranou 44 osob, což představuje 98% podíl. Pouze jeden respondent uvedl, že neotvírá přílohy, které jsou součásti e-mailu, což představuje podíl 2 %.

Uvedené hypotéza se potvrdila částečně, neboť pouze 32 (71 %) respondentů neinstaluje neznámý software na služební PC. Instalace neznámých aplikací představuje značné riziko pro celou počítačovou síť.

4.6 DOPORUČENÍ

Z výše uvedeného průzkumu vyplynulo, že jsou dodržovány interní předpisy a respondenti vědí, jak reagovat. Vzhledem k pravidelným školením dochází k dobré informovanosti a připravenosti na možné ohrožení. Důležitou roli mají administrátoři sítí, kteří dohlížení na bezchybný provoz celého složitého systému. Je potřeba si uvědomit, že bezpečnost je na každém jedinci, a stejně jako virus v lidském těle, se může namnožit a napáchat značné škody. Velká pozornost se musí zaměřit také na samotné zacházení s daty a se zálohou. Nemusí to být zrovna virus, který smaže důležité informace. Může se jednat o nezkušeného pracovníka, který nahraje soubory na pevný disk a nedopatřením je smaže. Během praxe u policie jsem se často setkal s tímto problémem. Obzvláště u policie je nutné k práci přistupovat zodpovědně, protože fotografie, videonahrávky ze zákroků jsou někdy jediným důkazem, jak prokázat pachateli jeho trestnou činnost.

Je důležité i nadále pokračovat v trendu školení policistů a dodržovat stanové bezpečnostní předpisy. Upozornit na nejnovější hrozby v oblasti šíření malware se zdůrazněním, že počítačová síť Ministerstva vnitra patří mezi kritickou infrastrukturu v České republice, což si někteří policisté neuvědomují. Je velká škoda, že i před důslednou bezpečnostní politiku ze strany správců, dochází občas k chybám, kdy jsou spouštěny neznámé aplikace nejrůznějších videopřehrávačů dodaných společně s videosouborem z kamerového systému. Na toto nebezpečí je potřeba upozornit a je potřeba instalovat vhodný software ze strany správců sítě, kteří již daný program dostatečně prověří, případně navrhnou jiné řešení. Také je nutné upozornit na přítomnost antivirového programu v počítači a zopakovat základní bezpečnostní zásady.

ZÁVĚR

Počítačová síť ministerstva vnitra je neustále monitorována a dokumenty interního charakteru nelze zveřejňovat. I já jsem se během příprav na bakalářskou práci setkal, z mého pohledu, se zajímavými informacemi, které ovšem není možné zveřejnit. V podstatě jde o bezpečnostní politiku zabezpečení sítě o takzvané know-how bezpečnostních odborů, kteří dohlížejí na funkčnost celého systému. V průběhu práce jsem se pokoušel získat informace, zda došlo k napadení intranetové sítě Ministerstva vnitra, případně, zda došlo k infiltraci malware do služebních počítačů. Tyto informace se mi nepodařilo zjistit z důvodu, že neexistují statistiky, které jsou veřejně přístupné a přístup k těmto informacím má omezený počet osob. Z uvedeného důvodu jsem zveřejnil výčet aktuálních virů, které ohrožují současné počítače a šíří se Internetem.

V teoretické části charakterizuji základní pojmy z Výkladového slovníku vydaného Policejním prezídiem a uvádím legislativní předpisy v oblasti kyberbezpečnosti. Na tuto kapitolu navazují informace o intranetové síti Hermes, kterou provozuje ministerstvo vnitra a povinnosti zaměstnanců a administrátorů, kteří síť využívají. Velká pozornost je v práci věnovaná heslům, které tvoří základ bezpečnosti.

Následující kapitola pojednává o ochraně osobních údajů a způsobu zpracování dat u Policie České republiky. Zde je výchozím legislativním dokumentem zákon č. 101/2000 Sb., ze dne 4. dubna 2000, o ochraně osobních údajů a zákon č. 273/2008 Sb., ze dne 17. července 2008, o Polici České republiky. V této kapitole popisuji 4 vybrané informační systémy, které jsou nejvíce užívané a kde se často zpracovávají osobní údaje, které je nutné ochraňovat.

Práce popisuje bezpečností hrozby, které jsou rozdělené na vnější a vnitřní. Zde jsou definované problémy, které mohou nastat a jakým způsobem se preventivně bránit. Další část je zaměřená na infiltraci a způsob, jakým hackeři získávají citlivé informace, přihlašovací údaje. Ne vždy je antivirus účinný, obzvlášť pokud se jedná o sofistikovaný vir. V závěru teoretické části se nachází výčet aktuálních virů, které ohrožují Českou republiku a jaké následky způsobují. V současnosti dochází k opakovaným útokům na významné servery vládních organizací a ministerstev v České republice. Napětí je v oblasti kyberbezpečnosti na vysokém stupni, obzvláště po nedávné volbě prezidenta ve Spojených státech amerických. Jednotlivé velmoci pracují v týmech a vytvoří aplikace, které mají za cíl získat citlivé data od nepřítele.

V praktické části jsem provedl kvalitativní analýzy formou dotazníku, kdy jsem respondentům z řad policistů položil 16 dotazů z oblasti výpočetní techniky. Z provedeného průzkumu jsem zjistil, že respondenti dodržují bezpečnostní zásady až na výjimky, kdy se jednalo

o jednotlivce. Bohužel i tito jednotlivci představují bezpečnostní riziko pro celý systém. Z uvedeného důvodu je jedna z možností, provést opětovné proškolení s cílem upozornit na bezpečnostní hrozby a zopakovat bezpečnostní zásady při práci s výpočetní technikou. V praktické části se při verifikaci potvrdily hypotézy, které jsem definoval. Celkově jsem dotazníkem oslovil 90 osob, zpět jsem obdržel 45 vyplněných dotazníků, které vyplnili policisté územního odboru Opava. Vyplněné dotazníky posloužily k analýze, která je součást mé bakalářské práce.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. s. 190. ISBN 80-251-0106-1.

GAVORA, Petr. *Úvod do pedagogického výzkumu*. 2., rozš. české vyd. Brno: Paido, 2010. s. 261. ISBN 978-80-7315-185-0.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012. s. 224. ISBN 97880-7387-545-9.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. s. 97. ISBN 978-80-7251-436-6.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007. s. 284. ISBN 978-80-2471561-2.

KOPECKÝ, Kamil; KREJČÍ Veronika. *Rizika virtuální komunikace.* Olomouc: Net University, 2010. s. 34. ISBN 978-80-254-7866.

KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. První vydání. Praha: Grada Publishing, 2016. s. 176. ISBN 978-80-247-5595-3.

KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada, 2015. s. 184. ISBN 978-80-247-5453-6.

NÁDBĚLA, Josef. *Velký počítačový slovník.* Vyd. 1. Kralice na Hané: Computer Media, 2004. s. 455. ISBN 80-86686-21-3.

PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny.* Vyd. 1. Liberec: Dialog, 2014. s. 248. ISBN 978-80-7424-066-9.

ZEMÁNEK, Jakub. *Slabá místa Windows, aneb, Jak se bránit hackerům.* Vyd. 1. Kralice na Hané: Computer Media, 2004. Vzdělávání, které baví. s. 156. ISBN 80-8668611-6.

Právní předpisy

Zákon č. 1/1993 Sb., ze dne 16. prosince 1992, Ústava České republiky.

Zákon č. 2/1993 Sb., ze dne 16. prosince 1992, Listina základních práv a svobod.

Zákon č. 40/2009 Sb., ze dne 8. ledna 2009, trestní zákoník.

Zákon č. 101/2000 Sb., ze dne 4. dubna 2000, o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 140/1961 Sb., ze dne 29. listopadu 1961, trestní zákon.

Zákon č. 200/1990 Sb., ze dne 8. ledna 2009, o přestupcích.

Zákon č. 273/2008 Sb., ze dne 17. července 2008, o Polici České republiky.

Zákon č. 361/2003 Sb., ze dne 23. září 2003, o služebním poměru příslušníků PČR.

Zákon č. 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Další zdroje

CHIP : magazín informačních technologií. Praha : Vogel, 1990- . Vychází měsíčně. ISSN 1210-0684.

Nařízení Ministerstva vnitra č. 21/2004, kterým se stanoví pravidla a způsob zabezpečování kontroly užívání počítačových programů v působnosti Ministerstva vnitra.

Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

Závazný policejního prezidenta č. 215 ze dne 31. prosince 2008, kterým se stanoví některé bližší podmínky a postupy pro zpracování osobních údajů.

Závazný pokyn policejního prezidenta číslo 80 ze dne 9. srpna 2005 o využívání datové sítě Intranet Ministerstva vnitra Hermes.

Seznam použitých internetových zdrojů

ESET Virus radar [online]. [cit. 2017-01-01]. Dostupné z: http://www.virovyradar.cz/

Integrované bezpečnostní centrum Moravskoslezského kraje [online]. [cit. 2017-01-01]. Dostupné z: http://www.hzscr.cz/soubor/2015-04-ibc-msk-cz-pdf.aspx

Letem světem Applem [online]. [cit. 2017-01-01]. Dostupné z: https://www.letemsvetemapplem.eu/

Ministerstvo vnitra České republiky [online]. [cit. 2017-01-01]. Dostupné z: http://www.mvcr.cz

Novinky.cz [online]. [cit. 2017-01-01]. Dostupné z: http://www.novinky.cz/

Odstranit virus [online]. [cit. 2017-01-01]. Dostupné z: https://odstranitvirus.cz/

Policie České republiky [online]. [cit. 2017-01-01]. Dostupné z: https://www.policie.cz/

Spy obchod [online]. [cit. 2017-01-01]. Dostupné z: http://www.spyobchod.cz/

Technet.cz [online]. [cit. 2017-01-01]. Dostupné z: http://technet.idnes.cz/

Wikipedie otevřená encyklopedie [online]. [cit. 2017-01-01]. Dostupné z: https://cs.wikipedia.org/

Zákony pro lidi [online]. [cit. 2017-01-01]. Dostupné z: https://www.zakonyprolidi.cz/

SEZNAM ZKRATEK

CERT	Computer Emergency Response Team
ČR	Česká republika
DoS	Denial of service
EKIS	Elektronický informační systém
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICQ	I Seek You
ICT	Information and Communication Technologies
ISVS	Informační systém veřejné zprávy
IBC	Informační bezpečnostní centrum
IT	informační technologie
MSN	Microsoft Network
PČR	Policie České republiky
POP	Post Office Protocol
SCADA	Supervisory Control And Data Acquisition
SIS	Schengenský informační systém
SMTP	Simple Mail Transfer Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
WIFI	Wireless Ethernet Compatibility Aliance
ZPPP	Závazný pokyn policejního prezidenta

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

Seznam obrázků

Seznam tabulek

Seznam grafů

SEZNAM PŘÍLOH

Příloha A – Dotazník

Dobrý den,

jmenuji se Tomáš Nestroj a jsem studentem University Jana Amose Komenského, kde vypracovávám bakalářskou práci na téma Počítačová bezpečnost a ochrana dat u Policie České republiky. Věnujte prosím několik minut svého času k vyplnění následujícího dotazníku. Dotazník je anonymní a obsahuje celkem 16 otázek. Získaná data použiji pro praktickou část své bakalářské práce. Předem moc děkuji za Vaši ochotu.

1) Pohlaví ☐ muž ☐ žena	9) S jakou formou narušení bezpečnosti jste se setkal na vašem služebním PC? ☐ nesetkal ☐ viry ☐ malware ☐ spyware ☐ phishing ☐ hacking ☐ nedokáži odpovědět, krom virů nevím, co výše uvedené pojmy znamenají
2) Věk ☐ do 20 let ☐ 21-30 let ☐ 31-40 let ☐ 41let a více	10) Instalujete nebo spouštíte na služební pracovním PC vlastní software? (např. dodaný videopřehrávač s videem z bezpečnostních kamer apod.) ☐ ano ☐ ne
3) Jak dlouho pracujete (počet let) u Policie České republiky. ☐ 1-3 ☐ 3-6 ☐ 6-10 ☐ 10-15 ☐ 15-20 ☐ více než 20 let	11) Pokud se setkáte s nevyžádanou poštou na služebním PC, jak se zachováte? ☐ email ihned odstraním ☐ email označím jako nevyžádaná pošta a neotevřu ☐ přečtu si obsah, včetně příloh
4) Kolik hodin v průměru pracujete na služebním PC během jednoho pracovního dne? 1 2 3 4 5 6 7 8 9 10 11	12) Otevíráte přílohy, které jsou součásti přílohy v e-mailu? ☐ ano, přílohy zkontroluji antivirovým programem ☐ ano, bez antivirové kontroly otevřu ☐ ne ☐ email s přílohou ihned smažu
5) Necháváte Vaše pracovní PC bez dohledu, pokud jste přihlášeni svým uživatelským jménem a heslem? ☐ ano ☐ ne	13) Byl/a jste seznámen/a s bezpečnostními pravidly používání pracovního počítače dle nařízení Ministerstva vnitra č. 21/2004, Čl. 2 písm. d) a ZPPP č. 80/2005? ☐ ano ☐ ne ☐ již si nevzpomínám
6) Předal/a jste vaše přihlašovací údaje k informačním systému jiné osobě? ☐ ano ☐ ne	14) Jak se zachováte a budete reagovat při nestandardním chování PC ? ☐ událost oznámím dozorčí službě ☐ informovat administrátora lokální sítě ☐ pokusit se závadu odstranit
7) Znáte softwarové a hardwarové vybavení své pracovní stanice? ☐ ano ☐ ne	15) Provádíte kontrolu antivirovým programem při vložení USB disku, CD do služebního počítače? ☐ ano ☐ ne ☐ nepravidelně
8) Je instalován ve služebním PC antivirový program. ☐ ano, využívám ho ☐ ano, nevyužívám ho ☐ antivirový program není nainstalován	16) Počítačová síť Ministerstva vnitra je součásti kritické komunikační infrastrukturu České republiky. Co tento pojem znamená? ☐ Komplex komunikačních systému, služeb nebo sítí, který ochraňuje utajované informace. ☐ Komplex komunikačních systémů, služeb nebo sítí elektronických komunikací, jejichž nefunkčnost by mohla způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. ☐ Komplex komunikačních systémů, služeb nebo sítí elektronických komunikací, které slouží výhradně Ministerstvu vnitra.

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Tomáš Nestroj
Obor: Bezpečnostní studia
Forma studia: kombinovaná
Název práce: Počítačová bezpečnost a ochrana dat u Policie České republiky
Rok: 2017
Počet stran textu bez příloh: 54
Celkový počet stran příloh: 1
Počet titulů českých použitých zdrojů: 20
Počet titulů zahraničních použitých zdrojů: 0
Počet internetových zdrojů: 11
Vedoucí práce: Ing. Michaela Melicharová