VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

BEZPEČNOST DAT VE VEŘEJNÉM SEKTORU

Autor práce: Martin Mužík

Studijní program: Bezpečnostně právní činnost

Forma studia: kombinované

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Martin Mužík

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Bezpečnost dat ve veřejném sektoru

Název bakalářské práce v anglickém jazyce: Data Security in the Public Sector
Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce: březen 2023

Cíl bakalářské práce: Cílem bakalářské práce je na základě dotazníkového šetření mezi zaměstnanci Úřadu práce a Armády České republiky zjistit, jaké je zabezpečení dat ve veřejné správě se zaměřením na jejich jednotlivé informační systémy, úroveň znalostí a proškolení v rámci kybernetické bezpečnosti a navrhnutí případných ochranných opatření.

Student: Martin Mužík	3.4.2023	podpis
Vedoucí práce: RNDr. Růžena Ferebauerová	3.4.2023	podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	23.5.2023	podpis
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	23.5.2023	podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	23.5.2023	podpis

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

MUŽÍK, M. *Bezpečnost dat ve veřejném sektoru: bakalářská práce.* Příbram: Vysoká škola evropských a regionálních studií, 2024. 72 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: data, šifrování, zabezpečení, veřejný sektor, uživatel, hesla

Bakalářská práce se v teoretické části zabývá bezpečnostními opatřeními, nástroji na obranu a bezpečnost počítačových sítí kvůli zabezpečení proti kybernetickým útokům, které jsou popsány na konci teoretické části.

V praktické části se pomocí dotazníkového šetření snaží zjistit, jak jsou na tom respondenti z Úřadu práce v Příbrami a pracovníci štábu 132. dělostřeleckého oddílu v Jincích se znalostmi v kybernetické bezpečnosti.

Na základě výsledků dotazníkového šetření budou doporučeny konkrétní postupy pro správné zabezpečení dat.

ABSTRACT

MUŽÍK, M. *Data security in the public sector: bachelor's thesis*. Příbram: University of European and Regional Studies, 2024. 72 pgs. Bachelor thesis supervisor: RNDr. Růzena Ferebauerová.

Key words: data, encryption, security, public sector, user, passwords

The theoretical part of the bachelor thesis deals with the security measures, tools to defend and secure computer networks against cyber attacks, which are described at the end of the theoretical part.

In the practical part, a questionnaire survey is used to find out how the respondents from the Labour Office in Pribram and the staff of the 132nd Artillery Battalion in Jince are doing with their knowledge in cybersecurity.

Based on the results of the questionnaire survey, specific procedures for proper data security will be recommended.

Obsah

Úvod

V dnešní době digitalizace a stále rostoucí závislosti společnosti na informačních technologiích představuje ochrana dat klíčový prvek v zachování bezpečnosti a stability jak na státní, tak na individuální úrovni. Bezpečnost dat se stává jedním z nejnaléhavějších témat v oblasti kybernetické bezpečnosti, a také právem. Nicméně, největší hrozbou pro kybernetickou bezpečnost není sofistikovaný hacker nebo nebezpečný malwarový kód, ale spíše uživatel, který nerespektuje bezpečnostní postupy a tím ohrožuje bezpečnost své organizace.

V průběhu mé profesní kariéry jako specialisty kybernetické bezpečnosti v Armádě České republiky jsem získal znalosti týkající se problematiky ochrany dat, a to zejména v kontextu vojenského prostředí. Tato zkušenost mě motivovala k výběru tématu "Bezpečnost dat ve veřejném sektoru" pro tuto bakalářskou práci.

Práce je dělena na dvě části. V první polovině se zabývá teoretickou částí zabezpečení dat, kde jsou nejdříve rozepsány bezpečnostní opatření, které mohou pomoci se zabezpečení informačních systémů a ochránit tak před kybernetickými útoky, které jsou popsány níže. Dále je pozornost věnována nástrojům na obranu a zabezpečení počítačové sítě. V praktické části se zabývá částí kvantitativního, tj. dotazníkového šetření pracovníků veřejného sektoru, které je zaměřeno na ověření jejich znalostí v kybernetické ochraně.

1 Cíl a metodika bakalářské práce

Cílem této bakalářské práce je zjistit stav, ve kterém se nachází zabezpečení dat ve veřejném sektoru. Konkrétně se budu dotazovat pracovníků štábu v Armádě České republiky a Úřadu práce.

Teoreticko-metodická část je vypracována prostřednictvím analýzy odborné literatury a elektronických materiálů, následně jsou tyto informace kombinovány a prezentovány ve formě srozumitelného textu. Práce je členěna do čtyř kapitol. V první kapitole se zabývá vysvětlením bezpečnostních opatření bezprostředně souvisejících s kyberprostorem, dále pak kapitolou nástrojů k obraně, které mohou pomoci zamezit kybernetickému útoku či jiné hrozbě. Třetí kapitola se zabývá zabezpečením počítačové sítě, která může posloužit nejen uživatelům, ale například i začínajícím správcům sítě a poslední kapitola teoretické části se zabývá samotnými kybernetickými útoky, kde jsou vypsány jednotlivé hrozby a na co by si uživatel měl dát pozor.

V praktické neboli empirické části je elektronický dotazník, který se dotazuje pracovníků štábu 132. dělostřeleckého oddílu v Jincích a pracovníků Úřadu práce v Příbrami. Praktická část je zaměřena na analýzu současného stavu znalostí kybernetické bezpečnosti uživatelů ve veřejném sektoru a navrhuje konkrétní opatření pro zlepšení bezpečnosti. Dotazník byl šířen prostřednictvím přímých odkazů, přičemž předtím, než byl distribuován respondentům, byla jeho srozumitelnost a funkčnost otestována na menším souboru respondentů, kteří poté nebyli zahrnuti do hlavního výzkumného souboru.

Elektronický formát dotazníku umožňuje rychlé oslovení a získání odpovědí od velkého počtu respondentů v krátkém časovém rámci. Dále umožňuje snadnější zpracování výsledků, protože data lze rychle extrahovat a zpracovat v přehledné tabulce. Respondenti byli oslovováni prostřednictvím odkazů posílaných elektronicky. Předtím, než respondenti začali vyplňovat dotazník, byli informováni o účelu dotazníkového šetření a o skutečnosti, že jimi poskytnuté údaje budou využity jen pro potřeby této práce.

Cílem této bakalářské práce je tedy zvýšit povědomí o kybernetické bezpečnosti a přispět ke zlepšení bezpečnosti informačních systémů a ochraně osobních údajů.

2 Bezpečnostní opatření

V dnešní době se stále více spoléháme na moderní technologie a digitální prostředí pro řadu našich každodenních činností. Tato digitalizace výrazně zvýšila efektivitu a pohodlí našich životů, ale současně přinesla nové výzvy v oblasti kybernetické bezpečnosti. Kybernetické hrozby a útoky jsou stále sofistikovanější a mnohem rozsáhlejší, což znamená, že ochrana našich digitálních aktiv a citlivých informací se stala klíčovým prvkem našeho bezpečnostního prostředí.

V rámci kybernetické bezpečnosti je jedním z nejdůležitějších faktorů bezpečnostní opatření související s uživateli. Uživatelé hrají klíčovou roli v prevenci kybernetických útoků a ochraně dat. Ať už se jedná o zaměstnance firem, vládní úředníky, či jednotlivé občany, jejich chování a rozhodnutí mají významný vliv na celkovou bezpečnost kyberprostoru.Tato kapitola se zaměřuje na význam bezpečnostních opatření, která jsou cílena na uživatele v kybernetické bezpečnosti. V dnešním globalizovaném světě jsou útoky na informační systémy, kybernetické úniky a krize spojené s kybernetickou bezpečností stále častější a sofistikovanější. Proto je nezbytné, abychom byli schopni chápat a provádět odpovídající bezpečnostní opatření v kybernetice.

2.1 Bezpečná komunikace

Pojem bezpečná komunikace je velmi často spojován s následujícími třemi procesy: identifikace (Authentication), zabezpečení (Confidentiality) a celistvost (Integrity)[1].

2.1.1 Proces identifikace (Authentication)

Ověřuje identitu jednotlivých uzlů a prvků sítě. Proces identifikace je obvykle založen na ověření přístupových údajů pověřenou autoritou. Přístupovými údaji může být například dvojice ve formátu uživatelské jméno a heslo. U složitějších (komplexnějších) systémů může být proces identifikace založen na prokázání vlastnictví určitého klíče či charakteristického znaku či prvku, který je obtížné odcizit nebo zfalšovat. K těmto prostředkům patří například certifikáty nebo čipové karty.[2]

[1] STALLINGS, W., *Wireless communications and networks*. 2nd ed. Upper Saddle River: 2005, s. 368.
[2] SALAZAR, J. Techpedia - Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.

2.1.2 Proces zabezpečení (Confidentiality)

Omezuje (znemožňuje) možnost odposlechu síťového provozu. Procesem zabezpečení je typicky zabezpečení obsahu zprávy pomocí šifrování. Proces šifrování aplikuje známou oboustrannou metodu transformace (nazývanou též šifra nebo šifrovací algoritmus) na původní (originální) obsah zprávy (označovaný též pojmem prostý text) a touto transformací je z něj vytvořen šifrovaný text. Obnovit původní obsah zprávy (tj. dešifrovat zprávu) mohou pouze ti, kteří znají metodiku zvolené transformace. [3]

2.1.3 Proces celistvost (Integrity)

Zajišťuje, že přenášené zprávy jsou doručovány bez dodatečných změn. V souvislosti s procesem zabezpečení komunikace je tedy nutné doplnit schopnost systému, která umožňuje ověřit, že přijatá zpráva nebyla žádným způsobem pozměněna a je tedy shodná (identická) se zprávou, která byla odeslána.[4]

2.2 Aktualizování

Udržování operačního systému a aplikací v aktuálním stavu patří mezi nejdůležitější, ale neprováděné postupy pro maximalizaci ochrany. Vezměte v úvahu následující: hacker se obvykle pokusí ukrást vaše informace jedním ze dvou obecných způsobů.

Nejjednodušší metodou je požádat vás o předání informací o vašem účtu nebo přihlašovacích údajů. Nejčastěji se tak děje prostřednictvím různých forem podvodů, phishingových útoků a škodlivých webových stránek nebo odkazů. Cílem je oklamat vás, abyste jim požadované informace poskytli prostřednictvím prostředků, které vypadají věrohodně a legitimně.[5]

---

[3] SALAZAR, J. Techpedia - Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.

[4] SALAZAR, J. Techpedia - Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.

[5] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity.* 2019, s. 23.

Další metodou je infikování vašeho zařízení pomocí některé z forem malwaru. Malware se pak snaží ukrást vaše informace a předat je hackerovi. Ti, kteří nadále používají zastaralý software (ať už se rozhodli neinstalovat záplaty, nebo používají software, který již není opravován), riskují zneužití zranitelnosti. Pokud se škodlivý software pokusí zneužít již opravenou zranitelnost v počítači, je na tomto počítači v podstatě neškodný. Pokud však byla vydána záplata, ale uživatel (včetně správce systému nebo společnosti) se rozhodne záplatu nebo aktualizaci nenainstalovat, může pak malware zranitelnost stále využít.

Běžně dochází k mnoha únikům dat, kterým bylo možné zabránit, kdyby byly systémy nejprve opraveny. Stejně jako lidé, kteří nejsou zaměstnanci IT, i správci systémů odkládají aktualizaci nebo záplatování systémů z různých důvodů: je to příliš složité, mohlo by to ovlivnit chod aplikací, jsou příliš zaneprázdněni nebo otálejí z lenosti. "Neznámé" zranitelnosti se obecně označují jako zranitelnosti nultého dne. Název pochází z toho, že vývojář o zranitelnosti neví a měl "nula" dní na vytvoření záplaty systému.[6]

2.3 Záloha

Ztráta dat může být pro každého uživatele počítače nebo chytrého zařízení velkým problémem. Může se jednat o smazané fotografie, ztracené pracovní dokumenty nebo cenné osobní údaje.[7]

Záloha může být neocenitelná pro jakoukoli organizaci v době, kdy dojde k hackerskému útoku, do systému pronikne virus, data se zašifrují, nebo když se systémy zničí vodou, ohněm nebo jiným dopadem. V takových situacích je záloha často vlastně poslední šancí na obnovu systému. Proto je nutné plánovat zálohování komplexně a pravidelně kontrolovat, zda je obnova možná. Způsob plánování záloh závisí na důležitosti zálohovaného systému a množství dat, která jsou v něm uložena a zpracována.[8]

[6] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity.* 2019, s. 23.
[7] Vlastní zdroj
[8] LENHARD, T. H. *Data security: Technical and organizational protection measures against data loss and computer crime.* SPRINGER. 2022, s. 67.

Obrázek 1 Zálohování[9]

Proč je zálohování dat důležité?

Prevence ztráty dat: Nikdo není imunní vůči chybám nebo selháním zařízení. Přírodní katastrofy, krádeže nebo poškození hardware mohou také způsobit ztrátu dat. Zálohování je nejlepší způsob, jak se chránit proti těmto rizikům.

Obnova po havárii: Když máte zálohu dat, můžete rychle obnovit svá data po havárii nebo selhání systému. To znamená, že nemusíte trávit hodiny, nebo dokonce dny pokoušením se získat ztracené informace z poškozeného zařízení.

Ochrana před malwarem: Ransomware a jiné druhy malwaru mohou zašifrovat vaše data a požadovat výkupné za jejich odemknutí. Pokud máte zálohu, nemusíte platit útočníkům, abyste získali svá data zpět.

Pohodlí a flexibilita: Zálohování dat umožňuje snadný přenos dat mezi zařízeními. Můžete například zálohovat svá data na externím disku a přenášet je mezi počítači nebo obnovit data na novém zařízení.[10]

Jak provést zálohování dat?

Jedna záloha je lepší než žádná, ale alespoň dvě kopie poskytují určitou redundanci. Dávejte přednost tomu, aby jedna záloha byla na přenosném úložném zařízení a druhá kopie na cloudovém úložišti (Obrázek 1).

[9] Backup de données : qu'est-ce que c'est ? À quoi cela sert-il ? [online]. [cit. 2023-26-10] Dostupné z WWW: <https://www.weodeo.com/la-securite-informatique/quest-ce-quun-backup-up-et-a-quoi-cela-sert/>.

[10] Vlastní zdroj

Co je to "cloud"?

Cloud je cokoli, co není lokálně umístěno ve vašem výpočetním zařízení (Obrázek 2). Obvykle se jedná o službu někde na internetu. Protože obvykle nevíme, kde je služba umístěna, je to mlhavý pojem a někdo někde rozhodl, že cloud je vhodný popis. Jako dodatečné bezpečnostní opatření je dobré pravidelně zálohovat soubory na úložné zařízení, které je běžně od počítače odpojeno. Například dočasně připojíte přenosný pevný disk, zkopírujete na něj své soubory a poté disk odpojíte.[11]

Obrázek 2 Cloudové uložiště[12]

2.4 Paměťová média

Pevné disky USB (Universal Serial Bus) a zejména USB flash disky dosáhly v posledních letech působivé kapacity a vysoké datové propustnosti. Dnes jsou nepostradatelnými součástmi ve světě počítačů. Vzhledem k tomu, že vyměnitelná média se nyní používají téměř všude, lidé stěží přemýšlejí o potenciálních nebezpečích při používání této technologie. Tato, většinou přehlížená nebezpečí, mohou být velmi různorodá a sahat od virových infekcí až po špionáž. Pokud si vzpomeneme na incident související s Wikileaks, byly zveřejněny tisíce souborů a dokumentů, které bývalý zaměstnanec Pentagonu jednoduše zkopíroval na USB flash disk a vzal s sebou.[13]

[11] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity*. 2019, s. 27-28.
[12] 10 Types of Cloud Computing You Should Know About [online]. [cit. 2023-26-10] Dostupné z WWW: <https://helpdeskgeek.com/reviews/10-types-of-cloud-computing-you-should-know-about/>.
[13] LENHARD, T. H. *Data security: Technical and organizational protection measures against data loss and computer crime.* SPRINGER. 2022, s. 47.

V minulosti byly také opakovaně známy případy špionáže, kdy byly použity infikované USB klíče. Princip je jednoduchý a zároveň účinný, takže lze s jistotou předpokládat, že hackování pomocí USB klíčenek je nejjednodušší, ale v žádném případě není nejúspěšnější varianta prolomení sítí. Hacker přitom využívá lidské zvědavosti.[14]

Obrázek 3 Nakažený USB Flash disk[15]

Přestože byly USB disky (nebo flash disky) dříve oblíbenějším způsobem přenosu souborů, stále se používají často. Pokud tyto disky mohou přenášet soubory, mohou přenášet i škodlivý software (Obrázek 3). Uživatelé si také musí být vědomi, že každé zařízení, které připojí k USB, může obsahovat malware. V nesčetných případech zločinci kompromitovali veřejné nabíjecí stanice (místa, kde si lidé mohou dobíjet své mobilní telefony) tím, že manipulovali s nabíjecími stanicemi tak, aby do mobilních telefonů nahráli malware, kdykoliv byl k nabíjecí stanici připojen kabel.

Došlo dokonce k incidentům s digitálními fotorámečky, které byly cíleně plně infikovány. Když pak někdo připojil rámeček k počítači, aby ho nabil a stáhl obrázky, počítač byl infikován. V současnosti jsou k dispozici ventilátory, ohřívače šálků, světla a další předměty, které se nabíjejí nebo fungují z portu USB. Dokonce i kabely mohou být nakonfigurovány se škodlivým softwarem. Majitelé zařízení si musí uvědomit, že by se měli vyhýbat neznámým zařízením nebo portům USB.[16]

[14] LENHARD, T. H. *Data security: Technical and organizational protection measures against data loss and computer crime.* SPRINGER. 2022, s. 47.
[15] USB Flash Drive Malware: How It Works & How to Protect Against It [online]. [cit. 2023-26-10] Dostupné z WWW: <https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/>.
[16] WINKLER, I. *Security awareness for dummies*. John Wiley & Sons. 2022, s. 82.

2.5 Personální bezpečnost

Personální bezpečnost hraje klíčovou roli v oboru kybernetické bezpečnosti. Zaměstnanci, kteří mají přístup k citlivým informacím a pracují s kybernetickou infrastrukturou, mohou buď posilovat, nebo ohrožovat bezpečnost organizace.[17]

Uživatelé počítačů v každé organizaci, škole nebo agentuře jsou kritickým aspektem obrany a ochrany citlivých dat a bezpečného provozu. Uživatelé se mohou rychle stát Achillovou patou každé bezpečnostní organizace, protože nelze předvídat, jak se budou za určitých okolností chovat. Jediný uživatel, kterého útočník oklame a donutí ho kliknout na škodlivý odkaz nebo prozradit své uživatelské jméno a heslo, může překonat všechny bezpečnostní technologie, které mohou být zavedeny.[18]

Důležitý je již samotný proces přijímání nových zaměstnanců. Tato problematika spadá spíše do oblasti řízení lidských zdrojů, ovšem i zde už mohou být uplatněny některé prvotní filtry. Pokud to povaha jeho práce vyžaduje, je možné u budoucího zaměstnance provádět kontrolu informací uváděných v profesním životopisu, včetně ověření informací o dosaženém vzdělání, kontrolovat trestní bezúhonnost, případně si zjistit doplňkové informace o uchazeči z veřejných zdrojů. Vždy je však potřeba postupovat v souladu s platnými zákony. Zaměstnanci by také, například v rámci pracovní smlouvy, měli být seznámeni s povinností ochrany informací a povinností mlčenlivosti v patřičném rozsahu.

Důležité je také pravidelné školení zaměstnanců. To může být realizováno fyzicky, ale i formou e-learningu. Praxe ukazuje, že je třeba uživatelům nejen vštípit určitá pravidla, ale také vysvětlit, proč je jejich dodržování důležité. Pokud si totiž uživatelé nevezmou pravidla týkající se bezpečnosti za svá, pravděpodobně je dříve či později začnou ignorovat, či dokonce záměrně obcházet.[19]

2.5.1 Need to know

Z hlediska bezpečnosti lidských zdrojů je důležité zavést systém klasifikace dat organizace tak, aby uživatelé věděli, jak s kterým druhem informací mohou nakládat a s kým jej mohou sdílet. Mezi známé principy patří **princip Need to know**, který v podstatě říká, že zaměstnanec by měl mít přístup pouze k informacím, které potřebuje pro svou práci, tedy ne na základě například své pozice ve firmě. [20]

[17] Vlastní zdroj
[18] VACCA, R. J. *Computer and Information Security Handbook*. 3rd ed. Burlington 2017, s. 414.
[19] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 489.
[20] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 490.

Tento princip je uplatňován především ve specializovaných organizacích. V běžné praxi závisí jeho smysluplné uplatnění na mnoha faktorech. Některé informace zaměstnanec běžně ke své práci nepotřebuje, nicméně ve specifických případech mu může informace, která mu nepřísluší, pomoci udělat správné rozhodnutí.[21]

2.5.2 Nejslabší článek zabezpečení: uživatelé

Koncoví uživatelé jsou jak první linií obrany proti kybernetickým útokům, tak nejslabším článkem v řetězci kybernetické bezpečnosti, a proto phishing zůstává tak rozšířenou kybernetickou hrozbou. Odhaduje se, že lidské chování způsobuje až 90 % kybernetických útoků, a proto je důležité neustále informovat koncové uživatele o iniciativách kybernetické bezpečnosti, aby je podpořili při rozhodování o inteligentní kybernetické obraně. Dokud lidé naletí phishingovým podvodům, používají slabá hesla a pracují na nezabezpečených sítích, jsou vystaveni zneužití. Vzhledem k tomu, že práce na dálku pokračuje i po pandemii a hybridní pracovní síly se v budoucnu zřejmě stanou normou, budou vzdálení pracovníci i nadále cílem útoků zlých aktérů.[22]

Povědomí o bezpečnosti se uživatelům nejlépe předává dvěma základními způsoby: během úvodního školení nových zaměstnanců a prostřednictvím průběžného cíleného školení uživatelů v různých odděleních s ohledem na konkrétní okruh uživatelů.[23]

Vše začíná u základů: pokud uživatelé neznají kybernetické hrozby a jejich fungování, nemohou je odhalit ani se vyhnout špatným bezpečnostním postupům. Navíc nevzdělaní a nevyškolení zaměstnanci nebudou vhodně reagovat, jakmile zjistí malware v akci, nebo když uvidí podezřelé chování účtu nebo aplikace.

Cena za to, že nevzdělaní a nezkušení uživatelé mají přístup k důležitým podnikovým systémům a sítím, zejména v prostředí stále vzdálenějších pracovníků, je vždy vysoká. Lidské chyby a škodlivé praktiky, jako jsou slabá hesla a připojování z nezabezpečených sítí Wi-Fi, jsou scénáře, které se každý hacker na světě snaží co nejlépe využít ve svůj prospěch.[24]

---

[21] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 490.
[22] Co je to kybernetická bezpečnost ? [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.sap.com/cz/products/financial-management/what-is-cybersecurity.html>.
[23] VACCA, R. J. *Computer and Information Security Handbook*. 3rd ed. Burlington 2017, s. 289.
[24] Why user education is important for cybersecurity resilience [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.lumificyber.com/blog/why-user-education-is-important-cybersecurity-resilience/>.

Jediná infekce ransomwarem způsobená slabým uživatelským heslem nebo uživatelem, který používá k práci veřejný hotspot Wi-Fi, může zničit podnikání průměrného podniku a ochromit jeho provoz na několik týdnů. Organizace proto musí vynaložit veškeré úsilí, aby své zaměstnance vzdělávaly v základech kybernetické bezpečnosti. Školení by mělo zahrnovat způsoby, jak rozpoznat phishingové e-maily, odhalit neobvyklé chování aplikací a účtů a reagovat na jakoukoli skutečnou nebo možnou kybernetickou hrozbu, kterou náhodou spatří.[25]

2.6 Přenosné počítačové systémy

Problematika přenosných systémů zahrnuje různé aspekty týkající se mobilních zařízení, laptopů a jiných přenosných technologií. Tyto problémy zahrnují bezpečnostní, technická, sociální a ekonomická hlediska. Níže jsou uvedeny některé klíčové otázky a problémy.

- **Bezpečnostní rizika**

Přenosné systémy jsou náchylné k různým bezpečnostním rizikům, jako jsou malware, ransomware, krádeže dat a útoky na přenosná zařízení. Uživatelé by měli být obezřetní při používání veřejných sítí a instalaci aplikací z neověřených zdrojů.

- **Ztráta nebo krádež zařízení**

Přenosná zařízení jsou snadno přenositelná, což znamená, že mohou být snadno ztracena nebo odcizena. To může způsobit ztrátu citlivých dat a informací.

- **Zabezpečení dat**

Uživatelé by měli pečlivě zabezpečovat data na svých přenosných zařízeních, včetně používání šifrování, silných hesel a dvoufaktorové autentizace.

- **Správa mobilních zařízení (MDM)**

Organizace se setkávají s výzvou, jak efektivně spravovat a zabezpečit mobilní zařízení zaměstnanců. Řešení jako Mobile Device Management (MDM) pomáhají organizacím spravovat a monitorovat tyto zařízení. [26]

[25] Why user education is important for cybersecurity resilience [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.lumificyber.com/blog/why-user-education-is-important-cybersecurity-resilience/>.
[26] Vlastní zdroj

Speciální podskupinou počítačových systémů přinášených do počítačové sítě organizace mohou být zařízení spadající do kategorie známé jako **BYOD** (Bring Your Own Device)[27]. BYOD je politika, která umožňuje zaměstnancům organizace používat k pracovním činnostem zařízení, která vlastní. Tyto činnosti zahrnují úkoly, jako je přístup k e-mailům, připojení k podnikové síti a přístup k podnikovým aplikacím a datům. Chytré telefony jsou nejčastějším mobilním zařízením, které si zaměstnanec může vzít do práce, ale zaměstnanci si na pracoviště berou také vlastní tablety, notebooky a USB disky.[28]

Jak politika BYOD funguje?

Zásady BYOD popisují, co společnost považuje za přijatelné používání technologie, jak ji provozovat a jak chránit společnost před kybernetickými hrozbami, jako je ransomware, hackerské útoky a úniky dat. Je velmi důležité mít dobře definovanou politiku BYOD a pochopit rizika a přínosy BYOD v organizaci.[29]

Zásady BYOD mohou zahrnovat všechny nebo některé z následujících bodů:

- Co představuje přijatelné používání osobních zařízení pro pracovní činnosti;
- typy mobilních zařízení schválené oddělením IT;
- software, který musí být nainstalován pro zabezpečení zařízení, například nástroje pro správu mobilních zařízení (MDM) nebo správu mobilních aplikací (MAM);
- bezpečnostní opatření, jako jsou požadavky na hesla;
- odpovědnosti uživatelů v souvislosti se zařízením a jeho přístupem k síti;
- případné pobídky nebo náhrady nákladů za používání osobních datových plánů pro činnosti související s prací;
- jasnou definici politiky ukončování;
- plán odchodu v případě, že zaměstnanci již nechtějí používat svá osobní zařízení k práci.[30]

[27] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 544.
[28] BYOD (bring your own device) [online]. [cit. 23-10-30] Dostupné z WWW: <https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device>.
[29] BYOD (bring your own device) [online]. [cit. 23-10-30] Dostupné z WWW: <https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device>.
[30] BYOD (bring your own device) [online]. [cit. 23-10-30] Dostupné z WWW: <https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device>.

2.7 Ověřování uživatelů

Ověřování uživatelů je proces, který zajišťuje, že osoba nebo entita, která se pokouší získat přístup k určitým systémům, službám nebo datům, je skutečně tím, za koho se vydává. Ověřování je klíčovým prvkem kybernetické bezpečnosti a zajišťuje, že pouze oprávnění uživatelé mají přístup k citlivým informacím a zdrojům. Existuje několik metod ověřování uživatelů, včetně následujících:

- **Ověření uživatele na základě toho, co zná,** v podobě hesla (určitého řetězce znaků), který uživatel obvykle na základě výzvy systému zadá. Zadané heslo je následně porovnáno s heslem již dříve uloženým uživatelem do systému. Pokud se hesla shodují, je uživatel přihlášen a jsou mu přidělena oprávnění.
- **Ověření uživatele na základě vlastnictví předmětu** bývá realizováno díky držení určitého tokenu uživatelem (např. čipové karty, klíče, aj.). Tuto funkci dnes může převzít například i mobilní telefon.
- **Ověřením uživatele na základě toho čím je** se zabývá biometrie, která rozpoznává jedinečné biologické charakteristiky daného uživatele.[31]

Za vhodnou a pro většinu běžných aplikací a systémů dostatečnou, lze označit autentizaci, která využívá dva z výše uvedených způsobů a kombinuje tak například znalost hesla s vlastnictvím zařízení, nebo s biometrickými údaji. V takovém případě mluvíme o dvoufaktorové autentizaci.[32]

Dvoufaktorové ověřování, které obvykle využívá něco, co znáte (heslo), a něco, co máte (například chytrý telefon), je stále běžnější. Některé organizace ho vyžadují. Jiné umožňují uživatelům, aby se pro něj rozhodli. Některé metody použití mobilního zařízení jako druhého faktoru zahrnují zaslání textové zprávy nebo e-mailu s kódem s omezeným použitím. Tento kód se pak zadává na samostatné přihlašovací stránce. Další možnou metodou dvoufaktorového ověřování je použití klíčenky, která poskytuje jednorázový kód, který se zadává na stránce druhého faktoru. Pokud vaše organizace nebo účet, který používáte, nabízí možnost dvoufaktorového (nebo vícefaktorového) ověřování, je ve vašem nejlepším zájmu se pro něj rozhodnout.[33]

[31] Školící materiál služebního školení
[32] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 463.
[33] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity*. 2019, s. 73-74.

2.8 Hesla

Hesla jsou jedním z nejběžnějších způsobů ověřování identity uživatelů a ochrany přístupu k různým systémům, službám a datům. Správná správa hesel je klíčová pro zajištění kybernetické bezpečnosti, protože hesla jsou často první linií obrany proti neoprávněnému přístupu.

Co se tedy stane, když se hackerům podaří získat vaše uživatelské jméno a heslo? Mohou se pokusit tyto údaje použít k přihlášení k vašemu e-mailovému účtu. Pokud se jim to podaří, co by mohli zjistit? Možná spoustu e-mailů z ostatních účtů, které máte. Upozornění na bankovní výpisy. Možná oznámení o ochraně osobních údajů z vaší společnosti vydávající kreditní karty. Co třeba e-maily od dalších institucí a organizací, z nichž mnohé mohou mít váš online účet. Nyní mají hackeři k dispozici seznam webových stránek, na kterých mohou vyzkoušet vaše uživatelské jméno (e-mailovou adresu) a heslo. Pokud jste na všech těchto stránkách jednoduše použili stejné heslo, otevřeli jste nyní hackerům dveře dokořán a v podstatě jim poskytli volný přístup k vašim osobním údajům.[34]

Hesla stále představují nejrozšířenější způsob autentizace uživatelů, a proto je vhodné jim věnovat větší pozornost. Jak již bylo uvedeno, heslo je po zadání uživatelem porovnáno s heslem, které uživatel zadal do systému již dříve. Tím vzniká první problém, který spočívá v **procesu uložení hesla do systému** tak, aby se k němu nedostal útočník, pokud se mu podaří do systému proniknout. Další potencionální riziko představuje i oprávněný správce systému, který má z principu přístup do celého systému a mohl by si tak přečíst heslo uživatele a následně jej zneužít. [35]

V současnosti rozeznáváme řadu útoků na hesla. Heslo může být:

- odchyceno z provozu na počítačové síti;
- z uživatele vylákáno sociálním inženýrstvím (např. phishingovým útokem aj.);
- získáno z počítačového systému za použití malware (např. pomocí keylogeru aj.);
- uhádnuto;
- „lámáno“.[36]

[34] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity*. 2019, s. 47-48.
[35] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 465-466.
[36] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 465-466.

Lámání on-line představuje situaci, kdy útočník zasílá různá hesla a čeká na jejich ověření v počítačovém systému. Obecně je tento způsob útoku relativně pomalý a útočníkovi hrozí, že si jeho počínání někdo všimne a v logu se objeví příliš mnoho pokusů o přihlášení z jedné IP adresy, případně na více účtů. Obranou proti on-line lámání hesel může být zamčení účtu po několika neúspěšných pokusech nebo zpomalení vyhodnocování hesel v systému. Protože je on-line lámání hesel pomalé a relativně snadno zjistitelné, je pro útočníka lepší variantou, pokud se dokáže dostat přímo k heslům uživatelů. Ta by však měla být ukládána ve formě, která neumožní jejich snadné přečtení, tedy v podobě hashe[37] hesla. Kromě samotného způsobu zabezpečení uložených hesel je třeba se zabývat i otázkou vynucování kvality hesel a stanovení politik pro nakládání s hesly.[38]

2.9 Logování

Důležitou součástí bezpečného provozu systémů, služeb a aplikací je zaznamenávání informací o jejich činnosti a běhu, tzv. logování. Záznamy mohou být ukládány ve formě prostého textového souboru, ale mohou být také ukládány do databázového souboru. Existuje řada různých formátů, ve kterých jsou data ukládána, nejčastěji ve formátu syslog, textovém formátu (XML, CSV, W3C), ale můžeme se setkat i s logováním v binární podobě. Úroveň detailu logování je dána možnostmi dané aplikace či systému. Často je možné nastavit několik různých úrovní logování, podle aktuální potřeby administrátora. Je potřeba si uvědomit, že ačkoliv by se mohlo zdát nejvýhodnější logovat veškeré události, které je aplikace schopna zaznamenat, není to obvykle v reálném provozu žádoucí. Příliš detailní logování znamená zvýšenou zátěž výpočetního systému a zároveň generuje více dat, která je potřeba uložit. Nastavení úrovně logování je proto potřeba pečlivě zvážit.

Z pohledu bezpečnosti musí vlastní implementaci logování předcházet rozvaha, ze které bychom měli zjistit, jaké bezpečnostní události či bezpečnostní incidenty poskytované služby, počítačové systémy či sítě ohrožují. Z této analýzy je následně možné vydefinovat, které data a informace je potřeba logovat, aby bylo možné zjistit, že k bezpečnostní události či incidentu došlo, jakož i zjistit zdroj škodlivé aktivity (např. úmyslná lidská činnost, incident způsobený selháním jiného počítačového systému v síti aj.).[39]

[37] Hašovací funkce je matematická funkce, která přijímá vstup (neboli "zprávu") a vrací řetězec znaků o pevné velikosti, což je hodnota haše.
[38] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 465-466.
[39] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 474-475.

3 Nástroje na obranu

Součástí zabezpečení před únikem dat jsou i bezpečností nástroje, kterým se zabývají IT týmy v jednotlivých organizacích. Mezi tyto nástroje patří:

- Řízení přístupu;
- SIEM (Security Information and Event Management);
- Antivirus, Antimalware.

3.1.1 Řízení přístupu

Řízení přístupu je základním prvkem zabezpečení, který určuje, kdo má povolený přístup k určitým datům, aplikacím a prostředkům – a za jakých okolností. Stejně jako klíče a předem schválené seznamy hostů chrání fyzické prostory, zásady řízení přístupu chrání digitální prostory. Jinými slovy, pouští dovnitř ty správné lidi, zatímco ty špatné ne. Zásady řízení přístupu se do velké míry spoléhají na techniky, jako je ověřování a autorizace, které organizacím umožňují explicitně ověřit, že uživatelé jsou ti, za které se vydávají, a že je těmto uživatelům udělena odpovídající úroveň přístupu na základě kontextu, jako je zařízení, umístění, role a mnoho dalších aspektů.

Řízení přístupu chrání důvěrné informace, jako jsou zákaznická data a duševní vlastnictví před odcizením aktéry se zlými úmysly nebo jinými neoprávněnými uživateli. Existují čtyři hlavní typy řízení přístupu, přičemž každý z nich řeší správu přístupu k citlivým informacím jedinečným způsobem.[40]

Volitelné řízení přístupu (DAC) - v modelech DAC má každý objekt v chráněném systému vlastníka a vlastníci udělují přístup uživatelům podle svého uvážení. DAC umožňuje kontrolu nad prostředky případ od případu.[41]

Povinné řízení přístupu (MAC) - v modelech MAC se uživatelům uděluje přístup formou povolení. Centrální autorita reguluje přístupová práva a organizuje je do úrovní, které se jednotně rozšiřují. Tento model je velmi běžný ve vládních a vojenských prostředích.[42]

[40] Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>.
[41] Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>.
[42] Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>.

Řízení přístupu na základě role (RBAC) - v modelech RBAC se přístupová práva udělují na základě definovaných firemních funkcí, nikoli na základě identity nebo seniority jednotlivců. Cílem je poskytnout uživatelům jenom ta data, která potřebují ke své práci a nic navíc.[43]

Řízení přístupu na základě atributů (ABAC) - v modelech ABAC se přístup uděluje flexibilně na základě kombinace atributů a podmínek prostředí, jako je čas a místo. ABAC je nejpodrobnější model řízení přístupu a pomáhá snížit počet přiřazení rolí.[44]

Při řízení přístupu je ověřována úroveň oprávnění a práv uživatele k určitému zdroji nebo objektu. **Zdrojem** může být připojení k síti, využití kapacity paměťového média, přístup k počítačovým systémům (serverům, síťovým prvkům, tiskárnám, atd.,). **Objektem** jsou například data uložená v určitém adresáři, nebo samostatný soubor. Ověřovaným objektem může být oprávnění uživatele, skupiny, ale i samotných počítačových systémů. Uživatel může mít stejná práva jako ostatní členové skupiny a zároveň i nějaká oprávnění, která má pouze dotyčný uživatel.[45]

3.1.2 Monitoring

Monitorování zabezpečení zahrnuje sledování událostí a činností ve všech kritických systémech v reálném čase nebo téměř v reálném čase. K řádnému monitorování bezpečnostních událostí, které mohou vést k incidentu nebo vyšetřování, organizace obvykle používá nástroj pro správu bezpečnostních informací a událostí (SIEM). Bezpečnostní analytici a manažeři musí filtrovat tuny dat o událostech, identifikovat a zaměřit se pouze na nejzajímavější události.

Pochopení regulačního a forenzního dopadu dat událostí a výstrah v daném podniku vyžaduje plánování a důkladné pochopení množství dat, které bude muset systém zpracovávat. Čím lépe lze protokoly ukládat, chápat a korelovat, tím lepší je možnost včas odhalit incident a zmírnit jeho následky. Reakce na incidenty, identifikace anomálního nebo neoprávněného chování a zabezpečení duševního vlastnictví nebyly nikdy důležitější.[46]

---

[43] Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>.
[44] Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>.
[45] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 462.
[46] VACCA, R. J. *Computer and Information Security Handbook*. 3rd ed. Burlington 2017, s. 411.

Data mohou být sbírána z webových serverů, routerů, firewallů, Active Directory serverů, databázových serverů a tyto informace mohou být dále doplněny o informace dávající těmto datům kontext, jako jsou informace o uživatelích, výsledcích bezpečnostních skenů, informace z externích zdrojů a informace o běžných návycích uživatelů. Získané informace jsou následně agregovány, korelovány a je nad nimi prováděna analýza, která má ukázat na možné bezpečnostní problémy. Je však třeba říci, že SIEM řešení není vhodné pro každou situaci. Zatímco firewall nebo antispam mají smysl v podstatě v každé organizaci, SIEM představuje robustní řešení, které vyžaduje poměrně dost zdrojů. Kromě samotné implementace je třeba počítat také v podstatě s každodenní údržbou, přičemž čím složitější je prostředí, tím větší jsou nároky na údržbu.[47]

3.1.3 Antivirus, Antimalware

Kromě výše uvedených nástrojů stojí za zmínku antivirus. Antivirový software je jedním z nejznámějších bezpečnostních softwarů pro širokou veřejnost. Antivirus nás chrání před hrozbami a především nám pomáhá je eliminovat.

Aby však tyto programy přinesly požadovaný úspěch, musí být řádně implementovány a pravidelně aktualizovány. IT týmy v jednotlivých organizacích by měly předem zvážit, jaký software zvolit jako obranu pro ochranu dat a dalším kybernetickým útokům.

Aktualizovaný antimalware by mohl infekci zachytit dříve, než způsobí problémy. Klíčové slovo je "může". Je mnohem lepší, když je systém i antimalware aktualizovaný. Antimalware by měl provádět pravidelné skenování systému a úložných zařízení. Měli byste také občas provést ruční kontrolu a zvolit možnost hloubkové kontroly, pokud je k dispozici.[48]

[47] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 461.
[48] COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity*. 2019, s. 22-23.

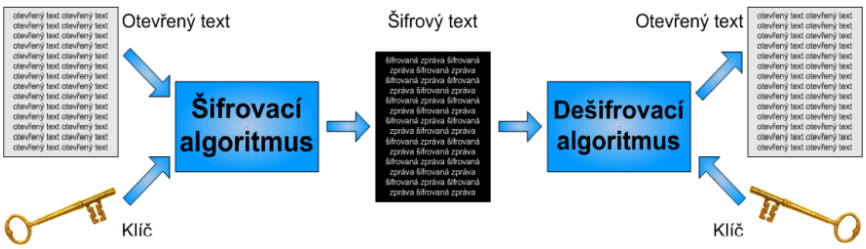
4 Bezpečnost sítě

Zajištění bezpečnosti počítačových sítí je jedním ze základních prvků, na kterých je vybudována kybernetická bezpečnost. Bez účinné ochrany počítačových sítí není možné efektivně zajistit ochranu počítačových systémů a dat v nich uložených. Výjimku z tohoto tvrzení samozřejmě představují zcela izolované počítačové systémy, jež nejsou úmyslně zapojeny do počítačové sítě.[49]

4.1 Šifrování

Šifrování je proces kódování informací tak, aby k nim neměly přístup neoprávněné osoby. Pokud dojde k úniku zašifrovaných dat vaší společnosti, kdokoli, kdo data ukradne, je nebude moci přečíst bez příslušného dešifrovacího klíče. Tento proces je určen k ochraně peněz a cenných informací. A v podnikatelském prostředí by se šifrování mělo používat také k ochraně duševního vlastnictví, know-how nebo osobních údajů, které se ve firmě zpracovávají.[50]

Obrázek 4 Šifrovací mechanismus[51]



4.1.1 Symetrické šifrování

Symetrická šifra je taková šifra, ve které je použit pro zašifrování zprávy ten samý klíč jako k jejímu dešifrování. Je zásadní, aby bez tohoto klíče nebylo možné zprávu rozšifrovat a zároveň aby byl algoritmus (většinou veřejný) takový, že po použití klíče získáme odpovídající původní text.[52]

---

[49] Vlastní text

[50] Proč Jsou šifrování a MFA Nezbytné Pro Vaši Firmu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://digitalsecurityguide.eset.com/cz/proc-jsou-sifrovani-a-mfa-nezbytne-pro-vasi-firmu#h2-0>.

[51] Šifrování dat - KRYPTOLOGIE [online]. [cit. 2023-26-10] Dostupné z WWW: <https://ucimeseit.cz/sifrovani-dat-kryptologie/>.

[52] DELFS, H., KNEBL, H. *Introduction to cryptography: principles and applications*. 2nd ed. New York: Springer, 2007, s. 237.

Protože zařízení používá pouze jeden klíč pro šifrování i dešifrování, symetrické šifrování může být zranitelné. Další nevýhodou symetrického šifrování je, že si všechny strany musí vyměňovat klíč (sdílení klíčů), aby šifrovaly a dešifrovaly data, což není vždy vhodné. K vyřešení tohoto problému je jiný typ šifrování, asymetrické šifrování, vytváří pár klíčů, jeden veřejný a jeden tajný.[53]

4.1.2 Asymetrické šifrování

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče.[54]

Odesílatel zašifruje zprávu pomocí veřejného klíče příjemce; příjemce však může tuto zašifrovanou zprávu dešifrovat pouze svým soukromým klíčem (Obrázek 4). Jeden klíč neprozradí druhý. Veřejný a soukromý klíč jsou vzájemně spojeny prostřednictvím matematického vztahu. Není možné vypočítat soukromý klíč z veřejného klíče, protože matematický vztah nemůže fungovat zpětně. Ve srovnání se symetrickým šifrováním je asymetrické šifrování mnohem pomalejší, ale nabízí lepší zabezpečení díky dvěma různým klíčům.[55]

[53] ALEXANDROU, A. *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices.* 1st ed. 2021, s. 263.

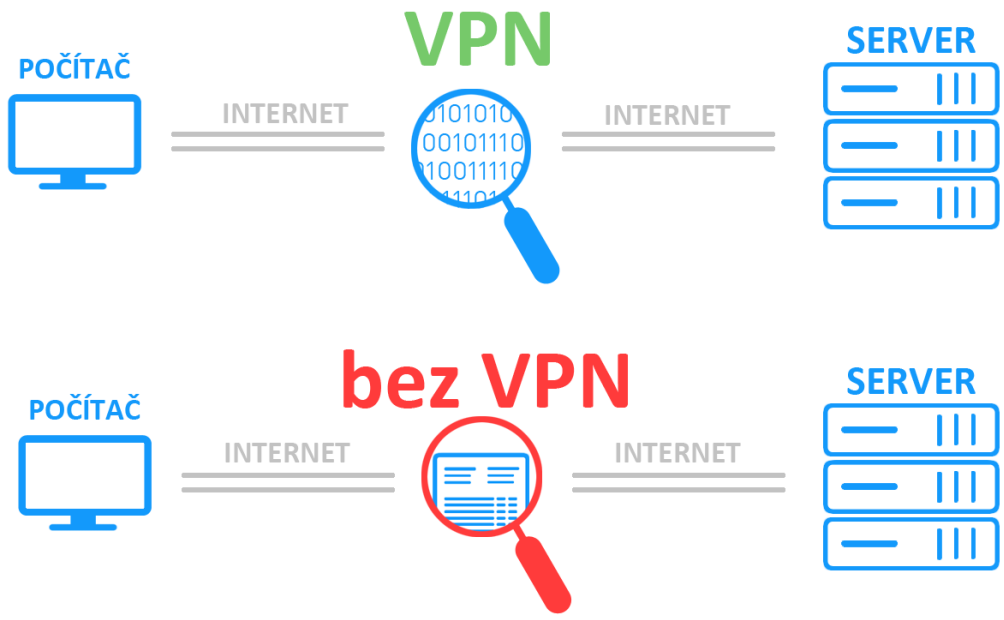
[54] Výběr skripta [online]. [cit. 2023-25-10]. Dostupné z WWW: <http://kbi.fbmi.cvut.cz/sites/default/files/Vyber-skripta.pdf>.

[55] ALEXANDROU, A. *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices.* 1st ed. 2021, s. 267.

4.2 VPN

VPN (virtuální privátní síť) je služba, která vytváří bezpečné a šifrované online připojení. Uživatelé internetu mohou používat VPN, aby si zajistili větší soukromí a anonymitu online nebo obešli blokování a cenzuru na základě zeměpisné polohy. VPN v podstatě rozšiřují soukromou síť přes veřejnou síť, což by mělo uživateli umožnit bezpečné odesílání a přijímání dat přes internet. VPN se obvykle používá přes méně zabezpečenou síť, například veřejný internet. Poskytovatelé internetových služeb (ISP) mají obvykle poměrně velký přehled o aktivitách zákazníka. Některé nezabezpečené přístupové body Wi-Fi či AP (Access Point) navíc mohou být pro útočníky vhodnou cestou k získání přístupu k osobním údajům uživatele (Obrázek 5). Uživatel internetu může použít síť VPN, aby se těmto zásahům do soukromí vyhnul.[56]

Obrázek 5 VPN[57]



VPN můžete snadno používat na svých zařízeních, ať už jste na telefonu, tabletu, notebooku nebo počítači. Jakmile VPN nakonfigurujete, poběží na pozadí a bude vás chránit 24 hodin denně, 7 dní v týdnu. Proto je důležitou součástí celkového řešení online zabezpečení.[58]

[56] VPN (virtual private network) [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.techtarget.com/searchnetworking/definition/virtual-private-network>.
[57] Co je VPN a k čemu je to dobré ? [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.czcloud.cz/cloud/co-je-to-vpn-a-k-cemu-je-to-dobre/>.
[58] What is VPN ? How It Works, Types of VPN [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://usa.kaspersky.com/resource-center/definitions/what-is-a-vpn>.

4.3 Fyzická bezpečnost

Fyzická bezpečnost je primárně zaměřena na ochranu technických aktiv daného subjektu. Maisner k fyzické bezpečnosti uvádí, že *„cílem tohoto opatření je především zamezení přístupu nepovolaných osob k jednotlivým prvkům infrastruktury, do serveroven, pracovišť správců systému apod. Snahou je vyloučit zcizení majetku přímo i nepřímo souvisejícího s informačním systémem, případně zamezit poškození hmotného i nehmotného vybavení nebo vybavení prostor. V neposlední řadě se snaží zamezit úniku informací a dat.“*[59]

Prostředky fyzické bezpečnosti jsou příkladmo uvedeny v § 3 až 10 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů[60]. Jedná se o:

- **mechanické zábranné prostředky** např. zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky, skříňové trezory, trezorové dveře a komorové trezory;
- **systém kontroly vstupu do zabezpečené oblasti** [poplachové a elektronické bezpečnostní systémy, detektory (pohybu, tříštění skla aj.) stanovení podmínek pro vstup: identifikační prvek, PIN, biometrie (případně jejich kombinace)];
- **zařízení elektrické zabezpečovací signalizace** (poplachové zabezpečovací a tísňové systémy – ústředny elektrické zabezpečovací signalizace, detektory elektrické zabezpečovací signalizace, otřesové detektory, perimetrické detekční systémy, tísňové systémy aj.);
- **speciální televizní systémy (kamerové systémy,** CCTV sledovací systémy aj.),
- **zařízení elektrické požární signalizace** (napojení do ústředny elektrické požární signalizace, nebo do ústředny elektrické zabezpečovací signalizace;
- **prostředky omezující působení požárů a živelných událostí** (poplachové systémy, detektory kouře, samočinné hasící systémy aj.;
- **zařízení pro zajištění ochrany před selháním dodávky elektrického napájení** (záložní zdroje – UPS, diesel agregáty aj.).[61]

[59] MAISNER, M., VLACHOVÁ, B., *Zákon o kybernetické bezpečnosti. Komentář.* Praha, 2015. s. 67.
[60] ČESKO. Vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.
[61] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity.* Praha, 2019, s. 283.

4.4 Síť a její rozdělení

Počítačové sítě lze rozdělit na lokální sítě (LAN) a rozsáhlé sítě (WAN). Síťová zařízení, jako jsou přepínače, rozbočovače, můstky, pracovní stanice a servery vzájemně propojené v jedné síti na určitém místě, se obecně označují jako LAN. VLAN neboli virtuální síť LAN je skupina složená ze zařízení v jedné nebo více než jedné síti LAN, které jsou nakonfigurovány pro komunikaci tak, jako kdyby všechna tato zařízení byla připojena stejným vodičem, zatímco se nacházejí na několika různých místech segmentech sítě LAN. VLAN jsou ve své podstatě velmi flexibilní, protože jsou založeny na logickém spojení namísto fyzického spojení. Síť VLAN se chová stejně jako dílčí síť. VLAN ulehčuje práci síťovým správcům rozdělit jednu jedinou přepínanou síť pro odpovídající bezpečnostní a funkční požadavky systémů, aniž by bylo třeba vedení nových kabelů nebo bez nutnosti provádět zásadní změny ve stávající síti. Jeden nebo více než jeden síťový přepínač může podporovat několik nezávislých sítí VLAN.[62]

Implementace VLAN má několik výhod spočívajících například v:

- snížení počtu potřebného hardware;
- omezení počtu broadcastů;
- oddělení speciálního provozu;
- zvýšení bezpečnosti;
- jednodušším přesouvání počítačových systémů mezi sítěmi (místo fyzického přepojování datového kabelu stačí překonfigurovat zapojení do jednotlivých VLAN).[63]

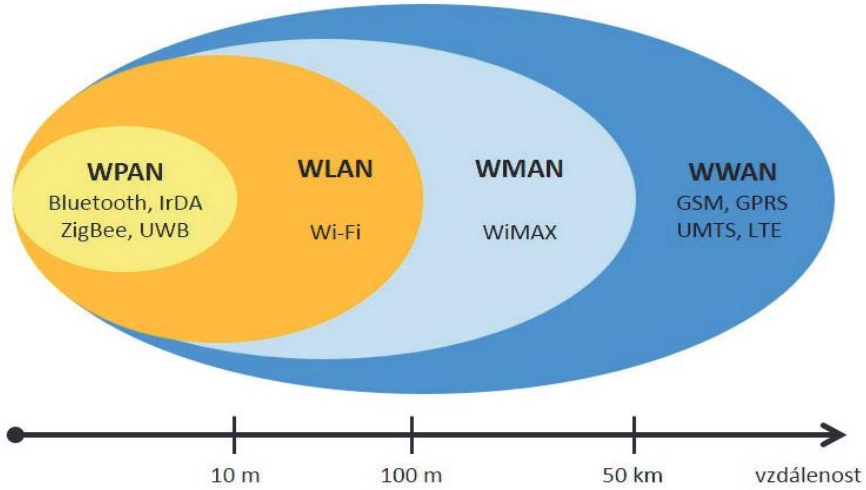
V souvislosti s VLAN je potřeba také zmínit **trunk port**. Jako trunk port je označován právě port sloužící k předávání dat jinému switchi či jinému zařízení. Trunk port k rámcům opouštějícím switch přidává tag, podle kterého následující zařízení pozná, do které VLAN data patří.[64]

[62] MEDICINE, J., *Networking for Beginners: The Complete Guide to Computer Network Basics, Wireless Technology and Network Security*. 2019. s. 76.
[63] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 428.
[64] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 428.

4.5 Bezdrátové sítě

Bezdrátové sítě mohou být rozděleny do čtyř specifických skupin v závislosti na účelu jejich použití a použitelném dosahu signálu: sítě WPAN (Wireless Personal Area Network), sítě WLAN (Wireless Local Area Network), sítě WMAN (Wireless Metropolitan Area Network) a sítě WWAN (Wireless Wide Area Network). Obrázek 6 graficky znázorňuje zmíněné čtyři kategorie a příklady některých technologií užívaných v daném typu sítí.[65]

Obrázek 6 Klasifikace bezdrátových sítí s příklady provozovaných technologií[66]



Bezdrátové sítě obecně nejsou tak bezpečné jako pevné (kabelové) sítě. Pevné sítě na své nejnižší úrovni přenášejí data mezi dvěma body A a B, které jsou fyzicky propojeny síťovým kabelem. Naopak bezdrátové sítě vysílají svá data všemi směry a ke všem zařízením, která mohou toto vysílání zachytit. Omezení je zde pouze v dostupném dosahu. Pevné sítě mohou být účinně zabezpečeny již na svých vstupních rozhraních, například omezením fyzického přístupu k síťovým zařízením a instalací firewallů. Bezdrátová síť je i přes zavedení stejných opatření jako v případě pevné sítě stále náchylná k nelegálnímu odposlechu. Proto bezdrátové sítě vyžadují mnohem propracovanější a důmyslnější přístup k zajištění bezpečnosti svého provozu.[67]

[65] SALAZAR, J. Techpedia – Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.
[66] SALAZAR, J. Techpedia – Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.
[67] SALAZAR, J. Techpedia – Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.

Existují a jsou využívány tři základní typy zabezpečení pro sítě WLAN. Od roku 1990 prošly bezpečnostní algoritmy Wi-Fi sítí několika zásadními upgrady a vylepšeními. Některé původní bezpečnostní algoritmy byly zcela odstraněny, a ty které zůstaly zachovány, jsou dnes výkonnější a z hlediska zabezpečení mnohem efektivnější. V chronologickém pořadí jde o tyto algoritmy:

- metoda WEP (Wired Equivalent Privacy);
- metoda WPA (Wi-Fi Protected Access);
- metoda WPA2 (Wi-Fi Protected Access version 2).[68]

Zaměstnanci, kteří využívají pohodlí bezdrátového připojení k firemní síti (obvykle prostřednictvím notebooku), musí mít své notebooky nakonfigurovány se silným šifrováním, aby se zabránilo úniku dat. Šifrování první generace známé jako WEP bylo snadno dešifrovatelné (prolomitelné) pomocí běžných hackerských nástrojů a již se běžně nepoužívá. Nejnovějším standardem v oblasti bezdrátového ověřování je WPA nebo WPA2 (802.11i), který nabízí silnější šifrování ve srovnání s WEP. Přestože bezdrátové karty v noteboocích mohou nabízet všechny dříve uvedené možnosti, měly by být pokud možno nakonfigurovány s WPA nebo WPA2. Bezdrátové sítě přinesly řadu výhod spočívajících například ve snížení nákladů na budování počítačových sítí, větší mobilitu uživatelů, snadnější a rychlejší připojování nových uživatelů aj. Na druhou stranu je využívání bezdrátových sítí spojeno s novými bezpečnostními riziky.[69]

[68] SALAZAR, J. Techpedia – Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.
[69] VACCA, R. J. *Computer and Information Security Handbook*. 3rd ed. Burlington 2017, s. 286.

4.6 Firewall

Firewall je hardwarový nebo softwarový systém navržený k monitorování a řízení toku dat mezi vaším počítačem nebo sítí a internetem. Jeho hlavním úkolem je filtrovat provoz (Obrázek 7) a rozhodovat, který provoz je povolen a který blokován na základě předem stanovených pravidel a pravidel bezpečnosti.[70]

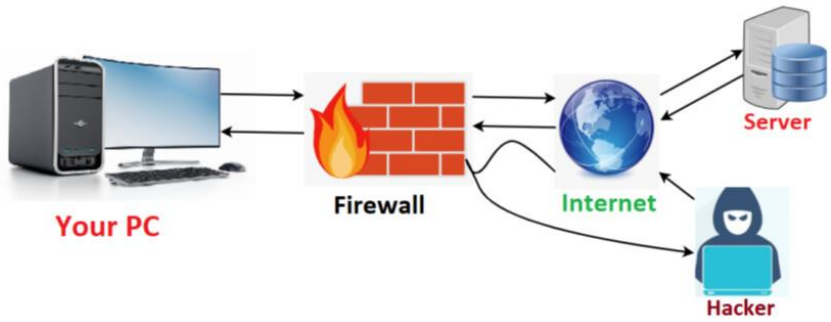
Jak funguje firewall?

Firewall funguje na několika úrovních a může používat různé techniky pro zabezpečení. Zde je několik klíčových způsobů, jakými firewall ochraňuje vaše zařízení:

- **Packet Filtering (Filtrování paketů):** Základní funkce firewallu je filtrování paketů dat na základě určitých kritérií, jako jsou IP adresy nebo porty. Firewall může povolit nebo blokovat pakety na základě těchto kritérií.
- **Stateful Inspection (Stavová kontrola):** Firewall sleduje stav spojení a pamatuje si, které pakety patří do již schválených spojení. Tímto způsobem může detekovat pokusy o vstup do sítě bez povolení.
- **Proxy Server (Proxy server):** Některé firewally pracují jako proxy servery a fungují jako prostředníci mezi vaším počítačem a internetem. Tímto způsobem mohou kontrolovat a filtrovat provoz.
- **Deep Packet Inspection (Hluboká analýza paketů):** Některé moderní firewally jsou schopny provádět hlubokou analýzu paketů a identifikovat potenciálně nebezpečný provoz, včetně malwaru.[71]

[70] WALKER, B., *Computer Networking The Complete Beginner's Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems (Including Cisco, CCENT, and CCNA).* 2019. s. 50.
[71] WALKER, B., *Computer Networking The Complete Beginner's Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems (Including Cisco, CCENT, and CCNA).* 2019. s. 50.

Obrázek 7 Princip Firewallu[72]



Smyslem firewallu je zabránit nechtěné síťové komunikaci mezi dvěma různými zónami, kterými mohou být dvě či více různých počítačových sítí, nebo rozhraní sítě a koncového počítačového systému.

Spolu s firewally jsou součástí i další systémy jako IDS (Intrusion Detection System) a IPS (Intrusion Detection System) prostředí zabezpečení sítě.

- Systém IDS detekuje útok, identifikuje jej pomocí databáze typu útoku, zaregistruje útok a odešle výstrahu IT správci, pokud je škodlivý.
- IPS kontroluje provoz v síti a hledá cokoli podezřelého a brání nebo blokuje pochybné připojení. Poskytuje také výstrahy a čistí škodlivý síťový provoz, aby jej udržel mimo zbytek sítě. Stejně jako IDS sídlí IPS mezi firewallem a zbytkem sítě.[73]

Hlavní rozdíl mezi systémy detekce narušení (IDS) a systémy prevence narušení (IPS) spočívá v tom, že IDS jsou monitorovací systémy a IPS jsou kontrolní systémy. IDS nemění síťový provoz, zatímco IPS brání doručení paketů na základě obsahu paketu, podobně jako brána firewall brání provozu podle IP adresy.[74]

[72] What is firewall ? [online]. [cit. 2023-26-10]. Dostupné z WWW: <https://forumautomation.com/t/what-is-a-firewall/10695#google_vignette>.
[73] ALEXANDROU, A. *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*. 1st ed. 2021, s. 257.
[74] IDS vs. IPS: What is the Difference? [online]. [cit. 2023-26-10]. Dostupné z WWW : <https://www.upguard.com/blog/ids-vs-ips>.

5 Kybernetické útoky

Jirásek a kol. definují kybernetický útok, jako: *„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.“*[75]

Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství, kde je jediným cílem získat informace, či naopak útok DoS, či DDoS, kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem primárně spočívá v otázce zavinění. Jak již bylo uvedeno dříve, kybernetický bezpečnostní incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, případně vyšší mocí. U kybernetického útoku však jde o úmyslné jednání člověka. Na základě výše uvedeného je tedy možné **kybernetický útok** definovat jako **jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.[76]

5.1 Malware

Za **malware** (složenina anglických slov malicious software – škodlivý software), je možné označit jakýkoli software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), či využitý k získání přístupu k počítačovému systému. Malware může mít celou řadu podob, přičemž mnohé druhy malware jsou pojmenovány podle toho, jakou činnost provádějí. Jeden malware je schopen plnit několik funkcí naráz. Může se například sám dále šířit prostřednictvím e-mailů (v rámci přílohy) nebo jako data v P2P (Peer to Peer) sítích a zároveň může získávat například e-mailové adresy z napadeného počítačového systému.

Z historického hlediska existovala nejdříve řada různých termínů pro software, který je v současnosti označován souborným pojmem malware. Vlastní názvy konkrétního škodlivého software vznikaly zpravidla podle činnosti, kterou daný program vykonával. I přes právě uvedené konstatování, že je v současnosti využíván primárně pojem malware, je stále možné se setkat i s historicky starším označením škodlivého software. Jedná se o následující skupiny:

[75]JIRÁSEK, P., NOVAK L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR, 2013, s. 59.
[76] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC z. s. p. o., 2016. s. 55.

- adware;
- spyware;
- viry (viruses);
- červi (worms);
- trojské koně (trojan horses);
- backdoor;
- rootkity;
- keylogger;
- ransomware aj.[77]

5.1.1 Trojský kůň

Vzpomínáte si na případ trojského koně v Tróji? Právě tento koncept je zde zastoupen. Jde jednoduše o situaci, kdy se malware skrývá za legitimním softwarem, aby si našel cestu do systému. Ve skutečnosti může přijít jako e-mail od lidí, které znáte. Po kliknutí na přílohu si malware najde cestu do vašeho počítače.

Jakmile si tento virus najde cestu do vašeho počítače, může ukládat vaše heslo zaznamenáváním různých stisků kláves. Může také ohrozit vaši webovou kameru nebo odnést kopii citlivých dat uložených v systému.[78]

Můžete obdržet nebo stáhnout program, který se tváří jako neškodný obchodní nástroj nebo hra. Pravděpodobnější je, že trojský kůň je pouze skript připojený k neškodně vypadajícímu e-mailu. Když program spustíte nebo otevřete přílohu, provede něco jiného nebo navíc k tomu, co jste si mysleli, že provede. Může provést některou z následujících akcí:

- Stáhne škodlivý software z webové stránky.
- Nainstaluje do počítače program pro záznam kláves nebo jiný špionážní software.
- Smaže soubory.
- Otevře zadní vrátka, která může hacker použít.[79]

[77] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC z. s. p. o., 2016. s. 206.
[78] WALKER, B., *Computer Networking The Complete Beginner's Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems (Including Cisco, CCENT, and CCNA).* 2019. s. 133.
[79] EASTTOM, CH. *Computer Security Fundamentals*. 2019. s. 187.

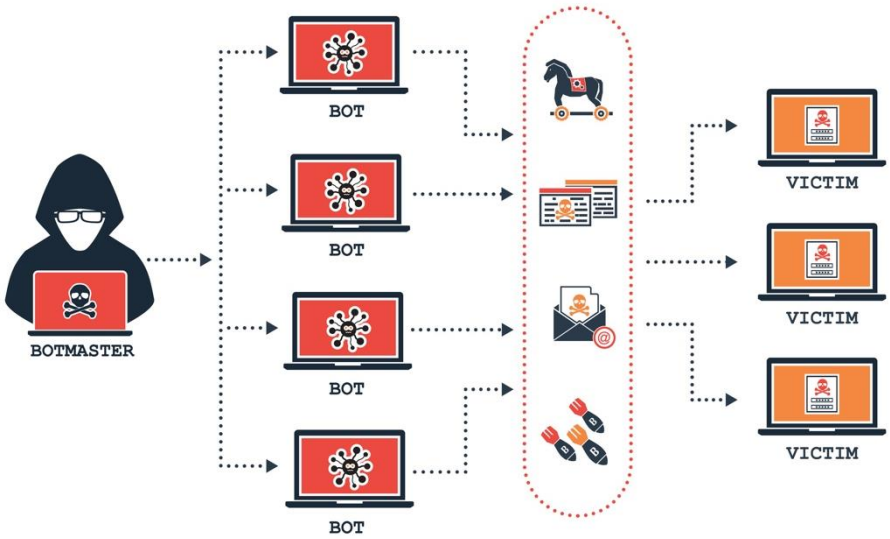
Trojský kůň může být také vytvořen speciálně pro jednotlivce. Pokud by hacker chtěl špehovat určitou osobu, například účetního společnosti, mohl by vytvořit program speciálně tak, aby upoutal pozornost této osoby. Pokud by například věděl, že účetní je vášnivý golfista, mohl by napsat program, který by vypočítal handicap a uvedl nejlepší golfová hřiště.

Tento program by umístil na bezplatný webový server. Poté by poslal e-mail několika lidem, včetně účetního, a informoval by je o bezplatném softwaru. Software by po instalaci mohl zkontrolovat jméno aktuálně přihlášené osoby. Pokud by se přihlášené jméno shodovalo se jménem účetního, mohl by software neznámému uživateli vyjít vstříc a stáhnout key logger nebo jinou monitorovací aplikaci. Pokud by software nepoškozoval soubory nebo se nereplikoval, pak by pravděpodobně zůstal poměrně dlouho neodhalen.[80]

5.1.2 Botnet

Botnet lze jednoduše definovat jako síť softwarově propojených botů, které provádí činnost na základě příkazu „vlastníka“ (resp. správce) této sítě (Obrázek 8). Takto postavená síť může být použita k legální činnosti (např. distribuované výpočty), nebo k činnosti nelegální.[81]

Obrázek 8 Botnet[82]



[80] EASTTOM, CH. *Computer Security Fundamentals*. 2019. s. 187.
[81] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 194.
[82] Botnets – What are they and why do they matter [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://adamlevin.com/2021/08/26/botnets-what-are-they-and-why-do-they-matter/>.

Útoky botnetů se mohou lišit podle metod a nástrojů, které používají. Podívejme se blíže na některé z běžných typů útoků botnetu.

- Útoky typu DDoS (Distributed Denial-of-Service)

Jedním z nejběžnějších typů útoků botnetů je útok DDoS – ten se provádí tak, že boti přetíží server webovým provozem s cílem ho zhroutit. Výpadku v provozu serveru způsobeného boty lze také využít spuštěním dalších útoků botnetu.

- Útoky hrubou silou

Útoky hrubou silou se týkají hackera, který metodou pokus-omyl hádá přihlašovací údaje, šifrovací klíče nebo hledá skryté webové stránky. Tyto útoky jsou prováděny metodou "hrubé síly", což znamená, že používají nadměrné množství pokusů o "násilné" proniknutí do vašich soukromých účtů.[83]

5.1.3 Ransomware

Do skupiny malware se řadí i tzv. vyděračský malware, pro nějž se ustálilo označení **ransomware** (z anglického *„ransom“* – výkupné, někdy také označovaný jako rogueware nebo scareware). Ransomware je malware, který brání či omezuje uživatele v řádném užívání počítačového systému do doby, než dostane útočník zaplaceno „výkupné“. Ransomware se nejčastěji dostane do počítače pomocí malware (trojského koně či červa), který je umístěn na webových stránkách, nebo je přílohou e-mailu. Jakmile je tento malware bezpečně „usídlen“ v počítačovém systému, dojde ke stažení vlastního ransomware.

Obecně je možné rozlišovat dva typy ransomware podle toho, jak moc zasahují do vlastního chodu počítačového systému. **Prvním typem je ransomware, který omezí funkčnost celého počítačového systému** a neumožní uživateli tento systém vůbec využívat (např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky). **Druhým typem pak je ransomware, jenž ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele.** [84]

[83] What is botnet attack ? 5 ways to prevent it [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://securityscorecard.com/blog/what-is-a-botnet-attack>.
[84] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 221.

V současnosti dochází spíše k využívání druhého typu ransomware, který je známý pod označením **crypto-ransomware**. Účelem tohoto malware je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému, přičemž primárně má tento malware za cíl zašifrovat soukromé soubory uživatele jako jsou obrázky, textové či tabulkové dokumenty, videa aj. Po skončení šifrování se zpravidla uživateli zobrazí zpráva, že jeho soubory jsou zašifrovány, a pokud je chce získat zpět (dešifrovat), musí poslat určitý obnos na účet útočníka. K transakcím jsou obvykle využívány virtuální měny jako je Bitcoin nebo různé předplacené služby. Ve většině případů je stanovena časová lhůta pro zaplacení. Po uplynutí této lhůty dochází k smazání klíče, jenž může zašifrované soubory otevřít.[85]

5.1.4 Spam

Definovat spam může být obtížné. Někteří lidé jej chtějí definovat jako nevyžádanou obchodní poštu. To nemusí být úplná definice spamu, protože jsou situace, kdy dostáváme žádané a skutečně žádoucí nevyžádané e-maily a jsme rádi, že je dostáváme. Jiní definují spam jako automatizované komerční e-maily; mnoho nevyžádaných a někdy i automatizovaných e-mailů však nemá komerční charakter. Abychom tedy pokryli všechny tyto aspekty a dosáhli rovnováhy, definujeme spam jako nevyžádané automatické e-maily.

Vzhledem k tomu, že internet je z více než 60 % využíván elektronickou poštou, týká se spamování velkého počtu uživatelů internetu.[86]

Spam je například běžným prostředkem pro šíření virů a červů. Spam se také používá k rozesílání e-mailů lákajících příjemce k návštěvě phishingových webových stránek za účelem krádeže jejich identity. V lepším případě spam obtěžuje, v horším případě je prostředkem pro spyware, viry, červy a phishingové útoky.[87]

Spam využívá různé komunikační kanály k odesílání nevyžádaných zpráv:

- e-mail;
- jiný messenger (ICQ, Skype atp.);
- SMS, MMS;
- diskusní fóra, blogy, sociální sítě, herní platformy aj.[88]

[85] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 221.
[86] KIZZA, J. M. *Guide to computer network Security*. 2020. s. 347.
[87] EASTTOM, CH. *Computer Security Fundamentals*. 2019. s. 200.
[88] KOLOUCH, J. *CyberCrime.* Praha, 2016. s. 232.

Spam může obsahovat informace:

- **obchodní či reklamní;**
- **o zdraví a medicíně** (Tato kategorie obsahuje spam nabízející produkty na snížení váhy, kosmetické přípravky, netradiční medicínu, léky nedostupné v daném regionu aj.);
- **finanční** (Zejména se jedná o nabídky různých půjček, možnosti přivýdělku aj.);
- **pornografické** (Tento spam buď nabízí různé, i farmaceutické přípravky na zvýšení sexuální potence, nebo odkazuje na stránky s pornografickým obsahem.);
- **edukační** (nabídky různých kurzů, tréninků aj.);
- **hoax** (řetězový dopis);
- **politické;**
- **náboženské;**
- **kriminální** (Do této kategorie spadají zprávy obsahující například malware, či odkazující na stránky se škodlivým kódem aj.[89]

5.1.5 Virus

Počítačový virus je program, který se šíří tak, že nejprve infikuje soubory nebo systémové oblasti pevného disku počítače nebo síťového směrovače a poté vytváří své kopie. Některé viry jsou neškodné, jiné mohou poškodit datové soubory a některé mohou soubory zničit. Dříve se viry šířily, když lidé sdíleli diskety a jiná přenosná média, nyní se viry šíří především prostřednictvím e-mailových zpráv.

Na rozdíl od červů vyžadují viry ke svému šíření často nějakou akci uživatele (např. otevření přílohy e-mailu nebo návštěvu škodlivé webové stránky).[90]

- Co viry dělají?

Virus je jednoduše počítačový program – může dělat cokoli, co může dělat jakýkoli jiný program spuštěný na vašem počítači. Některé viry jsou navrženy tak, aby záměrně poškozovaly soubory, jiné se mohou pouze šířit do jiných počítačů.[91]

[89] KOLOUCH, J. *CyberCrime.* Praha, 2016. s. 232.
[90] Virus Basics [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.cisa.gov/news-events/news/virus-basics>.
[91] Virus Basics [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.cisa.gov/news-events/news/virus-basics>.

- Co je to červ?

Červ je typ viru, který se může šířit bez lidské interakce. Červi se často šíří z počítače na počítač a zabírají cennou paměť a šířku pásma sítě, což může způsobit, že počítač přestane reagovat. Červi také mohou útočníkům umožnit získat přístup k počítači na dálku.[92]

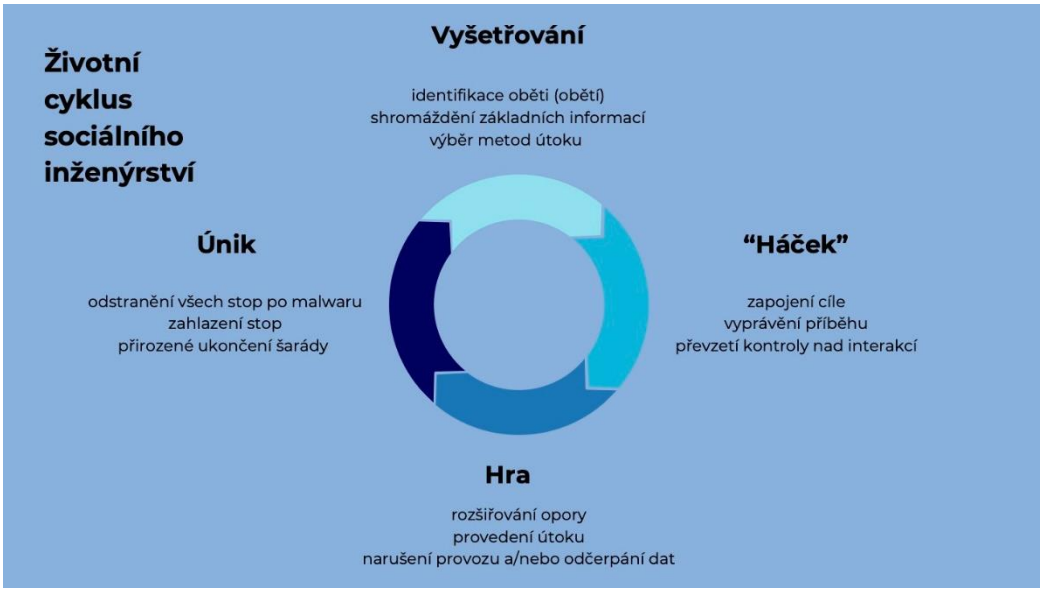
5.2 Sociální inženýrství

Sociální inženýrství je pojem, který si oblast kybernetické bezpečnosti přivlastnila za několik desetiletí. Kdysi tento termín označoval manipulaci společnosti jako celku. Postupem času si komunita kybernetické bezpečnosti tento termín přizpůsobila tak, aby označoval telefonické záminky, kdy útočník volá lidem, aby získal informace usnadňující přístup k počítačům nebo informacím. Zdálo se, že termín pak zahrnuje jakýkoli netechnický útok domnělého hackera. Phishing je nejoblíbenější formou sociálního inženýrství. Vzhledem k jeho širokým kořenům by se však osvětové kampaně o sociálním inženýrství měly podobně skládat ze široké škály témat.[93]

Sociální inženýrství nelze za každých okolností považovat přímo za kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná. Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli (Obrázek 9). Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je. Zjednodušeněji by se dalo říci, že se jedná o „umění klamu“, přičemž Mitnick rozlišuje dvě specializace v povolání umělce-manipulátora. *„Ten kdo mámí z lidí peníze je obyčejný podvodník, zatímco ten kdo využívá manipulace a přesvědčování vůči firmám – obvykle se záměrem získání informací – je sociotechnik.“*[94]

[92] Virus Basics [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.cisa.gov/news-events/news/virus-basics>.
[93] WINKLER, I. *Security awareness for dummies.* John Wiley & Sons. 2022, s. 80.
[94] MITNICK, K., SIMON, W. *Umění klamu*. Gliwice, 2003. s. 6.

Obrázek 9 Cyklus sociálního inženýrství[95]



Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, přičemž tyto způsoby jsou navzájem kombinovány:

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

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:

- **podvodný e-mail či falešná webová stránka;**
- **telefonický hovor;**
- **útok „tváří v tvář";**
- **prohledávání odpadků** („Dumpster diving" a také „cezení dat");
- **prohledávání webu, sociálních sítí aj.** (jedná se o jednoduše dosažitelný otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá zjistit, případně ověřit informace o potenciálním cíli). [96]

[95] Největší hrozby a zranitelnosti kybernetické bezpečnosti: #1 Sociální inženýrství [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://kybez.cz/nejvetsi-hrozby-a-zranitelnosti-kyberneticke-bezpecnosti-1-socialni-inzenyrstvi/>.
[96] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 188.

- **veřejné informace dostupné online** (např. životopisy, práce, teze, návrhy aj. uveřejněné na internetu);
- **výroční zprávy a jiné veřejně dostupné informace o společnosti;**
- **doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči;**
- **ponechání paměťového média** (USB aj.) **v zájmové oblasti** (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware);
- **nabídka vyzkoušení služby online** (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.);
- **dodávka či nalezení zařízení** (počítačového systému),
- **falešný servisní technik;**
- **jiné.** [97]

5.2.1 Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.

V užším slova smyslu phishing představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (zobrazující např. webovou stránku internetového bankovnictví, online obchodu aj.) a následné vyplnění „přihlašovacích informací“, případně jsou tyto informace vyžadovány přímo (např. při vyplnění formuláře aj.).

V širším slova smyslu se za phishing dá označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem. V tomto širším slova smyslu již není po uživateli požadováno vyplňování údajů, avšak je mu doručena zpráva (či je uživatel přesměrován na stránku) typicky obsahující malware, který si uvedené údaje posbírá sám. Dále do tohoto širšího pojetí mohou být zařazeny i dárcovské scamy atp.

V obou dvou případech dochází k oklamání uživatele, který je cílem phishingového útoku, rozdíl spočívá především v tom, jaká míra interakce je po uživateli vyžadována.[98]

[97] KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha, 2019, s. 188.
[98] Google says the best phishing scams have a 45 percent success rate. [online]. [cit. 2023-26-10]. Dostupné z: WWW: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>.

Podstatou phishingu je využívání sociálního inženýrství. Phishing je možné provádět i ve světě reálném (viz podvody aj.), avšak svět virtuální umožňuje útočníkovi rozesílat podvodné zprávy obrovskému množství potenciálních obětí s minimem námahy. Phishing je, se značnou mírou nadsázky, možné přirovnat ke „kobercovému bombardování." Stejně jako v případě bombardování phishing cílí na relativně neurčené množství obětí proto, aby měl útočník naději na úspěch. Google např. v roce 2014 uváděl, že scam mající povahu skutečně dobrého phishingu je při zisku dat o uživatelích úspěšný z 45 %.[99]

Spear phishing je phishingový útok, který se zaměřuje na konkrétní osobu - obvykle na osobu, která má privilegovaný přístup k citlivým datům nebo síťovým zdrojům nebo zvláštní oprávnění, které může podvodník využít k podvodným nebo nekalým účelům.

Spear phisher studuje cíl, aby získal informace potřebné k tomu, aby se mohl vydávat za osobu nebo subjekt, kterému cíl skutečně důvěřuje - přítele, šéfa, spolupracovníka, kolegu, důvěryhodného dodavatele nebo finanční instituci – nebo aby se mohl vydávat za cílovou osobu. Sociální média a sociální sítě – kde lidé veřejně blahopřejí spolupracovníkům, podporují kolegy a dodavatele a mají tendenci se dělit o schůzky, události nebo cestovní plány – se staly bohatým zdrojem informací pro výzkum spear phishingu.[100]

[99] Google says the best phishing scams have a 45 percent success rate. [online]. [cit. 2023-26-10]. Dostupné z: WWW: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>.

[100] What is a phishing attack? [online]. [cit. 2023-25-10]. Dostupné z WWW: < https://www.ibm.com/topics/phishing >.

6 Informační systémy Armády České republiky a Úřadu práce

6.1 Informační systémy Armády České republiky

V současné době je v rámci Ministerstva obrany a v Armádě České republiky využíváno více jak 10 informačních systémů, z nichž každý plní jinou funkci, avšak jejich obsahem je velké množství citlivých dat, které mohou být při jejich kompromitaci zneužity.

Příkladem jsou systémy:

- ŠIS – Štábní informační systém;
- ISL – Informační systém logistiky;
- IMO – Internet Ministerstva obrany;
- FIS – Finanční informační systém;
- ISSP – Informační systém služby a personálu;
- ZdravIS – Zdravotnický informační systém;
- OTS VŘ PozS – Operačně taktický systém velení a řízení pozemních sil.[101]

6.1.1 Štábní informační systém

Štábní informační systém (ŠIS) patří mezi nejvyužívanější informační systém v AČR vůbec. Jedná se o informační systém určený k podpoře každodenních činností velitelů a štábů. Účelem tohoto systému je podpora procesů velení, plánování a řízení. V rámci celého resortu Ministerstva obrany je ŠIS integrujícím prvkem systémů elektronické pošty. Kybernetická bezpečnost ŠIS je zajištěna výhradně příslušníky MO.

V rámci Štábního informačního systému je k dispozici tzv. Portál podpory uživatele, včetně vzdálené podpory HELPDESK, kde uživatel nalezne informace týkající se řešení běžných problémů v rámci ŠIS. V případě, že se jedná o problém, který není schopen uživatel vyřešit samostatně, lze vytvořit požadavek, který si převezme provozní správa ŠIS, která je schopna problém vzdáleným přístupem vyřešit.[102]

[101] Katalog 2007 [online]. [cit. 2023-25-10]. Dostupné z WWW: < https://www.army.cz/assets/files/9369/KATALOG_2007_part_4.pdf >.
[102] Katalog 2007 [online]. [cit. 2023-25-10]. Dostupné z WWW: < https://www.army.cz/assets/files/9369/KATALOG_2007_part_4.pdf >.

6.1.2 Internet Ministerstva obrany

Internet Ministerstva obrany (IMO) je služba, která příslušníkům MO zajišťuje přístup do celosvětové sítě Internet. IMO je určen k podpoře činností pracovníků, kteří v rámci své pracovní náplně potřebují získávat informace z veřejných zdrojů. Přístup do této sítě je možný pouze s využitím proxy serveru, který funguje jako filtr a blokuje přístup k určitým webovým stránkám.[103]

6.2 Informační systémy Úřadu práce

V roce 1993 dodala informační systém ministerstvu firma OKsystem a postupně vznikaly tyto systémy: [104]

- Portál MPSV (Ministerstva práce a sociálních věcí) – propojený se službou EURES (European Employment Services);
- OKdávky – výplata sociílních dávek (Informační systém na výplaty dávek měsíčně vyplácí cca 1,9 milionů dávek v objemu více než 6 miliard korun a pracuje s ním čtyři tisíce úředníků;
- OKpráce – pracovní příležitosti;
- OKnouze/OKslužby – systémy pomoci v hmotné nouzi a sociálních služeb;
- OKmzdy – zpracování mzdové agendy;
- Podání PVS – elektronické podání evidenčních listů;
- OKbase – správa lidských zdrojů;
- OKsmart – integrace kryptografických čipových karet do MS Windows. [105]

[103] Katalog 2007 [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.army.cz/assets/files/9369/KATALOG_2007_part_4.pdf>.
[104] Jednotný informační systém práce a sociálních věcí. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://cs.wikipedia.org/wiki/Jednotný_informační_systém_práce_a_sociálních_věcí>.
[105] Úřady práce nesmí používat IT systém, kvůli kterému obvinili Šišku. [online]. [cit. 2023-25-10]. Dostupné z WWW: <[https://zpravy.idnes.cz/ministerstvo-vnitra-dostalo-pulmilionovou-pokutu-za-chyby-v-it-zakazce-1qi-/domaci.aspx?c=A131218_185921_domaci_aha>.

Do konce roku 2011 výplata dávek vycházela z organizační struktury MPSV tvořené 77 úřady a 240 lokálními pracovišti. Každému lokálnímu pracovišti odpovídala jedna lokální databáze, přičemž jednotlivá lokální pracoviště byla propojena pomocí sítě WAN, data z lokálních databází byla sehrávána na nadřízená pracoviště (okres, následně kraj) a ukládána v datových centrech ve vlastnictví MPSV.[106]

Od července 2011 MPSV postupně přešlo na centralizovaný provoz v privátním cloudu a s tím související změnu topologie sítě WAN. Součástí dodávky byly i nové aplikace:

- Zaměstnanost;
- veřejná služba;
- zdravotně postižené osoby;
- sociální služby;
- hmotná nouze;
- elektronická spisová služba Athena. Ta k žádosti o výplatu dávky přiřadila spisovou značku, která je potřebná ke schválení žádosti a následné výplatě příslušné dávky.

Dávky pro státní sociální podporu měly být i nadále podporovány aplikacemi OKdávky a OKcentrum.[107]

[106] Analýza a vyhodnocení vynakládání finančních prostředků do Agendových systémů MPSV v letech 1993–2011. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.mpsv.cz/documents/20142/974645/Analyza_a_vyhodnoceni.pdf/e68e2516-1347-aa00-d3c8-a5ceb6bbcf4e>.

[107] Tisková zpráva Nejvyššího kontrolního úřadu. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.nku.cz/cz/pro-media/tiskove-zpravy/mpsv-podepsalo-osm-dodatku-ke-smlouve--navysilo-tak-cenu-systemu-pro-vyplatu-davek-o-1-5-miliardy-korun-id4808/>.

7 Dotazníkové šetření

7.1 Struktura dotazníkového šetření

Dotazník se skládá z 18 otázek. Z celkových 18 otázek jsou 4 otázky s výběrem z více možností.

7.1.1 Otázka 1-3

První 3 otázky slouží pro identifikaci respondenta, který vyplňuje dotazníkové šetření.

7.1.2 Otázka 4

Otázka č. 4 zjišťuje kolik času respondenti tráví na internetu.

7.1.3 Otázka 5

Otázka č. 5 se zaměřuje na provádění záloh, jak často a zda vůbec uživatelé zálohují.

7.1.4 Otázka 6

Otázka č. 6 zkoumá, jak často si respondent mění hesla u internetových účtů jako je e-mail, sociální sítě a internetové bankovnictví. Odpovědi byly – 1-4x za rok, méně než jednou ročně nebo případně, že ho nemění nikdy.

7.1.5 Otázka 7

Otázka č. 7 se zabývá také hesly, tentokrát ale zda respondenti mají odlišná hesla u svých internetových účtů. Varianty odpovědí byly – Ano, Jen u některých a Ne.

7.1.6 Otázka 8

V otázce č. 8 bylo zjišťováno, jaké heslo je podle nich dostatečně silné, u této otázky bylo možné vybrat více odpovědí pro případ, že by se jim zdálo dostatečně silné více než 1 heslo. Bylo možné vybrat z následujících odpovědí: Bety159, amalkazlaticko258, 123456, heslo1 a $laN@nink2_dOZe1í.

7.1.7 Otázka 9

V 9. otázce jsem chtěl otestovat s jakou ostražitostí kontrolují název odesílatele elektronické pošty, tudíž zda info@ceskasporitlena.cz je důvěryhodná.

7.1.8 Otázka 10

Otázka č. 10 zjišťovala, zda respondenti používají dvoufaktorové ověřování u jejich internetových účtů.

7.1.9 Otázka 11

U otázky č. 11 bylo dotazováno, zda používají služební výpočetní techniku pouze ke služebním záležitostem. Na výběr měli jednu z odpovědí – Ano, Občas si něco vytisknu, Používám ji i na internet pro osobní účely a poslední možnost byla – Ne, beru si ji i domu.

7.1.10 Otázka 12

Otázka č.12 zjišťuje, zda respondenti vnímají kybernetickou bezpečnost jako aktuální problém.

7.1.11 Otázka 13

U otázky č. 13, která se dotazuje, zda byl respondent někdy obětí kybernetického útoku je možnost více odpovědí. Na výběr má z těchto odpovědí : Ne, Nevím, Phishingem, Malwarem, DDoS útokem, Spamem, Ransomwarem, Jiné.

7.1.12 Otázka 14

Otázka č.14 zjišťuje použití obranných softwarů a má také více možných odpovědí v případě použití jejich kombinací. Odpovědi byly – Freeware antivirus, Antivirus s placenou licencí, Virtual Private Network (VPN), Jiné a Žádné.

7.1.13 Otázka 15

Otázka č.15 má možnost více odpovědí abych co nejlépe mohl zjistit jestli a případně jak se respondenti připojují k veřejným Wi-Fi sítí. Bylo možno vybrat tyto odpovědi – Ano, Ano, ale pouze pokud mi dojdou mobilní data, Ano, ale nezadávám citlivé údaje, Ano, ale používám VPN nebo poslední možnost Ne.

7.1.14 Otázka 16

16. otázka zkoumá jaký zámek používají na svých mobilních telefonech. Odpovědi byly – Žádný, Odemčení gestem, Odemčení otiskem prstu nebo skenem obličeje, Odemčení heslem, Jiné.

7.1.15 Otázka 17

Předposlední otázka směřuje na aktualizování aplikací v mobilu, možnost odpovědi byla – Ano, mám zapnuté aktualizace, Pouze když si vzpomenu, Nevím jak na to, Ne.

7.1.16 Otázka 18

U poslední otázky zjišťuji, jestli a jak často probíhají v zaměstnání školení na téma kybernetické bezpečnosti. Výběr byl z odpovědí – Ano, čtvrtletně, Ano, 1-2x ročně, Pouze 1x za několik let, Ne.

7.2 Cíle a hypotézy výzkumu

Hlavním cílem výzkumu bylo zjistit, v jakým rozsahu jsou pracovníci veřejného sektoru obeznámeni s problematikou kybernetické bezpečnosti. Výzkum byl zvolen na základě dotazníkového šetření. Dále byly sestaveny dvě hypotézy, které se na základě výsledků potvrdí či vyvrátí.

Stanovené hypotézy:

H1: Více jak 75% respondentů dokáže rozpoznat podvodný e-mail.

H2: Více jak 50% respondentů si mění heslo alespoň 1x za rok.

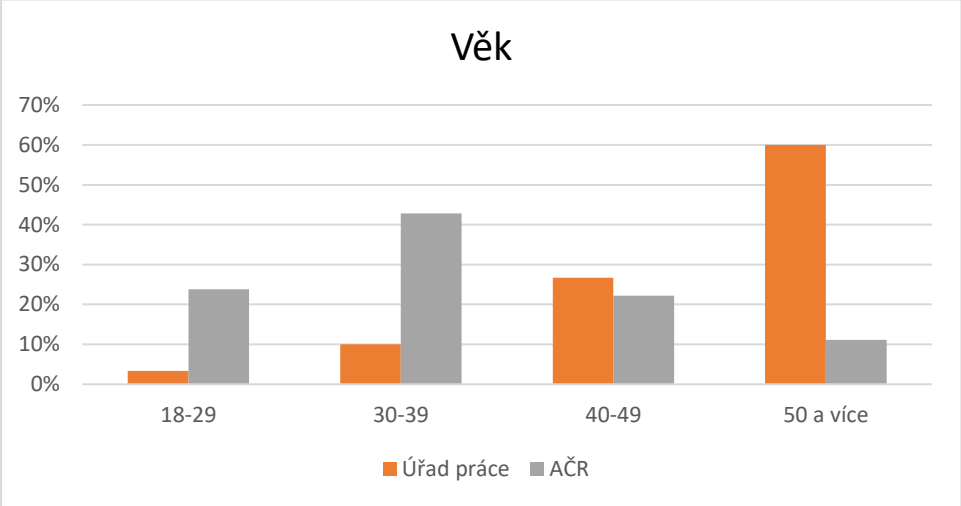
7.3 Interpretace výsledků dotazníku

V této podkapitole jsou uvedeny výsledky zkoumání, pro lepší přehlednost jsou znázorněny graficky v podobě grafů.

Otázka 1: Věk

Dotazníkového šetření se zúčastnilo 17 % respondentů ve věku 18-29, 32 % ve věku 30-39, 24 % ve věku 40-49 a 27 % ve věku 50 a více. AČR měla největší zastoupení ve věku 30-39 (43 %) zatímco Úřad práce měl největší zastoupení ve věku 50 a více (60 %).

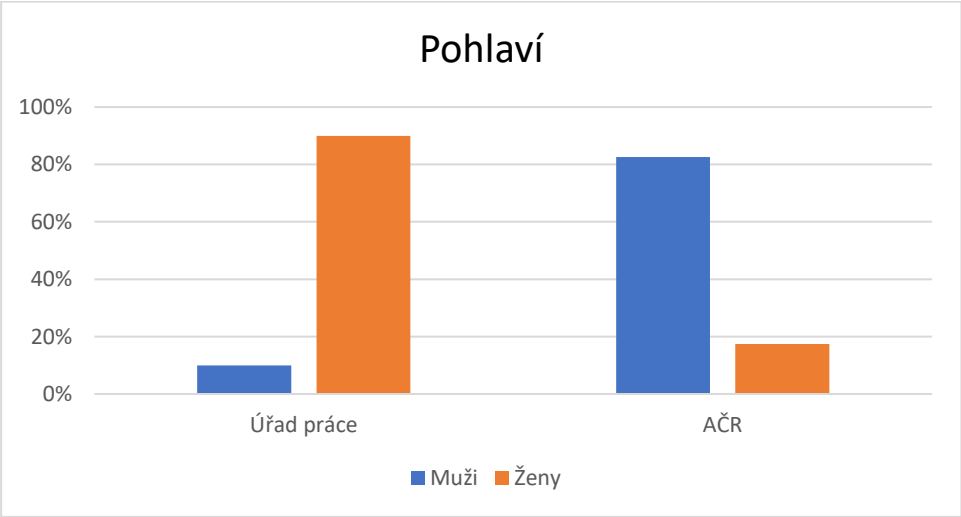
Graf 1 Věk[108]



Otázka 2: Pohlaví

Otázka zobrazuje, jaký byl poměr můžu a žen. V celkovém součtu bylo 59 % mužů a 41 % žen, přičemž u samotného Úřadu práce bylo zastoupení žen 90 %, u AČR bylo zastoupení 83 % muži.

Graf 2 Pohlaví[109]

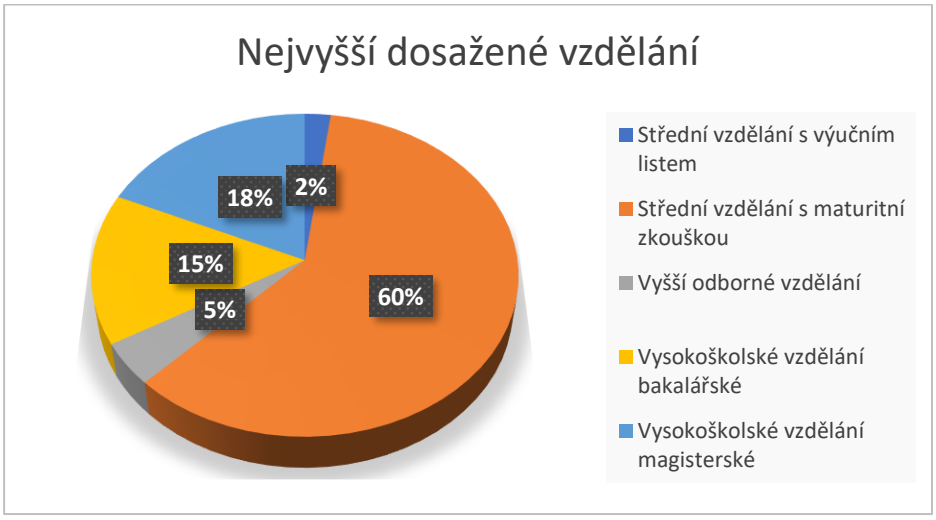


[108] *Vlastní zdroj*
[109] *Vlastní zdroj*

Otázka 3: Nejvyšší dosažené vzdělání

Tato otázka zjišťovala nejvyšší dosažené vzdělání u jednotlivých respondentů. U středního vzdělání s výučním listem bylo zastoupení pouze ve 2 %, nejvyšší podíl mělo střední vzdělání s maturitní zkouškou a to se 60 %, dále Vyšší odborné vzdělání mělo pouze 5 %. Bakalářské vzdělání měla 15 % a Magisterské 18 % respondentů.

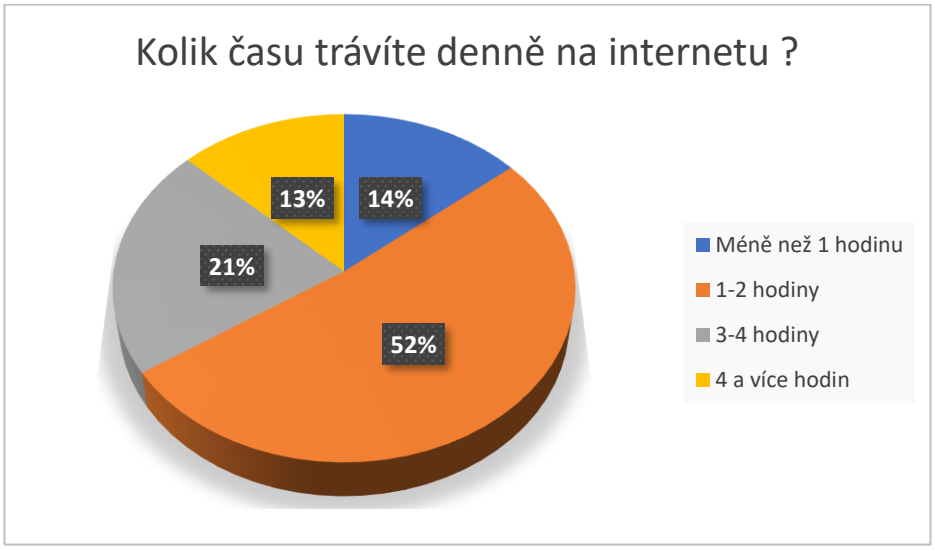
Graf 3 Nejvyšší dosažené vzdělání[110]



Otázka 4: Kolik času trávíte denně na internetu?

Otázka zjišťuje kolik času respondenti tráví denně na internetu. 14 % respondentů méně než hodinu denně, 52 % 1-2 hodiny denně, 21 % 3-4 hodiny denně a 4 a více hodin tráví na internetu 13 % respondentů.

Graf 4 Čas na internetu[111]

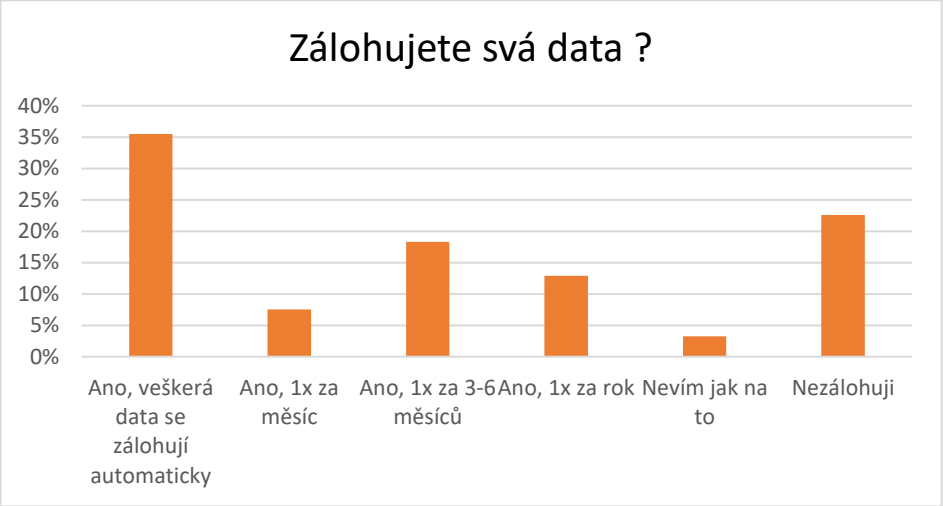


[110] *Vlastní zdroj*
[111] *Vlastní zdroj*

Otázka 5: Zálohujete svá data?

Tato otázka zjišťuje, jak jsou na tom respondenti se zálohováním. 35 % má nastaveny zálohy automaticky, 8 % zálohuje 1x za měsíc, 18 % zálohuje 1x za 3-6 měsíců, 13 % zálohuje 1x za rok, 3 % nevědí jak na to a zálohy neprovádí více než 23 %.

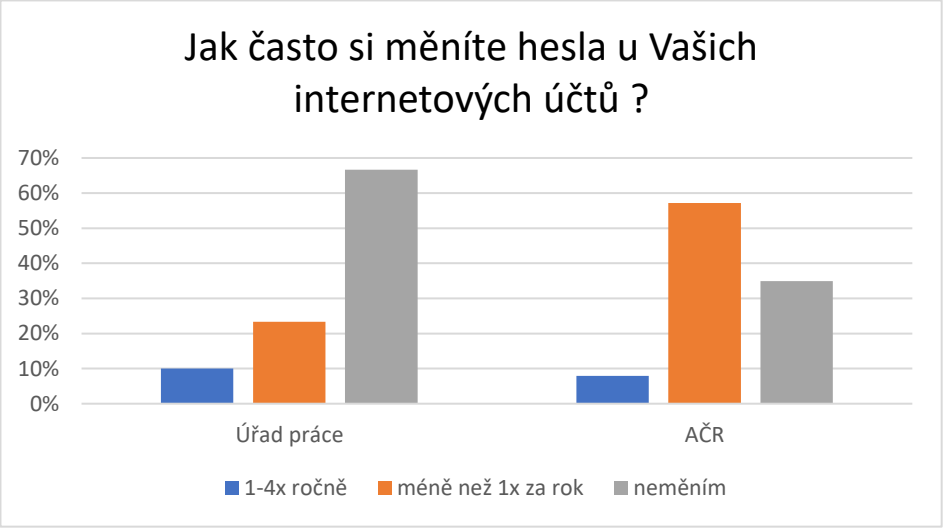
Graf 5 Zálohování[112]



Otázka 6: Jak často si měníte hesla u Vašich internetových účtů?

Na grafu níže můžeme vidět alarmující výsledky, především u Úřadu práce, kde pouze 10 % respondentů si mění hesla 1-4x ročně, 23 % si je mění méně než 1x za rok, a 67 % si hesla **nemění vůbec**. U AČR jsou výsledky o něco lepší – 8 % si hesla mění 1-4x ročně, 57 % si je mění méně než 1x za rok a 35 % si je nemění vůbec.

Graf 6 Změna hesla[113]



[112] *Vlastní zdroj*
[113] *Vlastní zdroj*

Otázka 7: Používáte odlišná hesla ke všem svým internetovým účtům?

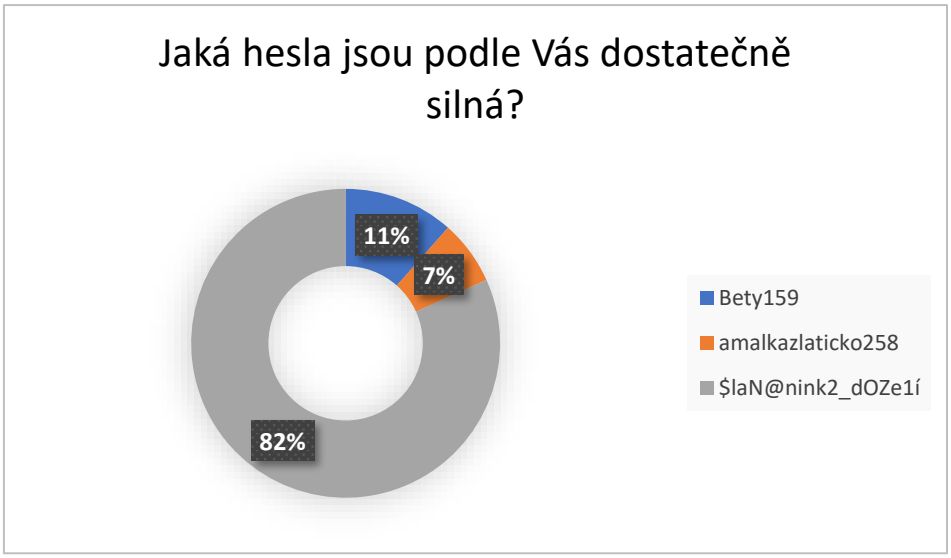
Tato otázka navazuje na předešlý graf a dotazuje se, zda respondenti používají odlišná hesla ke všem internetovým účtům. 31 % odpovědělo, že ano, 56 % pouze u některých služeb a 13 % má heslo všude stejné.

Graf 7 Odlišná hesla[114]

Otázka 8: Jaká hesla jsou podle Vás dostatečně silná?

Otázka pokračuje v dotazování ohledně hesel. Tentokrát zjišťovala, jaké z hesel přijde respondentům dostatečně silné. Na výběr bylo z těchto hesel: Bety159 (11 %), amalkazlaticko258 (7 %), 123456 (0 %), heslo1 (0 %) a $laN@nink2_dOZe1Í(82 %).

Graf 8 Silná hesla[115]

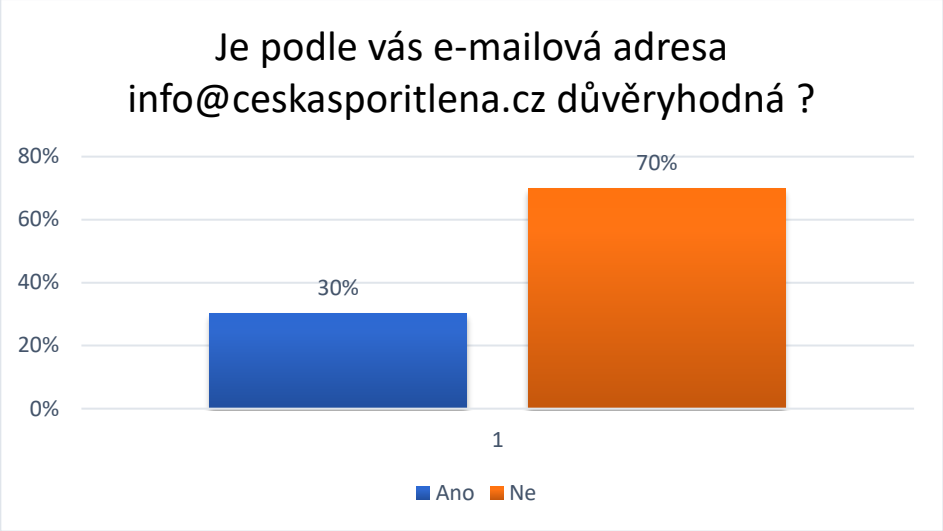


[114] *Vlastní zdroj*
[115] *Vlastní zdroj*

Otázka 9: Je podle vás e-mailová adresa info@ceskasporitlena.cz důvěryhodná?

Otázka zjišťovala, zda podle respondentů je e-mailová adresa info@ceskasporitlena.cz důvěryhodná. 30 % odpovědělo že Ano, 70 % odpovědělo Ne.

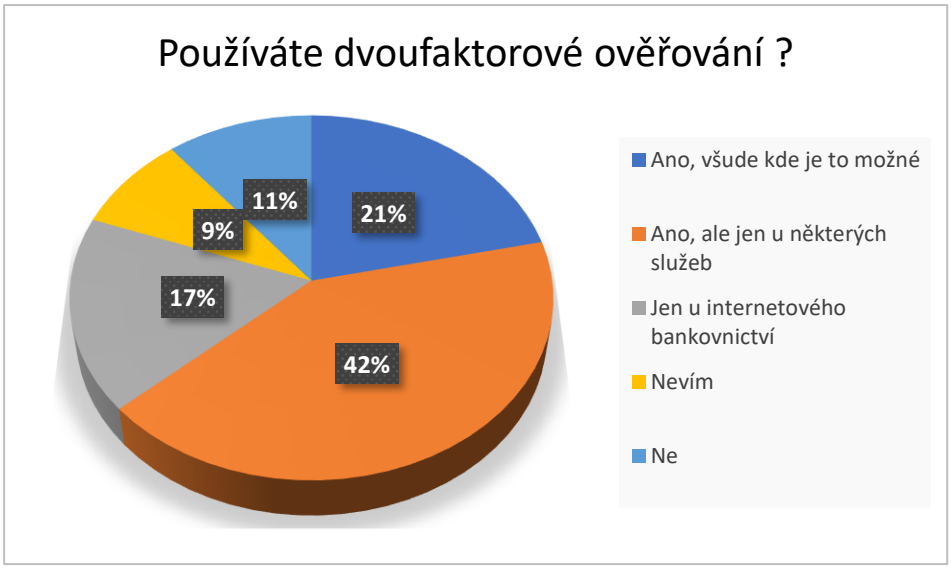
Graf 9 Důvěryhodný e-mail[116]



Otázka 10: Používáte dvoufaktorové ověřování?

Otázka se dotazuje, jestli a případně v jakém rozsahu respondenti používají dvoufaktorové ověřování. Na výběr bylo z těchto odpovědí – Ano, všude kde je to možné (21 %), Ano, ale jen u některých služeb (42 %), Pouze u internetového bankovnictví (17 %), Nevím (9 %) a Ne (11 %).

Graf 10 Dvoufaktorové ověřování[117]

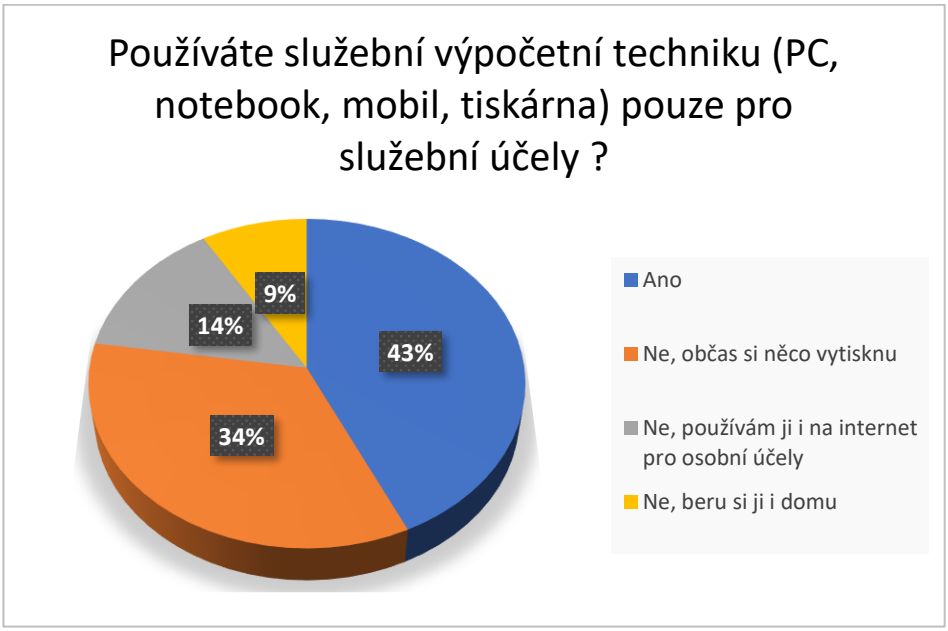


[116] *Vlastní zdroj*
[117] *Vlastní zdroj*

Otázka 11: Používáte služební výpočetní techniku (PC, notebook, mobil, tiskárna) pouze pro služební účely?

Otázka zjišťuje, zda respondenti používají služební výpočetní techniku pouze na služební účely, nebo jestli ji používají i pro osobní účely. Odpovědi byly Ano (43 %), Ne, občas si něco vytisknu (34 %), Ne, používám ji i na internet pro osobní účely (14 %) a Ne, beru si ji domu (9 %).

Graf 11 Služební výpočetní technika[118]

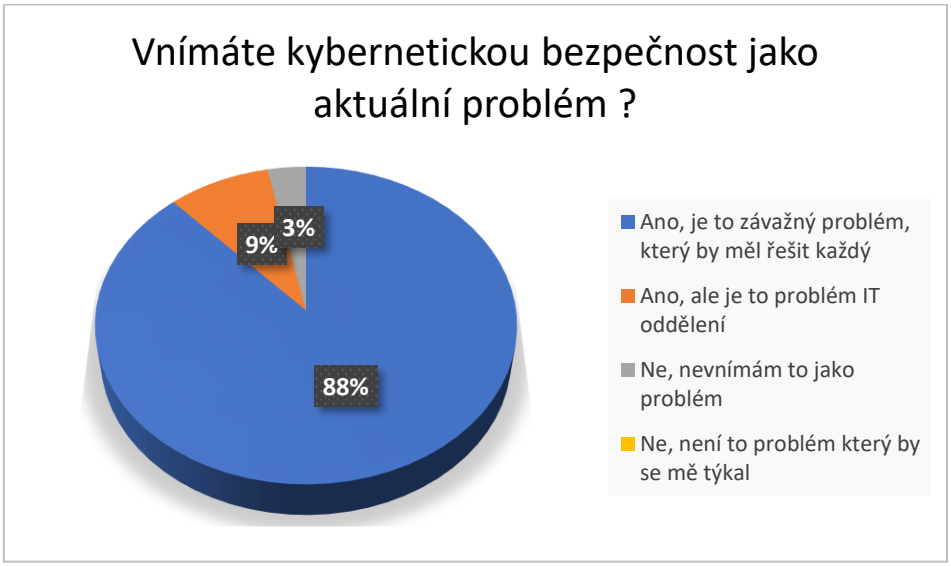


[118] *Vlastní zdroj*

Otázka 12: Vnímáte kybernetickou bezpečnost jako aktuální problém?

Tato otázka zjišťuje, jestli respondenti vnímají kybernetickou bezpečnost jako aktuální problém. 88 % vybralo odpověď, že je to závažný problém, který by měl řešit každý, 9 % že je to problém IT oddělení, 3 % to nevnímají jako problém, odpověď „Ne, není to problém který by se mě týkal“ nebyla vybrána ani jednou.

Graf 12 Vnímání kybernetické bezpečnosti[119]

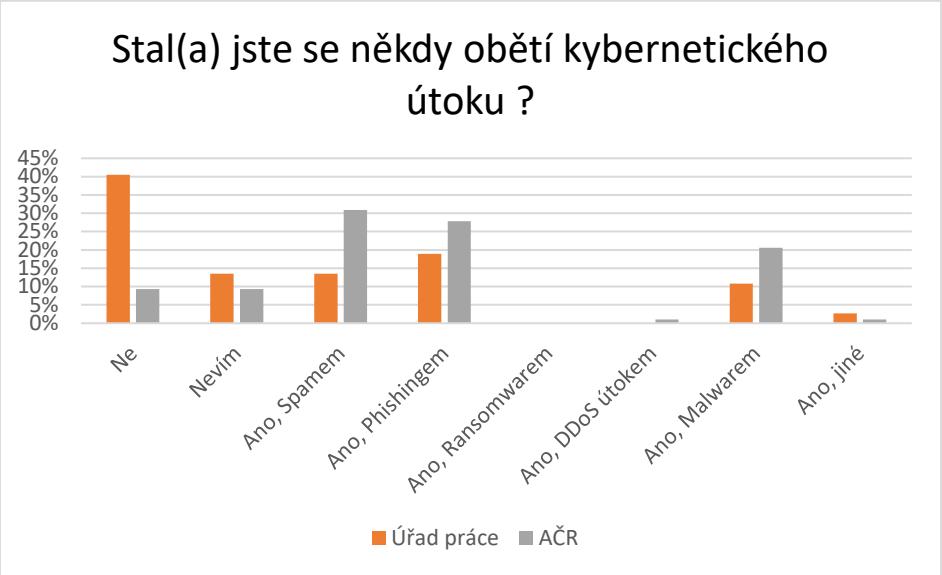


[119] *Vlastní zdroj*

Otázka 13: Stal(a) jste se někdy obětí kybernetického útoku?

Největší rozdíl můžeme vidět u první odpovědi – Úřad práce odpověděl, že 41 % respondentů se nikdy nestala obětí kybernetického útoku, zatímco respondenti z AČR odpověděli, že pouze 9 % se nestalo obětí. U odpovědí Nevím odpovědělo 14 % respondentů z ÚP a 9 % z AČR. Nejčastěji byli napadeni spamem, phishingem a malwarem, v součtu 70 % respondentů z AČR a 44 % z ÚP.

Graf 13 Oběti kybernetické bezpečnosti[120]

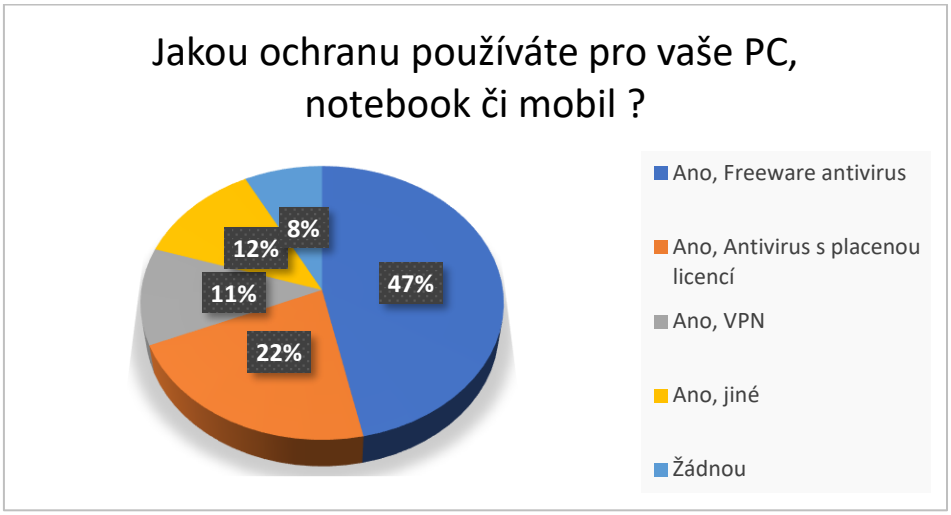


[120] *Vlastní zdroj*

Otázka 14: Jakou ochranu používáte pro vaše PC, notebook či mobil?

Otázka se dotazuje, jakou ochranu respondenti používají pro jejich PC, notebook či mobil. 47 % používá freeware antivirus (neplacená verze), 22 % antivirus s placenou licencí, 11 % používá virtuální privátní síť (VPN), 12 % používají jinou ochranu, než byla uvedena a 8 % nepoužívá žádnou.

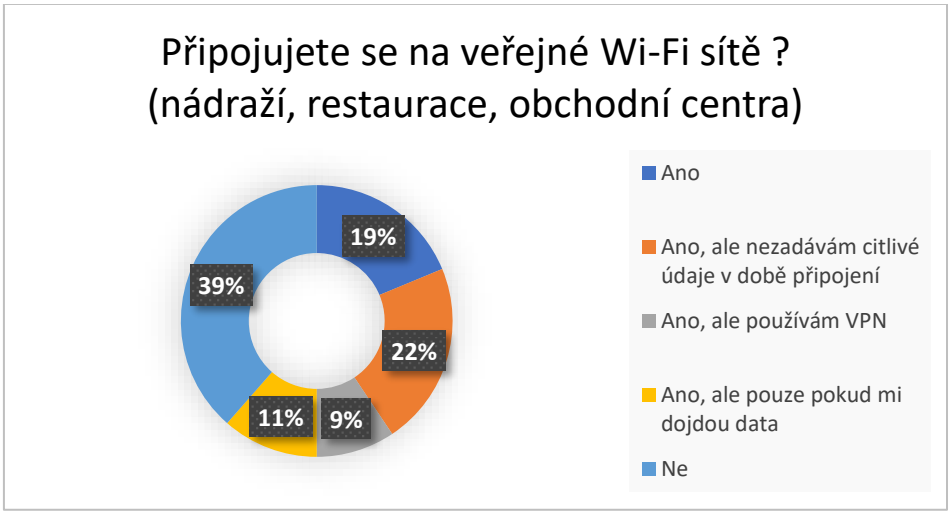
Graf 14 Ochrana PC[121]



Otázka 15: Připojujete se na veřejné Wi-Fi sítě? (nádraží, restaurace, obchodní centra,...)

Na otázku 19 % odpovědělo Ano, 22 % se připojuje, ale nezadává citlivé údaje v době připojení, 9 % se připojuje, ale používají VPN, 11 % se připojuje pouze pokud jim dojdou data a 39 % se nepřipojuje vůbec.

Graf 15 Veřejné Wi-Fi sítě[122]

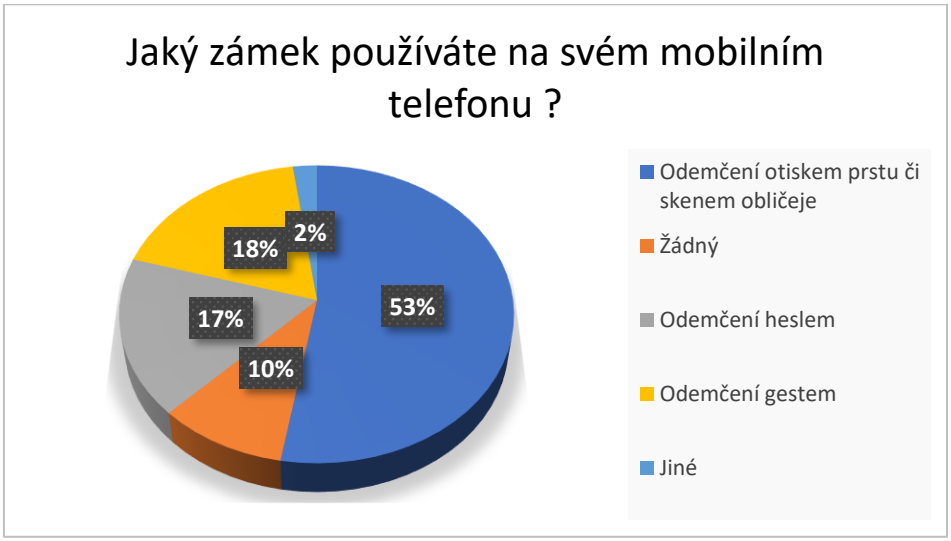


[121] *Vlastní zdroj*
[122] *Vlastní zdroj*

Otázka 16: Jaký zámek používáte na svém mobilním telefonu?

Otázka se dotazuje respondentů, jaký zámek používají na svém mobilním telefonu. 53 % odemykají mobil otiskem prstu či skenem obličeje, 10 % nepoužívá žádné heslo, 17 % odemykají heslem, 18 % odemyká gestem a 2 % odemykají jiným způsobem.

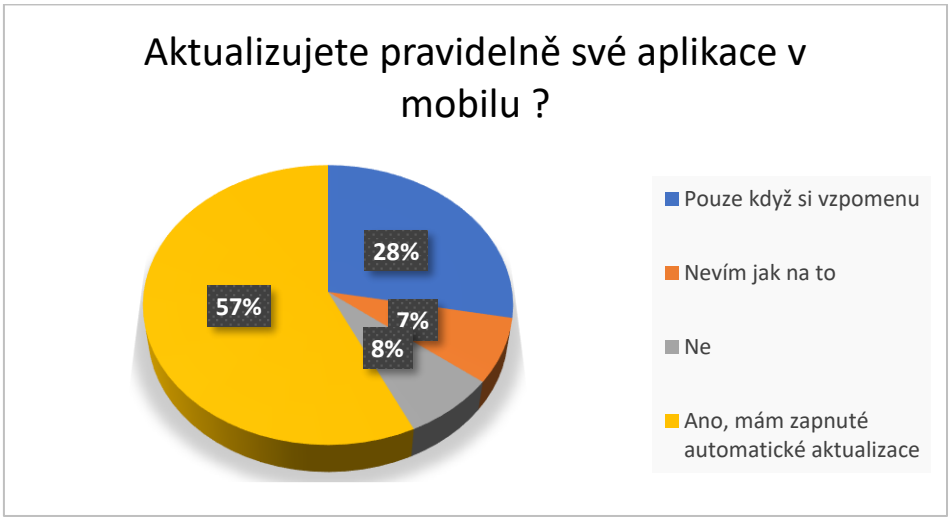
Graf 16 Zámek mobilního telefonu[123]



Otázka 17: Aktualizujete pravidelně své aplikace v mobilu?

Otázka navazuje na předešlou otázku. Tentokrát směřuje na pravidelné aktualizování aplikací v mobilu. 28 % odpovědělo, že aktualizují pouze když si vzpomenou. 7 % neví jak aplikace aktualizovat, 8 % aplikace neaktualizuje a 57 % má zapnuté automatické aktualizace.

Graf 17 Aktualizování mobilních aplikací[124]

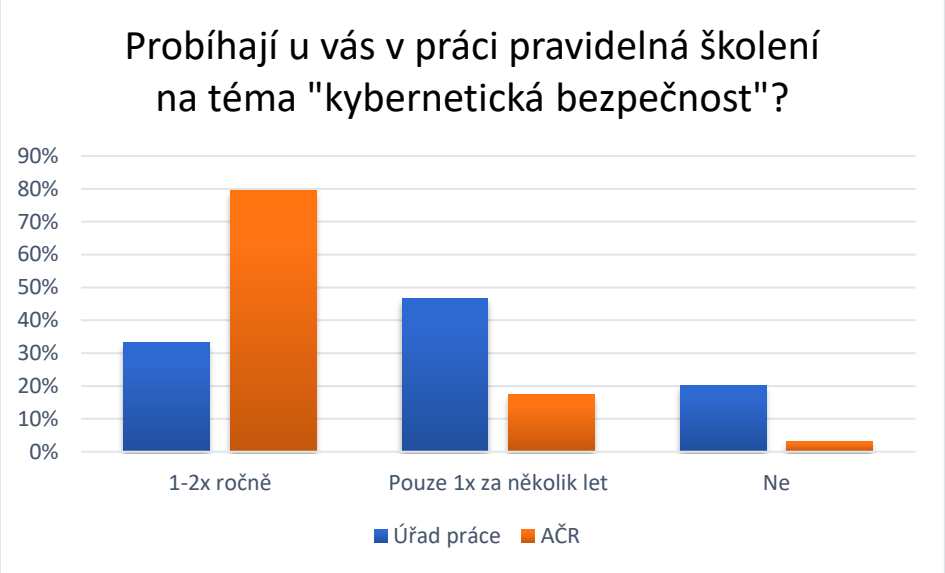


[123] *Vlastní zdroj*
[124] *Vlastní zdroj*

Otázka 18: Probíhají u Vás v práci pravidelná školení na téma "kybernetická bezpečnost"?

Otázka zjišťovala, jak je to se školením uživatelů a zda probíhají v zaměstnání pravidelné školení na téma kybernetické bezpečnosti. Zatímco u AČR odpovědělo 79 % respondentů, žeže probíhají 1-2× ročně, u ÚP takto odpovědělo pouze 33 %, u odpovědi Pouze 1× za několik let odpovědělo 47 % respondentů z ÚP a 17 % z AČR. 20 % respondentů z ÚP odpovědělo, že školení neprobíhají vůbec, tuto odpověď z AČR mělo pouze 3 %.

Graf 18 Školení kybernetické bezpečnosti[125]



7.4 Výsledky hypotéz

Stanovenou hypotézu č. 1: „Více jak 75 % respondentů dokáže rozpoznat podvodný e-mail." zjišťuje otázka č. 9. Tato hypotéza se vyvrátila.

Stanovenou hypotézu č. 2: „ Více jak 50 % respondentů si mění heslo alespoň 1x za rok" zjišťuje otázka č. 6. Tato hypotéza se potvrdila jen u AČR.

[125] *Vlastní zdroj*

7.5 Navržené opatření

Na základě výsledků dotazníkového šetření a zjištěných informací týkajících se zastoupení respondentů, jejich návyků a postojů ke kybernetické bezpečnosti, lze doporučit následující kroky pro zlepšení bezpečnosti:

Cílená vzdělávací opatření:

- Vzhledem k rozdílným návykům a povědomí o kybernetické bezpečnosti u různých věkových skupin je vhodné nabízet cílená školení, které budou specifické pro potřeby každé skupiny;
- doporučuji navýšit frekvenci a důraz školení na kybernetickou bezpečnost u Úřadu práce, kde je nižší povědomí o této problematice;
- vytváření pravidelného školení pro zaměstnance na téma kybernetické bezpečnosti, zejména ve služebním prostředí;
- zvýšení povědomí v oblasti kybernetické bezpečnosti: v rámci školení zdůraznit, že kybernetická bezpečnost je důležitá, protože chrání osobní a firemní data, zabrání finančním ztrátám, udržuje důvěru veřejnosti v online služby, zabezpečuje kritickou infrastrukturu a pomáhá prevenci kyberkriminality.

Hesla a autentizace:

- Pravidelná změna hesel má několik důležitých aspektů v oblasti kybernetické bezpečnosti. Za prvé, chrání vaše účty a data tím, že zabraňuje neoprávněnému přístupu. Hesla mohou být ohrožena různými způsoby, například při úniku dat nebo během síťových útoků. Pravidelná změna znamená, že i když někdo získá vaše staré heslo, bude mít omezený čas na jeho zneužití, než bude heslo změněno. Dále, pravidelná změna hesel zamezuje znovupoužití stejných hesel na různých účtech. Pokud používáte stejné heslo na několika místech a jedno z nich je ohroženo, váš celý digitální život může být v nebezpečí. Dále, pravidelná změna ztěžuje práci potenciálním útočníkům, kteří by mohli trávit čas pokusy o odhalení hesla;
- heslo by mělo být dlouhé (nejméně 12 znaků), obsahovat kombinaci písmen, číslic a speciálních znaků a nemělo by obsahovat snadno uhodnutelná slova nebo fráze;
- doporučuji použití unikátního hesla pro každý online účet a službu a používání dvoufaktorového ověřování, protože zajišťuje dodatečnou ochranu účtů a dat.

Zálohy dat:

- Je zřejmé, že většina respondentů má alespoň nějaký zálohovací proces, což je dobré z hlediska ochrany dat. Nicméně 22 % respondentů vůbec nezálohuje, což může představovat riziko pro jejich digitální data. Dále je třeba brát v úvahu, že 3 % respondentů neví, jak provádět zálohu, což naznačuje, že by mohla být potřeba zvýšit povědomí o správných postupech zálohování a jeho důležitosti.

Tipy pro efektivní zálohování dat:

- **Pravidelnost:** Zálohujte svá data pravidelně, ideálně denně nebo týdně, abyste minimalizovali riziko ztráty.
- **Důležitost dat:** Rozhodněte se, která data jsou pro vás nejdůležitější a zálohujte je prioritně.
- **Testování obnovy:** Pravidelně prověřujte, zda můžete obnovit data ze zálohy, abyste byli připraveni na případné potíže.
- **Šifrování:** Pokud zálohujete citlivá data do cloudu nebo na externí disk, použijte šifrování pro zabezpečení dat.

Ochrana zařízení:

- Klaďte důraz na používání aktualizovaného a licencovaného antivirového softwaru.
- Upozorněte uživatele na výhody používání virtuální privátní sítě (VPN) pro zabezpečené připojení k internetu, především pro ty, kteří pracují na služební výpočetní technice z domova. Stejně to platí pro ty, kteří používají vlastní výpočetní techniku v práci a nějakou formou mohou na nich zpracovávat služební informace.

Připojení na veřejnou Wi-Fi:

- Doporučuji se na veřejné Wi-Fi sítě nikdy nepřipojovat. Připojení na veřejnou Wi-Fi síť může znamenat rizika, jako je odposlouchávání dat, falešné sítě a malware. V případě nejvyšší nutnosti použití doporučuju používání VPN, aktualizovaný software a opatrnost při zadávání citlivých údajů.

Zabezpečení mobilních zařízení:

- U mobilních telefonů doporučuji jako heslo použít otisk prstu nebo sken obličeje, který se nedá obejít. Při odemykání krátkým heslem nebo gestem může dojít k tomu, že útočník může heslo lehce „okoukat" a použít ho ve Vaší nepřítomnosti, avšak je to lepší způsob než žádné heslo.
- Je důležité dbát na aktuálnost svých aplikací v mobilu, nejlepší způsob je povolit automatické aktualizace aplikací ve svém obchodě pro aplikace (App Store, Google Play,…). Aktualizované aplikace jsou důležité pro bezpečnost, stabilitu, nové funkce a kompatibilitu s vašimi zařízeními. Pravidelné aktualizace zajišťují, že aplikace pracují správně a jsou chráněny před bezpečnostními hrozbami.

Doporučení pro pracovní prostředí (při používání služební výpočetní techniky pro osobní účely):

- Dodržujte firemní politiku pro osobní používání;
- omezte osobní použití zařízení na minimum;
- nepoužívejte pracovní hesla pro osobní účely;
- udržujte zařízení aktualizovaná a chráněná antivirem;
- respektujte pravidla soukromí a osobních údajů;
- dodržujte právní předpisy;
- neposkytujte osobním účelům přístup k firemním datům;
- kontaktujte IT oddělení při pochybnostech;
- buďte zodpovědní a uvědomte si rizika;
- respektujte důvěrnost firemních dat.

Vnímání kybernetické bezpečnosti:

Posilujte povědomí o tom, že kybernetická bezpečnost je závažným problémem, který se týká všech.

E-mailové a internetové odkazy:

Vyvarujte se klikání na odkazy z nedůvěryhodných nebo nevyžádaných e-mailů zaslaných na váš e-mailový účet. Tyto odkazy mohou vést na podvodné nebo falešné stránky sloužící k získání vašeho uživatelského jména, hesla nebo osobních údajů, které může hacker okamžitě zneužít k získání přístupu do vašich systémů.

Závěr

Navzdory veškerým snahám lidí na ochranu před kyberzločinci stále pokračují útoky na společnosti, což ročně způsobuje škody v řádu milionů korun. Jsme zapojeni do nepřetržitého boje s hackery, kteří neustále mění své taktiky a postupy. S každým novým bezpečnostním opatřením se útočníci snaží najít nové a sofistikovanější metody, jak je obejít. Odborníci v oblasti kybernetické bezpečnosti zdůrazňují význam zvýšení ochrany jak fyzické, tak cloudové infrastruktury. Proto je klíčové, aby lidé byli informováni o tom, jak jejich chování může ovlivnit bezpečnost organizace nebo jejich vlastní osobní bezpečnost. Musí mít znalosti a dovednosti, které jim umožní rozpoznat a zastavit kybernetické útoky. Právě tomuto tématu se věnuje praktická část této bakalářské práce, která plní hlavní cíl práce, a to zjištění úrovně povědomí lidí o kybernetické bezpečnosti.

Je důležité, aby lidé měli v povědomí, jak kybernetický útok může vypadat, jak se před ním bránit, předcházet a jak je důležité provádět pravidelná školení. Proto se v teoretické části věnuje těmto pojmům – zálohování, aktualizace, problematika hesel, dvoufaktorové ověřování, školení, šifrování, nástrojům na obranu a nejznámějšími druhy kybernetických útoků.

Pomocí dotazníkového šetření se autor snažil zjistit úroveň znalostí týkajících se zabezpečení dat. Cílem této práce bylo zjistit, jaké mají respondenti zkušenosti se zabezpečením, jak jí vnímají, zda jsou školeni, jak útokům předcházejí a na základě výsledků navrhnout opatření, které mohou zlepšit úroveň zabezpečení a ochránit tak jednotlivce nebo organizace před kybernetickými útoky

Z dotazníku vyplynulo spoustu překvapujících informací. Za prvé, zděšující je nízká míra změny hesel mezi respondenty, přičemž 67 % respondentů z Úřadu práce si hesla vůbec nemění. Na druhou stranu je pozitivní, že většina respondentů chápe důležitost komplexních hesel, protože 82 % ví jak správně má vypadat silné heslo.

Dále je překvapující, že více než pětina respondentů neprovádí žádné zálohy svých dat, což může mít závažné důsledky v případě ztráty dat. Navíc, i přes zvýšené povědomí o kybernetické bezpečnosti (88 % respondentů vnímá tuto problematiku jako důležitou), stále existují oblasti, ve kterých je třeba zlepšení. To lze například vidět i v tom, že v průměru 57 % respondentů odpovědělo, že bylo někdy obětí kybernetického útoku, ačkoliv realita je taková, že každý kdo se pohybuje na internetu byl někdy určitou formou obětí kybernetického útoku – minimálně spamem.

Seznam použitých zdrojů

Literární zdroje

1. ALEXANDROU, A. *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices.* 1st ed. CRC Press, 2021, 454 s. ISBN 978-0367251574.
2. COX, CH. K. *Everyday Cybersecurity A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity*. 2019, 269 s. ISBN 978-1733018609.
3. DELFS, H., KNEBL, H. *Introduction to cryptography: principles and applications*. 2nd ed. New York: Springer, 2007, 367 s. ISBN 35-404-9243-7.
4. EASTTOM, CH. *Computer Security Fundamentals*. Pearson IT Certification, 2019. 512 s. ISBN 978-0135774779.
5. JIRÁSEK, P., NOVAK L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR, 2013, 200 s. ISBN 978-80-7251-397-0.
6. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC z. s. p. o., 2016. 524 s. ISBN 978-80-88168-15-7.
7. KOLOUCH, J., BAŠTA, P., KROPÁČOVÁ, A., KUNC, M. *CyberSecurity*. Praha: CZ.NIC z. s. p. o., 2019, 560 s. ISBN 978-80-88168-31-7.
8. KIZZA, J. M. *Guide to computer network Security*. Springer, 2020. 625 s. ISBN 978-3030381400.
9. LENHARD, T. H. *Data security: Technical and organizational protection measures against data loss and computer crime.* SPRINGER. 2022, 128 s. ISBN 978-3-658-35493-0.
10. MAISNER, M., VLACHOVÁ, B., *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. 91 s. ISBN 978-80-7478-818-5.
11. MEDICINE, J., *Networking for Beginners: The Complete Guide to Computer Network Basics, Wireless Technology and Network Security*. Independently published, 2019. 150 s. ISBN 978-1708219857.
12. MITNICK, K., SIMON, W. *Umění klamu*. Gliwice: Helion, 2003. 348 s. ISBN 83-7361-210-6.
13. STALLINGS, W., *Wireless communications and networks*. 2nd ed. Upper Saddle River: Pearson/Prentice Hall, 2005, 559 s. ISBN 0-13-191835-4.
14. VACCA, R. J. *Computer and Information Security Handbook.* 3rd ed. Morgan Kaufmann, Burlington 2017, 1280 s. ISBN 978-0128038437.
15. WALKER, B., *Computer Networking The Complete Beginner's Guide to Learning the Basics of Network Security, Computer Architecture, Wireless Technology and Communications Systems (Including Cisco, CCENT, and CCNA).* Benjamin Walker. Science & Technology, 2019. 226 s. ISBN 978-1951652166.
16. WINKLER, I. Security awareness for dummies. John Wiley & Sons. 2022, 288 s. ISBN 978-1119720928.
17. WYLD, D. C., WOZNIAK, M., CHAKI, N., MEGHANATHAN, N., NAGALAMAI, D. *Advances in network security and applications: 4th International Conference,* CNSA 2011, Chennai, India, July 15-17, 2011, Proceedings. Springer, 2011. 678 s. ISBN 978-3642225390.

Elektronické zdroje

1. 10 Types of Cloud Computing You Should Know About [online]. [cit. 2023-26-10] Dostupné z WWW: <https://helpdeskgeek.com/reviews/10-types-of-cloud-computing-you-should-know-about/>.
2. Analýza a vyhodnocení vynakládání finančních prostředků do Agendových systémů MPSV v letech 1993–2011. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.mpsv.cz/documents/20142/974645/Analyza_a_vyhodnoceni.pdf/e68e2516-1347-aa00-d3c8-a5ceb6bbcf4e>
3. Backup de données : qu'est-ce que c'est ? À quoi cela sert-il ? [online]. [cit. 2023-26-10] Dostupné z WWW: <https://www.weodeo.com/la-securite-informatique/quest-ce-quun-backup-up-et-a-quoi-cela-sert/>.
4. Botnets – What are they and why do they matter [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://adamlevin.com/2021/08/26/botnets-what-are-they-and-why-do-they-matter/>.
5. BYOD (bring your own device) [online]. [cit.23-30-10] Dostupné z WWW: <https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device>
6. Co je to kybernetická bezpečnost ? [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.sap.com/cz/products/financial-management/what-is-cybersecurity.html>.
7. Co je řízení přístupu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.microsoft.com/cs-cz/security/busines/security-101/what-is-access-control>
8. Co je VPN a k čemu je to dobré ? [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.czcloud.cz/cloud/co-je-to-vpn-a-k-cemu-je-to-dobre/>.
9. Google says the best phishing scams have a 45 percent success rate. [online]. [cit. 2023-26-10]. Dostupné z: WWW: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>
10. IDS vs. IPS: What is the Difference? [online]. [cit. 2023-26-10]. Dostupné z WWW: <https://www.upguard.com/blog/ids-vs-ips>
11. Jednotný informační systém práce a sociálních věcí. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://cs.wikipedia.org/wiki/Jednotný_informační_systém_práce_a_sociálních_věcí>
12. Katalog 2007 [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.army.cz/assets/files/9369/KATALOG_2007_part_4.pdf>
13. Největší hrozby a zranitelnosti kybernetické bezpečnosti: #1 Sociální inženýrství [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://kybez.cz/nejvetsi-hrozby-a-zranitelnosti-kyberneticke-bezpecnosti-1-socialni-inzenyrstvi/>.
14. Proč Jsou šifrování a MFA Nezbytné Pro Vaši Firmu? [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://digitalsecurityguide.eset.com/cz/proc-jsou-sifrovani-a-mfa-nezbytne-pro-vasi-firmu#h2-0>
15. SALAZAR, J. Techpedia – Bezdrátové sítě [online]. České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2023-25-10]. Dostupné z WWW: <https://upcommons.upc.edu/bitstream/handle/2117/100913/LM01_R_CZ-1.pdf>.

16. Tisková zpráva Nejvyššího kontrolního úřadu. [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.nku.cz/cz/pro-media/tiskove-zpravy/mpsv-podepsalo-osm-dodatku-ke-smlouve--navysilo-tak-cenu-systemu-pro-vyplatu-davek-o-1-5-miliardy-korun-id4808/>
17. USB Flash Drive Malware: How It Works & How to Protect Against It [online]. [cit. 2023-26-10] Dostupné z WWW: <https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/>.
18. Úřady práce nesmí používat IT systém, kvůli kterému obvinili Šišku. [online]. [cit. 2023-25-10]. Dostupné z WWW: <[https://zpravy.idnes.cz/ministerstvo-vnitra-dostalo-pulmilionovou-pokutu-za-chyby-v-it-zakazce-1qi-/domaci.aspx?c=A131218_185921_domaci_aha>.
19. Virus Basics [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.cisa.gov/news-events/news/virus-basics>.
20. VPN (virtual private network) [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.techtarget.com/searchnetworking/definition/virtual-private-network>.
21. Výběr skripta [online]. [cit. 2023-25-10]. Dostupné z WWW: <http://kbi.fbmi.cvut.cz/sites/default/files/Vyber-skripta.pdf>.
22. What is botnet attack ? 5 ways to prevent it [online]. [cit. 2023-10-25]. Dostupné z WWW: <https://securityscorecard.com/blog/what-is-a-botnet-attack/>.
23. What is firewall ? [online]. [cit. 2023-26-10]. Dostupné z WWW: <https://forumautomation.com/t/what-is-a-firewall/10695#google_vignette>.
24. What is a phishing attack? [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://www.ibm.com/topics/phishing>.
25. What is VPN? How It Works, Types of VPN [online]. [cit. 2023-25-10]. Dostupné z WWW: <https://usa.kaspersky.com/resource-center/definitions/what-is-a-vpn>.
26. Why user education is important for cybersecurity resilience [online]. [cit. 2023-24-10]. Dostupné z WWW: <https://www.lumificyber.com/blog/why-user-education-is-important-cybersecurity-resilience/>.

Legislativní dokumenty

1. ČESKO. Vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

Seznam zkratek

ABAC	Attribute-based access control
AP	Access point
AČR	Armáda České republiky
BYOD	Bring your own device
CD	Compact disc
CCTV	Closed circuit televison
DAC	Discretionary access control
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DVD	Digital Versatile Disc
EURES	European Employment Services
IDS	Intrusion Detection System
IPS	Intrusion prevention system
IT	Informační Technologie
LAN	Local area network
MAC	Mandatory access control
MDM	Mobile device management
MMS	Multimediální zprava
MPSV	Ministerstvo práce a sociálních věcí
P2P	Peer to peer
PIN	Personal identification number
RBAC	Role-based access control
SIEM	Security information and event management
SMS	Short message service
UPS	Uninterruptible power supply
USB	Universal serial bus
ÚP	Úřad práce
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network
Wi-Fi	Wireless fidelity
WLAN	Wireless local area network
WMAN	Wireless metropolitan area network
WPAN	Wireless personal area network
WWAN	Wireless wide area network

Seznam grafů a obrázků