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

VZDĚLÁVÁNÍ ÚŘEDNÍKŮ Z HLEDISKA KYBERNETICKÉ BEZPEČNOSTI NA VYBRANÉM MĚSTSKÉM ÚŘADĚ

Autor práce: Šárka Kaletová

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M., DSc.

Katedra: Katedra právních oborů a bezpečnostních studií

2025

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Šárka Kaletová

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

Název bakalářské práce: Vzdělávání úředníků z hlediska kybernetické bezpečnosti na vybraném městském úřadě

Název bakalářské práce v anglickém jazyce: Education of Officials in Terms of Cyber Security at the Selected Office

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M, DSc.
Datum zadání bakalářské práce (měsíc, rok): 7/2024

Cíl bakalářské práce: Hlavním cílem práce je posoudit efektivitu vzdělávání úředníků vybraného městského úřadu v oblasti kybernetické bezpečnosti. Vedlejším cílem je analyzovat současné vzdělávací programy úředníků se zaměřením na rizika kybernetických hrozeb v rámci informačních technologií a navrhnout tak konkrétní opatření k jejich minimalizaci.

Student: Šárka Kaletová	19.7.2024 *datum*	*podpis*
Vedoucí práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD.LL.M., DSc.	19.7.2024 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	13.9.2024 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	13.9.2024 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	16.9.2024 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. -2- ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracovala 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 vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Šárka Kaletová

Děkuji Dr. h. c. doc. JUDr. Miroslavu Felcanovi, PhD., LL.M., DSc., za cenné rady, trpělivost a vstřícnost při metodickém vedení práce. Poděkování patří také Ing. Davidu Smetánkovi, Ph.D., za odborné konzultace z oblasti kybernetické bezpečnosti. Dále děkuji všem respondentům Městského úřadu Vejprty, kteří se podíleli na výzkumném šetření této práce.

Abstrakt

KALETOVÁ, Š. *Vzdělávání úředníků z hlediska kybernetické bezpečnosti na vybraném městském úřadě: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 73 s. Vedoucí bakalářské práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M., DSc.

Klíčová slova: kybernetická bezpečnost, hlavní pilíře kybernetické bezpečnosti, vzdělávání v oblasti kybernetické bezpečnosti, úředníci městského úřadu.

Bakalářská práce zkoumá vzdělávání úředníků Městského úřadu Vejprty z hlediska kybernetické bezpečnosti a dále analyzuje jejich znalosti v oblasti kybernetických hrozeb v souvislosti s narušením počítačové sítě při výkonu správních činností v rámci působení v zaměstnání.

Teoretická část se zaměřuje na problematiku kybernetické bezpečnosti v souvislosti s narušením kybernetického prostoru. Prostřednictvím odborné literatury zkoumá hlavní pilíře bezpečnosti a obezřetnosti vůči kybernetickým hrozbám, které jsou zásadní pro eliminaci narušení kyberprostoru.

Praktická část se věnuje vlastnímu výzkumu prostřednictvím dotazníkového šetření, které je zaměřeno na vzdělávání úředníků z hlediska kybernetické bezpečnosti a znalostí v oblasti kybernetických hrozeb, na jehož základě byly zpracovány výsledky průzkumu a následně vyhotovena závěrečná doporučení.

Abstract

KALETOVÁ, Š. *Training of Officials in Terms of Cybersecurity at a Selected Municipal: bachelor thesis*. České Budějovice: The College of European and Regional Studies, 2025. 73 pp. Supervisor: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M., DSc.

Keywords: cybersecurity, main pillars of cybersecurity, cybersecurity training, municipal officials.

The bachelor's thesis investigates the cybersecurity training of public officials at the Vejprty Municipal Office, with a detailed analysis of their awareness and understanding of cyber threats, particularly in relation to disruptions in computer network systems during the execution of administrative duties within the scope of their professional responsibilities.

The theoretical part explores the concept of cybersecurity in relation to disruptions within cyberspace. Drawing on professional literature, it examines the fundamental principles of security and provides a comprehensive overview of strategies to mitigate cyber threats, which are critical for preventing disruptions in cyberspace.

The practical part is dedicated to the research conducted through a questionnaire survey, which focuses on the cybersecurity training of officials and their knowledge of cyber threats. Based on the survey results, the data was analysed, and subsequent recommendations were formulated.

Obsah

Úvod

Vzdělávání má smysl. Nezáleží na obsahu, tématu nebo době. Jakékoliv vědění přináší nové poznatky, které obohatí nejen člověka samotného, ale také celé lidstvo. Smyslem tohoto vědění je předávat myšlenky dál, aby se lidé do budoucna vyvarovali veškerých omylů a fatálních chyb. V oblasti kybernetické bezpečnosti to platí v maximální možné míře. Na dnešního člověka čekají ještě mnohá úskalí, dokud neporozumí veškerým kybernetickým hrozbám. Avšak smyslem vzdělávání úředníků v této oblasti je právě nejen těmto hrozbám porozumět, ale také umět kybernetické hrozby včas rozpoznat a identifikovat. Cílem tohoto vědění je tak znalostí odvrátit incidenty kybernetických útoků a minimalizovat negativní dopad v rámci kyberprostoru v souvislosti s jeho narušením. Útočníci jsou bohužel vždy napřed. To, co je známo o kybernetické bezpečnosti dnes, již nemusí platit pro zítřek. Vzdělávání v oblasti kybernetické bezpečnosti je neustálý proces a je potřeba se neustále rozvíjet a zdokonalovat. Čím intenzivněji se na toto téma bude společnost vzdělávat, tím více bude mít převahu nad potencionálními kybernetickými hrozbami.

Vývoj informačních a komunikačních technologií se primárně odehrává v kybernetickém prostoru, který jde ve svém vývoji neustále kupředu. Ovšem stejným tempem jdou i útočníci, kteří chtějí tento prostor ohrozit či narušit stále více promyšlenějšími kybernetickými útoky. Aby bylo možné těmto útokům úspěšně čelit, musí i vzdělávání v oblasti kybernetické bezpečnosti držet jasné tempo s moderními technologiemi a především je nutné se v této oblasti neustále vzdělávat. Jde především o dlouhodobý proces, nikoliv o jednorázovou záležitost. Vzdělávání je velmi účinným nástrojem ochrany proti kybernetickým útokům, a proto je velmi důležité hrozby také názorně simulovat, aby bylo možné pochopit celý proces narušení kybernetického prostoru.

Kybernetický svět je maximálně velkorysý z hlediska prostoru, je nutné se však chovat tak, aby lidé svým chováním tento prostor nikterak neohrozili. Je velmi složité představit si skutečnost prostoru, jenž nemá konec ani začátek, kterého se nelze dotknout, a který je navíc nutné chránit. Toto prostředí musí být chápáno jako komplexní záležitost za účelem jeho ochrany, a to i v případě bezpečnosti státní správy. Úředníci samospráv jsou klíčovými prvky v této obraně, proto je velmi důležité se v oblasti kybernetické bezpečnosti neustále vzdělávat.

1 Cíl a metodika bakalářské práce

Bakalářská práce na téma Vzdělávání úředníků z hlediska kybernetické bezpečnosti na vybraném městském úřadě se skládá z teoretické a praktické části. Teoretická část je rozdělena na pět kapitol. První kapitola se věnuje vymezení základních pojmů v kontextu úředníků a městského úřadu. Druhá kapitola pak vysvětluje pojem kybernetický prostor a hrozby související s jeho narušením. Třetí kapitola se věnuje kybernetické bezpečnosti spolu s hlavními pilíři ochrany počítačové sítě. Pátá kapitola se skládá ze samostatné praktické části a její součástí jsou i návrhy a doporučení.

Hlavním cílem této práce je zjištění a posouzení vzdělanosti úředníků v oblasti kybernetické bezpečnosti a zhodnocení jejich znalostí z hlediska obezřetnosti vůči kybernetickým hrozbám při výkonu správních činností v rámci zaměstnání. Stěžejní problematikou tohoto vzdělávání je rozpoznání rizik v této oblasti a zachování základních pilířů v oblasti kybernetické bezpečnosti, jakými jsou zálohování dat a informací, aktualizace systému, používání silných hesel, ale také bezpečné používání dálkového připojení. K dosažení tohoto cíle byla pomocí knižních zdrojů a jejich literárních rešerší vytvořena nejprve teoretická část. V této části je také vymezena problematika kybernetické bezpečnosti, na jejímž základě byla následně vytvořena praktická část této práce.

Úvod praktické části je zaměřen na Městský úřad Vejprty (dále jen MěÚ) a jeho odbory. Dále je uveden cíl výzkumného šetření spolu s metodikou praktické části, která popisuje konkrétní přípravu dotazníkového šetření včetně realizace a sběru dat. Analýza byla provedena prostřednictvím grafů na základě odpovědí úředníků MěÚ Vejprty. Cílem tohoto anonymního dotazníku bylo získání informací týkajících se vzdělanosti úředníků z hlediska kybernetické bezpečnosti a obezřetného chování při výkonu správních činností úředníků v rámci jejich zaměstnání. Dále byl pak dotazník zaměřen na aktivitu úředníků se v tomto oboru vzdělávat a jejich návrhy na zlepšení z hlediska kybernetické bezpečnosti v jejich zaměstnání.

Součástí samotného závěru práce jsou návrhy a doporučení pro zlepšení v oblasti kybernetické bezpečnosti v rámci zaměstnání při výkonu správních činností.

2 Vymezení základních pojmů

2.1 Úředník

Úředník je pověřená úřední osoba zařazená do úřadu, avšak v pracovním poměru je s organizací s právní subjektivitou. Jeho činnost spočívá v samostatném plnění úkolů svěřených úřadem v souladu s platnou pracovní smlouvou. Pojem úředník vymezuje zákon č. 312/2002 Sb., o úřednících územních samosprávných celků: *„Úředníkem se pro účely tohoto zákona rozumí zaměstnanec územního samosprávného celku podílející se na výkonu správních činností zařazený do obecního úřadu, do městského úřadu, do magistrátu statutárního města nebo do magistrátu územně členěného statutárního města, do úřadu městského obvodu nebo úřadu městské části územně členěného statutárního města, do krajského úřadu, do Magistrátu hlavního města Prahy nebo do úřadu městské části hlavního města Prahy.“*[1]

Úřadem se rozumí obecní úřad, městský úřad, krajský úřad nebo magistrát statutárního města. Vzdělávání úředníků je nedílnou součástí pracovní náplně při výkonu tohoto zaměstnání. Patří sem vstupní vzdělávání, průběžné vzdělávání, prohlubující vzdělávání nebo zvláštní odborná způsobilost. Faktorů, které ovlivňují úroveň vzdělávání úředníků, je několik. Patří sem například reakce na trh práce, dynamika doby, vzestup informačních technologií, ale také politická situace. Zatímco vstupní vzdělávání musí absolvovat každý úředník po nástupu do svého zaměstnání, průběžné a prohlubující zaměstnání jsou vedena jako celoživotní povinná vzdělávání ve formě akreditovaných kurzů zaměřených na výkon správních činností každého zaměstnance.

Vyhláškou Ministerstva vnitra o zvláštní odborné způsobilosti je definována zkouška úředníků z odborných znalostí potřebných k výkonu jejich povolání. *„Například pravidelné osobní školení zaměstnanců o novinkách v oblasti bezpečnosti lze poměrně snadno zajistit v rámci střední či malé organizace, která pořádá setkání všech zaměstnanců a jejíž zaměstnanci čelí obecně obdobným hrozbám (protože všichni pracují s omezeným počtem aplikací).“*[2]

[1] ČESKO. Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů. In: *Sbírka zákonů, Česká republika*. 2002, částka 114.
[2] NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Praha: Wolters Kluwer, 2022, s. 102.

Úředník kromě správních činností musí ovládat především nejrůznější softwarové systémy. V době prvních osobních počítačů musel úředník především umět odeslat a přijmout elektronickou poštu (mimochodem, spam byl ještě v daleké budoucnosti). Poté k této znalosti přibyla dovednost v ovládání programů Excel a Word, které jsou součástí balíčku Microsoft Office. Ale to už v dnešní době opět nestačí. Pokud se dnes takový úředník chce ucházet o místo na městském úřadě, samozřejmostí pro výkon tohoto zaměstnání je schopnost ovládat informační technologie ve formě elektronické úřední korespondence, softwarových databází, jakými jsou mzdové, účetní a daňové programy, prohlížečů dokumentů, spisové služby, datové schránky, elektronického portálu, jakým je např. Identita občana, a samozřejmostí jsou úpravy úřední korespondence a komunikační či prezentační dovednosti. V neposlední řadě však musí mít úředník znalosti o bezpečném zacházení v oblasti informačních technologií a z toho vyplývajících nařízení o možných kybernetických hrozbách. Ty jsou z pohledu dnešní doby nejdůležitější. *„V souvislosti s rozvojem počítačových sítí, především internetu a mobilních technologií, je jednou ze základních výhod takřka neomezený přístup k informacím, k vědění nebo vzdělávání.“*[3]

2.2 Městský úřad

Městský úřad je institucí, která vykonává správní činnost a své záležitosti spravuje samostatně. Jedná se o samosprávu, která je složkou veřejné správy a není závislá na státní správě. Vznikla decentralizací státní moci, která se tímto rozdělila na státní a nestátní instituce. V čele místní samosprávy je starosta a vedení této instituce náleží zastupitelstvu města. Samospráva je charakteristická tím, že o svých činnostech rozhoduje samostatně. Městský úřad je rozdělen na odbory, které zastávají určité funkce v rámci příslušného města či obce.

Stavební odbor

Vydává stavební povolení a územní rozhodnutí. Ke své činnosti v rámci svého resortu využívá počítačovou síť.

Správa majetku města

[3] ZOUNEK, J., JUHAŇÁK, L., STAUDKOVÁ, H., POLÁČEK, J. *E-learning: učení (se) s digitálními technologiemi: kniha s online podporou*. Praha: Wolters Kluwer, 2016, s. 232.

Spravuje svůj majetek nejen ve smyslu zákona o obcích, ale zároveň s tímto majetkem účelně nakládá např. pronajímáním ostatním subjektům. Správa majetku v rámci svých činností využívá jak počítačovou, tak internetovou síť.

Sociální odbor

Zabývá se velmi širokým obsahem sociálních činností, v rámci své kompetence poskytuje poradenské a mediační služby v oblasti sociálních služeb a vykonává matrikářské a archivační činnosti. Ke své činnosti využívá počítačovou síť, a pokud však sociální odbory nahrazují i matriční úřady, rozhodně ke své práci musejí využívat i globální síť.

Pracovní úřad

Eviduje uchazeče o zaměstnání a zároveň těmto osobám pomáhá při hledání nového pracovního uplatnění na trhu práce. Tento odbor je v rámci svých pracovních činností napojen na obě sítě, vnitřní i globální.

Odbor dotačních titulů

Tento obor je poměrně mladý a vznikl v reakci na nárůst dotačních titulů s širokým spektrem využití a rozsáhlými podmínkami pro jejich čerpání. Již z jeho samotného zaměření vyplývá, že při své práci musí využívat oficiální státní online platformy, jako jsou informační systémy pro správu dotací, databáze dotačních titulů nebo elektronické nástroje pro administrativní komunikaci. To vše vyžaduje přístup k relevantním informacím a práci v rámci globální sítě.

Ekonomický úsek

Slouží nejen pro spravování financí celého aparátu, ale zároveň poskytuje platební možnosti pro veřejnost za účelem nejrůznějších poplatků. Platby v rámci samosprávy jsou hrazeny prostřednictvím platebních internetových platforem.

Vedení města aj.

Odbory se zpravidla ještě dělí na jednotlivé úseky, jakými jsou kancelář starosty města, kancelář tajemníka, podatelna či sekretariát. Na těchto úsecích se hojně využívají portály jako e-pod**a**telna, spisová služba, elektronický podpis aj.

Všechny tyto odbory v kompetenci městského úřadu využívají ke své pracovní činnosti informační a komunikační technologie. Rozdíl je pouze v softwarovém zařízení určitého resortu, avšak všechny jsou hromadně připojeny k identické počítačové

a internetové síti. V daném úseku či resortu pracuje určitý počet zaměstnanců, z nich každý má k dispozici moderní počítačové zařízení s globálním připojením.

„V případě veřejnoprávního subjektu je velká část předmětu činnosti vymezena přímo právem. Typicky u úřadů či územní samosprávy zákon upravující jejich činnost jasně definuje, co je daný subjekt povinen dělat a jak, které agendy je povinen zajišťovat, se kterými dalšími subjekty sdílí data a jakým způsobem. A naopak veřejnoprávní subjekty nesmí činit nic, co jim zákon neukládá. I tak ale zbývají okruhy, které jsou právními předpisy vymezeny obecně nebo se nejedná o výkon veřejné moci, a veřejnoprávní organizace proto má větší možnost o své činnosti sama rozhodovat.“[4]

Městský úřad rámci své působnosti zajišťuje veškeré technické vybavení a dále připojení internetové a místní počítačové sítě pro své resorty. V jeho zájmu je také ochrana dat a informací všech odborů této instituce.

V rámci samosprávných činností pracují úřady s webovými či digitálními portály občanů, kde jsou městské úřady pro veřejnost otevřeny neomezeně. Občané mohou takto komunikovat s resorty, aniž by tyto museli fyzicky navštívit. Jde o jakési usnadnění komunikace občanů s úřady. Smyslem těchto portálů je rychlé a dostupné poskytování informací či odevzdávání formulářů v elektronické podobě. *„Elektronizácia verejnej správy predstavuje súčasť a jednu z agend procesu informatizácie spoločnosti.“*[5] V rámci elektronizace lze žádat o dotace v oblasti životního prostředí či hradit místní poplatky na půdě samosprávy. Souhrnně se digitalizace veřejné správy nazývá e-Government. Je tedy evidentní, že úředníci dnes skutečně intenzivně využívají ke svým činnostem internetové prostředí. Informační technologie prostoupily do všech oblastí státní i veřejné správy, a jsou tedy nedílnou součástí pracovních činností dnešních úředníků.

„Elektronizácia verejnej správy, resp. e-Government, predstavuje postup využívania moderných informačních a komunikačných technológií, ktorý sa vzťahuje na poskytovanie elektronických služeb v rámci štátnej správy, všetkých úrovní samosprávy a taktiež vo verejných inštitúciách. Ide o kontinuálny proces zlepšovania

[4] NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Praha: Wolters Kluwer, 2022, s. 79.
[5] ANDRAŠKO, J., DAŇKO, M., DRAŽOVÁ, P., GYURÁSZ, Z., MESARČÍK, M., SOPÚCHOVÁ, S. *Právo informačných a komunikačných technológií 2*. Bratislava: Tinct, 2021, s. 13.

služeb verejnej správy, a to vo verejnom záujme, pre optimalizáciu verejnej správy a v neposlednom rade prezvýšenie jej dôveryhodnosti a transparentnosti.“[6]

2.3 Vzdělávání úředníků

Z hlediska zmíněného zákona je prohlubování kvalifikace úředníků v rámci samosprávných činností nutností. Zákon přímo uvádí, v jakém rozsahu jsou úředníci povinni školení absolvovat a také v jakém časovém horizontu se po nástupu do svého zaměstnání těchto školení účastnit. Jedná se o vstupní a průběžné vzdělávání.

„Průběžné vzdělávání zahrnuje prohlubující, aktualizační a specializační vzdělávání úředníků zaměřené na výkon správních činností v územním samosprávném celku včetně získávání a prohlubování jazykových znalostí.“[7] O účasti na průběžném vzdělávání rozhoduje zpravidla tajemník MěÚ. V převážné části je vedeno formou e-learningových nebo prezenčních kurzů. Všechny kurzy jsou akreditované pro vzdělávání úředníků územně samosprávných celků. Absolvování průběžné kvalifikace je zakončeno osvědčením.

Efektivita v podobě vzdělávání úředníků je však významným profitem pro celý úřad, a to nejen v rámci průběžného vzdělávání. Pokud se takový zaměstnanec rozhodne například pro celoživotní vzdělávání, byť v podobě absolvování dobrovolných programů, vzrůstá tak jednoznačně bonus pro celý úřad. Lety vyškolený úředník, navíc v různých vzdělávacích oblastech, je pak nedocenitelnou pracovní silou, od které se následně může učit nastupující generace zaměstnanců. Lze tedy konstatovat, že mnoha lety získané zkušenosti úředníka pomohou generaci vykonávající činnost v budoucnu, a to nejen v orientaci v pracovních činnostech, ale také ve vědění samotném. Tímto procesem se efektivita celé organizace jednoznačně zvyšuje.

„Prohlubující se vzdělávání by mělo navazovat na vstupní a na zvláštní odbornou způsobilost a vzdělávání vedoucích úředníků. Účastí na prohlubujícím vzdělávání si úředník prohlubuje již získané znalosti a dovednosti potřebné pro výkon správních činností. Aktualizační vzdělávání zejména reaguje na změny v právních předpisech, jejichž znalost je nezbytná pro výkon jednotlivých oblastí výkonu působnosti územního samosprávního celku.“[8] Avšak možnost vzdělávání na rozdíl od povinných prohlubujících vědomostí není na všech úřadech zcela běžná. Především jde

[6] Tamtéž, s. 15.
[7] PONDĚLÍČKOVÁ, K. *Zákon o úřednících územních samosprávných celků: komentář*. Praha: Wolters Kluwer, 2016, s. 108.
[8] Tamtéž, s. 109.

o dobrovolné kurzy, jakými jsou komunikační dovednosti úředníka, budování vztahů na pracovišti, týmová spolupráce, syndrom vyhoření, vyjednávání a řešení konfliktů, osobní rozvoj, zdravý úřad aj. Do okruhu prohlubujícího vzdělávání však jednoznačně kybernetická bezpečnost patří. Chybí však pevné ukotvení, do jaké míry a v jakém rozsahu je třeba tomuto vzdělávání věnovat pozornost, proto je velmi potřebné se tématu kybernetické bezpečnosti věnovat v maximální možné míře i do budoucna. Vzděláváním úředníků vykonávajících správní činnost se zabývá vyhláška č. 413/2024 Sb., o zvláštní odborné způsobilosti, zkoušce vstupního vzdělávání a náležitostech osvědčení o vzdělávání úředníků územních samosprávných celků,[9] která konkretizuje správní činnosti, u nichž je zvláštní odborná způsobilost nezbytná.

Jako jsou informační technologie nedílnou součástí jednadvacátého století, tak i umělá inteligence prostupuje napříč všemi odvětvími a je třeba s ní také umět velmi dobře zacházet. Úředníkům městských úřadů může ušetřit mnoho času a ulehčit mnoho práce, ale v opačném případě také velmi uškodit. Proto jsou důležité vzdělanost a osvěta z hlediska kybernetické bezpečnosti. Je tedy prioritou dnešní doby porozumět kybernetickým hrozbám. V tomto směru je nedílnou součástí pracovního výkonu úředníka vzdělávání v oblasti kybernetické bezpečnosti. *„V porovnání s minulosťou sa nachádzame v období, kedy informačné technologie prenikajú takmer do všetkých oblastí života, čím sa informácie stávajú dostupnějšími, komunikácia flexibilnejšou a spoločnosť celkovo „rýchlejšou“. Na druhej strane sa ale komunikácia a celkovo spoločnosť stáva viac anonymnou a zranitelnou.“*[10]

Vzdělávání z hlediska kybernetické bezpečnosti v rámci pracovních školení je nejen efektivní, ale také skutečně nutné. Velkou výhodou je v dnešní elektronické době nízká náročnost na časové požadavky z hlediska vzdělávání úředníka. Avšak tou největší devízou tohoto vzdělávání je předcházení kybernetickým hrozbám. Za kybernetickou bezpečnost je odpovědný každý úředník, který vykonává práci v rámci své funkce na základě pracovní smlouvy a má přístup k počítačové síti. Jakožto koncový uživatel musí s informacemi zacházet odpovědně a obezřetně.

[9] ČESKO. Vyhláška č. 413/2024 Sb., o zvláštní odborné způsobilosti, zkoušce vstupního vzdělávání a náležitostech osvědčení o vzdělávání úředníků územních samosprávných celků. In: *Sbírka zákonů, Česká republika*. 2024, částka 413.

[10] VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava: Wolters Kluwer SR, 2019, s. 41.

2.4 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů, dále jen GDPR (z angl. General Data Protection Regulation), se týká každého, kdo jakýmkoliv způsobem nakládá s identifikačními údaji, tedy i úředníků městských úřadů. Ti absolvují v rámci tohoto nařízení akreditované školení, jak s osobními údaji obezřetně zacházet. Těmito údaji jsou veškeré informace, na jejichž základě je možné člověka identifikovat. Jedná se o rodná čísla, adresy, data narození, údaje o pohlaví, osobním stavu, věku či veškeré fotografie osob, ale také o telefonní čísla, nebo dokonce datové schránky. Osobní údaje nezletilých či mladistvých nebo zdravotní stav osob, ale také jejich vzdělání, životopis, insolvence, či dokonce náboženství spadají do tzv. osobních citlivých údajů. *„Zvláštní kategorií osobních údajů jsou osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech. Dále to jsou údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii osobních údajů jsou dále považovány genetické a biometrické údaje, slouží-li pro účely jedinečné identifikace fyzické osoby.“*[11] Nakládání s osobními údaji znamená nejen jejich šíření, shromažďování či vyhledávání, ale také bezprostřední zacházení s těmito údaji. Naprosto nezbytnou součástí úředníkovy práce je zachovávat informace v rámci GDPR v náležité opatrnosti, aby nemohly být nikým zneužity.

„Soukromí potvrdilo svůj význam. Je jedním z důležitých iniciátorů kreativity, jejíž význam v informační společnosti stále roste.“[12] Každý osobní údaj má nepochybně svou důležitou hodnotu a úředník s tímto musí být obeznámen. Důležitá jsou nejen veškerá opatření k ochraně osobních údajů v hardwarových či softwarových zařízeních, ale především informovanost zaměstnanců v podobě vzdělávání a prohlubování kvalifikace z hlediska nakládání s důležitými informacemi. To je prioritou a nedílnou součástí problematiky v rámci ochrany dat. Každý úředník musí být velmi podrobně obeznámen s tím, jak s těmito citlivými údaji zacházet a jak zamezit jejich eventuálnímu úniku, ztrátě či odcizení.

„Podle definice GDPR se zpracováním osobních údajů rozumí jakákoliv operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných přístupů, jako jsou

[11] ŽŮREK, J. *GDPR v personalistice*. 2. dopl. vyd. Olomouc: ANAG, 2022, s. 23.
[12] ZANDL, P. *Mýty a naděje digitálního světa: vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích*. Brno: Jan Melvil Publishing, 2022, s. 206.

shromáždění, zaznamenání, uložení, vyhledání, zpřístupnění přenosem atd.“[13] V kompetenci městských úřadů a jednotlivých odborů je nakládání s osobními údaji po mnoho let zcela běžnou záležitostí, a to nejen v rámci digitalizace. Má to ovšem své opodstatnění, jelikož každá žádost resortu musí být podložena osobními údaji žadatelů. Jejich nakládání a uchovávání je však kvůli obecnému nařízení o ochraně osobních údajů prioritou. Již nestačí informace uzamknout do kartotéky, jako tomu bylo v minulosti, ale také je třeba správně a systematicky uchovávat veškerá data v počítačové síti. Je tedy nutné do tohoto soukolí ochrany dat přizvat také oddělení informačních technologií, jež celý proces završí odpovídajícím zabezpečením.

„Nejen v IT oddělení by mělo zavádění nařízení GDPR začínat podrobnou analýzou rizik. Na základě této analýzy je totiž možné určit vhodná bezpečnostní opatření pro systémy a procesy, které sníží riziko na přijatelnou úroveň.“[14] Přijatelná úroveň znamená minimalizovat úniky dat a informací na nejmenší možnou míru. Opět i zde platí, že vzdělávání úředníků z hlediska GDPR je maximální prioritou pro kybernetickou bezpečnost.

Nejde však jen o údaj jako identifikátor osoby. *„Pokud se zaměříme na položku síťových identifikátorů a ověřovacích identifikačních údajů, zjistíme, že za osobní údaj může a zřejmě i bude považována řada dat umožňujících základní fungování počítačového systému v síti.“*[15] Je rozhodně nezbytné držet v opatrnosti veškerá data, která souvisejí s výkonem samosprávných činností úředníka. Avšak z tohoto pohledu by v budoucnu úředník nesl odpovědnost také za úkony spojené s informačními technologiemi, což jistě není úlohou úředníka, ale činností správce nebo administrátora počítačového systému. Nabízí se však otázka, zda skutečně v budoucnu data umožňující základní fungování počítačového systému převezmou status osobních údajů.

2.5 Data a informace

Samotná data neznamenají žádnou hrozbu. Nemají důležitou hodnotu. Tu jim vtiskne až informace. Pokud však informace využijí data správným způsobem, kybernetická bezpečnost není narušena, a nelze tedy hovořit o narušení tohoto prostoru. Pokud ale koncový uživatel na svém počítačovém zařízení tuto informaci změní, riziko ohrožení v kybernetickém prostoru stoupá. Množství informací je takřka neomezené,

[13] ŽŮREK, J. *GDPR v personalistice*. 2. dopl. vyd. Olomouc: ANAG, 2022, s. 24.
[14] STAŇKOVÁ, L. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018, s. 201.
[15] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 105.

proto zaměstnanci, kteří přicházejí do styku s těmito informacemi, by měli také přesně vědět, jak s nimi zacházet.

„Během posledních dvou dekád došlo díky informačním a komunikačním technologiím k transformaci lidské společnosti. „Informačními technologiemi“ lze chápat využívání počítačových a elektronických zařízení k ukládání a zprostředkování informací. Vlivem rozvoje počítačových sítí, v jejichž rámci spolu komunikují počítačové systémy, došlo k doplnění původního konceptu o prvek komunikace.“[16] V prostředí městského úřadu je tato komunikace běžná nejen mezi občany, ale i mezi úředníky. Převážnou část dokumentů, žádostí a evidencí pro veřejnost lze dnes díky digitalizaci vyřídit bez nutnosti vstupu občana na půdu samotného úřadu. Jde o prostoupení informačních technologií do veřejné správy, která tímto zesílila svou pozici v kybernetickém prostředí a umožnila tak široké veřejnosti být tzv. online ve věcech veřejných.

2.6 Hardware a software

Hardware (z angl. významu „technické vybavení“) je zařízení, se kterým má úředník přímý kontakt. Jedná se o komponenty, jakými jsou monitor, počítačová skříň, počítačová myš, notebook, tablet, zařízení k připojení internetové sítě (tzv. router), ale také tiskárna, scanner, základní deska, ventilátor, pevný disk aj. *„Jde o veškeré fyzické zařízení, které je třeba pro funkci systémů zpracování informací. Je to v podstatě počítač sám. Negativním vyjádřením lze uvést, že hardware je vše, co není programovým vybavením (software).“*[17] To vše dnes mají ve většině případů zaměstnanci městských úřadů plně k dispozici.

Z hlediska kybernetické bezpečnosti samotný hardware nepředstavuje žádnou hrozbu. Aby počítačová síť mohla být využívána, musí se hardware propojit se softwarem. Jedině tak spolu mohou tato zařízení vzájemně komunikovat. Propojení je nejen v rámci jednotlivých uživatelů, kteří takto komunikují se svým zařízením, ale tímto způsobem jsou vzájemně propojeni všichni úředníci celé instituce. Využívají tak místní počítačovou síť ke své pracovní činnosti. Je velmi důležité, aby taková zařízení splňovala bezpečnostní požadavky a byla odebírána pouze od důvěryhodných dodavatelů.

[16] RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Praha: C. H. Beck, 2023, s. 15.
[17] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, s. 59.

Oproti tomu software je programové vybavení, které se uvnitř hardwarového zařízení nachází. Jde především o takové softwarové programy, které lze v rámci užívání jednoduše nainstalovat do každého zařízení a rovněž také odinstalovat. V rámci městských úřadů se jedná o běžné účetní programy či různé interní databáze potřebné k vykonávání správních činností. Riziko kybernetické hrozby v počítačovém zařízení úředníka je v tomto případě na velmi nízké úrovni. Maximální obezřetnost nastává v okamžiku, jakmile se zařízení úředníka připojí k internetové síti. Internetová síť je globální propojení, které dokáže komunikovat takřka s libovolným zařízením po celém světě. Pokud má tedy úředník možnost nejen místního, ale i celosvětového připojení, je riziko kybernetické hrozby velmi vysoké.

„Svět prochází obrovskou transformací, která zahrnuje všechny aspekty života společnosti. Dostáváme do rukou úžasné nové technologie, jež nám přinášejí dříve nevídané příležitosti. Zároveň ale zásadně zvyšují momentální křehkost společenského systému, v něm jsme ještě nezavedli adekvátní opatření.“[18]

[18] ZANDL, P. *Mýty a naděje digitálního světa: vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích*. Brno: Jan Melvil Publishing, 2022, s. 287.

3 Kybernetický prostor

Kybernetický prostor je digitální svět bez hranic, který probíhá v rámci počítačové sítě. Jde o virtuální prostor, který v globálním měřítku urychluje komunikaci především v rámci internetového připojení. Na pozicích úředních osob se stal kyberprostor neodmyslitelnou součástí pracovních činností. Určité softwarové aplikace si zaměstnanci mohou za účelem své pracovní činnosti stáhnout do svého počítačového zařízení sami. Ovšem nelze si na takovou aplikaci sáhnout, jako tomu bylo dříve, například na účetní knihu. Tyto programy nejsou „uchopitelné“. A přesně tím je kyberprostor.

„Kyberprostor je virtuální realitou nemající konce ani začátku. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb atd.) se adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození či zániku kyberprostoru jako takového.“[19] Tato definice kyberprostoru od Koloucha vcelku jednoznačně objasňuje propojení virtuálního prostoru s hmotným zařízením koncového uživatele. O to více je s podivem, jak nehmotné zařízení dokáže zcela ochromit zařízení hmotné.

Avšak vzdělávání úředníků městských úřadů značně pokročilo, a takový zaměstnanec je díky prohlubování kvalifikace z hlediska kybernetické bezpečnosti informován o důležitosti kybernetického prostoru, ve kterém se v rámci pracovních činností nachází. Neméně podstatný úspěch této informovanosti je jistě dán dnešní dobou informačních technologií, díky níž vzdělanost dnešních úředníků probíhá vlastně formou nevědomou spolu s pokrokem dnešní doby. Kybernetická bezpečnost má však v rámci vzdělávání stále co nabídnout, jelikož neomezené hranice tohoto prostoru jsou a budou pro úředníky stále aktuální.

„Mezi znaky kyberprostoru je možné zařadit jeho decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost a možnost ovlivňování mínění skrze uživatele. Podstatným rysem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje,

[19] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 36.

že projev světa virtuálního může mít a má dopady ve světě reálném.“[20] Pokud se zachází s kybernetickým prostorem natolik důvěryhodně a existuje ochota svěřit mu veškeré kompetence, neměla by být ponechána byť jediná informace v kybernetickém prostředí bez dozoru. Zde více než kdekoliv jinde platí ostražitost a permanentní informovanost. V kyberprostoru jde tzv. o neuchopitelné území a nelze s ním zacházet tak přímočaře jako například s běžnou úřední žádostí.

„Neexistuje jednoznačná, všeobecne akceptovaná definícia pojmu kybernetický priestor. Kybernetický priestor možno chápať ako systém (ang. skr. SoS) zložený z rôzných digitálnych zariadení spojených počítačovými sieťami pripojenými na internet (vrátane programového vybavenia, údajov, aplikačních programov, technickej infrastruktury) a ľudí, ktorí v tomto prostore pôsobia, činností, ktoré v ňom prebiehajú, pravidiel, ktoré upravujú činnosti a vzťahy v priestore.“[21] Úředníci městských úřadů jsou značně zainteresováni v tomto systému kybernetického prostoru, a pokud je v rámci jejich pracovních činností také kybernetická bezpečnost, je pro tyto zaměstnance maximálně důležité se v tomto procesu orientovat. Aby se však v tomto procesu skutečně orientovali, musejí mít úředníci dnešní doby také povědomí o informačních technologiích, jinak by nebyli schopni celý tento proces efektivně pochopit. Spolupráce hardwaru a softwaru je tedy pro znalost úředníků stěžejní.

„Požadavky na boj proti nebezpečí v kyberprostoru jsou stále naléhavější úměrně tomu, jak se zvyšuje závislost lidské společnosti, společnosti států, samospráv, všech fyzických i právnických osob na fungování informačních a komunikačních technologií.“[22]

3.1 Kybernetická bezpečnost

Kybernetická bezpečnost znamená všeobecně obezřetné chování v rámci všech informačních technologií. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,[23] definuje pojmy, jakými jsou bezpečnostní opatření v rámci počítačové sítě či postup při hlášení incidentů z hlediska kyberprostoru a jeho narušení. Nutností je však dodržování

[20] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 36.
[21] ANDRAŠKO, J., DAŇKO, M., DRAŽOVÁ, P., GYURÁSZ, Z., MESARČÍK, M., SOPÚCHOVÁ, S. *Právo informačných a komunikačných technológií 2*. Bratislava: Tinct, 2021, s. 172.
[22] SMEJKAL, V., SOKOL, T., KODL, J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019, s. 15.
[23] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů, Česká republika*. 2014, částka 75.

zákonných opatření a doporučení, která dokážou zamezit, ale také předcházet kybernetickým hrozbám, či dokonce kybernetickým útokům.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) se na svých internetových stránkách zmiňuje o důležitosti bezpečnosti digitálních technologií a internetu, a přesto podle NÚKIB zůstává tato dovednost společností podceňovanou a nepochopenou.[24] Toto tvrzení není bohužel pro kybernetickou bezpečnost přívětivé, zvlášť pokud se o kybernetické a informační bezpečnosti velmi obsáhle zmiňuje také dokument Bezpečnostní strategie České republiky,[25] podle kterého i malá skupina aktérů může způsobit strategické narušení kybernetického prostoru.

„V súvislosti s meniacím sa charakterom bezpečnostního prostredia, ktorý ide ruka v ruke s pokrokom v oblasti vedy a techniky, sa stále častejšie stretávame aj s pojmom „kybernetická bezpečnosť". Súvisí to so stále častejšími prípadmi operácií, ktoré zasahujú do oblasti bezpečnosti v rámci kybernetického priestoru. Aktérmi v tejto súvislosti môžu byť štáty, ale aj neštátne entity či jednotlivci. Vo všeobecnosti možno pod kybernetickou bezpečnosťou rozumieť schopnost odolávať škodlivým aktivitám v rámci kybernetického priestoru."[26] Schopnost odolávat škodlivým aktivitám ovšem přímo souvisí právě s onou vzdělaností z hlediska kybernetické bezpečnosti. Zranitelnost kybernetického prostoru úředníka přímo souvisí s jeho zkušenostmi a především znalostmi v této oblasti. Městský úřad je schopen odolávat kybernetickým hrozbám natolik, nakolik jsou schopni odolávat těmto hrozbám jeho zaměstnanci.

„Kybernetická bezpečnost je úzce spojena se základními právy a svobodami zakotvenými v primárním právu, zejména v Listině základních práv EU. Uvedené propojení totiž umožňuje zajišťování dostatečné úrovně kybernetické bezpečnosti a také ochranu občanů v počítačových sítích a systémech."[27] Kybernetický prostor je neustále se vyvíjející dynamické virtuální prostředí, které nabízí neustálý přísun informací a velmi mnoho výhod. Avšak jedním z klíčových rizik je jeho anonymita. V kontextu kybernetických hrozeb a možností zneužití údajů hraje právě anonymita důležitou roli v narušení bezpečnosti informačních a komunikačních technologií.

[24] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vzdělávání.* Online. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/. [cit. 2025-01-09].
[25] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR *Bezpečnostní strategie České republiky 2023.* Dostupné z: https://mzv.gov.cz/file/5161086/Bezpecnostni_strategie_2023.pdf. [cit. 2025-01-09].
[26] VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava: Wolters Kluwer SR, 2019 s. 12.
[27] SVOBODOVÁ, M., SCHEU, H., GRINC, J. *Listina základních práv Evropské unie: deset let v praxi – hodnocení a výhled*. Praha: Auditorium, 2019, s. 148.

3.2 Narušení kybernetického prostoru

Přímé ohrožení kybernetického prostoru se nazývá kybernetická hrozba. Může znamenat narušení pracovních činností zaměstnance, ale také ohrožení v důsledku úniku informací. K takové hrozbě dochází nejčastěji v podobě prolomení hesel nebo zašifrováním sítě, především prostřednictvím škodlivých programů.

„Kybernetická hrozba je potencionální příčina nechtěného incidentu, vztahující se ke kyberprostoru, jehož výsledkem může být poškození systému nebo počítače.“[28] Oproti kybernetické hrozbě však může kybernetický útok skutečně znamenat vážné narušení počítačového systému. Pokud přímo hrozí kybernetický útok v rámci užívání zařízení ze strany úředníka, jde vždy o vážné narušení nebo omezení činnosti nejen tohoto jedince, ale i celého úřadu. Mohou být napadeny například webové stránky této instituce, které v určitou chvíli nebudou pro běžného návštěvníka dostupné. Takové ochromení organizace může znamenat nefunkčnost internetových stránek po několik hodin, ale velmi často i po mnohem delší časový úsek.

„S rastúcím počtom uživateľov ide ruka v ruke aj rastúci počet aktérov v kybernetickom prostore s rozdielnymi záujmami a cieľmi.“[29] Pokud by ale veškerá populace zachovávala zásady a pravidla obezřetného chování v kybernetickém prostoru, nehrozilo by žádné nebezpečí. Útočníci však nemají pravidla, proto musejí úředníci absolvovat vzdělávání v problematice kybernetické bezpečnosti, aby vždy byla možnost těmto útokům zabránit a nebezpečí včas odvrátit.

„Státy, organizace, ale i jednotlivci si čím dál více uvědomují, že informace a data představují významný potenciál, který je ve stále větší míře napadán kybernetickými útoky ať již s cílem zcizení, poškození, znepřístupnění, či vymazání dat.“[30] Jakmile však budou organizace na tuto možnost náležitě připraveny, lze nebezpečí kybernetické hrozby eliminovat. Důležitá je osvěta především z hlediska škodlivých programů, prolamování hesel, zálohování, aktualizací a především je stále zapotřebí dbát na vzdělanost v oblasti kybernetické bezpečnosti.

„Počítačová kriminalita sa čoraz viac dostáva do moderného každodenného jazyka s rôznymi významami a interpretáciami, ktoré sú s ňou spojené. Stala sa široko

[28] SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Brno: CERM, 2021, s. 55.
[29] VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava: Wolters Kluwer SR, 2019, s. 24.
[30] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 521.

a voľne používaným pojmom na označenie takmer akejkoľvek trestnej činnosti elektronickej povahy, ktorá zahŕňa počítačové zariadenia, elektronické siete, internet a kyberprostor.“[31] Kybernetický útok může vždy pro instituci znamenat velmi vážné následky. V takovém případě existuje možnost odcizení či ztráty dat. Těmi mohou být citlivé a osobní údaje v registrech celého městského úřadu. Dále mohou být narušeny nebo omezeny bankovní převody či pohyb peněz na bankovních účtech úřadu. Bohužel nikdy nelze předpokládat, kdy takový útok nastane, proto jsou vždy na místě veškerá preventivní opatření, a to především v oblasti informovanosti úředníků z hlediska škodlivých programů v počítačové síti.

3.3 Škodlivé programy

3.3.1 Malware

Malware je škodlivý program, který se dokáže propojit s nainstalovanými programy v počítači koncového uživatele např. prostřednictvím pracovního emailu, kde dokáže velmi intenzivně škodit. *„Za malware (složenina anglických slov malicious software – škodlivý software) je možné označit jakýkoli software využitý k 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.“*[32]

Tento škodlivý program dokáže nekontrolovatelně odesílat elektronickou poštu za uživatele, aniž by ten věděl, že byla vůbec odeslána. Tomuto uživateli se však takto odeslané správy nepodaří snadno odhalit, jelikož ty se již nikde nezobrazí. Tedy ani v odeslané poště ne.

„Od počiatkov operačných systémov sa objavujú nejaké škodlivé aplikácie, kterým vo všeobecnosti hovoríme malware. Toto pomenovanie vychádza z anglického malicious software, ktoré v sebe zahŕňa naozaj rôzny škodlivý software. Existujú také, ktoré už nemajú účinok a zmysel, no zostávajú živé svojím naprogramovaným replikovaním.“[33]

V důsledku neznalosti kybernetických hrozeb si bohužel tento škodlivý program uživatel stáhne do svého zařízení sám. Cílem bezpečného chování je tedy neotvírat elektronickou poštu a přílohy, s nimiž není úředník předem obeznámen nebo jež

[31] HALAS, N. *Dokazovanie počítačovej kriminality*. Praha: Leges, 2023, s. 15.
[32] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, s. 204.
[33] ŠALMON, T. *(Ne)bezpečný internet*. Lindeni, 2021, s. 223.

si předem sám nevyžádal. Obrana proti škodlivému programu malware je v nainstalování účinného programu, který umí zcela spolehlivě takový vir rozpoznat a okamžitě detekovat.

„Malvér umožňuje páchateľom získať vzdialený prístup k počítačovému systému a prevziať kontrolu nad jeho funkciami. Malvér možno napríklad použiť na ovládanie kurzora používateľa, zaznamenávanie stlačení klávesov (keylogger). Nahrávanie videa cez vstavanú webovú kameru, nahrávanie zvukov pomocou mikrofónu v počítači a vyhotovenie snímok obrazovky počítača. Tieto možnosti použitia malvéru možno ďalej použiť na páchanie iných počítačových trestných činov.“[34] Aby se úředníci úspěšně vyhnuli infiltraci škodlivého programu, musejí akceptovat kybernetická doporučení z hlediska eliminování kybernetických hrozeb.

3.3.2 Spyware

Spyware je typ malwaru, který rovněž dokáže sledovat uživatele při jeho pracovních činnostech, respektive sleduje jeho aktivitu na počítačovém zařízení a ukládá vše, co uživatel do svého počítače zapisuje. Jeho název je proto složen z anglického slova „spy“ jako špión, což naprosto vystihuje úlohu tohoto viru. Pro spyware jsou důležitá především hesla, která sbírá jako cenné informace, a ta pak následně odesílá útočníkovi či třetí osobě, která má o tyto údaje zájem.

„Spyware může být jednak nainstalován jako samostatný malware, jakož může být i součástí jiných, volně šířených a jinak zcela bezpečných programů.“[35] Ve zcela bezpečném programu by jistě spyware být neměl. Bohužel v těchto případech koncový uživatel nemá možnost škodlivý program sám rozpoznat a rozhodně ne v programu, který by měl uživatele primárně chránit. Ovšem i taková skutečnost se může stát, jako tomu bylo v minulosti v případě antivirové společnosti, která namísto ochrany nabídla údaje uživatelů jiné společnosti.[36] Tato skutečnost se zcela vymyká zásadám kybernetické bezpečnosti.

[34] HALAS, N. *Dokazovanie počítačovej kriminality*. Praha: Leges, 2023, s. 26.
[35] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, s. 207.
[36] SEDLÁK, J. *Avast dostal pokutu 350 milionů kvůli prodeji dat svých uživatelů*. Online. 25. 4. 2023. Dostupné z: https://www.lupa.cz/aktuality/avast-dostal-pokutu-350-milionu-kvuli-prodeji-dat-svych-uzivatelu/. [cit. 2025-01-15].

3.3.3 Vir

Vir je nákaza v systému počítačového prostředí, která je naprogramována člověkem. Dokáže sám sebe zmutovat a nekontrolovatelně se šířit do počítačových systémů koncových uživatelů. Může infikovat nejen veškeré informace a data, ale také počítačovou síť např. v rámci celé organizace.

„Jedná se o program či závadný kód, který sám sebe připojí k jinému existujícímu spustitelnému souboru (např. software aj.) či dokumentu. Virus se reprodukuje v momentě, kdy dojde ke spuštění tohoto softwaru či otevření infikovaného dokumentu.“[37] Jde o typický případ, kdy neopatrností či neznalostí základů kybernetické bezpečnosti ze strany uživatele dochází k napadení počítačového systému. Základním pravidlem pro obezřetné jednání je vyvarovat se jakéhokoliv otevírání příloh či neznámých dokumentů v pracovním e-mailu.

„Počítačové virusy, spyware, ransomware, trójské kone a ďalší nebezpečný software je správne chápať jako cielene vytvorený program, ktorý má za úlohu skrytú činnosť na počítačoch.“[38] Tyto viry jsou naprogramovány úmyslně k napadení počítačové či internetové sítě. *„Šíria sa internetom, samy sa replikujú a nepotrebujú nič ďalšie k tomu, aby mohli fungovať. Ničia súbory, premenúvajú, rušia kľúčové súbory v systémovej zložke operačného systému a niekedy len tak nezmyselne páchajú škody.“*[39]

Vir je z hlediska kybernetického prostoru velmi nebezpečný, jelikož je schopen nejen ohrozit, ale i poškodit celý počítačový systém. Úředníci musejí být obeznámeni s nebezpečím hrozby prostřednictvím viru, který se dokáže nekontrolovatelně a svévolně šířit. Informace a data v elektronické podobě dnes nestačí jen zavřít do kartotéky a opatřit bezpečnostním zámkem, jako je tomu v případě nakládání s tištěnými dokumenty. Jedná se o opatření, která v sobě zahrnují veškeré aspekty pro kybernetickou bezpečnost, jakými jsou vzdělávání úředníků v této oblasti, dále následná školení či prohlubování kvalifikace z hlediska nových kybernetických hrozeb, ale také informační a bezpečnostní opatření. Vir může být nebezpečný v podobě ochromení celé společnosti, jako je tomu v případě rozsáhlých kybernetických incidentů.

[37] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, 2016, s. 207.
[38] ŠALMON, T. *(Ne)bezpečný internet*. Lindeni, 2021, s. 222.
[39] Tamtéž, s. 225.

3.3.4 Phishing

Phishing je podvodné jednání ze strany útočníka, který se na základě klamavé informace snaží přinutit uživatele u jeho počítačového zařízení, aby svěřil své bezpečnostní údaje do rukou neznámé osoby. Phishing se ale velmi důvěryhodně tváří, že vše, co dělá, je pro samotné dobro uživatele, aniž by ten vůbec tušil, že se jedná o podvod. Informace, které vycházejí například od bankovního sektoru, skutečně jako informace z bankovního institutu vypadají. Stejně tak podvodné webové stránky jsou od těch skutečných k nerozeznání. Cílem phishingu je získat přihlašovací údaje a hesla ať již k bankovním účtům, či jiným webovým platformám.

„Ide o útoky, pri ktorých sa phishingové stránky maskujú ako legitímne webové stránky s cieľom ukradnúť osobné informácie. Vyskytujú sa v prípadoch, keď páchatelia posielajú SMS alebo e-maily so škodlivými adresami URL, čím oklamú obete, aby otvorili škodlivý odkaz, ktorý ich nasmeruje na falošnú webovú stránku s veľmi podobným vzhľadom, akým disponuje legitímna webová stránka. Obeť tak sprístupní svoje osobné údaje týkajúce sa napr. bankového účtu, pričom pachateľ môže tieto informácie použiť na získanie finančných prostriedkov na predmetnom bankovom konte.“[40]

Phishing je odvozen z anglického slova fishing, tedy „rybolov.“ Útočník tzv. hodí návnadu a čeká, až se uživatel na tuto návnadu doslova chytí.

3.4 Hesla a prolamování hesel

Prolamování hesel patří k velmi častým, dnes je možné říci, k velmi běžným kybernetickým útokům. Útočník prolamuje hesla způsobem, který systematicky zkouší mnohé kombinace, až se nakonec do některého z obvyklých hesel tzv. trefí. Slabá hesla jsou velmi snadno rozluštitelná a zpravidla jde o chabé kombinace slov a základních řad čísel. Dají se tak proto velmi snadno prolomit. Pokud je například heslo složeno ze čtyř čísel, což je skutečně chatrná kombinace, vznikne z tohoto hesla 9 999 kombinací. Útočník dokáže takové heslo prolomit do několika vteřin. Je proto velmi důležité zadávat do systému tzv. silná hesla v kombinaci malých a velkých písmen nejlépe nejen spolu s čísly, ale také se znaky a diakritikou. Při použití hesla, které obsahuje všechny tyto alternativy, by prolomení trvalo i několik desítek let.

[40] HALAS, N. *Dokazovanie počítačovej kriminality*. Praha: Leges, 2023, s. 29.

„V ideálním případě by znaky hesla neměly dohromady dávat vůbec žádný smysl, jen tak je heslo skutečně bezpečné!“[41] Odborníci rozhodně nedoporučují používat heslo, které obsahuje jméno uživatele navíc spolu s čísly, kterými jsou například data narození nebo narození svých blízkých. Jedná se o základní poučku z hlediska kybernetické bezpečnosti, aby používaná hesla byla co nejméně spojována s konkrétním uživatelem počítačové sítě. *„Nevinnými oběťmi zákeřných hackerských praktik bývají obvykle neopatrní jedinci, kteří po sobě v kyberprostoru zanechávají mnoho viditelných digitálních stop, používají příliš slabá hesla typu přímé posloupnosti jako třeba 1-2-3-4, své jméno, datum narození nebo mají zastaralý a neaktualizovaný software.“*[42]

Útočník v systému k prolomení hesel postupuje tak, že nejprve vyzkouší notoricky známé kombinace jednoduché číselné řady. Dále tuto číselnou řadu kombinuje se jmény uživatelů. Tyto varianty mohou být vyhledávány pomocí hackerských programů, které jsou velmi rychlé a útočník tak může měnit desítky až stovky známých uživatelských hesel, a to za velmi krátkou dobu.

Z tohoto důvodu mají některé internetové platformy pouze tři pokusy na přihlášení heslem, aby uživatel, který je k tomuto úkonu oprávněn, využil tento způsob pouze v omezeném čase s co nejmenším počtem pokusů. V rámci bezpečnosti jde o naprosto běžnou věc. Pokud se však uživateli nepodaří v rámci chybného pokusu správně identifikovat, je přístup k navázání spojení s platformou blokován. Toto je však z bezpečnostních důvodů správný krok právě kvůli eliminaci prolomení hesel.

„Vedle příliš jednoduchého hesla je druhou velkou chybou příliš krátké heslo. Čistě z matematického pohledu prodlužuje každý další znak jeho možné prolomení o několikanásobek.“[43]

Avšak v některých případech nejsou aplikace v rámci bezpečnosti zdaleka tak přínosné. Pak by ovšem úředníci, kteří nakládají s citlivými informacemi, měli být velmi obezřetní a samozřejmě v tomto směru také důkladně proškoleni. Stává se, že systém nutí uživatele měnit pravidelně hesla z důvodu bezpečnosti, což se ovšem z dlouhodobého hlediska ukazuje jako neefektivní způsob ochrany a zabezpečení. Hesla, která uživatel již jednou do systému zadal, jsou naopak velmi snadno zneužitelná. Pokud například úředník musí takto často měnit hesla, vyčerpá tím svou databázi obvyklých kombinací, které používá k zabezpečení aplikací, což není

[41] PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014, s. 105.
[42] MAREŠ, P. *Kyberkultura, hackeři a digitální revoluce: informace chce být svobodná.* Praha: Grada, 2022, s. 90.
[43] PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014, s. 104.

z dlouhodobého hlediska příznivé. Navíc je zřejmé, že software eviduje všechna historicky zadaná hesla v počítačovém zařízení. Útočníkovi, který se těchto informací zmocní, pak stačí tato hesla pouze přenést.

Účinná obrana proti prolamování hesel je velmi jednoduchá. Používat silná hesla v kombinaci nejen s malými a velkými písmeny, ale také s čísly. Dále je na místě používat frázovaná hesla, která obsahují diakritiku a různé pády českého jazyka.

3.5 Pracovní e-mail

Pracovní e-mail dnes slouží jako běžný způsob elektronické komunikace a je nezbytným nástrojem v rámci pracovní činnosti úředníků. Tato aplikace slouží pouze k pracovním účelům, a pokud možno v rámci bezpečnosti jen na půdě samosprávy. Dálkové připojení v rámci práce z domova již není z hlediska ochrany dat bezpečné. Pracovní e-mail by měl být používán jen v pracovním zařízení k tomu určeném. Při odesílání zpráv je velmi účinné použít šifrovaný protokol, kdy je pošta zašifrována a při otevření příjemcem je opět automaticky odšifrována. Je to velmi jednoduché a efektivní opatření, o které se softwarový program v rámci nastavení stará sám. Takto šifrovanou komunikací by v rámci bezpečnosti měly odcházet všechny pracovní e-maily úředníků městských úřadů.

„E-mail je vynimočný nástroj, ktorý nám v súčasnosti dovolí komunikovať s celým svetom, riešiť dôležité veci, odosielať potvrdenia o úhrade, objednávať tovar, ale pokojne môže predstavovať aj nástroj vydierania a zneužívania.“[44] Jedná se o cílené nástroje kybernetických útoků, vůči kterým je velmi účinné vzdělávání úředníků z hlediska kybernetických hrozeb. Městské úřady mohou být terčem útoků ze strany hackerů za účelem odcizení dat a informací, které mohou následně posloužit jako zdroj vydírání.

„Súčasní e-mailoví poskytovatelia v posledných rokoch pridali zložky pre spam a najnovšie aj pre hromadné e-maily. E-mailový obsah tak rozdělujú na správy čisté a podozrivé, prípadne reklamné. Do spamu by mali prepadávať e-maily odoslané zo spamovacích systémov, podozrivých IP adries a z podozrivých adries, prípadne s podozrivým obsahom.“[45] Každý úředník by měl nejen v rámci prohlubování kvalifikace z informačních technologií, ale zároveň také z hlediska pokroku dnešní doby náležitě rozpoznat rozdíl mezi přijatými pracovními e-maily a mezi nevyžádanou

[44] ŠALMON, T. *(Ne)bezpečný internet*. Lindeni, 2021, s. 137.
[45] Tamtéž, s. 139.

poštou. Rozhodně není na místě nevyžádané e-maily otevírat či prozkoumávat. Vždy je potřeba potenciální útok svým jednáním maximálně eliminovat.

3.6 Cookies

Myšlenka cookies je velmi přínosná. Jde o soubory, které mají uživateli zjednodušit práci na počítačovém zařízení. Jedná se např. o načítání webových stránek, přihlašovacích údajů, personifikaci, ale především o plynulý chod na internetové síti. Pokud úředník například denně nahlíží do katastru nemovitostí, lze si jen stěží představit, že po sobě pokaždé v dobrém úmyslu smaže soubory cookies a při každém dalším přihlášení tak bude trpělivě čekat na opětovnou obnovu údajů. Navíc bez technických cookies by úředník webovou stránku načetl jen velmi obtížně. Cookies se ukládají hluboko do souborů počítačového systému a tam zůstávají bez povšimnutí. Pokud na ně však opět přijde řada, například v podobě otevření již jednou prohlížené webové stránky, cookies se přihlásí o slovo a díky nim se stránka plynule načte.

„Princip cookies umožňuje odlišit jednotlivé uživatele a uložit o nich konkrétní údaje. Cookies usnadňují personalizaci. Na principu cookies jsou zpracovávány také různé statistiky, jelikož umožňují sledovat chování uživatelů v internetovém prostředí. Cookies se také používají například pro uložení potvrzení, že je uživatel přihlášen (např. do e-shopu, na sociální síť, na rozhraní administrátora, do databáze). Pro tyto cookies se používá výraz autentizací cookies. Bez nich by totiž server nevěděl, že už k přihlášení a ověření uživatele došlo, a vyžadoval by je při návštěvě každé další stránky.“[46]

Pokud se úředník pravidelně odhlašuje z aplikací, nejsou soubory cookies nikterak nebezpečné. Problém nastává tehdy, pokud úředník aplikaci opustí a neodhlásí se, tedy aplikaci pouze zavře. Ta je pak bohužel uložená v souborech cookies i s tímto přístupným heslem. A zde nastává příležitost pro zneužití dat třetích stran. Cookies je tedy z tohoto důvodu přínosné jednou za určitou dobu vymazat, avšak z hlediska bezpečnosti je vždy důležité konečné odhlášení z jakékoliv aplikace. Zamezí se tím zneužití hesla a tím i neoprávněnému vstupu třetích stran do počítačového systému úředníka.

[46] STAŇKOVÁ, L. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018, s. 219.

4 Kybernetická bezpečnost

Cílem bezpečnostních opatření je pochopit jednoduché zásady koncových uživatelů počítačové sítě, a to především v rámci kybernetických hrozeb a následných kybernetických incidentů. Je nutné chovat se maximálně obezřetně především v internetovém prostředí. V tomto ohledu platí sice velmi mnoho zásad, avšak není tak zcela obtížné je dodržovat. Postačí pravidelné odhlašování z pracovní elektronické pošty, používání silných hesel, omezení dálkového připojení a především je nutné se vyvarovat otvírání neznámých souborů či příloh, u kterých není znám jejich autor.

„Pokud říkáte, že s kybernetickou bezpečností ve firmě nemáte problémy, tak o nich ještě nevíte nebo se dějí právě teď."[47] Není proto od věci, aby organizace vyčlenila určeného zaměstnance, který v určitém režimu dohlédne na to, zda a v jaké míře jsou bezpečnostní opatření dodržována. Tento zaměstnanec by měl být zároveň koncovým uživatelům v tomto ohledu také nápomocen. Dále je potřebné ze strany úředníka pravidelné zálohování nejlépe na externí disky. Tyto disky jsou velmi efektivní z hlediska manipulace, např. pokud by organizaci hrozilo nenadálé riziko.

„Kybernetický prostor má svá specifika, neboť má virtuální povahu, nejsou zde žádné územní hranice, a vzniká tak otázka legitimity právní úpravy a uplatňování moci státních orgánů."[48] Územní samosprávné celky stojí před úkolem, jak zajistit bezpečnost počítačových systémů, jelikož legislativní rámec sice poskytuje základní strukturu pro kybernetickou bezpečnost, avšak klíčový význam má provádění konkrétních opatření. Také investice do technologií, školení a spolupráce s odborníky jsou pro ochranu kybernetického prostoru zcela zásadní.

„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."[49]

Organizační opatření je celý soubor pravidel, který s tímto opatřením souvisí. Jde o pochopení všech procesů informačních technologií zároveň spolu s analýzami rizik, nařízením o ochraně osobních údajů a školením zaměstnanců v oblasti kybernetické bezpečnosti. Z důvodu přehlednosti je velmi vhodné předat tato pravidla

[47] SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, 2021, s. 52.
[48] SVOBODOVÁ, M., SCHEU, H., GRINC, J. *Listina základních práv Evropské unie: deset let v praxi – hodnocení a výhled*. Praha: Auditorium, 2019, s. 141.
[49] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 425.

pro zaměstnance v tištěné formě. Mělo by být jasně zřetelné, co a především kdo je v tomto procesu zainteresován, aby nedošlo ke zbytečným nedorozuměním.

„Velmi důležité je dobře zabezpečit připojování a práci z domova nebo jiných vzdálených míst (coworkingová centra, kavárny, knihovny, vlaky, autobusy apod.), jelikož existuje větší riziko, že data někdo zneužije, než při práci z kanceláře.“[50] Dálkové připojení z domova, tzv. home office, není z hlediska bezpečnosti adekvátním pracovním nástrojem již kvůli zmíněnému riziku zneužití dat. Dříve byla tato možnost vítána, ale se zkušenostmi s narůstajícími kybernetickými hrozbami není tato alternativa odborníky na kybernetickou bezpečnost doporučována.

„Schopnosť nových technológií zhromažďovať obrovské množstvo údajov a následné kombinovanie týchto informácii poskytuje stále podrobnější prehľad o životě používateľov a vytvára tak predpoklady na zneužitie takýchto informácií. Zabezpečenie technológií predstavuje jednu u nejdôležitejších moderných výziev globálnej spoločnosti.“[51] Úloha zabezpečení je obtížná z důvodu tzv. neuchopitelných technologií, které nemají hranice. Internetové prostředí je propojená síť, kterou úředníci využívají v rámci registrů, jako jsou Portál občana nebo Portál veřejné správy. Slouží k vykonávání pracovních záležitostí. Veškerá data a informace je nutné ochránit tak, aby nebyly volně přístupné a aby nakládání s nimi bylo svěřeno pouze pověřeným zaměstnancům. Cizí osoba by neměla mít k informacím přístup.

4.1 Zálohování dat a informací

Jednou z možností ochrany dat v rámci kybernetické bezpečnosti je zálohování dat a informací. Tímto způsobem se veškerá data a informace pravidelně uchovávají. Jsou zabezpečeny heslem a při ztrátě dat se veškeré informace ze záloh obnoví. Pokud se jedná o ochranu osobních údajů, ty podléhají důkladné evidenci včetně jejich ochrany a zákazu přístupu neoprávněným osobám k těmto informacím. Ochranu dat přímo řeší zákon o ochraně osobních údajů a vztahuje se na veškeré osobní údaje, které orgány samosprávy zpracovávají. Proto je důležité poskytovat zaměstnancům dílčích odborů informační povědomí na základě školení o ochraně dat.

[50] STAŇKOVÁ, L. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018, s. 202.
[51] ANDRAŠKO, J., DAŇKO, M., DRAŽOVÁ, P., GYURÁSZ, Z., MESARČÍK, M., SOPÚCHOVÁ, S. *Právo informačných a komunikačných technológií 2*. Bratislava: Tinct, 2021, s. 316.

„Z hlediska zajištění kybernetické bezpečnosti jednotlivých počítačových systémů koncových uživatelů a zejména ochrany dat v nich uložených je vhodné nastavit uzamčení pevného disku či jeho šifrování.“[52]

Zálohování by mělo být naprostou prioritou z hlediska ochrany dat a informací. Koncovým uživatelům počítačových zařízení na městských úřadech běžně postačí USB Flash Disk, případně hard disk. Zálohování dat síťových úložišť organizace je pak úkolem IT specialisty.

4.2 Antivirové programy

Antivirový program je ochrana dat před škodlivými programy či nežádoucími útoky z vnějšího prostředí. Pokud uživatel na svém počítačovém zařízení otevře odkaz s virem, může infikovat nejen svůj počítač, ale i počítačovou síť. Rozdíly v antivirových programech jsou různé, avšak všechny spojuje snaha detekování škodlivých programů v počítači uživatele tak, aby počítačové zařízení bylo pod neustálou kontrolou. Některé tyto detekce se týkají samotného viru v systému, jiné přímo monitorují nebezpečné či podezřelé webové stránky, jako je tomu v případě phishingu. Principem antivirového programu je tedy detekce škodlivých programů a dohled nad komunikací s internetovým prostředím za účelem ochrany dat a informací.

„Instalovat si do stolního počítače, laptopu či mobilu nějaký antivirus dříve, než dojde k jejich napadení, by mělo být naprostým základem osobní kybernetické bezpečnosti.“[53]

4.3 Identifikační systémy

Identifikační systémy slouží ke kontrole prostředí a osob, které mají oprávnění a přístup na půdu instituce, jakou je městský úřad. Jde o zjištění identity zaměstnanců prostřednictvím přihlášení k počítačové síti. Do této evidence spadá především docházkový systém, který zahrnuje nejen evidenci příchodů a odchodů, ale také jejich identifikaci a přítomnost na pracovišti. Následným uložením do systémové databáze se monitoruje přehled pohybu zaměstnanců na pracovišti, čímž je zvýšena ochrana proti zneužití či odcizení dat a informací. Mezi další identifikační systémy patří snímače otisků prstů (biometrie), čipy, kontaktní přihlašovací karty např. přes hardware

[52] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 418.
[53] MAREŠ, P. *Kyberkultura, hackeři a digitální revoluce: informace chce být svobodná.* Praha: Grada, 2022, s. 91.

úředníka, jakým je klávesnice, ale také ostatní přístupové systémy, které zaznamenávají průchod osob do prostor úřadu. V neposlední řadě mezi bezpečnostní prvky patří také kamerový systém, který monitoruje společné prostory. Všechny tyto identifikační systémy jsou přenášeny počítačovým softwarem, který eviduje v rámci bezpečnosti veškerý pohyb na půdě instituce, do databáze.

„Je třeba si uvědomit, že bezpečnost není v současné době jen otázkou státu, který však v oblasti zajištění bezpečnosti stále hraje primární roli, ale jde o proces realizovaný i jinými subjekty (právnické a fyzické osoby), které byly v poslední době nuceny se stále více zabývat právě otázkou bezpečnosti, respektive zabezpečení svých aktivit před útoky.“[54]

Identifikační systémy kontrolují vstup osob nejen na území reálného úřadu, ale také virtuálního. Pokud při užití aplikace Identita občana vstoupí jakákoliv osoba do tohoto portálu, i ona prochází identifikačními systémy k zjištění její totožnosti. Principem všech těchto identifikačních systémů je zajištění bezpečnosti a tím zamezení a předcházení riziku kybernetického útoku z vnějšího prostředí.

4.4 Aktualizace systému

Aktualizace systému jsou důležitým úkonem z hlediska kybernetické bezpečnosti. Tyto aktualizace obsahují nové instalační verze systému, které chrání počítačové prostředí proti vniknutí viru a následnému potencionálnímu útoku ve virtuálním prostředí. Při spuštění aktualizace systému probíhají v rámci sítě opravy, kterých si úředník nemůže při své činnosti všimnout ani je sám opravit. To dokážou pouze aktualizační systémy. Smyslem těchto systémů je zvýšení bezpečnosti v kybernetickém prostředí.

Může nastat situace, že útočníci, kteří cílí bezprostředně na data městských úřadů kvůli zneužití informací, jsou o krok napřed a spolehlivý antivirový program takový útok detekuje s jistou časovou prodlevou. Z tohoto důvodu je nutné počítač úředníka aktualizovat pravidelně každý den. Takto aktualizovaný počítač je neustále v pohotovosti proti aktuálním hrozbám a riziko kybernetických hrozeb se tak účelně snižuje.

[54] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 41.

4.5 Firewall

Firewall neboli bezpečnostní brána je softwarový program filtrující internetovou komunikaci, přes kterou proudí veškerá internetová data. Tato v překladu „hořící zeď" je velmi účinná již při prvním náznaku vniknutí kybernetické hrozby směřující do počítače úředníka. Jedná se tzv. o obranu první linie, proto právem patří mezi vysoký stupeň ochrany. Brána firewall se spouští automaticky při aktualizaci systému, proto je na místě počítačové zařízení pravidelně aktualizovat.

„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."[55]

4.6 Lidský faktor v kybernetické bezpečnosti

Z hlediska celého systému je lidský faktor nejslabším článkem v soukolí kybernetické bezpečnosti, a to již od samého počátku tvorby počítačového systému až po uživatelský přístup koncového uživatele. Ten se ani nemusí dopustit výrazně fatální chyby. Stačí tak prostá věc jako zadání slabého hesla, opomenutí odhlášení z aplikace nebo absence aktualizace systému.

Úředník má jisté povědomí z hlediska možných rizik informačních technologií, to však neznamená, že nemůže být omylný. Je mnoho nástrah, které lze z hlediska zaměstnance podcenit. Dá se totiž předpokládat, že útočník je v jistém ohledu vždy napřed. Zpravidla si je dobře vědom skutečnosti, že úředník není hacker, který by dokázal do detailu domýšlet rizika kybernetického útoku. Proto jsou bezesporu tím nejdůležitějším opatřením pro organizace bezpečnostní školení z hlediska kybernetické bezpečnosti.

„Nemenej dôležité je taktiež vypracovanie analýzy rizik či vytvorenie a udržiavanie záznamu aktiv. Taktiež školenie zamestnancov organizácie v oblasti kybernetickej bezpečnosti predstavuje bezpečnostné opatrenie, ktoré môže pomôcť k zlepšeniu úrovne kybernetickej bezpečnosti v danej organizácii."[56]

Analýza rizik nejen počítačové sítě, ale celého subjektu je opatření, díky němuž se efektivita v rámci kybernetické bezpečnosti ještě zesílí. Tato analýza obsahuje

[55] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 455.
[56] ANDRAŠKO, J., DAŇKO, M., DRAŽOVÁ, P., GYURÁSZ, Z., MESARČÍK, M., SOPÚCHOVÁ, S. *Právo informačných a komunikačných technológií 2*. Bratislava: Tinct, 2021, s. 177.

veškerá opatření potřebná ke kybernetické bezpečnosti na půdě městského úřadu. Dále zohledňuje jednotlivé hardwarové komponenty včetně routerů, ale také počet zaměstnanců či velikost budovy organizace. Na základě této analýzy se následně vyhotoví soubor opatření.

Orientace a znalost úředníků v oblasti kybernetické bezpečnosti skutečně může ovlivnit chod celé organizace, jelikož i jediný zaměstnanec tak může ohrozit chod celého úřadu. Opatření pro úředníky jakožto pro koncové uživatele počítačové sítě by rozhodně měla být jasná a srozumitelná. Nabízejí se pravidla, která by mohla v tištěné formě sloužit jako jakýsi manuál pro pověřené osoby, pokud zrovna budou v obtížné situaci. Také pokyny pro správce počítačové sítě by měly obsahovat jasné formulace, jak postupovat v rámci eliminace kybernetických hrozeb.

„Cílem administrativních opatření je mít nastavené procesy, pravidla a důležité události a rozhodnutí dokumentovat. Jednak jako návod pro zaměstnance, jak mají postupovat, dále pro možnost poučit se z minulých kybernetických incidentů a vlastních slabostí či chyb a zároveň pro doložení postupu organizace a snížení regulatorního rizika.“[57]

Velká míra rizika kybernetické bezpečnosti z hlediska lidského faktoru spočívá v dálkovém připojení. *„Využívání vzdálených přístupů k počítačovým systémům umožňuje efektivněji využívat finanční i lidské zdroje. Na druhou stranu nesprávně řešený vzdálený přístup může znamenat značné bezpečnostní riziko.“*[58] Zaměstnanci by o tomto měli být informováni a používat dálkové připojení skutečně jen v nezbytných případech. Rozhodně by měli znát veškerá rizika dálkového připojení, kde hrozí také vysoká míra nebezpečí kybernetického útoku z důvodu slabého či neznámého zabezpečení přístupu z cizí sítě.

[57] NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Praha: Wolters Kluwer, 2022, s. 105.
[58] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019, s. 481.

5 Vzdělávání úředníků Městského úřadu Vejprty

Horské město Vejprty leží v Ústeckém kraji v okrese Chomutov v Krušných horách na hranici s německou obcí Bärenstein. Celkem zde žije 2 776 obyvatel (Český statistický úřad, k 1. 1. 2024) a v čele tohoto města stojí starostka, místostarosta, rada města a zastupitelstvo města.

Zdejší městský úřad je rozdělen do několika odborů, na jejichž výkon dohlíží tajemník MěÚ jako vedoucí úřadu. Jedná se o stavební odbor, sociální odbor, odbor správy bytového fondu, odbor správy majetku města, odbor dotačních titulů, ekonomický odbor a sekretariát úřadu.

Na MěÚ ve Vejprtech pracuje 21 zaměstnanců podílejících se na výkonu správních činností místního úřadu a dle zákona č. 312/2002 Sb., o úřednících územních samosprávných celků, jsou vymezeni pod pojmem úředník. Vzdělávání úředníků MěÚ ve Vejprtech je plně v kompetenci tajemníka, který řídí a kontroluje činnost zaměstnanců a zároveň podporuje zvyšování jejich kvalifikace. Úředníci se rovněž mohou podílet na výběru vzdělávacích kurzů a školení. Tento MěÚ disponuje externím IT specialistou, který je v případě potřeby čtyřiadvacet hodin plně k dispozici. Zpravidla dochází na MěÚ každý den v dopoledních hodinách a úředníci mohou s tímto externistou řešit veškeré dotazy osobně, popřípadě kdykoliv po telefonu. Tento IT specialista není zaměstnancem MěÚ ve Vejprtech.

5.1 Cíl výzkumného šetření

Cílem výzkumného šetření bylo posoudit vzdělanost úředníků MěÚ Vejprty v oblasti kybernetické bezpečnosti. Dále bylo cílem zhodnocení jejich znalostí z hlediska základních pilířů obezřetnosti proti kybernetickým hrozbám v rámci zaměstnání na MěÚ Vejprty při výkonu správních činností. Vedlejšími cíli pak bylo zanalyzovat efektivitu vzdělávání úředníků se zaměřením na oblast kybernetických hrozeb a navrhnout poté závěrečná opatření.

5.2 Metodika

Metodika pro účely vlastního průzkumu byla založena na dotazníkovém šetření mezi úředníky MěÚ Vejprty a byla rozvržena do konkrétních bodů:

1. **Příprava dotazníkového šetření**

Dotazník byl připraven tak, aby obsah korespondoval s určeným tématem tohoto výzkumu. Otázky byly sestaveny s ohledem na jasnost a srozumitelnost tak, aby respondenti správně porozuměli jejich obsahu. Dle Chrásky je *„samotný dotazník soustava předem připravených a pečlivě formulovaných otázek, které jsou promyšleně seřazeny a na které dotazovaná osoba (respondent) odpovídá písemně“*.[59]

Na oboustranném formuláři dotazníkového šetření velikosti A4 bylo respondentům osobně předloženo celkem patnáct předem připravených otázek, z nichž poslední zůstala otevřená s cílem dát respondentům prostor pro vlastní vyjádření. U uzavřených otázek měli respondenti možnost volit zpravidla mezi čtyřmi odpověďmi. Na úvodní stránce dotazníku bylo sdělení o anonymitě respondentů a také informace o zvolení jen jedné z uvedených odpovědí na každou otázku. Dále dotazník obsahoval objasnění účelu tohoto výzkumu a v případě zájmu byla respondentům nabídnuta analýza s výsledky šetření k prostudování. Závěrem bylo uvedeno také poděkování za ochotu k vyplnění.

2. **Realizace a sběr dat**

Dotazník byl ve dvou dnech osobně předložen jednotlivě všem respondentům s žádostí o jeho vyplnění. V jeden den byl předán dotazník osmnácti respondentům a druhý den byly předány zbylé tři, jelikož všichni zaměstnanci předchozí den nebyli přítomni. Další den po předložení byl proveden sběr těchto dotazníků. Vyplnění bylo zcela dobrovolné a bylo provedeno anonymní formou. Nikdo z respondentů neodmítl dotazník vyplnit, proto byla ve vlastním šetření dosažena návratnost 100 %. Sběr dotazníků byl proveden následující den, a sice 5. 12. 2024.

3. **Analýza**

V této části byla provedena analýza dat prostřednictvím grafů, a to na základě odpovědí všech respondentů, kteří se účastnili dotazníkového šetření. Tohoto průzkumu

[59] CHRÁSKA, M. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. 2., aktualiz. vyd. Praha: Grada, 2016, s. 158.

se zúčastnilo 21 úředníků, jejichž odpovědi byly důkladně zaevidovány a poté s procentuální přesností zanalyzovány do výsledků výzkumného šetření.

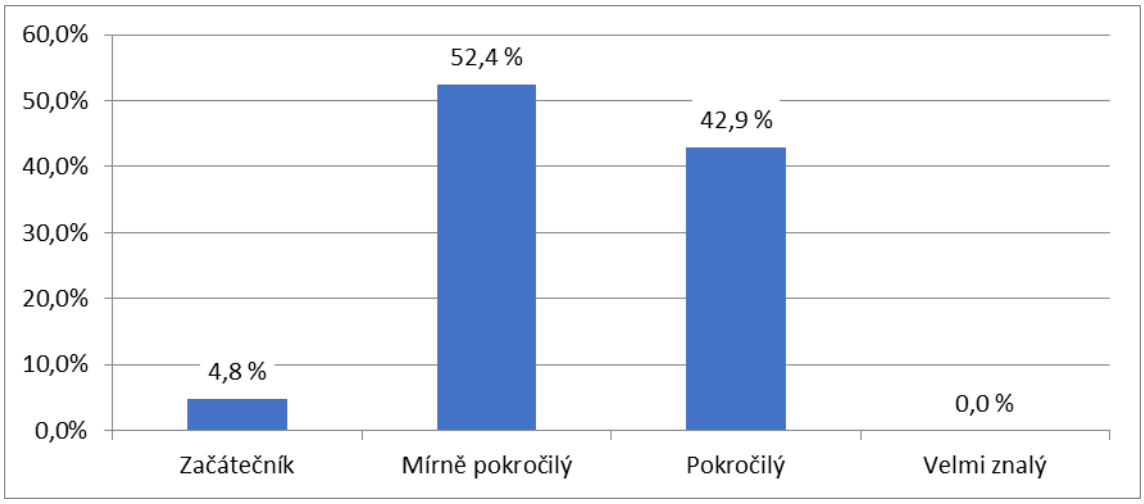
4. **Vyhodnocení**

Vyhodnocení výsledků výzkumného šetření se týká vzdělanosti úředníků z hlediska kybernetických hrozeb, ale také vzdělávání v oblasti kybernetické bezpečnosti a dále obezřetného chování při výkonu pracovních činností v zaměstnání za účelem bezpečného zacházení v rámci počítačové sítě a kybernetického prostoru. V této části jsou vyhodnoceny všechny otázky, na které respondenti prostřednictvím výzkumného šetření odpověděli.

5.3 Dotazníkové šetření

Otázka č. 1: Jak byste sám/sama sebe ohodnotil/a jako uživatele počítačového zařízení?

Graf 1: Hodnocení respondentů jako uživatelů počítačového zařízení[60]

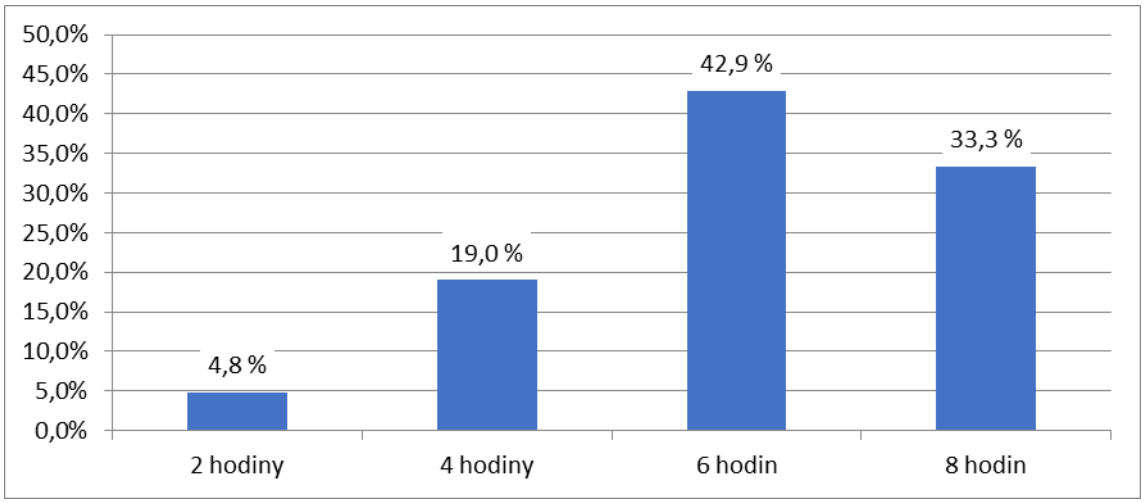


Otázka č. 1 dotazníku o kybernetické bezpečnosti měla na úvod respondenty zhodnotit jako uživatele počítačového zařízení. Variantu odpovědi „mírně pokročilý“ zvolilo 52,4 % respondentů. Druhou nejčastější odpověď „pokročilý“ zvolilo 42,9 % dotazovaných. Pouze 4,8 % respondentů se domnívá, že jsou „uživatelé začátečníci“. Žádný z respondentů se nepovažuje za „velmi znalou osobu“ v tomto oboru. Varianta „velmi znalý“ tedy nebyla nikým z dotazovaných zvolena. Je však velmi pravděpodobné, že převážná část respondentů tuto znalost přisuzuje klíčovému IT specialistovi, který na tomto městském úřadě působí.

[60] Vlastní zpracování.

Otázka č. 2: Kolik hodin ze své pracovní doby průměrně věnujete činnosti na počítačovém zařízení?

Graf 2: Denní průměrná činnost na počítačovém zařízení[61]

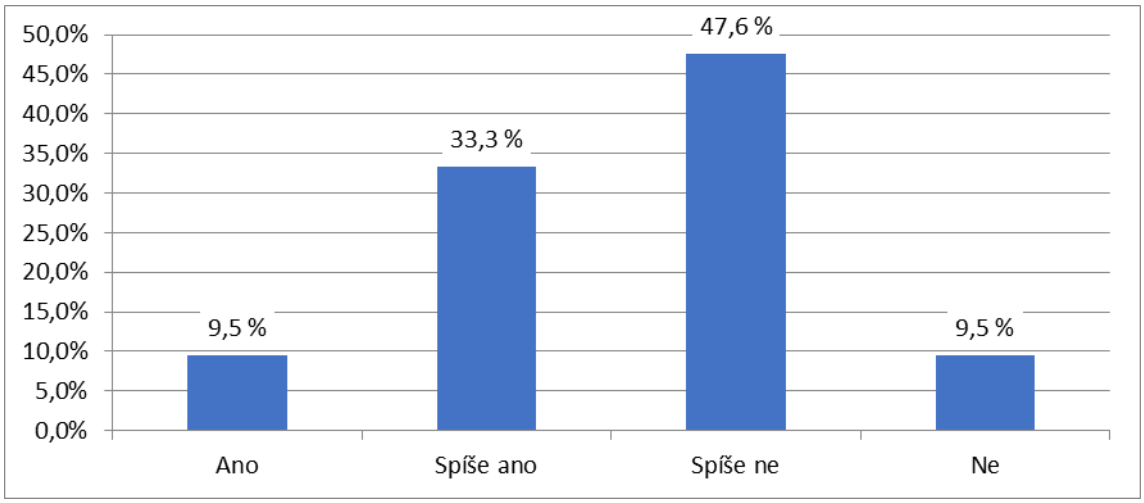


Otázka č. 2 měla zmapovat, kolik času běžný úředník věnuje své pracovní činnosti na počítačovém zařízení. Tato otázka přinesla překvapující výsledky v podobě šesti hodin denní činnosti na počítačovém zařízení u 42,9 % respondentů, a 33,3 % dotazovaných dokonce své počítačové zařízení používá v průměru osm hodin denně. Variantu čtyři hodiny zvolilo 19 % respondentů. Pouze 4,8 % dotazovaných zvolilo dvě hodiny denně.

[61] Vlastní zpracování.

Otázka č. 3: Domníváte se, že se orientujete v problematice kybernetické bezpečnosti?

Graf 3: Orientace respondentů v problematice kybernetické bezpečnosti[62]

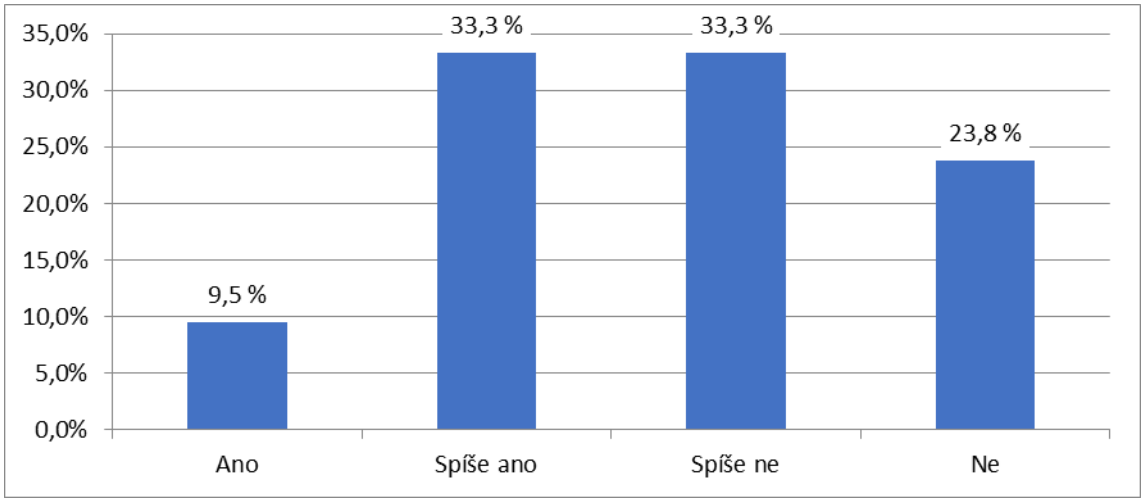


Otázka č. 3 byla klíčová pro zjištění orientace úředníků v rámci kybernetické bezpečnosti. Na otázku, zda se v této problematice respondenti orientují, zvolilo 47,6 % dotazovaných odpověď „spíše ne“. Variantu „spíše ano“ uvedlo 33,3 % respondentů. Odpověď „ano“ zvolilo 9,5 % dotazovaných a znamená to tedy, že tato skupina se v problematice jednoznačně orientuje. Ovšem stejný počet uvedl také variantu „ne“, tedy opět 9,5 %.

[62] Vlastní zpracování.

Otázka č. 4: Je Vám téma kybernetické bezpečnosti blízké?

Graf 4: Blízkost tématu kybernetické bezpečnosti[63]

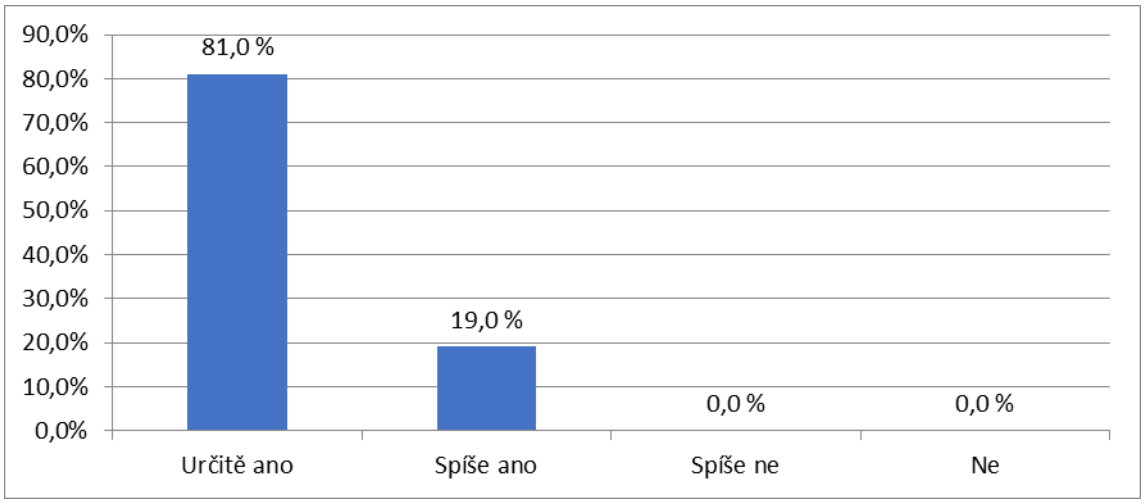


Otázka č. 4 se zaměřila na osobní názor respondentů v tom smyslu, zda zaujímají k tématu kybernetické bezpečnosti blízký postoj. Z dotazovaných 33,3 % respondentů zvolilo variantu „spíše ano“ a stejný počet respondentů 33,3 % odpověděl „spíše ne“. Variantu „ne“ uvedlo 23,8 % dotazovaných. Téma kybernetické bezpečnosti je blízké 9,5 % dotazovaných, kteří uvedli variantu „ano“.

[63] Vlastní zpracování.

Otázka č. 5: Je při výkonu Vašeho zaměstnání důležitá obezřetnost vůči kybernetickým hrozbám?

Graf 5: Obezřetnost vůči kybernetickým hrozbám[64]

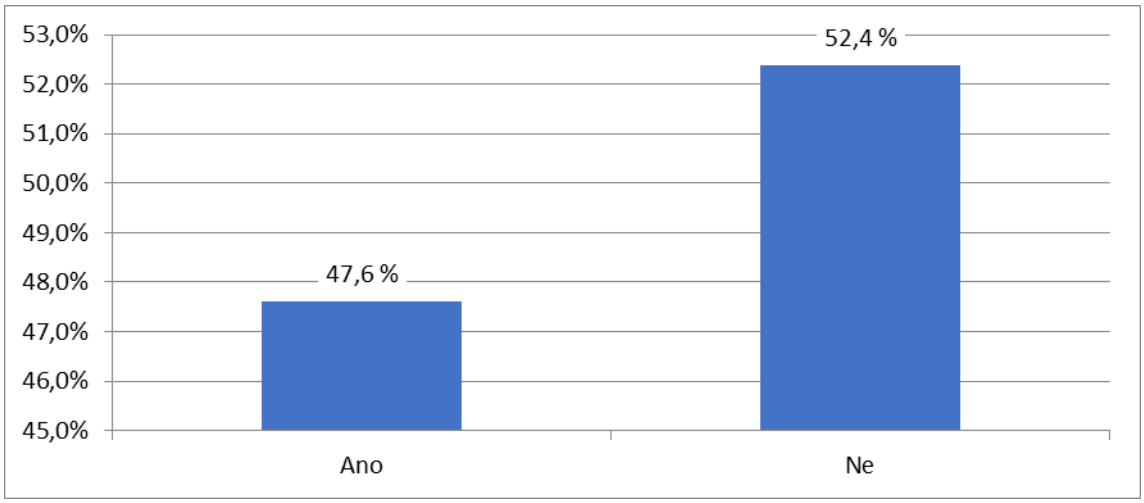


Otázka č. 5 zjišťovala, zda je pro respondenty důležitá obezřetnost vůči kybernetickým hrozbám v rámci výkonu jejich zaměstnání. Na vyhodnoceném grafu je evidentní, že respondenti zvolili pouze dvě varianty ze čtyř odpovědí. V této otázce se projevila takřka jednotnost respondentů, a sice 81 % označilo variantu „určitě ano“. Odpověď „spíše ano“ označilo 19 % dotazovaných. Žádný z respondentů nezvolil variantu odpovědí „ne“ a „spíše ne“.

[64] Vlastní zpracování.

Otázka č. 6: Absolvoval/a jste školení o kybernetické bezpečnosti v rámci vzdělávání ve Vašem zaměstnání?

Graf 6: Absolvování školení o kybernetické bezpečnosti[65]

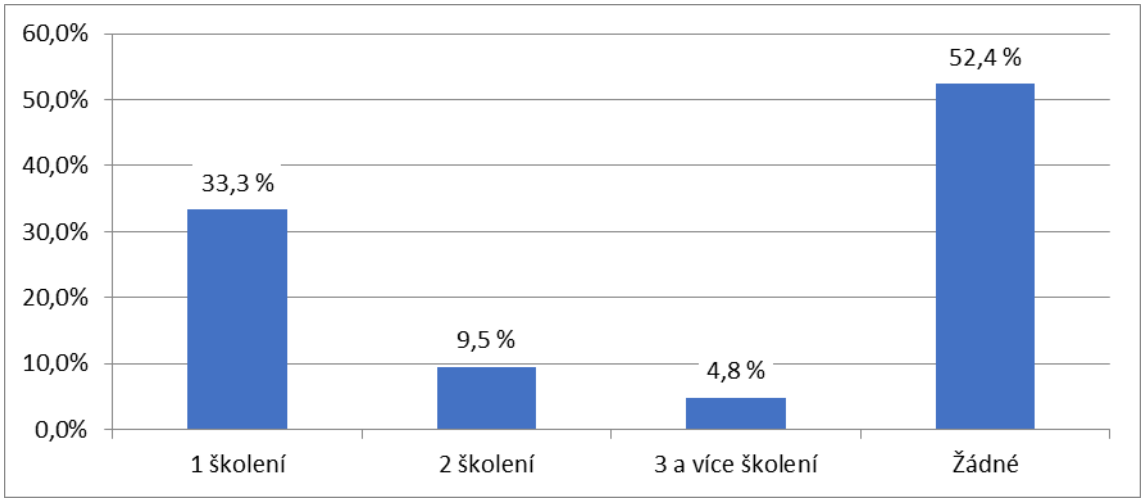


Otázka č. 6 nabízela pouze dvě varianty odpovědí a jejím úkolem bylo zjistit, zda se úředníci v oblasti kybernetické bezpečnosti vzdělávají a zda v této oblasti již nějaká školení absolvovali. Na otázku, zda úředníci již absolvovali školení, zvolilo 47,6 % respondentů variantu „ano“. Ostatních 52,4 % respondentů zvolilo variantu „ne“. Je třeba však zohlednit také zaměstnance, kteří působí na úřadě velmi krátce, a neměli tudíž možnost se tohoto školení prozatím zúčastnit.

[65] Vlastní zpracování.

Otázka č. 7: Pokud ano, kolik takových školení bylo?

Graf 7: Počet školení[66]

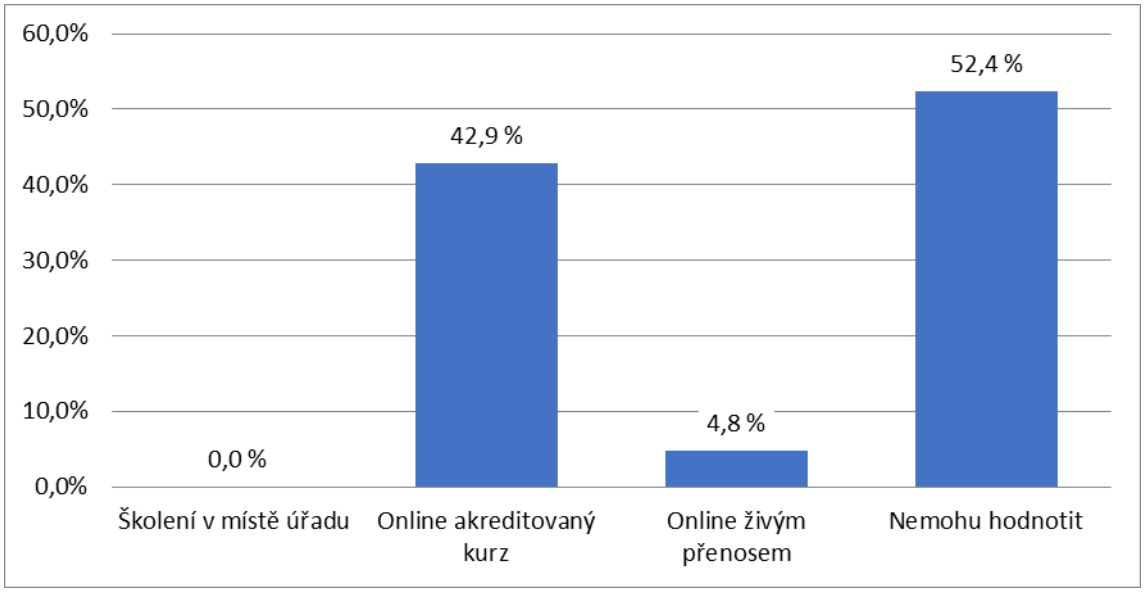


Otázka č. 7 navazovala na otázku č. 6 a zabývala se počtem absolvovaných školení v rámci kybernetické bezpečnosti. Respondenti, kteří v otázce č. 6 uvedli odpověď „ne“, zvolili v této otázce jako variantu „žádné“ (52,4 %). Variantu „1 školení“ využilo 33,3 % dotazovaných, „2 školení“ uvedlo 9,5 % dotazovaných a „3 a více školení“ 4,8 % dotazovaných.

[66] Vlastní zpracování.

Otázka č. 8: Jakou formou školení probíhalo?

Graf 8: Forma školení[67]

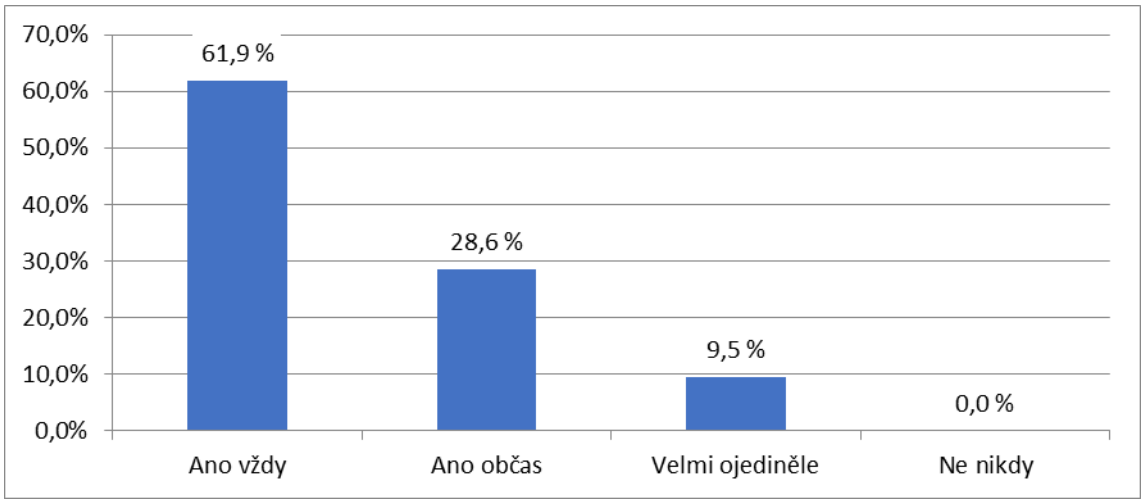


Otázka č. 8 se zabývala konkrétní formou školení v oblasti kybernetické bezpečnosti. Respondenti zvolili pouze tři ze čtyř odpovědí. Na výběr byla varianta „školení v místě úřadu“, „online akreditovaný kurz“, „online školení tzv. živě“ a samozřejmě varianta „nemohu hodnotit“ pro ty, kteří ještě žádné školení neabsolvovali. Jako svou odpověď „nemohu hodnotit“ uvedlo 52,4 % respondentů. Variantu „online akreditovaný kurz“ zvolilo 42,9 % a „online živým přenosem“ uvedlo 4,8 % dotazovaných. Varianta „školení v místě úřadu“ nebyla nikým zvolena.

[67] Vlastní zpracování.

Otázka č. 9: Používáte silná hesla, tj. kombinaci malých a velkých písmen spolu s čísly a diakritikou?

Graf 9: Používání silných hesel[68]

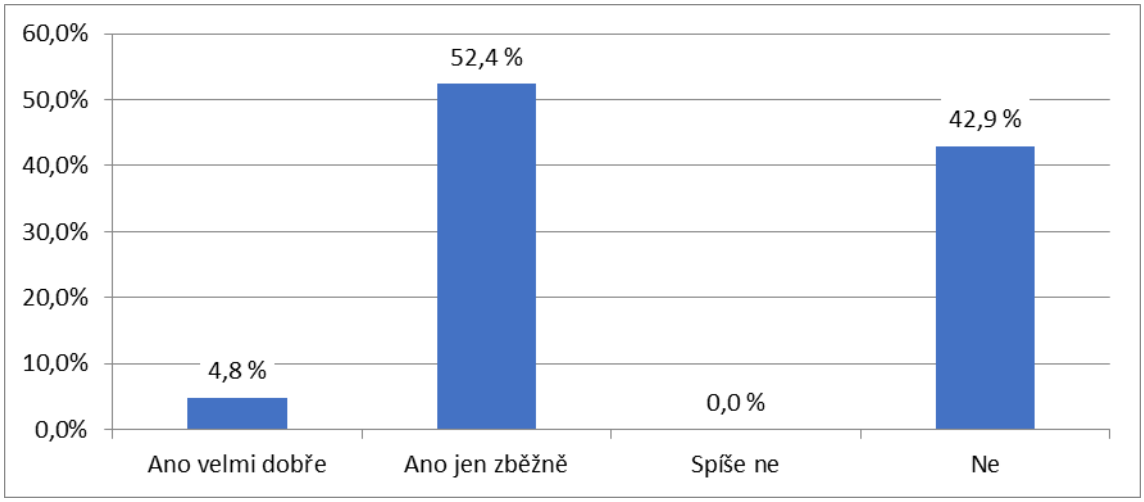


Otázka č. 9 zjišťovala, zda respondenti používají silná hesla. Z hlediska kybernetické bezpečnosti patří používání silných hesel k základním pilířům ochrany kybernetického prostoru. Úředníci MěÚ Vejprty tyto zásady s většinovou převahou dodržují. Variantu odpovědi „ano, vždy“ zvolila převážná část respondentů, a sice 61,9 %, což je velmi pozitivní zjištění. Druhou nejčastější odpovědí byla varianta „ano, občas“, kterou uvedlo 28,6 % respondentů. Nejméně odpovědí získala varianta „velmi ojediněle“, kterou si zvolilo 9,5 % dotazovaných. Velmi pozitivně lze hodnotit, že žádný z respondentů nevyužil variantu „ne, nikdy“, která zůstala v nulovém procentu.

[68] Vlastní zpracování.

Otázka č. 10: Znáte škodlivý program spyware?

Graf 10: Znalost škodlivého programu spyware[69]

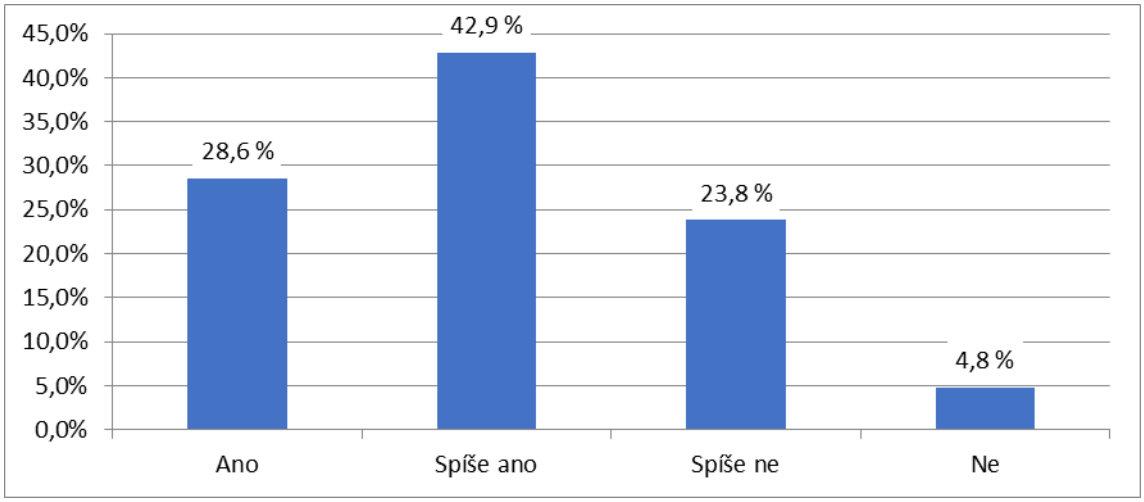


Otázka č. 10 prověřila znalost úředníků týkající se konkrétního škodlivého programu spyware, který dokáže sledovat aktivitu na počítačovém zařízení uživatele. Škodlivých programů je mnohem více, tento však patří mezi ty, které se vyskytují velmi často. Respondenti měli na výběr ze čtyř odpovědí, z nichž více jak polovina dotazovaných respondentů (52,4 %) zvolila variantu „ano, jen zběžně“. Znamená to tedy, že tato skupina má o tomto škodlivém programu alespoň částečný přehled. Variantu „ne“ zvolilo 42,9 % respondentů. Odpověď „ano, velmi dobře“ zvolilo 4,8 % dotazovaných. Varianta „spíše ne“ nebyla zvolena žádným z respondentů.

[69] Vlastní zpracování.

Otázka č. 11: Používáte zálohování dat na svém počítačovém zařízení?

Graf 11: Zálohování dat na počítačovém zařízení[70]

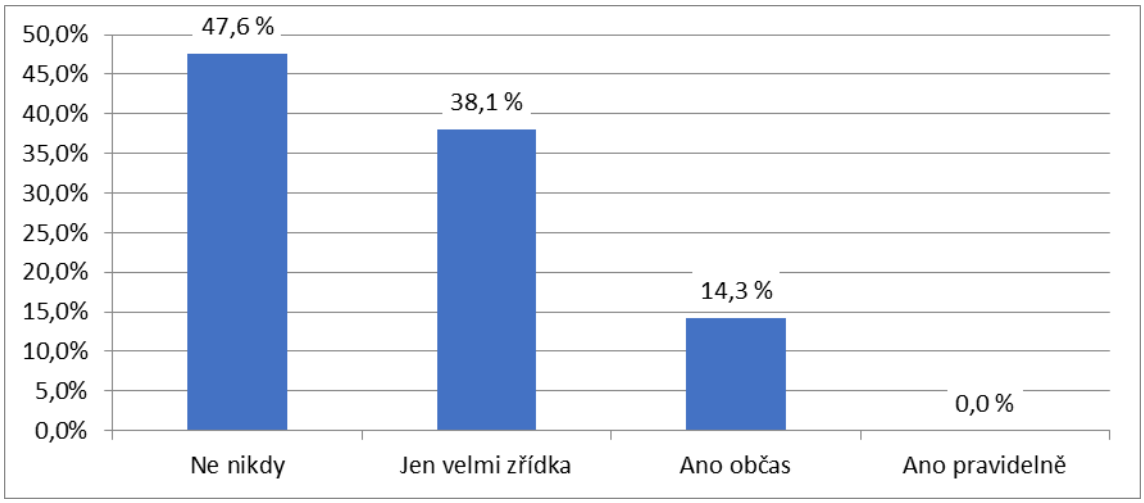


Otázka č. 11 zjišťovala, zda respondenti používají zálohování dat na svém počítačovém zařízení. Zálohování je proces pravidelného ukládání dat a informací. Variantu „spíše ano“ zvolilo 42,9 % respondentů a variantu „ano“ zvolilo 28,6 % respondentů, což znamená většinovou část úředníků, kteří zálohují data na svých počítačových zařízeních. Odpověď „spíše ne“ uvedlo 23,8 % respondentů a variantu „ne“ zodpovědělo 4,8 % dotazovaných.

[70] Vlastní zpracování.

Otázka č. 12: Pracujete z domova na svém pracovním zařízení prostřednictvím dálkového připojení?

Graf 12: Práce z domova prostřednictvím dálkového připojení[71]

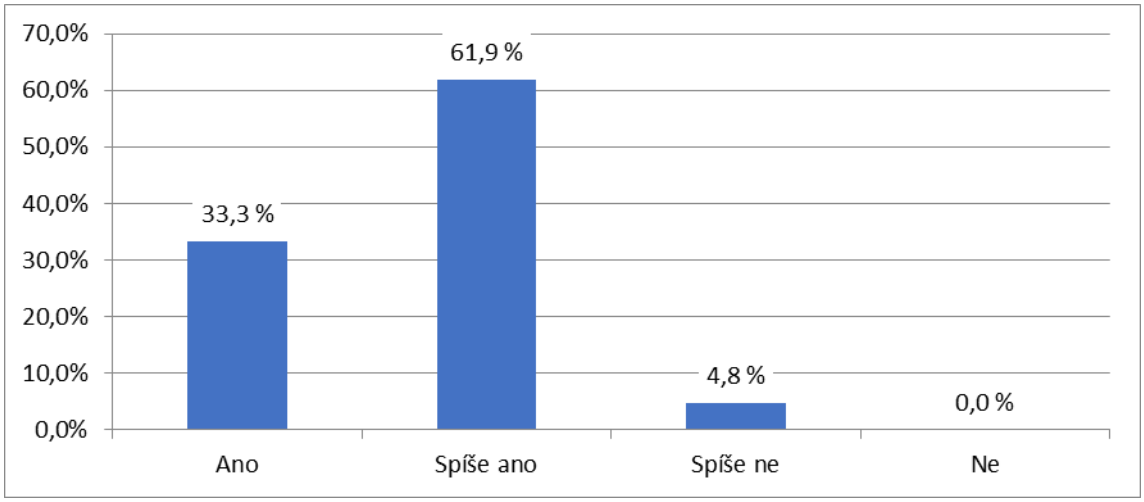


Otázka č. 12 byla zaměřena na dálkové připojení prostřednictvím vlastního počítačového zařízení z domova. Respondenti měli na výběr ze čtyř odpovědí, využity však byly pouze tři. Nejčetnější variantu „ne, nikdy“ zvolilo 47,6 % respondentů. Druhou variantu „jen velmi zřídka“ zvolilo 38,1 % respondentů. Odpověď „ano, občas“ uvedlo 14,3 % respondentů. Odpověď „ano, pravidelně“ nebyla uvedena žádným z respondentů, což znamená velmi zodpovědné jednání ze strany úředníků vůči prevenci kybernetických hrozeb.

[71] Vlastní zpracování.

Otázka č. 13: Uvítal/a byste více vzdělávání v oblasti kybernetické bezpečnosti?

Graf 13: Více vzdělávání v oblasti kybernetické bezpečnosti[72]

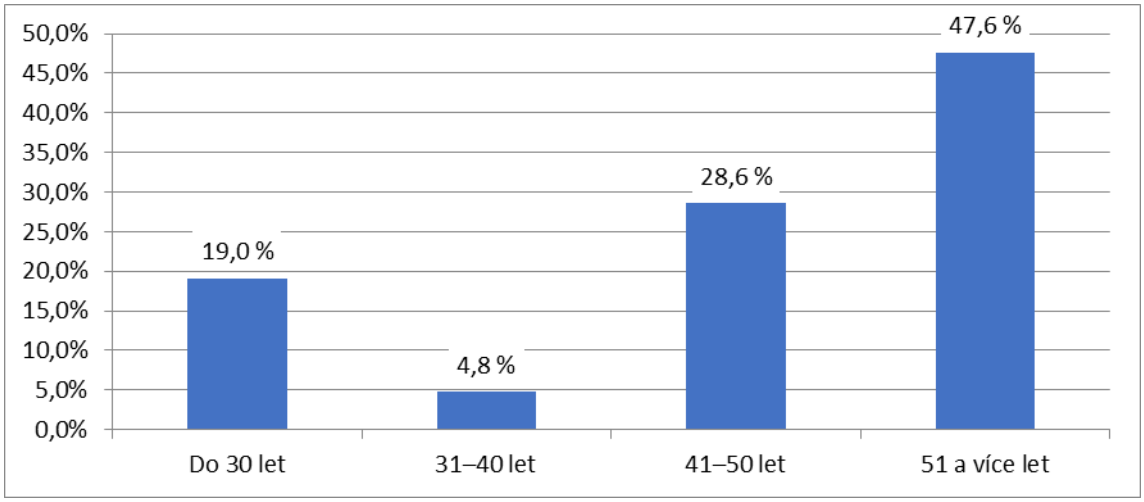


Otázka č. 13 zjišťovala u respondentů, zda by uvítali více vzdělávání v oblasti kybernetické bezpečnosti. V této otázce variantu „spíše ano“ zvolilo 61,9 % respondentů a variantu „ano“ 33,3 % respondentů. Tento výsledek je velmi příznivý pro zaměstnance MěÚ Vejprty, jelikož snaha a ochota se v této oblasti vzdělávat je pro kybernetickou bezpečnost zcela zásadní. Variantu „spíše ne“ zvolilo 4,8 % respondentů. Odpověď „ne“ nebyla zvolena žádným z dotazovaných respondentů.

[72] Vlastní zpracování.

Otázka č. 14: Kolik je Vám let?

Graf 14: Otázka na věk respondentů[73]



Otázka č. 14 byla spíše informativního charakteru a měla informovat o věku respondentů. Variantu „51 a více let“ využilo 47,6 % respondentů. Dále kategorii „41–50“ let zvolilo 28,6 % respondentů. 19 % dotazovaných zvolilo variantu „do 30 let“ a 4,8 % respondentů uvedlo odpověď „31–40 let“. Nejpočetnější věkovou kategorii na MěÚ Vejprty tvoří tedy úředníci nad padesát let.

Otázka č. 15: Máte nějaký návrh na zlepšení z hlediska kybernetické bezpečnosti ve Vašem zaměstnání?

Otázka č. 15 byla otázkou otevřenou a zjišťovala u respondentů, zda mají ve svém zaměstnání nějaký návrh na zlepšení z hlediska kybernetické bezpečnosti. Respondenti měli možnost k vlastnímu vyjádření, a mohli tak volit libovolnou odpověď. Na tuto otázku odpověděli tři respondenti. Dvě odpovědi byly shodné, respondenti uvedli „více školení“. Třetí odpověď byla o něco konkrétnější a zněla: „Investice do zabezpečení, častější školení včetně bezpečného používání mobilního telefonu.“ Tato odpověď vede k zamyšlení z hlediska kybernetické bezpečnosti v rámci používání chytrých telefonů. Zcela úzce totiž s kybernetickou bezpečností souvisí a je skutečně vhodné mít na paměti obezřetnost při užívání i těchto zařízení.

[73] Vlastní zpracování.

5.4 Vyhodnocení dotazníkového šetření

V uvedeném anonymním dotazníku bylo úředníkům Městského úřadu Vejprty nabídnuto k zodpovězení patnáct otázek. Cílem tohoto šetření bylo zjistit vzdělanost a proškolení úředníků v oblasti kybernetických hrozeb, ale také vzdělávání v oblasti kybernetické bezpečnosti v rámci pracovní činnosti.

Otázka č. 1: Jak byste sám/sama sebe ohodnotil/a jako uživatele počítačového zařízení?

Osoby zaměstnané v kancelářském prostředí nebo v administrativě tráví velmi mnoho času na počítačovém zařízení, a to platí i pro úředníky. Na základě průzkumu měli úředníci MěÚ Vejprty ohodnotit sami sebe jako uživatele a lze tedy vyjádřit spokojenost nad tím, že se drtivá většina ohodnotila jako „pokročilý“ (42,9 %) a „mírně pokročilý“ (52,4 %) uživatel počítačového zařízení.

Koncový uživatel je zaměstnanec organizace, který má možnost využívat aplikace a webové stránky a součástmi jeho zodpovědnosti jsou také dodržování bezpečnostních pravidel a ochrana osobních údajů. Znalost práce na počítačovém zařízení je v dnešní digitální době pro úředníky nutná k výkonu samosprávných činností.

Otázka č. 2: Kolik hodin ze své pracovní doby průměrně věnujete činnosti na počítačovém zařízení?

Pro zaměstnance úřadů je nezbytné vykonávat činnost, která zpravidla zahrnuje práci s tabulkami, texty nebo analýzami. Na otázku, kolik hodin věnují této činnosti, respondenti odpověděli, že v rámci své pracovní doby průměrně stráví u počítačového zařízení šest hodin (42,9 %) a osm hodin (33,3 %) denně. Tolik hodin však činí i průměrná denní odpracovaná doba těchto zaměstnanců. Znamená to tedy, že někteří úředníci používají svá počítačová zařízení v rámci své pracovní činnosti takřka nepřetržitě.

Otázka č. 3: Domníváte se, že se orientujete v problematice kybernetické bezpečnosti?

Respondenti se v této otázce měli vyjádřit, zda se orientují v problematice kybernetické bezpečnosti. Většina respondentů zvolila „spíše ne“ (47,6 %), avšak druhá nejpočetnější skupina uvedla jako svou variantu „spíše ano“ (33,3 %). Naprosto shodné odpovědi vznikly u zbylých dvou odpovědí, kdy stejný počet respondentů uvedl

odpověď „ano“ (9,5 %) i „ne“ (9,5 %). Z průzkumu tak zcela jasně vyplývá skutečnost rozdílných názorů na tuto problematiku. Úředníci jsou však klíčoví zaměstnanci pro udržení kybernetické bezpečnosti v organizaci a jejich role je zásadní pro ochranu a prevenci možných kybernetických hrozeb.

Otázka č. 4: Je Vám téma kybernetické bezpečnosti blízké?

V této otázce se respondenti zcela rozcházejí. Otázka směřovala k tématu kybernetické bezpečnosti, a to zda je respondentům toto téma blízké. Stejný počet odpovědí zazněl u varianty „spíše ano“ (33,3 %) a „spíše ne“ (33,3 %). Z výsledků je tedy patrná různorodost vztahu k tématu. Otázka směřovala spíše k sympatiím k tomuto oboru, avšak ty mohou být ovlivněny mnoha faktory, jako jsou věk, vzdělání nebo porozumění problematice v této oblasti.

Otázka č. 5: Je při výkonu Vašeho zaměstnání důležitá obezřetnost vůči kybernetickým hrozbám?

Na základě tohoto průzkumu je evidentní, jak je pro úředníky MěÚ Vejprty důležitá obezřetnost vůči kybernetickým hrozbám, ačkoliv jsou mezi těmito osobami i ti, kteří v předchozí otázce odpověděli, že jim téma kybernetické bezpečnosti není nikterak blízké. Zároveň se však takřka jednotně všichni respondenti shodují na obezřetném chování vůči kybernetickým hrozbám, kdy převážná část zvolila variantu „určitě ano“ (81 %). Zbylý počet respondentů odpověděl „spíše ano“ (19 %). Varianty odpovědi „spíše ne“ a „ne“ nebyly nikým z respondentů zvoleny. Je zřejmé, že všichni úředníci MěÚ Vejprty zcela jasně chápou toto téma jako velmi důležité pro svůj výkon v zaměstnání.

Otázka č. 6: Absolvoval/a jste školení o kybernetické bezpečnosti v rámci vzdělávání ve Vašem zaměstnání?

Dobře informovaní a vyškolení úředníci mohou lépe čelit kybernetickým hrozbám a minimalizovat tak riziko úniků dat. Dále si tak mohou lépe osvojit základní principy ochrany osobních údajů v souladu s právními předpisy. V této otázce byly jen dvě varianty odpovědí, kdy 52,4 % respondentů odpovědělo „ne“ a 47,6 % „ano“. Důležité jsou proto podpora otevřené komunikace a povzbuzování zaměstnanců, aby se v kybernetické bezpečnosti orientovali, a dokázali tak hlásit podezřelé aktivity. Kybernetická bezpečnost je dynamická sféra, která se bohužel nepřetržitě vyvíjí a jde o dlouhodobý proces, nikoliv o jednorázovou záležitost.

Otázka č. 7: Pokud ano, kolik takových školení bylo?

Otázka na konkrétní počet školení v zaměstnání úředníků v rámci kybernetické bezpečnosti byla opět zodpovězena pouze určitou skupinou úředníků, jelikož zde opět odpovídalo 47,6 % respondentů a z tohoto počtu převážná část (33,3 %) uvedla jako svou odpověď jedno školení. Veškerá vzdělávání úředníků jsou však bezesporu velmi významným profitem pro celou společnost. Zde skutečně platí: čím více, tím lépe. Z hlediska pokroku a dynamiky v této oblasti je nutné sdílení nových trendů v oblasti kybernetické bezpečnosti a rovněž reakce na bezpečnostní incidenty je nutné pravidelně simulovat.

Otázka č. 8: Jakou formou školení probíhalo?

Respondenti měli na výběr ze tří variant odpovědí, a sice školení v místě úřadu, online akreditovaný kurz a online živým přenosem, z nichž na tuto otázku opět odpovídalo 47,6 % respondentů. Z této skupiny uvedlo variantu „online akreditovaný kurz“ 42,9 % respondentů. Na základě posouzení informací z uvedených odpovědí je zřejmé, že preferovanou formou školení úředníků na MěÚ Vejprty, které je zaměřeno na kybernetickou bezpečnost, je online akreditovaný kurz.

Otázka č. 9: Používáte silná hesla, tj. kombinaci malých a velkých písmen spolu s čísly a diakritikou?

Silná hesla hrají důležitou roli v oblasti kybernetické bezpečnosti tím, že zajišťují ochranu osobních a firemních informací před neoprávněným přístupem a následným únikem dat. Úředníci MěÚ Vejprty tímto jednáním zajišťují vysoký stupeň zabezpečení proti kybernetickým hrozbám, jelikož v otázce používání silných hesel většina respondentů (61,9 %) uvedla variantu odpovědi „ano, vždy“, což je velmi dobrý postup z hlediska ochrany dat a informací. Silná hesla patří mezi základní opatření proti kybernetickým hrozbám.

Otázka č. 10: Znáte škodlivý program spyware?

Otázka zjišťující znalost konkrétního škodlivého programu spyware měla zhodnotit určitý přehled respondentů v oblasti škodlivých programů. Více jak polovina respondentů (52,4 %) vybrala variantu „alespoň zběžně“ a 4,8 % dotazovaných zvolilo variantu „ano, velmi dobře“. Z výsledků tedy vyplývá většinová informovanost úředníků v této oblasti, avšak je důležité rozšířit přehled o škodlivých programech, které účelově narušují kyberprostor. Pro spyware jsou důležitá především hesla, proto je

v oblasti kybernetické bezpečnosti velmi důležitá vzdělanost v boji proti konkrétním škodlivým programům.

Otázka č. 11: Používáte zálohování dat na svém počítačovém zařízení?

Zálohování je jedním z prvků ochrany dat v kybernetickém prostředí a slouží k prevenci možné ztráty dat v případě odcizení nebo poruchy systému. Převážná část respondentů (42,9 %) uvedla variantu „spíše ano“ a také variantu „ano“ zodpověděla početná část respondentů (28,6 %). Skutečnost, že úředníci MěÚ Vejprty zálohují počítačová data, je velmi zodpovědným jednáním vůči kybernetickým hrozbám. Zálohování na počítačovém zařízení umožňuje opětovné obnovení dat a minimalizaci negativních dopadů způsobených jejich ztrátou.

Otázka č. 12: Pracujete z domova na svém pracovním zařízení prostřednictvím dálkového připojení?

Používání vzdáleného připojení je doporučováno jen v nezbytných případech za předpokladu použití vhodných technologií k tomu určených a při dodržování veškerých zásad a bezpečnostních opatření. Velká část respondentů (47,6 %) zvolila variantu „ne, nikdy“ a druhá početnější skupina (38,1 %) zvolila variantu „jen velmi zřídka“. Je tedy evidentní, že úředníci MěÚ Vejprty eliminují svým zodpovědným chováním dálkové připojení na minimum, čímž přispívají k minimalizaci rizik kybernetického prostoru.

Otázka č. 13: Uvítal/a byste více vzdělávání v oblasti kybernetické bezpečnosti?

S rostoucí digitalizací a rozvojem informačních technologií je stále velmi důležité rozvíjet znalosti o kybernetických hrozbách, které jsou zásadním faktorem ochrany dat celé společnosti. Úředníci MěÚ Vejprty jednoznačně prokázali ochotu se v této oblasti vzdělávat, jelikož převážná část z nich (61,9 %) na tuto otázku odpověděla „spíše ano“ a jako druhá velmi početná odpověď byla zvolena varianta „ano“, kterou uvedlo 33,3 % respondentů. Velmi dobrým zjištěním této výzkumné otázky bylo, že nikdo z respondentů nezvolil variantu „ne“. Z tohoto je zřejmé, že úředníci MěÚ Vejprty by uvítali, aby se mohli více vzdělávat v oblasti kybernetické bezpečnosti.

Otázka č. 14: Kolik je Vám let?

Z odpovědí na tuto otázku bylo jednoznačně prokázáno, že na MěÚ Vejprty pracuje převážná část úředníků ve věku 51 a více let (47,6 %) a dále úředníci ve věku 41–50 let (28,6 %). Nejméně zastoupeni byli respondenti ve věku 31–40 let.

Otázka č. 15: Máte nějaký návrh na zlepšení z hlediska kybernetické bezpečnosti ve vašem zaměstnání?

Tato otázka byla otevřená a respondenti tak mohli vyjádřit nějaký návrh na zlepšení v oblasti kybernetické bezpečnosti, avšak tuto možnost využili pouze tři respondenti. Dvě odpovědi byly zcela totožné, a sice respondenti uvedli „více školení“. Dále v dotazníku zazněla odpověď, která apeluje i na vzdělávání z hlediska jiných technologií, a sice „investice do zabezpečení, častější školení včetně bezpečného používání mobilního telefonu“. Toto zařízení prostoupilo do běžného života a de facto napodobuje počítačové médium, tudíž by k němu mělo být také v tomto směru přistupováno podobně. Používání aplikací v mobilním zařízení a v počítačovém zařízení je v jistých ohledech zcela totožné. Mobilní zařízení na rozdíl od počítačového však nedokáže přinutit uživatele k úplnému vypnutí či restartování přístroje za účelem obnovení veškerých ochranných prvků v rámci kybernetické bezpečnosti, což mobilnímu přístroji zvyšuje rizikovost z hlediska kybernetických hrozeb.

V odpovědi třetího respondenta zazněly také požadavky na častější školení a investice do zabezpečení. Vložené investice do zabezpečení informačních technologií jsou velmi přínosné pro celou organizaci a jistota ve smyslu ochrany proti kybernetickým hrozbám je tím největším přínosem pro celou společnost.

5.5 Shrnutí výzkumného šetření

Cílem výzkumného šetření bylo posoudit vzdělávání úředníků MěÚ Vejprty v oblasti kybernetické bezpečnosti, které je základním aspektem pro eliminaci kybernetických hrozeb. Úředníci se sice mohou podílet na rozhodování a výběru vzdělávacích kurzů, avšak je třeba mít na paměti, že kybernetické školení není pouze jednorázovou záležitostí. Přestože někteří zaměstnanci organizace absolvovali na téma kybernetické bezpečnosti tři a více školení, oproti tomu značná skupina úředníků neabsolvovala v rámci svého zaměstnání doposud žádné. Je třeba posílit vzdělávání v oblasti kybernetické bezpečnosti a také zacílit na přímé kurzy s lektorem, který lépe dokáže simulovat hrozby v rámci výukových školení.

Cílem bylo také zhodnotit znalosti úředníků z hlediska základních pilířů kybernetické bezpečnosti a obezřetnosti vůči kybernetickým hrozbám při výkonu správních činností. Úředníci MěÚ Vejprty dokázali, že se orientují v problematice kybernetických hrozeb v rámci počítačové sítě, a to i přesto, že četnost školení v kybernetické oblasti není nijak vysoká. Také je potřeba se zmínit o nejpočetnější

věkové skupině zaměstnanců tohoto subjektu, a tou jsou osoby starší jednapadesát a více let. Znamená to tedy, že tito lidé mají již letité zkušenosti nejen s informačními technologiemi, ale také s kybernetickou bezpečností. Lze tedy úředníkům přisuzovat tyto znalosti z hlediska pokroku a dynamiky dnešní doby, která díky svému zrychlenému tempu vyžaduje totéž od zaměstnanců. Důkazem je skutečnost přijetí vysokých nároků na stále se vyvíjející oblast informačních technologií ze strany úředníků v rámci správních činností. Takovému zaměstnanci dnes již nestačí k výkonu práce papír a tužka, jako tomu bylo kdysi, avšak je nutné, aby dnešní úředník dokázal používat celou řadu inovativních programů, které musí při výkonu své práce velmi dobře ovládat. Pokud se jedná o základní programy, jakými jsou spisové služby, docházkové či komunikační systémy, dokumentové a výpočetní programy, účetní a podúčetní programy, interní aplikace, archivační systémy a další, stále se vyvíjející softwarové programy k výkonu správních činností úředníka, je proto pochopitelné, že v době informačních technologií úředník musí toto tempo akceptovat a vlivem pokroku sám sebe vzdělávat a především se v kybernetické oblasti velmi dobře orientovat.

- Na MěÚ Vejprty působí na pozici úředníků nebo pověřených osob vykonávajících samosprávnou činnost jedenadvacet žen, z nichž většina tvoří věkovou kategorii nad padesát let.
- Na základě vyhodnocení dotazníkového šetření se tito úředníci považují za mírně pokročilé až pokročilé uživatele počítačového zařízení.
- Převážná část zaměstnanců na tomto zařízení pracuje šest až osm hodin denně v rámci správních činností v zaměstnání.
- Polovina ze všech úředníků uvádí, že jim je téma kybernetické bezpečnosti dokonce blízké.
- Dle průzkumu je pro všechny úředníky MěÚ Vejprty důležitá obezřetnost vůči kybernetickým hrozbám.
- Drtivá většina úředníků používá silná hesla.
- Více než polovina úředníků MěÚ je obeznámena se škodlivým programem spyware.
- Zálohování dat, které je pilířem v oblasti kybernetické bezpečnosti, používá rovněž převážná část úředníků.
- Téměř polovina těchto zaměstnanců úřadu zachovává obezřetnost vůči dálkovému připojení, které nikdy nepoužívá.

- Absolvovaných školení z oblasti kybernetické bezpečnosti se zúčastnila necelá polovina úředníků tohoto úřadu a z tohoto počtu převážná část (33,3 %) uvedla jako svou odpověď dosavadní absolvování jednoho školení.
- Preferovanou formou vzdělávání na téma kybernetická bezpečnost je podle úředníků MěÚ Vejprty akreditované online školení.
- Takřka všichni úředníci tohoto městského úřadu se shodli, že by uvítali více vzdělávání v oblasti kybernetické bezpečnosti.

5.6 Závěrečná doporučení

- Podpora vzdělávání v oblasti škodlivých programů a kybernetických hrozeb. Rozšíření nabídky školení nejen v rámci online kurzů, ale také o přímá školení s lektorem, který dokáže efektivně prezentovat teoretické poznatky v praxi, a mnohem lépe se tak dokáže napojit na samotné posluchače. Dát prostor k diskuzi, podnětům a dotazům z hlediska kybernetických hrozeb a pravidelně simulovat bezpečnostní incidenty.
- Pověření určitého zaměstnance organizace jako poradce při dohlížení na dodržování bezpečnostních opatření. Tato osoba při zjištění některých nedostatků např. z důvodu neznalosti kybernetické bezpečnosti může dát zaměstnanci podnět k jeho opětovnému proškolení. Stejně tak v případě výskytu nového druhu kybernetických hrozeb by tato pověřená osoba měla apelovat na nová školení v oblasti kybernetické bezpečnosti.
- Zpracování analýzy rizik, která zohlední veškerá technická zařízení organizace. Z hlediska nákladů je třeba využít eventuálních dotačních titulů cílených primárně na územně samosprávné celky a jejich opatření z hlediska zabezpečení kybernetické bezpečnosti organizace, jelikož analýzy tohoto typu jsou pro samosprávy finančně velmi náročné.
- Rozšíření vědomostí o silných heslech, která jsou klíčová k eliminaci kybernetických hrozeb. Silná hesla patří k základním bezpečnostním opatřením z hlediska kybernetické bezpečnosti.
- Omezení stahování souborů a příloh, pokud není jasně definován jejich autor. Eliminace otvírání nevyžádaných souborů a důkladná kontrola adresáta při příjmu elektronické komunikace.
- Pravidelné odhlašování ze všech aplikací, řádné ukončení souborů a úplné vypnutí počítačového zařízení. Při opětovném startu počítačového zařízení

se aktivují ochranné programy, které jsou první linií obrany při vniknutí kybernetických hrozeb.

- Zavedení znalosti zabezpečení souborů a jejich zálohování, nejlépe na externí disky. Zálohování dat patří ke klíčovým prvkům kybernetické bezpečnosti v oblasti rizika jejich ztráty. Územní samosprávy spravují velké množství databází, které je nutno velmi dobře zabezpečit především kvůli úniku citlivých a osobních údajů.
- Mít na paměti nepřetržitý vývoj technologií a brát v úvahu pravidelný proces vzdělávání úředníků z hlediska bezpečnostních hrozeb. Kybernetická bezpečnost není jednorázová záležitost.

Závěr

Hlavním cílem bakalářské práce bylo zhodnotit vzdělávání úředníků z hlediska kybernetické bezpečnosti na MěÚ Vejprty a zanalyzovat tak jejich přehled v rámci základních opatření proti kybernetickým hrozbám. Metodický výzkum byl proveden dotazníkovým šetřením a na základě těchto výsledků byl vytvořen návrh vhodných doporučení ke zkvalitnění vzdělávání úředníků v oblasti kybernetické bezpečnosti. Veškerá školení zaměstnanců tohoto úřadu jsou plně v kompetenci tajemníka úřadu. Zaměstnanci si mohou vybrat libovolný okruh akreditovaných kurzů včetně kybernetické bezpečnosti. Tajemník úřadu do jejich výběru nijak nezasahuje, pouze apeluje na dostatečné množství splněných kurzů. Úředníci MěÚ Vejprty se školí nejen v oblastech potřebných pro svůj odbor, ale dále si mohou vybrat také z témat, která jsou pro výkon správních činností z jejich pohledu atraktivní.

Závěrem lze konstatovat velmi dobrý přehled zaměstnanců v oblasti kybernetické bezpečnosti a dále ochotu se v tomto oboru více vzdělávat. Průměrná věková skupina zaměstnanců nepatří do generace, která s informačními technologiemi tzv. vyrostla, ale díky jejich snaze se v této problematice orientovat především v rámci dosavadního výkonu správních činností je jejich přehled velmi překvapivý. Přestože ne všichni úředníci absolvovali školení na dané téma, v problematice kybernetické bezpečnosti se z velké části orientují a převážná většina považuje obezřetnost vůči kybernetickým hrozbám za důležitou.

Dnešní doba je obdobím, kdy informační technologie zcela posilují svou pozici, a důležitost vzdělávání z hlediska kybernetické bezpečnosti se v budoucnu stane běžnou rutinou. Než k tomu však dojde, je nyní nutné klást neustálý důraz na vzdělávání v této oblasti. Kybernetický prostor dnes využívá téměř každý, ale ne každý ho umí používat. Za kybernetickými hrozbami je vždy útočník, který využil slabého místa koncového uživatele. Počítačová zařízení sama o sobě nejsou hrozbou, avšak úředníci dnes v rámci svých správních činností využívají globální připojení, které již představuje riziko nejen pro celou instituci v podobě kybernetických útoků.

Je docela možné, že informační technologie v budoucnu prostoupí do všech oblastí našeho života, a ačkoliv je člověk svou podstatou nejinteligentnějším tvorem na světě, paradoxně je to právě on, kdo je tím nejslabším článkem v soukolí kybernetické bezpečnosti. Informační technologie mají neuvěřitelný potenciál, ale také křehkost v podobě narušení kyberprostoru. Bezpečnost jde v první linii především

se vzděláváním v této oblasti. Klást důraz na znalosti v této oblasti je tedy úkolem nejen úředníků, ale i všech ostatních. Data v počítačových systémech nemají důležitou hodnotu, tu jim dá až informace. A informace jsou velmi žádanou komoditou pro útočníky. Nelze tedy podceňovat jejich úmysly a na každé ohrožení ze strany narušitelů kyberprostoru je nutné být připraven. Pokud společnost dokáže ochránit kybernetický prostor, dokáže těmto útokům jednoznačně čelit.

Seznam použitých zdrojů

Literární zdroje

1. ANDRAŠKO, J., DAŇKO, M., DRAŽOVÁ, P., GYURÁSZ, Z., MESARČÍK, M., SOPÚCHOVÁ, S. *Právo informačných a komunikačných technológií 2*. Bratislava: Tinct, 2021. 322 s. ISBN 978-80-973837-2-5.
2. HALAS, N. *Dokazovanie počítačovej kriminality*. Teoretik. Praha: Leges, 2023. 140 s. ISBN 978-80-7502-681-1.
3. CHRÁSKA, M. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. 2., aktualiz. vyd. Praha: Grada, 2016. 254 s. ISBN 978-80-271-9225-0.
4. NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Právní monografie. Praha: Wolters Kluwer, 2022. 229 s. ISBN 978-80-7676-515-3.
5. KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, 2016. 522 s.
6. KOLOUCH, J., BAŠTA, P. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, 2019. 556 s. ISBN 978-80-88168-31-7.
7. MAREŠ, P. *Kyberkultura, hackeři a digitální revoluce: informace chce být svobodná.* Praha: Grada, 2022. 230 s. ISBN 978-80-271-3358-1.
8. PONDĚLÍČKOVÁ, K. *Zákon o úřednících územních samosprávných celků: komentář*. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2016. 236 s. ISBN 978-80-7552-301-3.
9. PETROWSKI, T. *Bezpečí na internetu: pro všechny*. Tajemství. Liberec: Dialog, 2014. 243 s. ISBN 978-80-7424-066-9.
10. RAMEŠOVÁ, K. *Právní regulace kybernetické bezpečnosti a její meze*. Právní instituty. Praha: C. H. Beck, 2023. 249 s. ISBN 978-80-7400-931-0.
11. SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Brno: CERM, 2021. 429 s. ISBN 978-80-7623-068-2.
12. SMEJKAL, V., SOKOL, T., KODL, J., *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Aleš Čeněk, 2019. 378 s. ISBN 978-80-7380-765-8.

13. STAŇKOVÁ, L. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8.
14. SVOBODOVÁ, M., SCHEU, H., GRINC, J. *Listina základních práv Evropské unie: deset let v praxi – hodnocení a výhled*. Praha: Auditorium, 2019. 267 s. ISBN 978-80-87284-78-0.
15. ŠALMON, T. *(Ne)bezpečný internet*. Lindeni, 2021. 290 s. ISBN 978-80-566-1941-4.
16. VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Monografie. Bratislava: Wolters Kluwer SR, 2019. 159 s. ISBN 978-80-571-0154-3.
17. ZANDL, P. *Mýty a naděje digitálního světa: vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích*. Pod povrchem. Brno: Jan Melvil Publishing, 2022. 288 s. ISBN 978-80-7555-175-7.
18. ZOUNEK, J., JUHAŇÁK, L., STAUDKOVÁ, H., POLÁČEK, J. *E-learning: učení (se) s digitálními technologiemi: kniha s online podporou*. Praha: Wolters Kluwer, 2016. 279 s. ISBN 978-80-7552-217-7.
19. ŽŮREK, J. *GDPR v personalistice*. 2. dopl. vyd. Práce, mzdy, pojištění. Olomouc: ANAG, [2022]. 206 s. ISBN 978-80-7554-365-3.

Elektronické zdroje

20. MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR *Bezpečnostní strategie České republiky 2023*. Dostupné z: https://mzv.gov.cz/file/5161086/Bezpecnostni_strategie_2023.pdf. [cit. 2025-01-09].
21. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vzdělávání*. Online. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/. [cit. 2025-01-09].
22. SEDLÁK, J. *Avast dostal pokutu 350 milionů kvůli prodeji dat svých uživatelů*. Online. 25. 4. 2023. Dostupné z: https://www.lupa.cz/aktuality/avast-dostal-pokutu-350-milionu-kvuli-prodeji-dat-svych-uzivatelu/. [cit. 2025-01-15].

Legislativní dokumenty

23. ČESKO. Vyhláška č. 413/2024 Sb., o zvláštní odborné způsobilosti, zkoušce vstupního vzdělávání a náležitostech osvědčení o vzdělávání úředníků územních samosprávných celků. In: *Sbírka zákonů, Česká republika*. 2024, částka 413.
24. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů, Česká republika*. 2014, částka 75.
25. ČESKO. Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů. In: *Sbírka zákonů, Česká republika*. 2002, částka 114.

Seznam zkratek

Cookies	Textové soubory uložené v počítači a sloužící k rychlému načtení údajů a k personalizaci
E-Government	Názvosloví pro elektronizaci veřejné správy
E-learning	Vzdělávání prostřednictvím informačních technologií
GDPR	Obecné nařízení o ochraně osobních údajů
Hardware	Technické vybavení
IT	Informační technologie
Malware	Škodlivý software
MěÚ	Městský úřad Vejprty
Microsoft Office	Kancelářské programy od firmy Microsoft
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Osobní počítač
Phishing	Podvodné jednání v kyberprostoru
Scanner	Digitální snímač zajišťující přenos tištěných informací
Software	Programové vybavení
Spyware	Sledovací software
USB	Universal Serial Bus

Seznam grafů

Seznam příloh

Přílohy

Příloha I: Anonymní dotazník z hlediska kybernetické bezpečnosti

Dobrý den, vážení kolegové,

jelikož jsem studentkou kombinovaného studia Vysoké školy evropských a regionálních studií, ráda bych Vás tímto požádala o vyplnění anonymního dotazníku, který bude použit k vlastnímu průzkumu za účelem zpracování bakalářské práce na téma Vzdělávání úředníků na Městském úřadě Vejprty z hlediska kybernetické bezpečnosti. Prosím zakroužkujte podle Vás jednu správnou odpověď. Na vyžádání mohu předložit konečnou analýzu s výsledky tohoto šetření.

Děkuji za pomoc a ochotu s vyplněním tohoto dotazníku.

Šárka Kaletová

1. Jak byste sám/sama sebe ohodnotil/a jako uživatele počítačového zařízení?
   a) Začátečník
   b) Mírně pokročilý
   c) Pokročilý
   d) Velmi znalý

2. Kolik hodin ze své pracovní doby průměrně věnujete činnosti na počítačovém zařízení?
   a) 2 hodiny
   b) 4 hodiny
   c) 6 hodin
   d) 8 hodin

3. Domníváte se, že se orientujete v problematice kybernetické bezpečnosti?
   a) Ano
   b) Spíše ano
   c) Spíše ne
   d) Ne

4. Je Vám téma kybernetické bezpečnosti blízké?
    a) Ano
    b) Spíše ano
    c) Spíše ne
    d) Ne

5. Je při výkonu Vašeho zaměstnání důležitá obezřetnost vůči kybernetickým hrozbám?
    a) Určitě ano
    b) Spíše ano
    c) Spíše ne
    d) Ne

6. Absolvoval/a jste školení o kybernetické bezpečnosti v rámci vzdělávání ve Vašem zaměstnání?
    a) Ano
    b) Ne

7. Pokud ano, kolik takových školení bylo?
    a) 1 školení
    b) 2 školení
    c) 3 a více školení
    d) Žádné

8. Jakou formou školení probíhalo?
    a) Školení v místě úřadu
    b) Online akreditovaný kurz
    c) Online živým přenosem
    d) Nemohu hodnotit

9. Používáte silná hesla, tj. kombinaci malých a velkých písmen spolu s čísly a diakritikou?
    a) Ano, vždy
    b) Ano, občas
    c) Velmi ojediněle
    d) Ne, nikdy

10. Znáte škodlivý program spyware?
    a) Ano, velmi dobře
    b) Ano, jen zběžně
    c) Spíše ne
    d) Ne

11. Používáte zálohování dat na svém počítačovém zařízení?
    a) Ano
    b) Spíše ano
    c) Spíše ne
    d) Ne

12. Pracujete z domova na svém pracovním zařízení prostřednictvím dálkového připojení?
    a) Ne, nikdy
    b) Jen velmi zřídka
    c) Ano, občas
    d) Ano, pravidelně

13. Uvítal/a byste více vzdělávání v oblasti kybernetické bezpečnosti?
    a) Ano
    b) Spíše ano
    c) Spíše ne
    d) Ne

14. Kolik je Vám let?
    a) Do 30 let
    b) 31–40 let
    c) 41–50 let
    d) 51 a více let

15. Máte nějaký návrh na zlepšení z hlediska kybernetické bezpečnosti ve Vašem zaměstnání?