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

BAKALÁŘSKÁ PRÁCE

VZDĚLÁVÁNÍ A ZKUŠENOSTI ZAMĚSTNANCŮ VEŘEJNÉ SPRÁVY V SAMOSTATNÉ MĚSTSKÉ ČÁSTI PRAHA - DOLNÍ CHABRY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Autor práce: Gabriela Chamrová, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M, DSc.
Katedra: Právních oborů a bezpečnostních studií

2024

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Gabriela Chamrová, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Vzdělávání a zkušenosti zaměstnanců veřejné správy v samostatné městské části Praha - Dolní Chabry v oblasti kybernetické bezpečnosti

Název bakalářské práce v anglickém jazyce: Education and Experience of Public Administration Employees in the Separate Municipal District of Prague - Dolní Chabry in the Field of Cyber Security

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): listopad 2023

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je zanalyzovat systém vzdělávání zaměstnanců na Úřadě městské části Praha-Dolní Chabry v oblasti kybernetické bezpečnosti. Vedlejším cílem je vyhodnotit stav současných kybernetických znalostí a navrhnout vhodná opatření ke zlepšení znalostí zaměstnanců.

Student: Gabriela Chamrová, DiS.	*25. 10. 2023*	
Vedoucí práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M, DSc.	30. 10. 2023	

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	13. 11. 2023	
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	13. 11. 2023	
Rektor: doc. Ing. Jiří Dušek, Ph.D.	8. 12. 2023	

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 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.

.....

Děkuji vedoucímu bakalářské práce panu Dr. h. c. doc. JUDr. Miroslavovi Felcanovi, PhD., LL.M, DSc. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

CHAMROVÁ, G. Vzdělávání a zkušenosti zaměstnanců veřejné správy v samostatné městské části Praha - Dolní Chabry v oblasti kybernetické bezpečnosti: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2024. 70 s. Vedoucí bakalářské práce: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M, DSc.

Cílem bakalářské práce je identifikovat nedostatky v oblasti vzdělávání kybernetické bezpečnosti z pohledu zaměstnanců veřejné správy v samostatné městské části Praha – Dolní Chabry a navrhnout možná doporučení pro zlepšení situace. Dílčím cílem je zjistit spokojenost se vzděláváním zaměřeným na oblast kybernetické bezpečnosti.

Práce je rozdělena na dvě části: teoretickou a praktickou. První teoretická část práce je věnována kybernetické bezpečnosti, kybernetickým útokům, jejich specifikům ve vztahu k veřejné správě a možnostem prevence a obrany. V následné části je text zaměřen na oblast vzdělávání úředníků.

Na tuto kapitolu navazuje praktická část, jejíž součástí je realizace dotazníkového šetření zaměstnanců vybraného úřadu se záměrem zjistit jejich zkušenosti a názory na oblast vzdělávání v kybernetické bezpečnosti.

Klíčová slova: bezpečnost, kybernetická bezpečnost, legislativa, veřejná správa, vzdělávání, zaměstnanec

ABSTRACT

CHAMROVÁ, G. Education and Experience of Public Administration Employees in the Separate Municipal District of Prague - Dolní Chabry in the Field of Cyber Security: bachelor's thesis. České Budějovice: University of European and Regional Studies, 2024. 70 pgs. Bachelor thesis supervisor: Dr. h. c. doc. JUDr. Miroslav Felcan, PhD., LL.M., DSc.

The aim of the bachelor thesis is to identify shortcomings in the field of cyber security education from the perspective of public administration employees in the separate municipal district of Prague - Dolní Chabry and to propose possible recommendations for improving the situation. A sub-objective is to determine satisfaction with cybersecurity education.

The thesis is divided into two parts, theoretical and practical. The first theoretical part of the thesis is devoted to cyber security, cyberattacks, their specifics in relation to public administration and possibilities of prevention and defence. In the subsequent part, the text focuses on the field of education of public officials.

This chapter is followed by a practical part, which includes the implementation of a questionnaire survey of the employees of the selected office with the intention to find out their experiences and opinions on the field of cybersecurity education.

Keywords: security, cybersecurity, legislation, public administration, education, employee

Obsah

Úvod

Vzdělávání je v současné době naprostou nezbytností v každé z existujících profesí. Díky nebývalému rozvoji technologií, ale i různých postupů a přístupů ve všech sférách současných činností včetně výrobní sféry, dochází k tomu, že vše, co se učilo ve školách před 20, někdy i 10 lety poměrně rychle zastarává a ztrácí hodnotu. I když lidé dosáhli určitého vzdělání, v praxi to znamená, že je třeba s nástupem do nového zaměstnání nutnost jejich dalšího návazného vzdělávání v dané oblasti, sféře. Nutnost neustále se vzdělávat patří k současným požadavkům moderní společnosti a v případě úředníků či obecně veřejné správy je dokonce tato povinnost zakotvena legislativně.

Zaměstnanci veřejné správy mají stanovena různá školení, která se obvykle zaměřují zejména na jejich odbornost, eventuálně na rozšíření jejich jazykových schopností, školení ve formě rozvoje informačních a komunikačních technologií apod. Navíc s tím, jak i do veřejné správy více a více pronikají digitální technologie, jsou zaměstnanci veřejné správy vedeni k průběžnému, čili následnému vzdělávání jak v digitální gramotnosti, tak s tím související i schopnosti rozpoznávat případná rizika.

Není pochyb o tom, že právě veřejná správa se stává vděčným cílem pro různé kybernetické hrozby a útoky. Je tak na místě, aby se právě rozvoj znalostí v oblasti kybernetické bezpečnosti stal i v oblasti veřejné správy důležitou součástí vzdělávání zaměstnanců, v našem případě úředníků. V nové digitální době je nutné naučit se pracovat s novými technologiemi. Jako příklad uvádím například identitu občana, datové schránky, elektronické doklady. Nové digitální technologie s sebou přinášejí i nové možnosti a rozmach kybernetických útoků, které míří hlavně na získávání informací. Právě na uvedenou oblast se zaměří tato závěrečná práce.

Text práce bude rozdělen na dvě části, část teoretickou a část praktickou. V první teoretické části práce bude pozornost věnována zejména kybernetické bezpečnosti, kybernetickým útokům, jejich specifikům ve vztahu k veřejné správě a možnostem prevence a obrany. Další část teoretické části se zaměří už na oblast vzdělávání úřadníků. Tato část zmíní a vypíchne především specifika vzdělávání v oblasti veřejné správy, používané metody a příslušnou legislativu. Následně součástí praktické části bude realizace dotazníkového šetření zaměstnanců vybraného úřadu se záměrem zjistit jejich zkušenosti a názory na oblast vzdělávání v kybernetické bezpečnosti.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce bude identifikovat nedostatky v oblasti vzdělávání kybernetické bezpečnosti z pohledu zaměstnanců veřejné správy v samostatné městské části Praha – Dolní Chabry a navrhnout možná doporučení pro zlepšení situace. Dílčím cílem bude zjistit spokojenost se vzděláváním zaměřeným na oblast kybernetické bezpečnosti.

Pro zpracování teoretické části bakalářské práce je využita metoda analýzy a komparace. Data a informace jsou čerpány z odborné literatury, legislativních zdrojů, veřejně dostupných zdrojů a směrnic Městské části Praha - Dolní Chabry.

Pro praktickou část jsem zvolila formu elektronického dotazníkového šetření, kde moji spolupracovníci byli předem informováni o jeho účelu a o tom, že poskytnuté údaje budou použity jen pro potřeby bakalářské práce. Vzhledem k malému počtu zaměstnanců našeho úřadu jsem zvolila anonymní formu odpovědí. Cílem bylo získat relevantní a důvěryhodné informace. Elektronické získání výsledků umožňuje přehledné zpracování a identifikaci problémů ve zvolené oblasti.

Sběr dat je proveden anonymní formou dotazníkového šetření mezi úředníky, které doplní grafické znázornění názorů a znalostí respondentů.

2 Kybernetická bezpečnost z pohledu veřejné správy

Digitální technologie se v současné době vyvíjejí rychlým tempem a každým rokem se náš svět významně mění. V přímém přenosu jsme tak svědky jevu zvanému digitální revoluce, a to se všemi jejími klady i zápory, jak kulturními a sociálními, tak i environmentálními. Zmíněná revoluce v průběhu několika málo desítek let významně změnila paradigma vnímání identity jedince, jeho zvyklosti, chování, kulturu, jazyk a mimo to i jeho životní prostředí.[1]

Zřetelný nárůst zavádění a používání informačních a komunikačních technologií způsobil zformování informační společnosti, urychlení komunikace a nebývalý rozvoj služeb. Tím se pochopitelně zvýšila závislost společnosti na uvedených technologiích. S narůstající závislostí společnosti na informačních technologiích stoupá riziko jejich zneužívání, které může způsobit nedozírné škody. V tomto ohledu se tak začalo intenzivně pracovat na vývoji kvalitní ochrany informačních technologií před útoky, které by mohly ohrozit jejich fungování. Cílené útoky proti informačním technologiím představují celosvětový fenomén a jejich dopad zapříčiňuje velké ekonomické škody ve veřejném i v soukromém sektoru, a to jak v národním, tak v globálním měřítku. V situacích, kdy je útok směřován proti prvkům kritické infrastruktury, je možné v konečném důsledku ohrozit bezpečnost či samotnou existenci státu.[2]

Ve vztahu k názvu kapitoly je pak na místě si onu **kybernetickou bezpečnost** definovat. Vymezuje ji např. Jirásek a kol.[3] jako „*…schopnost odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky.“* Používá se nejčastěji ve vztahu k politicky či vojensky motivovaným útokům. Jiná definice vymezuje kybernetickou bezpečnost jako soubor opatření, která se přijímají pro ochranu počítačového systému před neoprávněným vniknutím nebo útokem.[4] Sak[5] upozorňuje, že kybernetická bezpečnost má však širší rozpětí, neboť v sobě zahrnuje

[1] MAREŠ, P. Kyberkultura, hackeři a digitální revoluce Informace chce být svobodná. Praha: Grada Publishing, a.s. 2022, s. 16.
[2] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 5.
[3] JIRÁSEK, P., NOVÁK, POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA. 2012, s. 16.
[4] BAŠTA, P.; KROPÁČOVÁ, A.; KUNC, M. a kol. CyberSecurity. CZ.NIC. 2019, s. 39.
[5] SAK, P. Úvod do teorie bezpečnosti nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva. Petrklíč. 2018, s. 234.

nejen informace, ale i jejich zpracování a nově i virtuální realitu v kyberprostoru, přičemž vrcholem tohoto typu hrozby je umělá inteligence.

Opomenout nelze ani pojem **kybernetický útok**, který si lze objasnit jako aktivitu, při níž je záměrem útočníka získat, modifikovat či zničit data (informace), negativně ovlivnit či převzít kontrolu nad prvky infrastruktury systému kybernetického prostoru.[6] Zmínit lze také pojem **kybernetická hrozba,** jakožto potenciální schopnost způsobit nežádoucí incident, který může následně poškodit systém či organizaci jako celek a její aktivity. Kybernetická hrozba se může velmi rychle a nečekaně změnit ve skutečný kybernetický útok na systémy a způsobit jejich zničení či nefunkčnost (např. zničení dat a informací, jejich zpřístupnění, modifikaci, nedostupnost či ztrátu). Narušení aktiv systémů využívá hrozba jejich zranitelnost. Kybernetické hrozby mohou být náhodné (např. vymazání souboru, chybné směřování, různá opomenutí apod.), ale i úmyslné (např. hacking systému, malware, odposlech, špionáž apod.).[7]

Kybernetické hrozby je možné dělit dle různých kritérií. Kybernetická hrozba zapříčiněná člověkem může být **úmyslná** (například průnik útočníka do systému) nebo **neúmyslná** (například chyba operátora, uživatele či systému) potenciální schopnost člověka způsobit nežádoucí událost v kybernetickém prostoru. Úmyslné hrozby je možné pak dále dělit na **pasivní hrozby** a **aktivní hrozby**. Pasivní hrozbou je například monitorování provozu s cílem identifikace obsahu předávaných informací. Při pasivní hrozbě se nemění obsah přenášených informací. Aktivní hrozbou je již útok na systém samotný. Jiné dělení kybernetických hrozeb je na základní, aktivační a podkladové. **Základní hrozby** reflektují čtyři hlediska bezpečnosti informačního systému. Jde o únik informace (informace je prozrazena či odhalena), narušení integrity (zformování nových dat, změny či vymazání současných dat), potlačení služby (viz DDoS útoky) a nelegitimní použití (informační systém používá neautorizovaný subjekt). **Aktivační hrozby** aktivují základní hrozby. Jejich význam tkví v tom, že jejich provedení způsobuje okamžité zformování základní hrozby a poté i přímé ohrožení bezpečnostních parametrů systému. Je možné je následně dělit na *penetrační hrozby* (například maškaráda, obejití řízení nebo narušení autorizace) a na *implementační hrozby* (například trojský kůň a zadní vrátka). **Podkladové hrozby** prezentují takové hrozby, které zapříčiňují provedení několika základních hrozeb zároveň.[8]

[6] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 29.
[7] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 32.
[8] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 31.

V České republice mělo (až do roku 2007) řešení záležitostí kybernetické (informační) bezpečnosti ve své kompetenci Ministerstvo informatiky. To však bylo v roce 2007 zrušeno a část ministerstva zabývající se kybernetickou bezpečností se sloučila s Ministerstvem vnitra. Jelikož však Ministerstvo vnitra svou roli gestora kybernetické bezpečnosti v ČR nezvládalo podle závazků, byl gestorem problematiky kybernetické bezpečnosti v ČR v roce 2011 usnesen Národní bezpečnostní úřad. Vláda České republiky dne 19. října 2005 schválila usnesení č. 1340 o „Národní strategii informační bezpečnosti České republiky“ a o zřízení Výboru pro informační bezpečnost České republiky. Tato strategie vymezila úkoly v oblasti formování důvěryhodných informačních a komunikačních systémů v podmínkách České republiky. Na tento dokument navázal Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky. Dne 15. března 2010 schválila Vláda České republiky usnesení č. 205 o řešení problematiky kybernetické bezpečnosti. V tomto usnesení schválila řešení problematiky kybernetické bezpečnosti České republiky a ustanovila Ministerstvo vnitra České republiky gestorem problematiky kybernetické bezpečnosti a současně národní autoritou pro tuto sféru. Uvedené dokumenty byly následně několikrát novelizovány a aktualizovány na daná budoucí období. Dne 19. října 2011 přijala pak Vláda České republiky usnesení č. 781, kterým určila Národní bezpečnostní úřad zástupcem pro problematiku kybernetické bezpečnosti a současně národní autoritu pro tuto oblast. Následně pak 20. dubna 2012 Ministerstvo obrany jako první ministerstvo v ČR schválilo dokument „Koncepce kybernetické obrany rezortu Ministerstva obrany“.[9]

2.1 Digitalizace veřejné správy

Proměna soudobé společnosti na infomační společnost pochopitelně zvyšuje požadavky na digitalizaci veřejné správy a jí poskytované služby. Veřejná správa je z pohledu její digitalizace formována 8 247 informačními systémy, které jsou provozovány orgány státní správy a samosprávy. Z nich více než polovinu (4 658) tvoří dle evidence v registru práv a povinností, agendové informační systémy, které jsou napojeny na základní registry a poskytují služby občanům ČR. Rozvoj digitalizace veřejné správy je přesto v České republice pomalejší např. ve srovnání s reálným využitím digitální komunikace eBankingu.[10]

[9] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 24-26.
[10] 5. NKÚ. Souhrnná zpráva o digitalizaci veřejné správy v ČR. [online]. 2019. [cit. 26-12-2023] Dostupné z WWW: <chrome-

Digitalizace veřejné správy prezentuje zásadní součást moderního vládnutí. Umožňuje efektivní kontakt mezi občanem a státem a přináší přitom důležité organizační a ekonomické přínosy. Rozšiřování individuálních možností občana díky větší variabilitě řešení nejenže vychází vstříc modernímu životnímu stylu, ale může být i důležitým nástrojem pro zlepšování inkluze, a to jak ve vztahu ke geografickým faktorům, tak i k individuálním dispozicím. Digitalizace veřejné správy je však závislá jak na dosažení technického řešení a jeho kvalitě, tak na připravenosti občanů s digitálními nástroji pracovat. [11]

V tomto ohledu se dnes už situace zlepšuje (Internet alespoň občas používá 85 % veřejnosti, internet v mobilním telefonu má 77 %), na straně veřejné správy je problémem dosud nedostatečná digitalizace, kdy lidé stále ještě některé záležitosti mohou vyřídit pouze osobně a vnitřním limitem je nadměrná roztříštěnost vybraných systémů. Tato roztříštěnost směřuje k ekonomicky neefektivní správě. Potíže na straně poskytovatele souvisí dále s modernizací a údržbou systémů, na něž se váže problematická dodavatelská struktura. Zásadním omezením je pak nedostatek kvalifikovaných zaměstnanců veřejné správy v oblasti ICT. Omezením je rovněž schopnost státu poskytovat bezpečný a bezproblémový přístup ke svým digitálním službám a propojovat množství komplexních systémů.[12]

Ovšem i zahraniční výzkumy potvrzují, že mezi občany a úředníky veřejné správy lze považovat za jednu z hlavních překážek zavádění e-governmentu obavy z kybernetické bezpečnosti.[13]

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf>.

[11] STEM. Připravenost české společnosti na digitalizaci veřejné správy Přehledová studie vybrané teoretické a empirické literatury. [online]. 2023. [cit. 26-12-2023] Dostupné z WWW: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://osf.cz/wp-content/uploads/2023/06/Nadace-OSF_STEM_Pripravenost_ceske_spolecnosti_na_digitalizaci_verejne_spravy_2023.pdf>.

[12] STEM. Připravenost české společnosti na digitalizaci veřejné správy Přehledová studie vybrané teoretické a empirické literatury. [online]. 2023. [cit. 26-12-2023] Dostupné z WWW: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://osf.cz/wp-content/uploads/2023/06/Nadace-OSF_STEM_Pripravenost_ceske_spolecnosti_na_digitalizaci_verejne_spravy_2023.pdf>.

[13] WIRTZ, B. W. Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration. 2017, 40(13): 1085-1100.

2.2 Rizika a formy útoku v kyberprostoru z pohledu veřejné správy

Některé charakteristické útoky hackerů (jde v současnosti o nejpoužívanější typy útoků) lze rozdělit následovně:[14]

- **Bombing** – útok vycházející ze zahlcování služby pakety.
- **Defacement** – nahrazení určitých stránek jejich ideologickou nebo zesměšňující variantou (nejčastěji se tento útok objevuje v reakci na politickou situaci v regionu či ve světě).
- **DoS (Denial of Service)** – tento typ útoku nelze zařadit mezi útoky průniku do sítě, ale jedná se „pouze" o vyřazení sítě z provozu. Útočník záměrně zaplaví přístupový bod sítě svým vysíláním tak, že dochází k zahlcení datového kanálu. V důsledku toho dochází buď k jeho velkému zpomalení, či úplnému zablokování provozu sítě, která není schopna navazovat žádoucí spojení či přenášet další data.
- **DDoS (Distributed DoS)** – varianta DDoS útoku, který se realizuje z velkého množství počítačů v jednom časovém úseku.
- **MITM (Man in the Middle)** – úsilí útočníka odposlouchávat komunikaci mezi aktéry tak, že se stane aktivním prostředníkem.
- **Phreaking** – neplacené využívání telefonních linek (hovory na účet někoho jiného či jiné telekomunikační společnosti).
- **Phishing** – získávání a zneužití personálních a osobních informací z napadeného počítače s cílem technického nebo osobního zneužití.
- **Ransomware** – útok při kterém útočník prostřednictvím vzdáleného přístupu napadne počítač, zašifruje soubory či rovnou soubory systému a poté vyžaduje za odšifrování odměnu.
- **Spoofing** – útok zaměřený na falšování identity zdroje.
- **Útoky na klíčové uzly Internetu –** především jde o útoky na doménové servery.

Malý[15] uvádí, že za nejvýznamnější kybernetické hrozby ve veřejné správě se v současnosti považuje **ransomware** jakožto typ škodlivého programu, který brání v přístupu k informacím infikovaného počítače a za zpřístupnění počítače obvykle

[14] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 30.
[15] MALÝ, Z. Kybernetické hrozby ve veřejné správě a zdravotnictví. Aktuální hrozby a legislativní změny (ZKB, GDPR). [online]. 2017. [cit. 26-12-2023] Dostupné z WWW: <https://www.systemonline.cz/clanky/kyberneticke-hrozby-ve-verejne-sprave-a-zdravotnictvi.htm?mobilelayout=false>.

vyžaduje zaplacení výkupného. Obecně lze ransomware dělit na dva typy – hlasitý a tichý. Hlasitý ransomware po zašifrování počítače ihned žádá zaplacení výkupného a nedovolí jakoukoliv další činnost. Tichý ransomware po aktivaci začne pomalu šifrovat veškeré informace na discích přístupných z nakaženého počítače (i síťových) a poté se šíří po celé síti. Po určité době se smažou šifrovací klíče a až pak se zobrazí žádost na platbu výkupného. Tento typ ransomwaru je nebezpečnější, jelikož v případě chybně nastaveného zálohování můžou být i zálohy nečitelné, čili obnova nedostupných informací nereálná.

O tom, že došlo k napadení hackerem, se mohou pracovníci veřejné správy dozvědět na základě těchto projevů:[16]

- nenadálé zatížení procesoru,
- nedostupnost síťové služby,
- vyšší síťový provoz,
- ztráta či modifikace dat,
- zmenšení diskového prostoru,
- přeměna webových stránek,
- podezřelé či neznáme procesy,
- smazané/změněné/zmenšené logy,
- noví uživatelé v systému,
- cílová strana informuje, že je někým napadána,
- destabilizace systému.

Ve veřejné správě lze jako rizikovou spatřovat v tomto ohledu nedostatečnou dostupnost informací ve zdravotnickém sektoru a další problémy, jako podfinancování, nízké povědomí zaměstnanců o kybernetické bezpečnosti a problémy se zálohováním dat.[17]

2.3 Formy prevence a řešení kybernetických hrozeb

Problémem souvisejícím s řešením kybernetických útoků a hrozeb je skutečnost, že zdroj počítačového útoku je obvykle náročné odhalit, z toho důvodu je komplikované

[16] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 30-31.
[17] MALÝ, Z. Kybernetické hrozby ve veřejné správě a zdravotnictví. Aktuální hrozby a legislativní změny (ZKB, GDPR). [online]. 2017. [cit. 26-12-2023] Dostupné z WWW: <https://www.systemonline.cz/clanky/kyberneticke-hrozby-ve-verejne-sprave-a-zdravotnictvi.htm?mobilelayout=false>.

eventuální zacílení odvety. Se zvyšováním množství síťového propojování konkrétních systémů se stávají aktiva systémů více a více cílem mnoha variant hrozeb.[18]

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) nabízí pro veřejnou správu několik možností, jak předcházet a řešit kybernetické hrozby. Oporou má být zejména dokument NÚKIB s názvem **Minimální bezpečnostní standard**. Jeho součástí jsou zjednodušené principy, postupy a doporučení v oblasti kybernetické bezpečnosti právě pro organizace, které nepatří pod zákon o kybernetické bezpečnosti. Jeho součástí jsou požadavky na klasifikaci a ochranu informací, řízení dodavatelů nebo auditu kybernetické bezpečnosti. Technická část zahrnuje opatření od fyzické bezpečnosti, řízení přístupů a politiky hesel po nároky v oblasti ochrany před škodlivým kódem nebo vymezení postupů při kybernetické bezpečnostní události a incidentech. Jedním z důležitých bodů je i **potřeba zvyšování povědomí v oblasti kybernetické bezpečnosti u všech zaměstnanců** a nastavení náležitého systému jejich vzdělávání. Bez zaměstnanců důsledně proškolených a seznámených se základními bezpečnostními postupy a hrozbami mohou přijít i jinak nákladné investice do technické infrastruktury a dalších opatření vniveč. Nejslabším článkem systému kybernetické bezpečnosti organizace je člověk, který svou nevědomostí či neuváženým chováním může ohrozit jakýkoliv informační systém. Pro zvyšování povědomí o kybernetické bezpečnosti u organizací veřejné správy nabízí Národní úřad pro kybernetickou a informační bezpečnost on-line kurz základů kybernetické bezpečnosti „**Dávej kyber**“. Součástí tohoto kurzu je šest okruhů – registrace a přihlašování, e-maily a přílohy, aplikace a služby, zařízení a média, odkazy a weby, připojení a internet. Pro manažery je nabízen kurz kybernetické bezpečnosti „**Šéfuj kyber**“.[19]

Ve všech dobách byly, jsou a budou hlavním zdrojem ochrany informace. Čím vyšší hodnotu informace mají, tím je třeba věnovat větší pozornost jejich zabezpečení. Nezbytným aspektem kybernetické bezpečnosti je ochrana před krádeží identity. Pro správné nastavení bezpečnosti informací vznikly normy. Normu (standard) lze vymezit jako směrnici či pravidlo, jehož zachování je většinou závazné, např. mravní, právní, technické. Normy v oblasti bezpečnosti informací řeší nastavení řízení a hodnocení bezpečnosti informací. Normy kybernetické bezpečnosti byly zhotoveny poměrně nedávno, jelikož až v posledních letech přibývá citlivých informací uložených

[18] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 15.
[19] Deník veřejné správy. Kybernetická bezpečnost v obci – role starostů při jejím zajištění. [online]. 2022. [cit. 26-12-2023] Dostupné z WWW: <https://www.dvs.cz/clanek.asp?id=6824726>.

v počítačích, které jsou připojeny k Internetu. Instituce a podniky mají vyšší potřebu k zabezpečení informační (počítačové) bezpečnosti, jelikož potřebují chránit své obchodní tajemství, důvěrné informace a osobní údaje (například o jejich partnerech, zákaznících anebo zaměstnancích. Pro řešení bezpečnosti informací v organizaci, kde se mimo elektronických nosičů informací vyskytují i neelektronické (například v listinné podobě), je tak nutné zabezpečit veškeré formy informací, se za nejlepší normu pro oblast řízení bezpečnosti jeví norma ČSN ISO/IEC 27001 a pro praktické zavedení pak ČSN ISO/IEC 27002.[20]

[20] HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012, s. 14-15.

3 Vzdělávání zaměstnanců ve veřejné správě

Veřejnou správu lze definovat jako správu, v rámci které spravovaný objekt prezentuje věc veřejnou, případně představuje spravovaný objekt veřejný majetek. Veřejnou správou se myslí především správa území (státu, kraje, obce), správa věcí, správa záležitostí (veřejné problémy, služby veřejnosti, občanům), správa financí nebo správa objektů (užívání veřejných objektů aj.).[21] V současnosti se chápe veřejná správa jako činnost služby pro obyvatelstvo, služba veřejnosti. Jednou z nejdůležitějších zásad ve veřejné správě je zásada zákonnosti. Jedná se o formu ochrany veřejného zájmu, činnost preventivní a represivní. Aktivita veřejné správy je kontrolována, a to především volenými orgány na dané úrovni, např. parlamentem, vládou, nebo nezávislými soudy, včetně soudů správních, speciálně zřizovanými kontrolními orgány (u nás např. Nejvyšší kontrolní úřad, třeba ale i občany prostřednictvím petic aj.).[22] Veřejná správa se poté rozděluje na státní správu a samosprávu.

Co se týče vymezení vzdělávání, pak například Zormanová[23] uvádí, že vzdělávání je proces, konkrétně *„…proces formování osobnosti, názorů a zájmů.“* Vzdělávání má spojitost především se socializací člověka, přičemž největší důraz se při vzdělávání klade na rozvoj poznávacích oblastí a kvalit jedince. Při vzdělávání si vzdělávající se úředník osvojuje znalosti, dovednosti, postoje, včetně hodnot, norem a metod dalšího nabývání poznatků. Výsledek vzdělávání pak prezentuje vzdělání.

Nejefektivnější je vždy systematické vzdělávání pracovníků. Důležitým prvkem systematického vzdělávání je promyšlenost a jeho logická návaznost. Musí se jednat o plánované, správně cílené a organizované aktivity.[24]

Hlavním účelem vzdělávání pracovníků je systematicky formovat, prohlubovat a rozšiřovat vědomosti a schopnosti zaměstnanců k realizaci domluvené práce a dosahování žádaných výkonů. Pakliže se vzdělávání realizuje v organizaci systematicky, dokáže připravit pracovníky na neustálé změny podmínek a požadavků různých pracovních míst i celé organizace. Připravenost na změny, související se

[21] KÁŇA, V. Základy veřejné správy. Montanex. 2007, s. 9.
[22] PEKOVÁ, J., JETMAR, M., PILNÝ, J. Veřejná správa a finance veřejného sektoru. Praha: ASPI. 2005, s. 87-88.
[23] ZORMANOVÁ, L. Obecná didaktika: Pro studium a praxi. Praha: Grada Publishing, a.s., 2014, s. 21.
[24] URBANCOVÁ, H.; FAJČÍKOVÁ, A. Vzdělávání zaměstnanců. Je to aktivita managementu lidských zdrojů jen pro některé? Práce a mzda, 2019, (7): 46-50.

schopností a motivací pracovníků využít změnu jako příležitost, zajišťuje organizaci potřebnou konkurenceschopnost.[25]

Začátek 21. století představuje období zřetelného přelomu ve společenských podmínkách, které vyvolávají podstatnou změnu v nahlížení na místo, funkci i očekávaný vývoj vzdělávání. Vychází to z toho, že je současná společnost označována za společnost založenou na vědění – tzv. „znalostní společnost“. Znalosti se na jedné straně stávají čím dál více neopominutelnou ekonomickou kategorií, na druhé straně i předmětem tržní směny. Uvedené si žádá změnu současných vzdělávacích soustav směrem k systémovému vzdělávání. Systémové pojetí výuky a vzdělávání počítá s potřebou adekvátně reagovat na potřeby praxe i na vývoj vnějšího prostředí, klade důraz na myšlení v termínech vztahů, souvislostí a kontextů – tj. na systémové myšlení. Jen systémové vzdělávání může přinést novou cestu v pohledu na svět. Stejné je to i u pracovníků veřejné správy, kteří musí odpovídat evropskému standardu odborníka pro třetí tisíciletí, tj. musí být konkurenceschopní a plně se orientovat a etablovat v politické realitě České republiky, Evropské unie, středoevropského prostoru i světa.[26]

Ve vztahu k tomu, že se ekonomiky a trhy práce permanentně mění, začíná být pořád důležitější schopnost učit se a přizpůsobovat se novým úkolům a zaměstnáním. Přechod k digitální ekonomice pozvolna proměňuje soubor nezbytných kompetencí, což se týká pochopitelně i úředníků. Digitální dovednosti sehrávají v současné ekonomice a společnosti nesporně důležitou roli. Do budoucna se jeví jako zásadní především kombinace specifických digitálních dovedností s mediální gramotností, sociálně-behaviorálními a dalšími průřezovými kompetencemi, včetně kritického myšlení, týmové práce, odolnosti, komunikace, sebevyjádření a kreativity. Mezi klíčové dovednosti a dovednostní skupiny, které zaměstnavatelé považují na prvních místech a rostoucí do roku 2025, náleží skupiny jako kritické myšlení a analýza, podobně jako řešení problémů a dovednosti v sebeřízení, jako je aktivní učení, odolnost, tolerance stresu a flexibilita.[27]

[25] ŠIKÝŘ, M. Personalistika pro manažery a personalisty: 2., aktualizované a doplněné vydání. Praha: Grada Publishing a.s., 2016, s. 138.
[26] ŠIMKOVÁ, E. Systémový přístup ke vzdělávání pracovníků veřejné správy. Olomouc: Univerzita Palackého v Olomouci, 2005, s. 142-147.
[27] VALA, J. Celoživotní vzdělávání a dovednosti pro 21. století. Bezpečnost a hygiena práce. 2022, (2): 26-28.

3.1 Specifika vzdělávání úředníků

Tak jako každý jiný zaměstnanec, i u úředníků platí, že se učí různými způsoby. Někteří upřednostňují spíše formální prostředí, např. v kurzech vedených instruktorem či učebně. Jiní mohou upřednostňovat samostudium, eventuálně si sami chtějí vybrat, co se mají učit. Tento fakt je nezbytné vnímat, jelikož některé orgány veřejné služby mohou pokládat školení buď za poskytovanou „výhodu“ nebo benefit, zatímco jiné ji mohou považovat jako akci, která se může zrealizovat jen ve chvíli, když se prokáže přímá a explicitní spojitost mezi výkonem úředníka a poskytovaným vzděláváním. Mnozí zaměstnanci se učí neformálně plněním pracovních úkolů či s pomocí mentora. Poskytování různých příležitostí ke vzdělávání a oslovení maximálního množství zaměstnanců je pro úspěch profesního vzdělávání podstatné. Na výsledky vzdělávání mají vliv i jiné faktory. Například zaměstnanci pečující o děti nebo mající jiné povinnosti mohou mít potíže se účastnit školení v určitou denní dobu nebo kdekoliv mimo místo bydliště. Ne všichni zaměstnanci budou mít zájem plnit roli mentora nebo lídra a uvedené techniky profesního rozvoje nemusí představovat nejlepší volbu pro všechny pracovní pozice. Účinná strategie profesního rozvoje by měla brát ohled na různé styly vzdělávání a potřeby zaměstnanců a měly by se umět flexibilně přizpůsobovat a poskytovat takové vzdělávací příležitosti, které reálně zabezpečí nejlepší výsledky.[28]

Vzdělávání úředníků, respektive pracovníků veřejné správy je stejně důležité jako vzdělávání odborníků v jakékoli firmě. Pouze na základě základních ekonomických, sociálních a environmentálních vědomostí mohou být úředníci schopni systematicky analyzovat veškeré procesy a děje a poskytovat tak praktická a logicky zdůvodnitelná doporučení. Šimková[29] navrhuje rámcový návrh obsahu vzdělávání pracovníků veřejné správy, který se skládá z:

Oblast vzdělávání:	**Obsah vzdělávání:**
Ekonomická	- ekonomie (základy mikro a makroekonomie, trh, tržní hospodářství), - ekonomika (daně a daňové právo, ekonomické analýzy a rozbory),

[28] OECD. Přehled o stavu veřejné správy: Česká Republika. Česká republika na cestě k modernější a efektivnější veřejné správě. OECD Publishing. 2023, s. 294.
[29] ŠIMKOVÁ, E. Systémový přístup ke vzdělávání pracovníků veřejné správy. Olomouc: Univerzita Palackého v Olomouci, 2005, s. 142-147.

	- ekonomika zahraničního obchodu (mezinárodní organizace, mezinárodní právo, integrační procesy a EU), - marketing (prezentace a vybrané způsoby propagace), - management (strategický management, management jako proces, mýtus manažerského týmu a týmové role, time management, SWOT analýza, podnikatelský záměr, jeho typy a postup při zpracování), - personalistika (řízení lidských zdrojů, vedení a motivace zaměstnanců, jejich hodnocení, odměňování a vzdělávání, získávání pracovníků, adaptace a orientace, řešení konfliktů), - účetnictví (vedení účetnictví, hospodářský výsledek a účetní závěrka, mzdová agenda a daňové přiznání) atd.
Sociální	- antropologie (sociální a kulturní), - sociologie (sociologie politiky, sociologie rodiny, města, průmyslu, kultury, sociologický průzkum atd.), - filosofie a historie-psychologie (obecná a psychologie osobnosti), - veřejná a sociální politika, sociální zabezpečení, - sociální a charitativní práce, - komunikace a komunikační služby, asertivita, - etika a etické chování atd.
Environmentální	- státní politika v oblasti ŽP (strategie TUR, Agenda 21, regionální rozvoj a TUR, Program obnovy venkova a revitalizační programy), - environmentalistika (základní prvky ŽP, indikátory TUR, globální problémy ŽP Země, environmentální rizika), - legislativa a právo ŽP (souhrn základních legislativních norem v oblasti ŽP, mezinárodní úmluvy o ŽP, Česká inspekce ŽP), - ekonomie a ekonomika ŽP (trh a ŽP, globalizace a dopady na ŽP, strukturální fondy, registr environmentálně šetrných technologií a výrobků, jejich označování, ekologické daně), - technická a technologické stránka péče o ŽP (technologické principy čištění vod, ovzduší, recyklace a likvidace odpadů,

	zavádění EMAS, IPPC a certifikací omezujících vliv podniku na ŽP), - environmentální vzdělávání a výchova (státní program EVVO, principy ekologické výchovy, ekologické poradenství, environmentální etika, řešení ekologické krize) atd.

Pro vzdělávání úředníků je specifické, že neexistuje žádná společná strategie nebo plán vzdělávání a profesního rozvoje pro všechny úřady. Vzdělávání je decentralizované a každý úřad musí realizovat identifikaci vzdělávacích potřeb a vytvořit roční plán vzdělávání. Je však otázkou, do jaké míry se současná struktura a nabídka vzdělávání (forma a obsah) podílí na budování vysoce výkonné veřejné správy. Jedním z hlavních problémů veřejné správy je, že iniciativy ohledně vzdělávání nevychází z žádné národní strategie. Většina úřadů provádí své vlastní vzdělávací iniciativy na podkladě analýzy potřeb, které v žádném případě nejsou standardizovány napříč ostatními úřady.[30]

Svoboda[31] vyzdvihuje, že pro vzdělávání ve veřejné správě může být přínosnější, pokud je realizováno mimo státní sektor. Další vzdělávání úředníků pomáhá zvyšovat kvalitu veřejné správy. K tomu se využívají různé vzdělávací programy. Vhodné může být právě využití i vzdělávacích institucí, které stojí mimo, a nejsou na ní závislé. Taková instituce může poskytnout službu, kterou nemohou splnit nadřízené správní úřady či jimi zřízené instituce. Veřejné správě může prospět pohled odlišný od pohledu správních úřadů. Soukromá vysoká škola či obdobná soukromá vzdělávací instituce dokážou nabídnout odborné vzdělání a nastavit vhodné zpětné zrcadlo. V těchto vzdělávacích programech učí zkušení odborníci, u nichž se kombinuje zkušenost z veřejného sektoru se zkušeností v oblasti soukromého práva. Nejlepší pro splnění očekávaného poslání může být vzdělávací instituce, která funguje bez veřejné podpory. Ideálně vysoká škola, které prospívá jen ze školného, neboť ta si může dovolit nutnou akademickou svobodu. Může nabídnout vlastní vzdělávací programy a kvalitní učitele, teoretiky i zkušené praktiky. Navíc platí, že soukromá vzdělávací instituce, která funguje pouze ze školného, si nemůže dovolit nezajímavé nebo nekompetentní učitele.

[30] OECD. Přehled o stavu veřejné správy: Česká Republika. Česká republika na cestě k modernější a efektivnější veřejné správě. OECD Publishing. 2023, s. 291.
[31] SVOBODA, C. Vzdělávání veřejné správy v soukromých rukách. [online]. 2021. [cit. 26-12-2023] Dostupný z https://www.epravo.cz/top/aktualne/vzdelavani-verejne-spravy-v-soukromych-rukach-113834.html.

3.1.1 Legislativa

Systém vzdělávání úředníků řeší **zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů.** Nová úprava byla schválena 13. června 2002 a účinnosti nabyla 1. ledna 2003 s výjimkou ustanovení dotýkajících se akreditace vzdělávacích institucí a vzdělávacích. Dle tohoto zákona je vzdělávání úředníků povinné. Povinnost zajistit prohlubování kvalifikace má územní samosprávný celek a současně i vytvořit plán vzdělávání, který obsahuje časový rozvrh prohlubování kvalifikace úředníka v rozsahu nejvýše 18 dní po dobu následujících tří let. Úředník se musí účastnit vstupního vzdělávání (do 3 měsíců), průběžného vzdělávání, přípravy a ověření zvláštní odborné způsobilosti, přípravy vedoucích úředníků, přičemž zákon určuje také lhůtu, v níž musí vzdělávání absolvovat. Vzdělávání mohou poskytovat akreditované instituce.[32]

Součástí vstupního vzdělávání je:[33]

a) *„znalosti základů veřejné správy, zvláště obecných zásad organizace a činnosti veřejné správy a územního samosprávného celku, základy veřejného práva, veřejných financí, evropského správního práva, práv a povinností a pravidel etiky úředníka,*
b) *základní dovednosti a návyky potřebné pro výkon správních činností,*
c) *znalosti základů užívání informačních technologií,*
d) *základní komunikační, organizační a další dovednosti vztahující se k jeho pracovnímu zařazení.“*

Zakončení vstupního vzdělávání se prokazuje osvědčením vydaným vzdělávací institucí, která vstupní vzdělávání zařídila. Povinnost absolvovat vstupní vzdělávání se netýká úředníka, který má zvláštní odbornou způsobilost.[34]

Součástí průběžného vzdělávání je „*…prohlubující, aktualizační a specializační vzdělávání úředníků zaměřené na výkon správních činností v územním samosprávném celku, včetně získávání a prohlubování jazykových znalostí.“*[35] Průběžné vzdělávání bývá realizováno prostřednictvím kurzů. O účasti úředníka na jednotlivých kurzech činí

[32] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 17.
[33] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 19.
[34] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 19.
[35] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 20.

rozhodnutí vedoucí úřadu na podkladě potřeb územního samosprávného celku a s ohledem na plán vzdělávání úředníka; úředník se kurzu zúčastnit musí. Účast na kurzu, který je součástí průběžného vzdělávání, se prokazuje osvědčením vydaným vzdělávací institucí, která kurz pořádala.

Správní činnosti určené prováděcím právním předpisem zabezpečuje územní samosprávný celek úředníky s prokázanou **zvláštní odbornou způsobilostí**. Úředník musí prokázat zvláštní odbornou způsobilost k výkonu správních činností určených prováděcím právním předpisem do 18 měsíců od vzniku pracovního poměru k územnímu samosprávnému celku případně ode dne, kdy začal vykonávat činnost, která je podmíněna prokázáním zvláštní odborné způsobilosti. Zvláštní odborná způsobilost se skládá z vědomostí a dovedností nutných pro výkon činností určených prováděcím právním předpisem. Zvláštní odborná způsobilost se skládá z obecné a zvláštní části. Součástí obecné části je znalost základů veřejné správy, zejména obecných principů organizace a činnosti veřejné správy, znalost zákona o obcích, zákona o krajích, zákona o hlavním městě Praze a zákona o správním řízení, a schopnost nabyté vědomosti využít. Zvláštní část zahrnuje znalosti nutné k výkonu správních činností určených prováděcím právním předpisem, hlavně znalost působnosti orgánů územní samosprávy a územních správních úřadů vztahující se k uvedeným činnostem, a schopnost jejich využití. [36]

Zvláštní odbornou způsobilost musí prokazovat úředníci územních samosprávných celků vykonávajících konkrétní správní činnosti, které stanovuje Vyhláška č. 512/2002 Sb., o zvláštní odborné způsobilosti úředníků územních samosprávných celků.[37] Další podstatnou vyhláškou je pak Vyhláška č. 304/2012 Sb., *o* uznání rovnocennosti vzdělání úředníků územních samosprávných celků. Dále se k profesi úředníků vztahuje Vyhláška č. 162/2015 Sb., o podrobnostech úřednické zkoušky a další.

Zákon o úřednících se specificky staví ke vzdělávání vedoucích úředníků[38]. Vedoucí úředníci zabezpečují řízení úředníků. Musí mít ukončené vzdělávání vedoucích úředníků. Účast na vzdělávání vedoucích úředníků se prokazuje osvědčením vytvořeným vzdělávací institucí, která kurz vedla. Vedoucí úředník si musí ukončit vzdělávání vedoucích úředníků do 2 let ode dne, kdy nastoupil do funkce vedoucího úředníka.

[36] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 21.
[37] ČESKO. Vyhláška č. 512/2002 Sb., o zvláštní odborné způsobilosti úředníků územních samosprávných celků, § 1.
[38] ČESKO. Zákon č. 312/2002 Sb., o úřednících uzemních samosprávných celků a o změně některých zákonů, § 27.

Součástí vzdělávání vedoucích úředníků je obecná a zvláštní část. V rámci obecné části se seznamují se znalostmi a dovednostmi v oblasti řízení úředníků. Ve zvláštní části pak s přehledem o činnostech určených prováděcím právním předpisem vykonávaným podřízenými úředníky. Pokud náklady na vzdělávání hradí územní samosprávný celek, má vedoucí úředník povinnost setrvat po ukončení tohoto vzdělávání v pracovním poměru k tomuto územnímu samosprávnému celku alespoň 3 roky. Pokud by tento úředník rozvázal s územním samosprávným celkem pracovní poměr před touto lhůtou, musí zaplatit územnímu samosprávnému celku náklady s tímto vzděláváním související (pakliže by došlo k rozvázání pracovního poměru po necelém splnění této lhůty, uhradí vedoucí úředník poměrnou část).

Zákon o úřednících od svého přijetí zaznamenal několik dílčích novelizací, žádná z nich se hlouběji nezabývala sférou vzdělávání úředníků. Prohlubování kvalifikace úředníků je bezpochyby jedním ze základních požadavků kvalitního výkonu veřejné správy v území. Na začátku roku 2023 byl předložen návrh zaměřující se hlavně na oblast vzdělávání úředníků. Jádro zamýšlených změn tvoří nově utvářené vstupní vzdělávání úředníků, zrušení obecné části zvláštní odborné způsobilosti a ponecháním jen její zvláštní části zaměřené prakticky na míru potřebám konkrétní správní činnosti. V oblasti průběžného vzdělávání úředníků má dojít k jeho jasné orientaci na vědomosti a dovednosti nutné pro výkon správních činností. Mělo by také dojít k omezení rozsahu předepsaného vzdělávání pro úředníka z 18 pracovních dnů v průběhu 3 let na 9 pracovních dnů s tím, že do průběžného vzdělávání úředníků se budou počítat i školení na tzv. měkké dovednosti (soft skills) za podmínky, že jsou v přímé vazbě na některou ze správních činností. Záměrem návrhu zákona je i zjednodušení a zpřehlednění procesu akreditace vzdělávacích institucí a vzdělávacích programů.[39]

3.2 Metody vzdělávání úředníků

Jak upozorňuje Šikýř[40], úspěšná realizace vzdělávání zaměstnanců závisí na využití správné metody vzdělávání, která zaměstnancům umožní osvojit si žádoucí znalosti, dovednosti a schopnosti pro výkon jejich profese a dosahování žádoucího výkonu. Správnost vybrané metody se hodnotí se zřetelem na potřebu vzdělávání, cíl vzdělávání,

[39] Deník veřejné správy. Vzdělávání úředníků územní samosprávy. [online]. 2023. [cit. 27-12-2023] Dostupné z WWW: <https://www.dvs.cz/clanek.asp?id=6883203>.
[40] ŠIKÝŘ, M. Personalistika pro manažery a personalisty: 2., aktualizované a doplněné vydání. Praha: Grada Publishing a.s., 2016, s. 141.

cílovou skupinu účastníků vzdělávání, organizační podmínky vzdělávání aj. Efektivní využití daných vzdělávacích metod vzdělávání si žádá kontrolu dodržování plánu vzdělávání, podobně jako vyhodnocení výsledků vzdělávání. Jako velmi důležité se pak jeví následné vyhodnocení míry osvojení si nových schopností (vědomostí, dovedností a chování) a jejich využití na jejich pracovním místě.

Metody vzdělávání zaměstnanců se dělí na ty, které je možné provádět na pracovišti a mimo něj. Metody vzdělávání **mimo pracoviště** (off the job training) zajišťují zpravidla externí školicí firmy. Většinou jde o nákladnější způsob, kterým mohou zaměstnanci nové vědomosti a dovednosti získat, ovšem někdy je využití této možnosti nutné (například když na úřadě není nikdo, kdo by školení v určité oblasti mohl zajistit). Z konkrétních metod lze zmínit:[41]

Přednáška – jedna z nejběžnějších metod vzdělávání nejen zaměstnanců. Uskutečňuje se prostřednictvím prezentace teoretických vědomostí a faktů. Za výhodu lze považovat možnost účastníků klást v průběhu či na konci otázky a diskutovat s přednášejícím. Pokud má ale jen podobu výkladu, bývá příliš statická a teoretická, nebývá příliš efektivní.

Workshop – jde o interaktivní seminář nebo tvořivou dílnu, na které účastníci hledají řešení a přístupy konkrétního problému, čímž si tak nabyté vědomosti a dovednosti prakticky procvičují. Během workshopu se účastníci musí aktivně zapojovat, využít vlastní kreativitu a do jisté míry i spolupráci s ostatními. Není příliš vhodná pro introverty nebo specialisty.

Hraní rolí – každý zúčastněný dostává určitou roli a hrají dané situace. Jejich úkolem je chovat se jako v reálném životě. Mnohdy bývá používána pro pracovníky, kteří bývají často v kontaktu se zákazníky (businessmani apod.). Setkat se s ní mohou i uchazeči během výběrového řízení, které probíhá v assessment centru.

Případová studie – vhodné pro vzdělávání vedoucích pracovníků. Ti jsou seznámeni s určitou situací, ke které v praxi došlo či by mohla nastat a poté je rozebírána. Vychází se z reálného případu, používá se k inspiraci i k řešení daného problému. Případových studií se též využívá při testování uchazečů v assessment centrech.

[41] KADEŘÁBKOVÁ, M. Metody vzdělávání zaměstnanců: Víte, jaké lze použít? [online]. 2020. [cit. 28-12-2023] Dostupný z https://orangeacademy.cz/clanky/metody-vzdelavani-zamestnancu/.

E-learning – dnes častěji využívána metoda. Je vhodná v situacích, kdy zaměstnanec nemůže, nebo nechce za studiem dojíždět. Ke vzdělávání mu stačí počítač a připojení k internetu. Přihlašovacími údaji se dostane k výuce, může komunikovat s lektory a opakovaně provádět různá cvičení. Studovaný obor si tímto lépe zažije.

Stáž – vhodné, pokud má být na danou pozici přijat absolvent středních nebo vysokých škol. Nejprve je lepší přijmout je na stáž. Tím vedení pozná a uvidí, jak se na určitou pozici uchazeč hodí a jak by do organizace zapadl. Současně však samotní budoucí uchazeči mohou sbírat cenné pracovní zkušenosti, díky kterým si ujasní, v čem spočívají jejich silné a slabé stránky.

Metody vzdělávání **na pracovišti** (on the job training) se obvykle zaměřují na praktické dovednosti i znalosti, které mají zaměstnanci získat. Řadí se k nim:[42]

Koučování – může být realizováno jak na pracovišti, tak mimo něj. Jde zejména o dlouhodobý trénink tzv. soft skills – manažerských schopností nebo komunikačních dovedností, při kterém kouč pracovníkovi pomáhá najít účinné a správné postupy k dosažení cílů (získávání zákazníků aj.).

Instruktáž – vhodná například pro výrobní organizace při zaškolení nových zaměstnanců obsluhujících linky. Instruktor při této metodě předvádí a objasňuje správné pracovní postupy a úkony, které si mají nováčci osvojit a poté je provádět již samostatně.

Asistování – je podobné instruktáži, ovšem zaměřuje se na náročnější pracovní úkoly a pozice. Pracovník asistuje profesně staršímu spolupracovníkovi, sleduje způsob vykonávání práce a zkouší si činnosti, které má převzít. Starší pracovník na něj dohlíží a zajišťuje mu zpětnou vazbu.

Rotace práce – ideální pro budoucí manažery. Jejím záměrem je, aby se prostřednictvím vykonávání různých úkolů na různých pracovištích obeznámili s organizací (útvarem) v širším kontextu.

Briefing – jedná se o neformální porady členů týmu před započetím jakékoli akce. Využívaly se např. britským Královským letectvem (RAF) za 2. světové války. Jeho

[42] KADEŘÁBKOVÁ, M. Metody vzdělávání zaměstnanců: Víte, jaké lze použít? [online]. 2020. [cit. 28-12-2023] Dostupný z https://orangeacademy.cz/clanky/metody-vzdelavani-zamestnancu/.

záměrem je pracovníky motivovat, uvolnit od napětí, pozvednout týmového ducha a morálku.

Pracovní porady – vhodná metoda vzdělávání zaměstnanců pro organizace buďto s cílem řešení určitého úkolu, na němž pracovníci pracují společně, nebo vzdělávání, kdy jsou školeni vybraným pracovníkem zevnitř organizace.

Do vzdělávání zaměstnanců pronikají i některé velmi moderní metody. Farkačová[43] například zmiňuje virtuální realitu. Virtuální realita utváří plně pohlcující virtuální prostředí, v němž se uživatel pohybuje. Virtuální realita umožňuje simulovat libovolnou situaci, a to bez jakýchkoliv bezpečnostních nebo finančních rizik. Výhodou je možnost zajištění 100% pozornosti vzdělávajícího se, který plní úkony v tréninkovém scénáři naprosto přirozeně a podvědomě, čímž dochází k lepšímu zapamatování většího množství informací. Velkou výhodou je i to, že aplikace virtuální reality zvládá detailně monitorovat chování uživatele, jeho silné a slabé stránky, podle nichž je možné vzdělávací lekce upravovat, opakovat apod. Často vzdělávání probíhá tak, že vzdělávající se shlédne několik videí, kvízů, prezentací a případových studií skrze online platformy. Až následně se přechází k procvičení a ukotvení vědomostí prostřednictvím virtuální reality. Může docházet ke spojení virtuální reality s umělou inteligencí. Právě díky umělé inteligenci existuje možnost získat okamžitou zpětnou vazbu o vlastním výkonu. Pro úředníky může sloužit virtuální realita pro nácvik měkkých dovedností, kdy součástí zpětné vazby bývají i klíčové aspekty pro měkké dovednosti, jako jsou informace o očním kontaktu, tónu, hlasitosti mluveného slova až po tempo řeči. Navíc, rozhraní bývá koncipováno tak, že zahrnuje i různorodé klienty a uživatel si tak například může vyzkoušet, jak reagovat na kritické otázky, připomínky z publika či dokonce na arogantní chování klientů.

V současné praxi je možné na základě realizovaných výzkumů sumarizovat, že je v organizacích se upřednostňuje využívání on-the-job metod, přičemž důraz se klade na sebevzdělávání zaměstnanců a e-learning. Aktuálně narůstá využívání videokonferencí, které ještě před dvěma lety nebyly tolik využívány, v dnešní době jsou ovšem využívány i v menších firmách. Je možné usuzovat, že důvodem je zvyšování kompetencí zaměstnanců v technické oblasti a tito zaměstnanci již zvládají náročnost kladenou na přenos videokonference. Vzrůstající trend má také koučink, a to hlavně z důvodu, že

[43] FARKAČOVÁ, L. Virtuální realita a další trendy ve vzdělávání zaměstnanců. Práce a mzda. 2023, (1): 36-40.

koučink je aktuálně upřednostňován jako možný nástroj řízení a plánování kariéry. Kariéra se více zaměřuje na oblast prohlubování znalostí a zkušeností.[44]

Výsledky výzkumu ohledně vzdělávání v zemích OECD poukazují na to, že za nejpoužívanější nástroje vzdělávání úředníků lze považovat různé „live“ vzdělávací moduly, ať už online, nebo prezenční. Hned za nimi se na žebříčku nejpoužívanějších nástrojů umístily pravidelné tematické semináře. Online vzdělávací akce jsou pro úředníky výhodné zejména proto, že si vzdělávání můžou řídit i vyhodnocovat sami. Ačkoli většina orgánů veřejné správy stále pokládá za základ školení pod vedením instruktora, mnoho z nich plánuje zvýšit využívání školících programů, nad kterými mají zaměstnanci větší kontrolu a mohou si do určité míry jít svou vlastní cestou. Jedná se o důležitý činitel ve vzdělávání, neboť některé orgány veřejné správy využívají celkem striktní přístup a o vzdělávání musí zaměstnanci formálně žádat a nadřízení jejich žádosti musejí schválit, přičemž potřebují vidět přímý vztah mezi vzděláváním a pracovní náplní zaměstnance.[45]

[44] URBANCOVÁ, H. Vzdělávání zaměstnanců v českých organizacích. Práce a mzda, 2018, (7): 44-47.
[45] OECD. Přehled o stavu veřejné správy: Česká Republika. Česká republika na cestě k modernější a efektivnější veřejné správě. OECD Publishing. 2023, s. 294.

4 Vzdělávání úředníků v samostatné městské části Praha – Dolní Chabry

„Městskou část nalezneme na severním cípu Prahy, rozloženou v mírně zvlněné urbanizované krajině. Tvoří ji dvě administrativně složené části, a to starší Dolní Chabry (původně zástavba v okolí kostela sv. Jana Křtitele) a mladší Horní Chabry (okolí dnešního Hrušovanského náměstí).“[46]

Jedná se o malou městskou část, která je součástí katastrálního území hlavního města Prahy, tvořící území městské části Praha-Dolní Chabry v městském obvodu Prahy 8, s více než čtyřmi tisíci obyvateli. Úřad městské části je rozdělen na referáty, vedoucí celého úřadu je tajemnice. V čele městské části stojí starostka, místostarosta, rada městské části a zastupitelstvo městské části.

Z celkového počtu 21 zaměstnanců je 5 zaměstnanců v pracovním poměru (zaměstnanci zařazeni do místního úřadu) a zbytek zaměstnanců vykonává správní činnosti v oblasti přenesené působnosti místního úřadu na území Dolních Chaber.

Plán vzdělávání připravuje vedoucí úřadu. Zaměstnanci se spolupodílí na výběru a metodě vzdělávání.

4.1 Formy vzdělávání úředníků v samostatné městské části Praha – Dolní Chabry v oblasti kybernetické bezpečnosti

Úřad městské části Praha – Dolní Chabry v plánu vzdělávání svých zaměstnanců podporuje všechny formy a metody vzdělávání v rámci rozvoje každého jednotlivce. Zaměstnanci musí respektovat autorská práva třetích stran a jsou oprávněni využívat přidělený osobní počítač pouze se softwarovým vybavením zaměstnavatele.

Autorizovaná osoba pro informační technologie, která provádí instalaci, implementaci a servisní podporu pracoviště, školí nové zaměstnance v oblasti užívání výpočetní techniky v souvislosti s jeho pracovním zařazením. Základní školení obsahuje ochranu datových souborů vnitřního systému, systémy autentifikace a přístup do sdílených programů, ochrana a likvidace dat, zajištění bezpečnosti při opuštění

[46] KRÁKOROVÁ, Jaroslava. *Dolní Chabry*. Praha: Městská část Dolní Chabry, 2006. ISBN 80-239-7114-x,s. 5.

pracoviště, bezpečné používání externích datových zařízení a nepovolené užívání počítače pro soukromé účely, které mohou ohrozit vnitřní bezpečnost systému.

Průběžné školení v oblasti kybernetické bezpečnosti probíhá pravidelně v reakci na aktuální hrozby, zvýšení četnosti phishingových útoků na pracovní emaily zaměstnanců s cílem získání osobních dat nebo narušení vnitřního systému zaměstnavatele. Na základě interního nařízení jsou všichni zaměstnanci povinni hlásit IT technikovi podezřelé emaily včetně oznámení antivirového systému, který detekuje škodlivé kódy a potencionálně nechtěné aplikace, které mohou snížit výkon počítače nebo zobrazit nevyžádaný obsah.

Na základě novelizace Zákona č. 226/2022 Sb., o kybernetické bezpečnosti, v roce 2024 vstoupí v platnost směrnice Evropského parlamentu a Rady Evropské unie, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Evropské unii. Jedním z pilířů této novely je i zajištění vzdělávání lidských zdrojů v oblasti bezpečnosti.

Hlavní město Praha umožnila všem zaměstnancům úřadů městských částí přihlásit se do realizovaného on-line kurzu: „Moderní rizika informačních technologií pro MČ Prahy“. Kurz je akreditován Ministerstvem vnitra České republiky ve smyslu zákona č. 312/2002 Sb., o úřednících územních samosprávných celků.

4.2 Cíl výzkumného šetření

Cílem výzkumného šetření bude zjistit, zdali si zaměstnanci samostatné městské části Praha – Dolní Chabry připadají dostatečně vzdělaní v oblasti kybernetické bezpečnosti. Dílčím cílem bude identifikovat spokojenost zaměstnanců s průběhem a formami vzdělávání v oblasti kybernetické bezpečnosti.

Pro naplnění cíle výzkumu byly stanoveny tyto výzkumné předpoklady:
Výzkumný předpoklad 1: Více než 50 % dotázaných respondentů potvrzuje, že jsou ve své profesi vystaveni různým kybernetickým hrozbám.

Výzkumný předpoklad 2: Více než 50 % dotázaných respondentů se domnívá, že jsou dostatečně připraveni na to, aby dokázali kybernetické hrozby identifikovat a ubránit se jim.

Výzkumný předpoklad 3: Více než 50 % dotázaných respondentů vyjadřuje spokojenost se vzděláváním v oblasti kybernetické bezpečnosti zajišťované úřadem.

Výzkumný předpoklad 4: Více než 50 % dotázaných respondentů vyjadřuje zájem o další vzdělávání v oblasti kybernetické bezpečnosti.

4.3 Organizace výzkumu a použitá metoda

Pro naplnění cíle výzkumu bylo zvoleno použití metody dotazníkového šetření, a to zejména z důvodu toho, že při dotazníkovém šetření je možné zachovat anonymitu respondentů, a tím eliminovat obavy z poskytnutí pravdivých odpovědí (zvláště, když se hodnotí zaměstnavatel jako v případě tohoto výzkumu). Dotazník v této práci obsahoval 20 otázek, z nichž první 2 tvořily základní informační otázky, ve kterých byli respondenti požádáni o sdělení pohlaví a délku praxe. Otázky dotazníku byly formulovány vesměs jako uzavřené a polo uzavřené (s variantou doplnit vlastní odpověď, aby byla eliminována nevýhoda plynoucí z nevyhovující nabídky variant odpovědí). V úvodu dotazníku byli respondenti seznámeni s tím, k čemu bude dotazník sloužit, jak mají při jeho vyplňování postupovat s ujištěním, že dotazování je zcela anonymní.

V první části výzkumu bylo osloveno výzkumné zařízení, zde úřad samostatné městské části Praha – Dolní Chabry s žádostí a povolením k provedení výzkumu. Po odsouhlasení žádosti bylo přistoupeno k vytvoření dotazníku a jeho ověření v rámci předvýzkumu u dvou vybraných respondentů, kteří měli dotazník vyplnit a poskytnout zpětnou vazbu ke srozumitelnosti a komplexnosti dotazníku. Poté bylo možné přistoupit k realizaci dotazování, které probíhalo v online podobě na serveru Survio.com, kde byl dotazník vytvořen a odkaz na něj byl zaslán zaměstnancům emailem. Po měsíci sběru dat bylo dotazování ukončeno a dotazník na webu Survio.com byl vyhodnocen včetně vygenerování grafů, které jsou dále interpretovány v textu. Na základě grafů a prezentovaných dat bylo následně možné přistoupit k vyhodnocení výzkumných předpokladů.

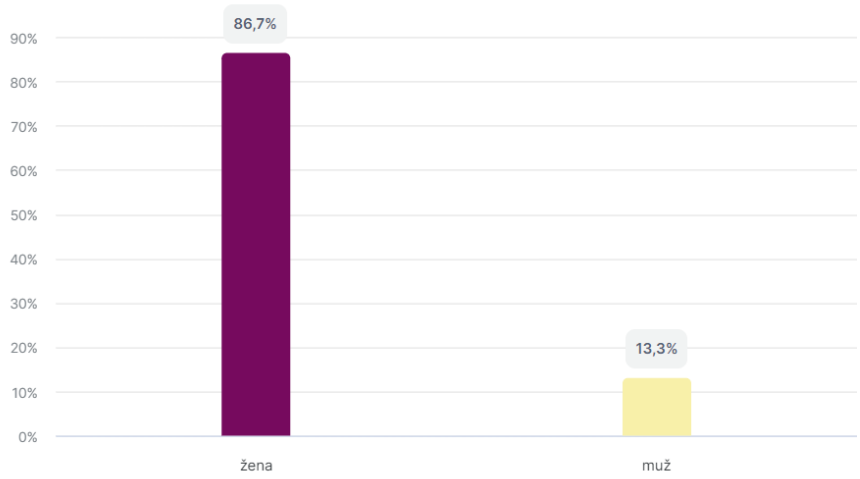
4.4 Interpretace výsledků výzkumu

Dotazníkového šetření se zúčastnilo celkem 15 úředníků ze samostatné městské části Praha – Dolní Chabry. Důvodem nižší účasti byla zvýšená nemocnost v době provádění výzkumu. Odpovědi respondentů jsou zobrazeny níže ve sloupcových a pruhových

grafech v relativních hodnotách, které vygeneroval server Survio.com. Tento server dokáže nejen vyhodnotit výsledky, ale také zaznamenává další statistiky. Z nich lze například zmínit, že dotazník vyplňovali respondenti z přímého odkazu (zaslaného emailem). Celkem navštívilo dotazník 19 respondentů, kompletně ho vyplnilo jen 15, tímto tak úspěšnost vyplnění dosáhla 78,9 %. Respondenti dotazník vyplňovali průměrně mezi 2 až 5 minutami (více než polovina dotázaných). Více než třetina věnovala vyplnění dotazníku 10 až 30 minut.

4.5 Dotazníkové šetření – jednotlivé vyhodnocení

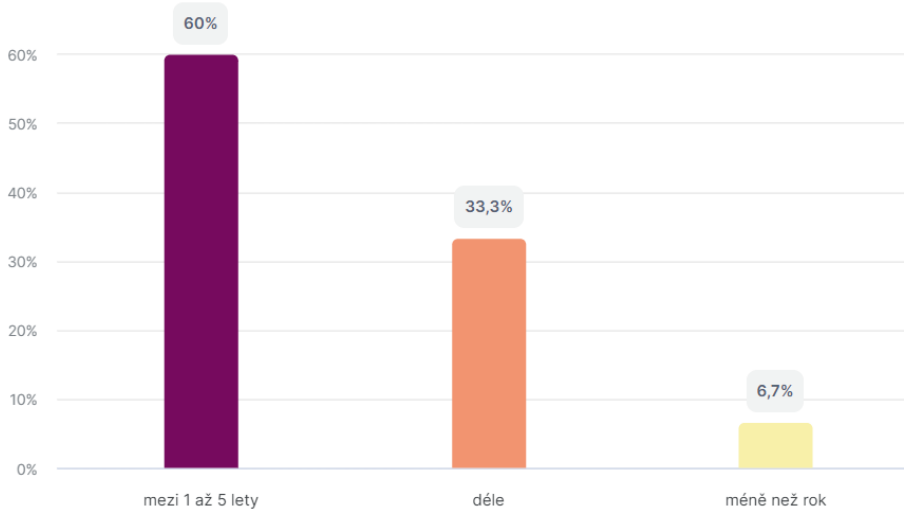
Jste:



Graf 1 Pohlaví respondentů (Zdroj: Survio.com).

Mezi dotázanými respondenty převážily významně ženy, které prezentovaly 86,7 % dotázaných. Zbylých 13,3 % dotázaných respondentů tvořili muži. Uvedené rozložení respondentů koresponduje s rozložením zaměstnanců v prostředí úřadu.

Jak dlouho pracujete na úřadu samostatné městské části Praha – Dolní Chabry?

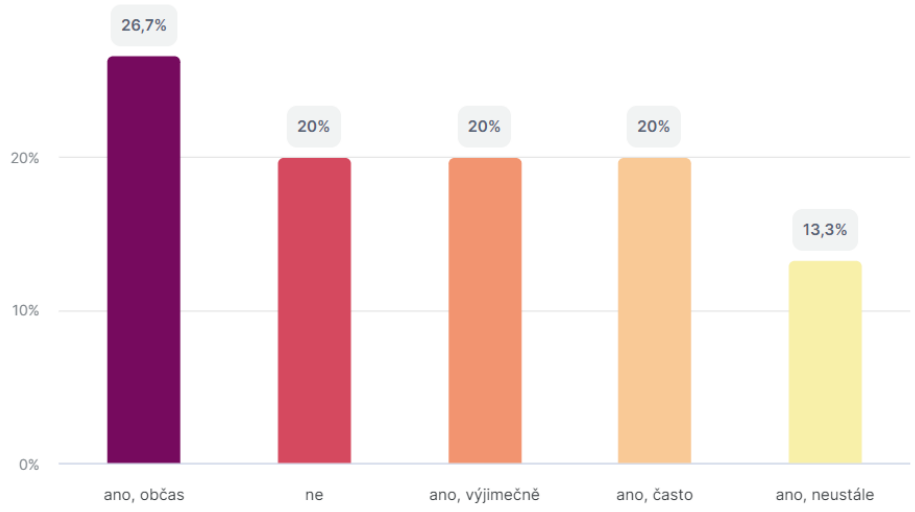


Graf 2 Délka praxe respondentů na úřadu (Zdroj: Survio.com).

V další otázce byli respondenti dotázáni na to, jak dlouho pracují na úřadu samostatné městské části Dolní Chabry. Jak je možné si všimnout, více než polovina dotázaných respondentů odpověděla, že pracují na úřadu mezi 1 až 5 lety. Dále pak 33,3 % dotázaných odpovědělo, že pracují na úřadě déle než 5 let a zbylých 6,7 % dotázaných odpovědělo, že pracují na úřadu méně než rok.

Jedná se o pozitivní zjištění, protože více jak polovina zaměstnanců pracuje na úřadě městské části déle než 5 let a z toho vyplývá, že již mají dlouhodobé zkušenosti s průběžným vzděláváním a jsou schopni objektivně posoudit stávající systém vzdělávání v oblasti kybernetické bezpečnosti na pracovišti.

Zaznamenáváte ve svém zaměstnání různé hrozby a rizikové události v souvislosti s online či off-line prostorem využívaným v zaměstnání (podvodné emaily, hlášení antivirového systému aj.)?



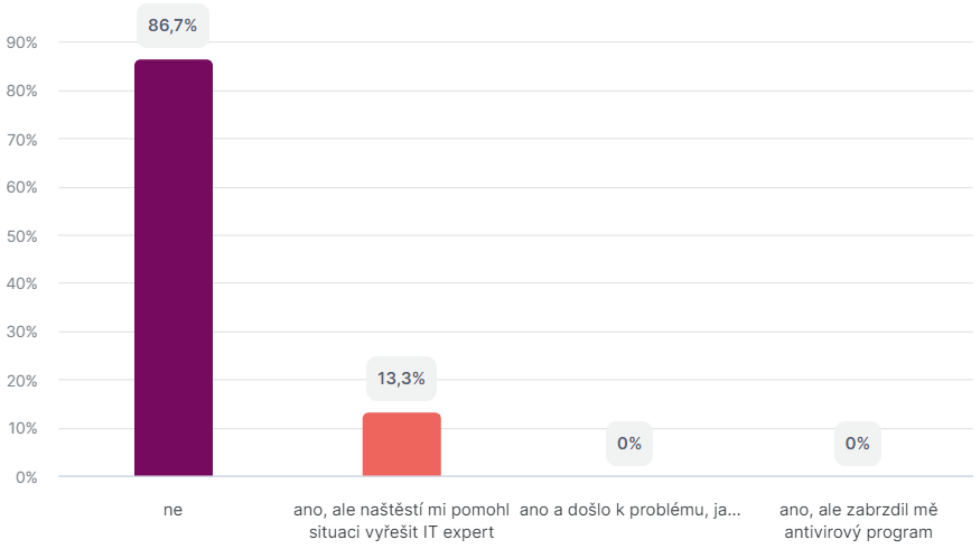
Graf 3 Zkušenost respondentů s hrozbami a rizikovými událostmi v práci na úřadě (Zdroj: Survio.com).

Tato otázka se již zaměřovala na poznání skutečnosti ohledně kybernetických hrozeb na pracovišti respondentů. Nejvíce dotázaných respondentů (26,7 %) odpovědělo, že občas zaznamenávají ve svém zaměstnání různé hrozby a rizikové události v souvislosti s online či off-line prostorem využívaným v zaměstnání. Dalších 20 % dotázaných odpovědělo, že nezaznamenávají ve svém zaměstnání žádné hrozby a rizikové události v souvislosti s online či off-line prostorem využívaným v zaměstnání. Dále rovněž 20 % dotázaných odpovědělo, že výjimečně zaznamenávají ve svém zaměstnání různé hrozby a rizikové události v souvislosti s online či off-line prostorem

využívaným v zaměstnání a dalších 20 % zaznamenává tyto hrozby často. Zbylých 13,3 % dotázaných odpovědělo, že neustále zaznamenávají ve svém zaměstnání různé hrozby a rizikové události v souvislosti s online či off-line prostorem využívaným v zaměstnání.

Na základě vyhodnocení této otázky je možné potvrdit výzkumný předpoklad 1, kdy více než 80 % dotázaných potvrdilo, že jsou vystaveni ve své profesi kybernetickým útokům.

Stalo se Vám už, že jste si neuvědomil/a nebo nevšiml podvodného či útočného jednání někoho skrze kyberprostor a ohrozil/a jste bezpečnost své práce?

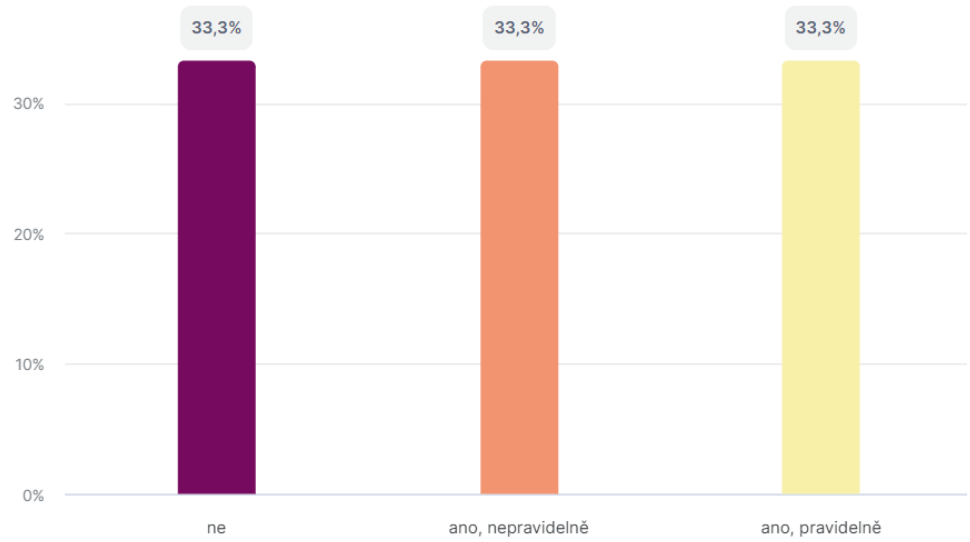


Graf 4 Zkušenost respondentů s opomenutím podvodného či útočného jednání skrze kyberprostor, které ohrozilo jejich práci (Zdroj: Survio.com).

Nejvíce respondentů na tuto otázku odpovědělo, že se jim ještě nestalo, že si neuvědomili nebo nevšimli podvodného či útočného jednání někoho skrze kyberprostor a ohrozili tak bezpečnost své práce (86,7 %). Zbývajících 13,3 % dotázaných pak uvedlo, že se jim stalo, že si neuvědomili nebo nevšimli podvodného či útočného jednání někoho skrze kyberprostor a ohrozili tak bezpečnost své práce, ale naštěstí jim pomohl IT expert situaci vyřešit.

Z tohoto zjištění vyplývá, že 13,3 % zaměstnanců nezaregistrovalo podvodné jednání a mohli tak ohrozit bezpečnost své práce. V okamžiku, kdy ale hrozbu zaznamenali, jednali na základě vnitřního nařízení a okamžitě kontaktovali IT technika.

Absolvujete v rámci výkonu své profese vzdělávání zaměřené na bezpečnost v kybernetickém prostoru?

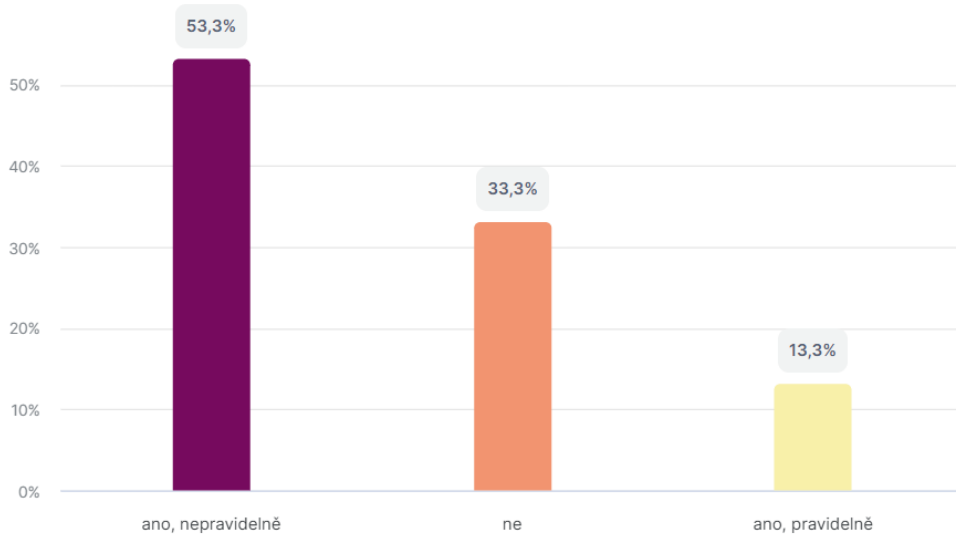


Graf 5 Zkušenost respondentů se vzděláváním orientovaným na bezpečnost v kyberprostoru (Zdroj: Survio.com).

U této odpovědi se pro každou variantu odpovědi objevil stejný počet respondentů. Tímto je možné říct, že 33,3 % dotázaných odpovědělo, že neabsolvují v rámci výkonu své profese vzdělávání zaměřené na bezpečnost v kybernetickém prostoru. Stejný počet respondentů (33,3 %) pak uvedl, že absolvují nepravidelně v rámci výkonu své profese vzdělávání zaměřené na bezpečnost v kybernetickém prostoru. Zbývajících 33,3 % dotázaných pak odpovědělo, že pravidelně absolvují v rámci výkonu své profese vzdělávání zaměřené na bezpečnost v kybernetickém prostoru. Obecně tak převážily kladné varianty odpovědí.

Ze zjištěných výsledků vyplývá doporučení pro zaměstnavatele, aby v rámci spolupráce na výběru vzdělávacích kurzů apeloval na své zaměstnance, a ti by se při výběru školení měli více zaměřit na oblast kybernetické bezpečnosti.

Doplňujete si vzdělávání v kybernetické bezpečnosti i v rámci samostudia?

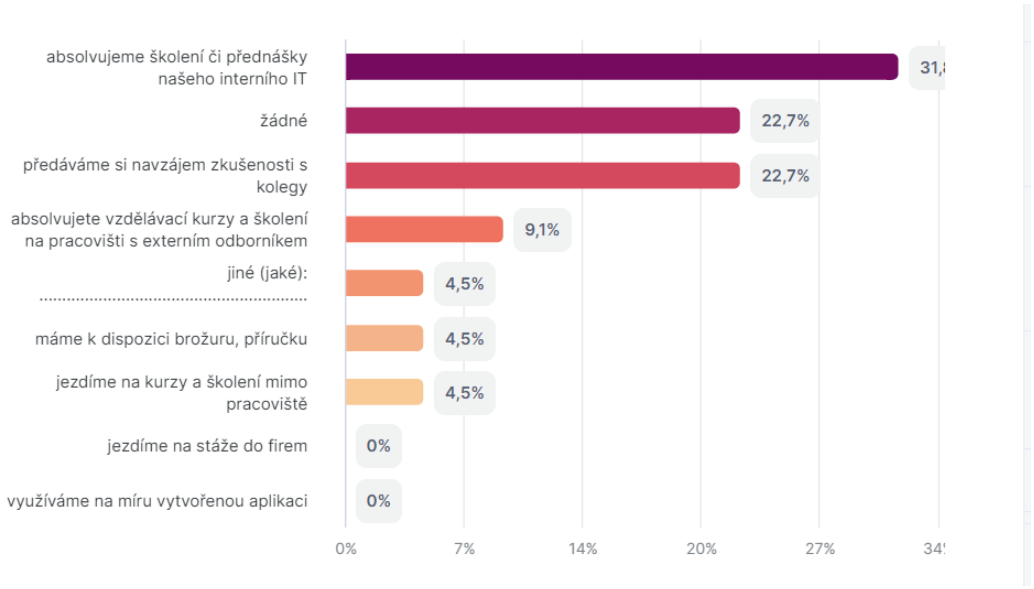


Graf 6 Využívání samostudia v rámci doplnění si vzdělávání respondenty (Zdroj: Survio.com).

V další otázce byli respondenti požádáni, aby odpověděli, zda se v oblasti kybernetické bezpečnosti vzdělávají i v rámci samostudia. Více než polovina dotázaných respondentů odpověděla (53,3 %), že se samostudiu v oblasti kybernetické bezpečnosti věnují nepravidelně. Dalších 33,3 % dotázaných odpovědělo, že se nevěnují samostudiu, aby se dozvěděli více z oblasti kybernetické bezpečnosti. Zbývajících 13,3 % dotázaných odpovědělo, že se samostudiu v oblasti kybernetické bezpečnosti věnují pravidelně.

Z uvedeného výsledku bylo zjištěno, že 33,3 % zaměstnanců nemá zájem o samostudium v oblasti kybernetických hrozeb.

Jaké formy vzdělávání v oblasti kybernetické bezpečnosti v rámci svého zaměstnání absolvujete (můžete zvolit více možností)?

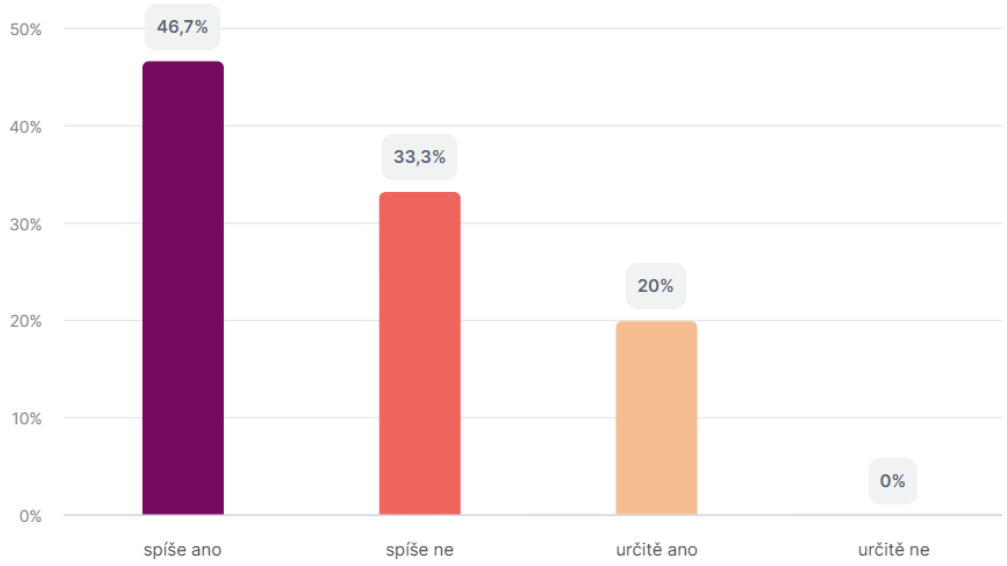


Graf 7Formy vzdělávání v oblasti kybernetické bezpečnosti v rámci zaměstnání respondentů (Zdroj: Survio.com).

V této otázce dostali respondenti na výběr několik různých variant odpovědí, aby uvedli, jaké formy vzdělávání v oblasti kybernetické bezpečnosti absolvují. Mohli zvolit více než jednu odpověď. Nejvíce respondentů (31,8 %) uvedlo, že absolvují školení a přednášky od interního IT. Dále 22,7 % dotázaných uvedlo, že si předávají navzájem zkušenosti s kolegy mezi sebou. Zmínit lze i 9,1 % dotázaných, kteří uvedli, že absolvují vzdělávací kurzy a školení na pracovišti s externím odborníkem. Ještě pak 4,5 % dotázaných uvedlo jiné formy vzdělávání. Také 4,5 % dotázaných odpovědělo, že mají k dispozici příručku nebo brožuru a 4,5 % dotázaných uvedlo, že jezdí i na kurzy a školení mimo pracoviště. Opomenout nelze pochopitelně i 22,7 % dotázaných, kteří odpověděli, že v oblasti kybernetické bezpečnosti neabsolvují žádnou z uvedených forem vzdělávání.

Nejvíce zaměstnanců úřadu preferuje způsob vzdělávání v oblasti kybernetické bezpečnosti formou přednášek IT technika a konzultacemi mezi spolupracovníky.

Domníváte se, že jste na základě absolvovaného vzdělávání aktuálně dostatečně připraven/a pro předcházení kybernetických hrozeb souvisejících s výkonem Vašeho povolání?

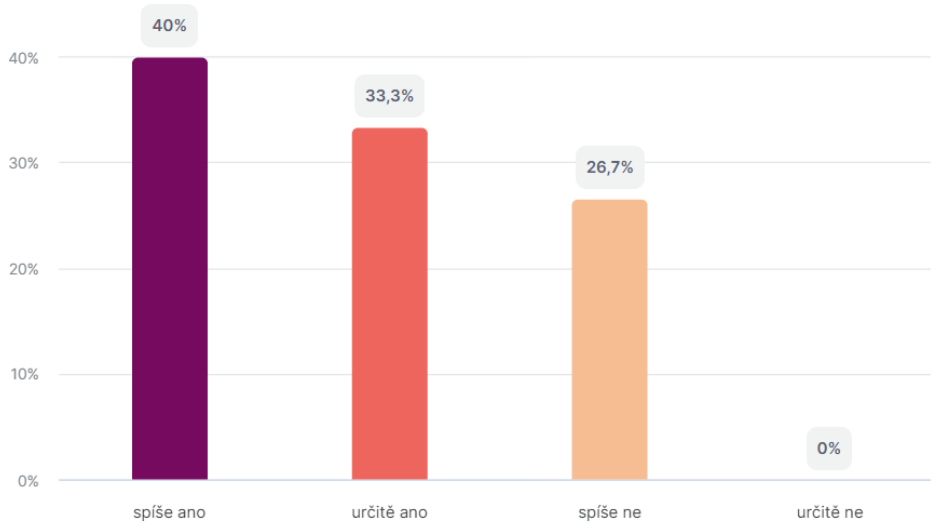


Graf 8 Názor na dostatečnost přípravy respondentů pro prevenci kybernetických hrozeb souvisejících s výkonem povolání (Zdroj: Survio.com).

Respondenti byli v této otázce dotázáni, zda podle nich jimi absolvované vzdělání vedlo k tomu, že se cítí dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s jejich prací. Zde odpovědělo více než 50 % dotázaných kladně (66,7 %). Konkrétně uvedlo 20 % dotázaných, že si spíše připadají dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s výkonem jejich povolání. Nejvíce dotázaných respondentů odpovědělo, že si určitě připadají dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s výkonem jejich povolání (46,7 %). Zbývajících 33,3 % dotázaných odpovědělo, že si spíše nepřipadají dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s výkonem jejich povolání.

Vyhodnocení výsledků této otázky potvrdilo výzkumný předpoklad 2, že více jak 50 % respondentů se domnívá, že jsou dostatečně připraveni identifikovat kybernetické hrozby a ubránit se jim.

Zaznamenáváte, že po absolvování vzdělávání v oblasti kybernetické bezpečnosti jste lépe schopni odhalovat rizika a řešit je?

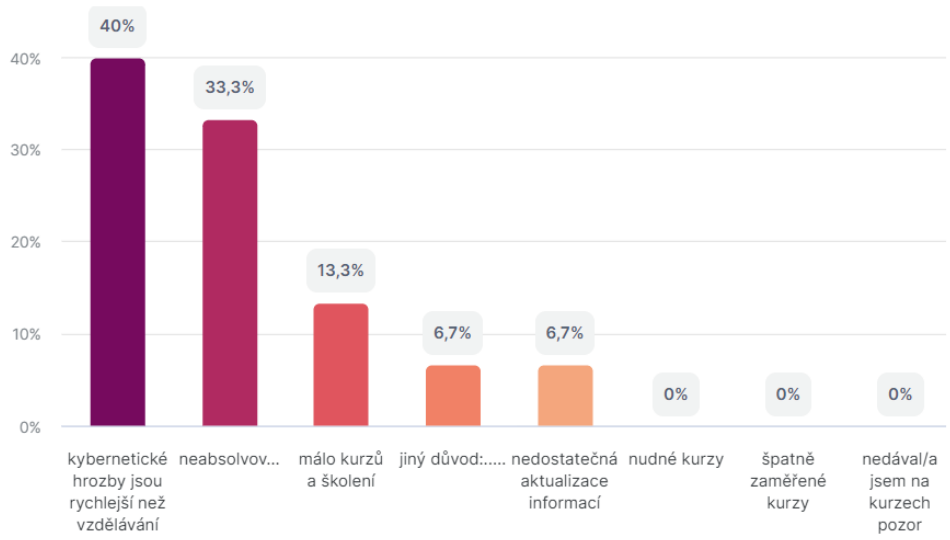


Graf 9 Zkušenost se zlepšením schopností odhalovat a řešit rizika po absolvování vzdělávání v oblasti kybernetické bezpečnosti (Zdroj: Survio.com).

Respondenti dále byli dotázáni na to, zda jsou po absolvování vzdělávání v oblasti kybernetické bezpečnosti lépe schopni odhalovat rizika a řešit je. i zde více než polovina odpověděla kladně (73,3 %). Konkrétně 33,3 % respondentů odpovědělo, že po absolvování vzdělávání v oblasti kybernetické bezpečnosti se cítí určitě více schopni odhalovat rizika a řešit je. Dalších 40 % dotázaných odpovědělo, že po absolvování vzdělávání v oblasti kybernetické bezpečnosti se cítí spíše více schopni odhalovat rizika a řešit je. Zbylých 26,7 % dotázaných odpovědělo, že si spíše nepřipadají schopni odhalovat rizika a řešit je.

Více jak polovina respondentů potvrdilo, že po absolvování školení jsou lépe schopni odhalovat kybernetická rizika a řešit je.

Pokud ne, co je podle Vás důvodem?

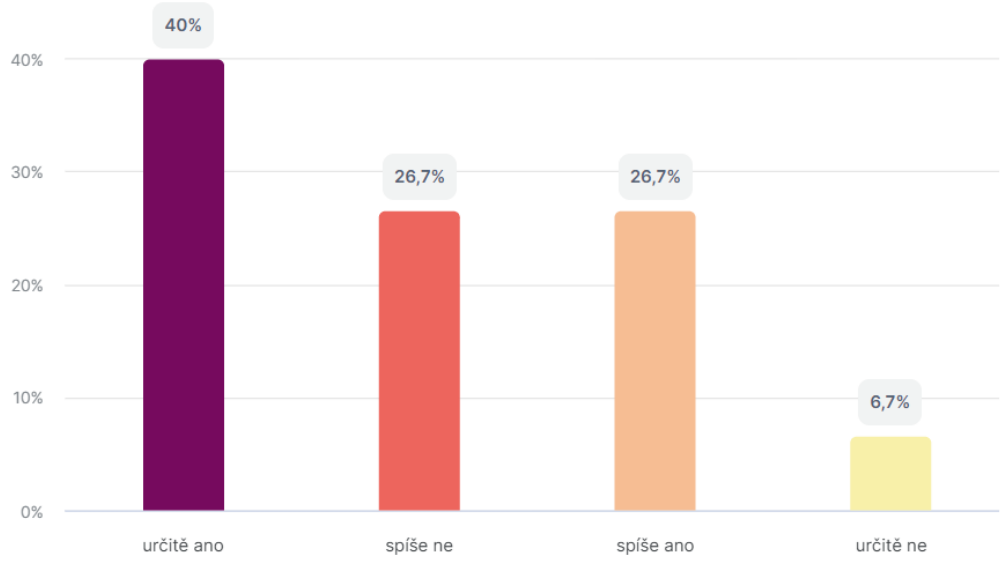


Graf 10 Důvody neschopnost odhalovat kybernetická rizika po vzdělávání (Zdroj: Survio.com).

U této otázky nejvíce respondentů odpovědělo, že důvodem toho, že si nepřijdou schopni čelit kybernetickým hrozbám, je, že kybernetické hrozby jsou rychlejší než vzdělávání (40 %). Dále pak 33,3 % dotázaných odpovědělo, že vzdělávání neabsolvovali, tudíž nemohou odpovědět. Zmínit lze i 13,3 % dotázaných, kteří uvedli, že důvodem je malý počet kurzů a školení. Poté ještě 6,7 % dotázaných odpovědělo, že důvodem je nedostatečná aktualizace informací a zbylých 6,7 % dotázaných uvedlo jiný důvod.

Z výsledků vyplývá, že 40 % respondentů potvrdilo, že nové kybernetické hrozby jsou rychlejší než vzdělávání a 33,3 % respondentů neabsolvovalo vzdělávání v oblasti kybernetické bezpečnosti.

Jste spokojen/a se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno Vašim zaměstnavatelem?

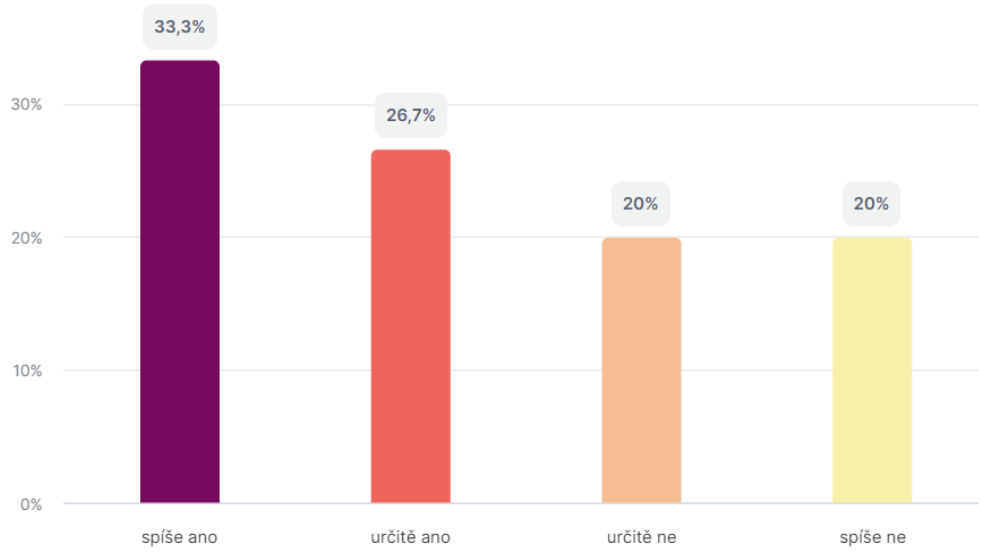


Graf 11 Spokojenost respondentů se vzděláváním v oblasti kybernetické bezpečnosti zajišťovaném zaměstnavatelem (Zdroj: Survio.com).

I zde převážily pozitivní varianty odpovědí, když celkem 66,7 % zvolilo kladnou variantu odpovědi. Konkrétně 40 % dotázaných uvedlo, že jsou určitě spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem. Dalších 26,7 % dotázaných odpovědělo, že spíše jsou spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem. Stejně tak ale 26,7 % dotázaných odpovědělo, že spíše nejsou spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem. Zbývajících 6,7 % dotázaných odpovědělo, že určitě nejsou spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem.

Toto šetření potvrdilo výzkumný předpoklad 3, že více než 50 % respondentů vyjadřuje spokojenost se vzděláváním v oblasti kybernetické bezpečnosti, které zajišťuje zaměstnavatel.

Vyhovuje Vám četnost vzdělávání v oblasti kybernetické bezpečnosti?

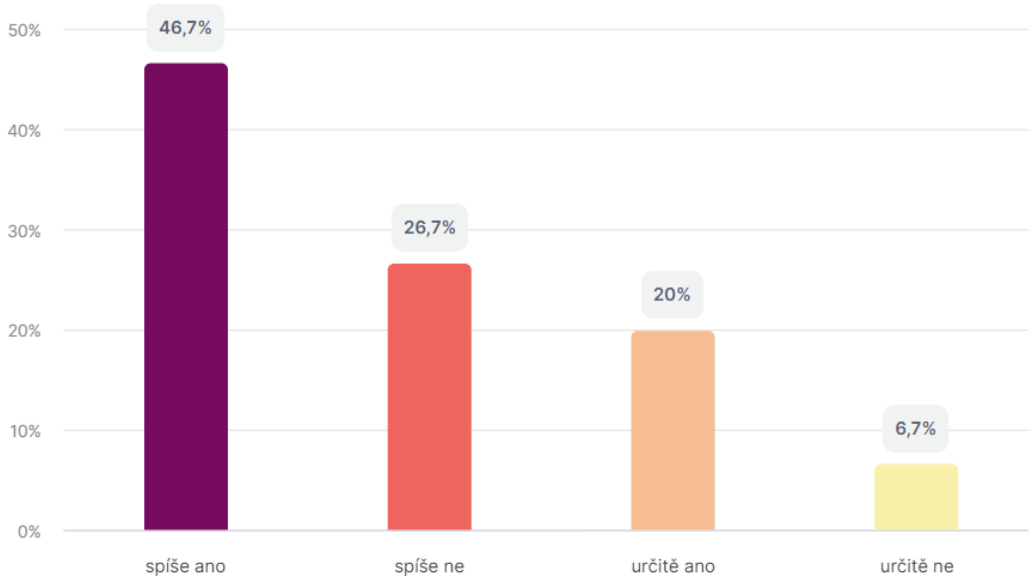


Graf 12 Spokojenost s čerností vzdělávání v oblasti kybernetické bezpečnosti (Zdroj: Survio.com).

Opět zde více než polovina dotázaných respondentů odpověděla, že jim vyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti (60 %). Konkrétně 33,3 % dotázaných uvedlo, že jim spíše vyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti, dalších 26,7 % dotázaných uvedlo, že jim určitě vyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti. Dále pak 20 % dotázaných odpovědělo, že jim spíše nevyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti a zbylých 20 % pak zmínilo, že jim určitě nevyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti.

Z výsledku vyplývá, že více jak polovina respondentů je spokojena s četností vzdělávání v oblasti kybernetické bezpečnosti, které zajišťuje zaměstnavatel.

Vyhovuje Vám kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti?

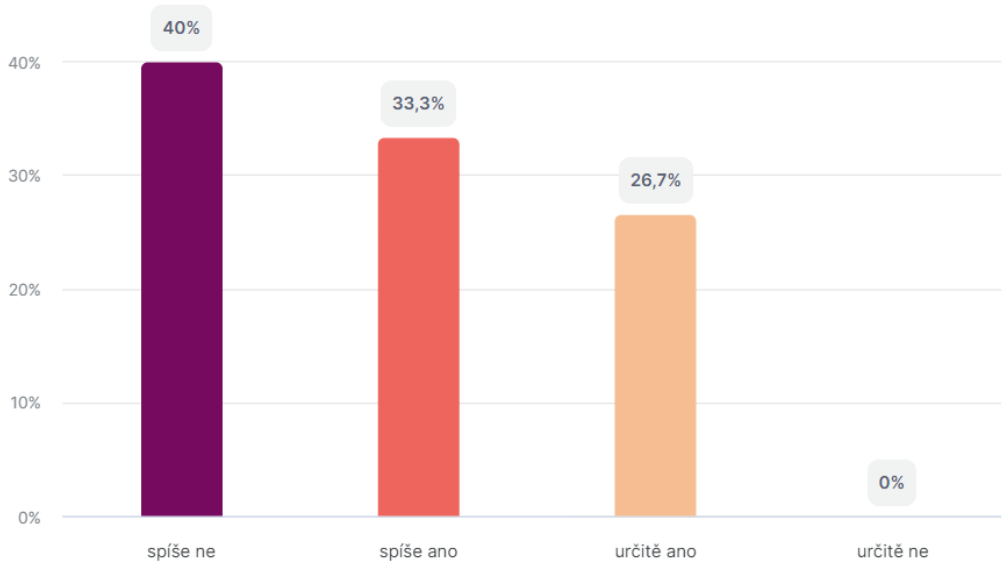


Graf 13 Spokojenosti s kvalitou a aktuálností informací v rámci vzdělávání v kybernetické bezpečnosti (Zdroj: Survio.com).

Více než polovina dotázaných respondentů i zde kladně odpověděla, že jim vyhovuje kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti (66,7 %). Konkrétně 20 % respondentů uvedlo, že jim určitě vyhovuje kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti. Dále pak 46,7 % dotázaných uvedlo, že jim spíše vyhovuje kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti. Dále pak 36,7 % dotázaných respondentů odpovědělo, že jim spíše nevyhovuje kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti a zbylých 6,7 % dotázaných respondentů uvedlo, že jim určitě nevyhovuje kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti.

Výsledek tohoto šetření potvrdil výzkumný předpoklad 3, že více jak 50 % dotázaných respondentů je spokojeno se vzděláváním v oblasti kybernetické bezpečnosti zajišťované úřadem.

Jste spokojen/a s praktickým přesahem informací nabízených na kurzech?

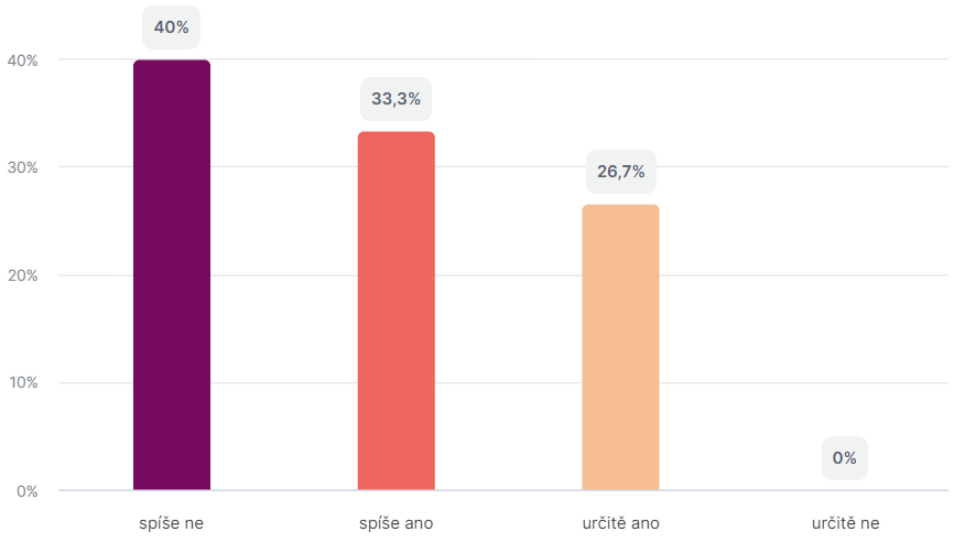


Graf 14 Spokojenost s praktickým přesahem informací nabízených na kurzech (Zdroj: Survio.com).

I zde se respondenti ve většině shodli, že jsou spokojeni s praktickým přesahem informací nabízených na kurzech (60 %). Nejvíce respondentů konkrétně ale odpovědělo, že spíše nejsou spokojeni s praktickým přesahem informací nabízených na kurzech (40 %). Dále pak 33,3 % dotázaných respondentů uvedlo, že jsou spíše spokojeni s praktickým přesahem informací nabízených na kurzech. Zbylých 26,7 % dotázaných zmínilo, že jsou určitě spokojeni s praktickým přesahem informací nabízených na kurzech.

Zjištění u této otázky prokázalo, že 40 % respondentů není spokojeno s praktickým přesahem informací nabízených na kurzech.

Vyhovuje Vám kvalita a odbornost lektora?

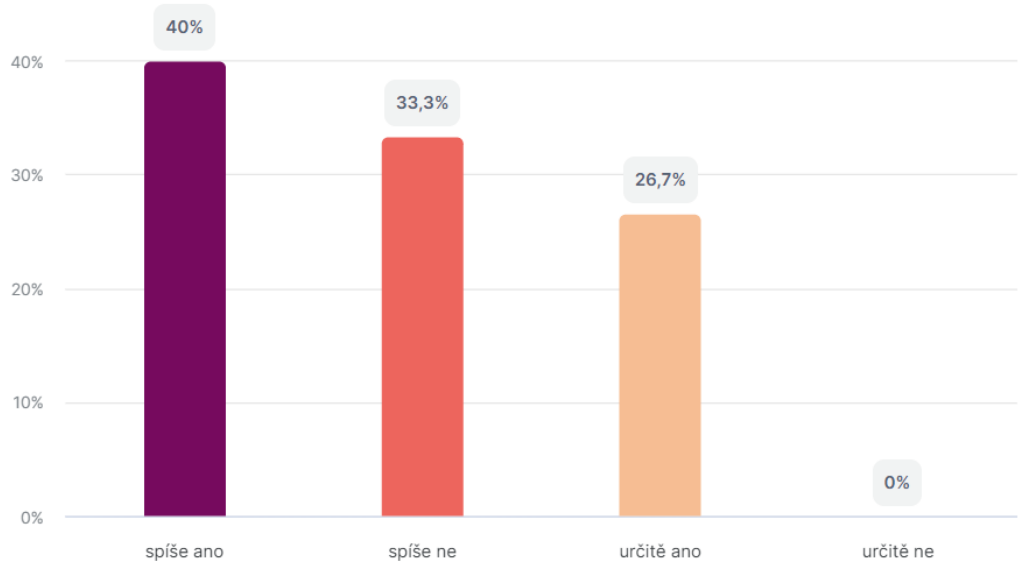


Graf 15 Spokojenost s kvalitou a odborností lektora (Zdroj: Survio.com).

Jednou z důležitých podmínek kvality vzdělávání je i kvalita daného lektora. i zde se respondenti shodli na převazujících kladných odpovědích. Konkrétně odpovědělo 26,7 % dotázaných, že jsou určitě spokojení s odborností lektora. Dále pak 33,3 % dotázaných odpovědělo, že jsou spíše spokojení s odborností lektora. Zbylých 40 % dotázaných respondentů pak uvedlo, že spíše nejsou spokojení s odborností lektora.

Dotazníkové šetření ukázalo, že jen 40 % respondentů není spokojeno s odborností lektora.

Vyhovují Vám použité metody vzdělávání v oblasti kybernetické bezpečnosti?

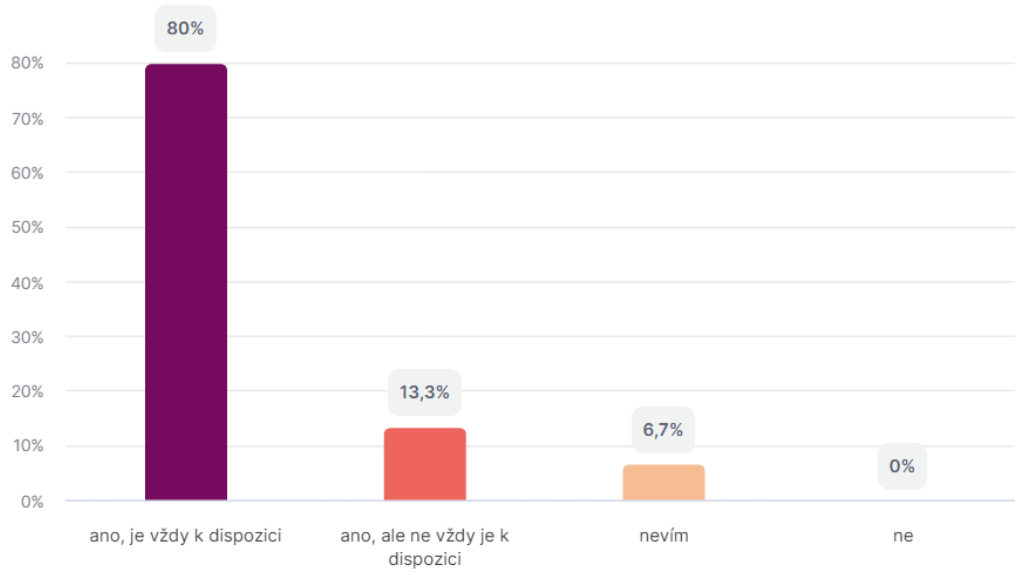


Graf 16 Spokojenost s použitými metodami vzdělávání v oblasti kybernetické bezpečnosti (Zdroj: Survio.com).

Co se týče použitých metod, tam respondenti vyjádřili podobný trend odpovědí, čili spokojenost. Je možné tak říct, že 26,7 % dotázaných odpovědělo, že jim určitě vyhovují použité metody vzdělávání v oblasti kybernetické bezpečnosti. Dále pak 33,3 % dotázaných odpovědělo, že jim spíše vyhovují použité metody vzdělávání v oblasti kybernetické bezpečnosti. Zbylých 40 % dotázaných odpovědělo, že jim spíše nevyhovují použité metody vzdělávání v oblasti kybernetické bezpečnosti.

Z výsledného grafu vyplývá, že více jak 50 % respondentů je spokojeno s používanými metodami vzdělávání v oblasti kybernetické bezpečnosti.

Máte na pracovišti možnost okamžité konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud byste si nevěděl/a rady při nějaké rizikové události?

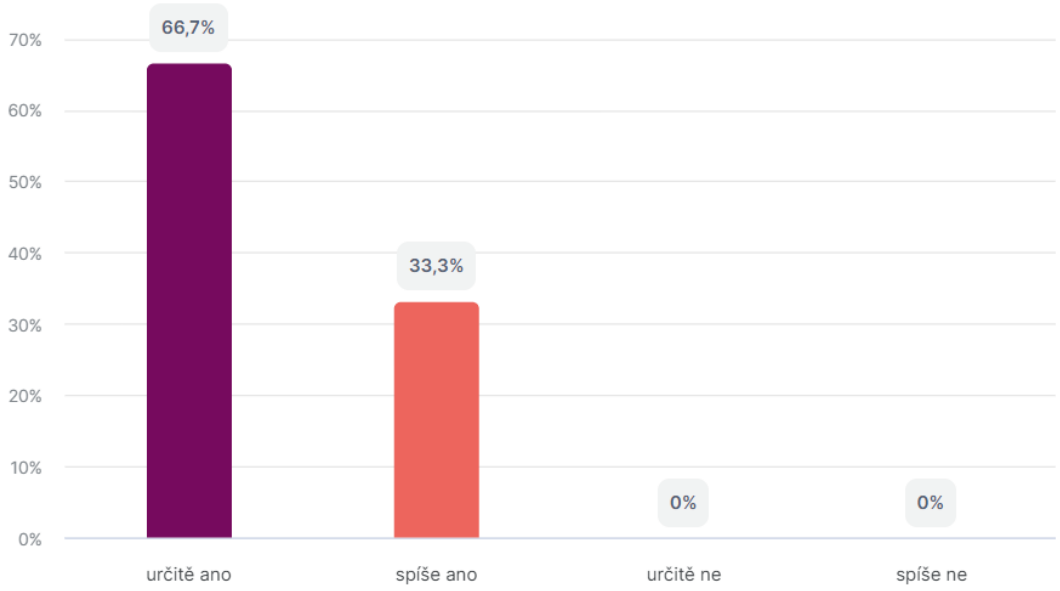


Graf 17 Zkušenost respondentů s možností konzultace s odborníkem v oblasti kybernetické bezpečnosti (Zdroj: Survio.com).

U této otázky bylo od respondentů zjišťováno, zda mají možnost okamžité konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud by si nevěděli rady při nějaké rizikové události. Nejvíce respondentů uvedlo, že mají možnost okamžité konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud by si nevěděli rady při nějaké rizikové události, neboť jde vždy IT odborník k dispozici. Dále pak 13,3 % dotázaných respondentů odpovědělo, že mají sice možnost konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud by si nevěděli rady při nějaké rizikové události, ale ne vždy je tento odborník k dispozici. Zbylých 6,7 % dotázaných uvedlo, že neví, zda mají možnost okamžité konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud by si nevěděli rady při nějaké rizikové události.

Graf zobrazuje zjištění, že 6,7 % zaměstnanců neví o možnosti okamžité konzultace s IT technikem při rizikové události.

Měl/a byste zájem i v budoucnu o vzdělávání v oblasti kybernetické bezpečnosti?

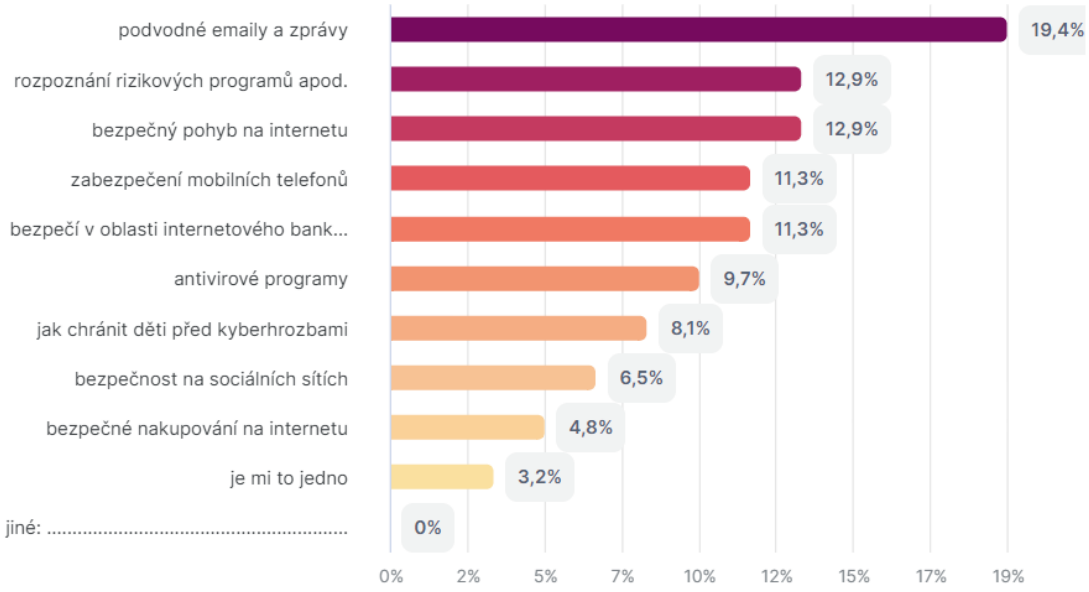


Graf 18 Zájem respondentů o vzdělávání v oblasti kybernetické bezpečnosti i v budoucnu (Zdroj: Survio.com).

Všichni dotázáni respondenti potvrdili, že by v budoucnu měli zájem o vzdělávání v oblasti kybernetické bezpečnosti. Konkrétně odpovědělo 66,7 % dotázaných respondentů a uvedlo, že by určitě v budoucnu měli zájem o další vzdělávání v oblasti kybernetické bezpečnosti. Zbylých 33,3 % dotázaných pak odpovědělo, že spíše mají v budoucnu zájem o další vzdělávání v oblasti kybernetické bezpečnosti.

Z výsledného šetření vyplývá, že pouze 33,3 % zaměstnanců má „spíše“ zájem v budoucnu se vzdělávat v oblasti kybernetické bezpečnosti a potvrzuje výzkumný předpoklad 4, že více jak 50 % dotázaných respondentů vyjadřuje zájem o další vzdělávání v oblasti kybernetické bezpečnosti.

V jaké oblasti konkrétně (můžete vybrat více možností)?

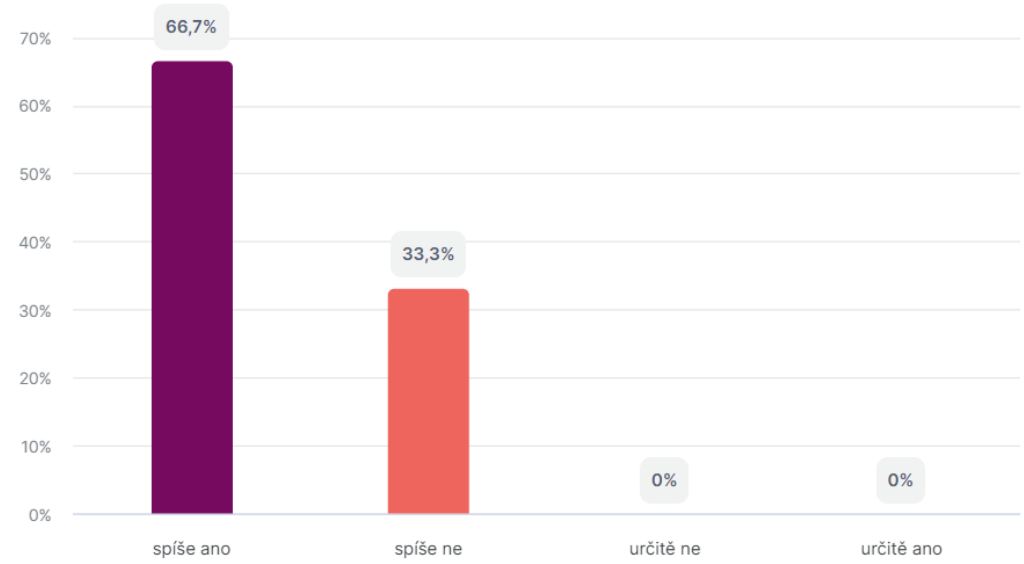


Graf 19 Vybrané preferované oblasti v rámci vzdělávání v kybernetické bezpečnosti (Zdroj: Survio.com).

V další otázce mohli respondenti vybrat konkrétní možnosti, na které by chtěli vzdělávání v budoucnu zaměřit. Konkrétně 19,4 % dotázaných respondentů odpovědělo, že by chtěli získat informace ohledně podvodných emailů a zpráv. Dále pak 12,9 % dotázaných odpovědělo, že by měli zájem o rozpoznávání podvodných a rizikových programů. Dále by 12,9 % dotázaných mělo zájem i o bezpečný pohyb na internetu a jeho pravidla. Pro 11,3 % dotázaných by bylo zajímavé školení v oblasti zabezpečení mobilních telefonů. Stejně tak by 11,3 % dotázaných mělo zájem i o přednášku či vzdělávání v oblasti bezpečnosti v internetovém bankovnictví. Dále by 9,7 % dotázaných mělo zájem o znalosti z oblasti antivirových programů, 8,1 % by mělo zájem o informace o tom, jak chránit děti v oblasti kybernetické bezpečnosti. Pro 6,5 % by měly význam informace o bezpečnosti na sociálních sítích, 4,8 % dotázaných by mělo zájem zase o informace z oblasti bezpečného nakupování na internetu a 3,2 % dotázaných uvedlo, že jim to je jedno.

Nejvíce respondentů projevilo zájem o vzdělávání v kybernetické bezpečnosti v oblasti rozpoznávání rizikových programů, podvodných emailů a zpráv.

Byl/a byste eventuálně ochoten/na se i finančně podílet na takovém vzdělávání?



Graf 20 Ochota respondentů podílet se vlastními prostředky na tomto vzdělávání (Zdroj: Survio.com).

V poslední otázce dostali respondenti otázku, zdali by byli třeba i ochotni se sami nějakou částkou podílet na úhradě za vzdělávání. Je možné si zde všimnout, že 66,7 % dotázaných uvedlo, že by spíše byli ochotni se i finančně podílet na takovém vzdělávání. Zbylých 33,3 % dotázaných pak odpovědělo, že by spíše nebyli ochotni se podílet na takovém vzdělávání.

Více jak polovina zaměstnanců úřadu projevila ochotu podílet se vlastními prostředky na vzdělávání v oblasti kybernetické bezpečnosti.

4.6 SWOT analýza vzdělávání zaměstnanců

Vyhodnocené výsledky dotazníkového šetření byly také využity pro zpracování SWOT analýzy se zaměřením na analýzu vzdělávání a zkušeností zaměstnanců v samostatné městské části Praha – Dolní Chabry v oblasti kybernetické bezpečnosti.

SWOT analýza je strategický nástroj používaný k hodnocení síly a slabostí, příležitostí a hrozeb spojených s určitým podnikem, projektem nebo situací. Zkratka SWOT označuje čtyři hlavní složky analýzy:

1. **Síly (Strengths)**: Interní faktory, které podniku poskytují konkurenční výhodu nebo jiný druh pozitivního vlivu. Mohou zahrnovat výhodné aspekty jako je dobrá značka, inovativní výrobky, silný tým, nebo účinné procesy.
2. **Slabosti (Weaknesses)**: Interní faktory, které mohou bránit podniku v dosahování jeho cílů nebo snižovat jeho konkurenční postavení. Mohou to být nedostatky v infrastruktuře, nedostatek zdrojů, nedostatek odborných znalostí, nebo špatné řízení.
3. **Příležitosti (Opportunities)**: Externí faktory, které podniku nabízejí možnosti růstu, rozvoje nebo jiné pozitivní změny. Mohou to být změny v trhu, nové trendy, změny v zákaznických preferencích nebo změny v regulacích.
4. **Hrozby (Threats)**: Externí faktory, které mohou ohrozit podnik a jeho schopnost dosahovat cílů. Mohou to být konkurenční tlak, změny ve vnějším prostředí, ekonomické problémy, nebo změny v legislativě.[47]

[47] KNÁPKOVÁ, Adriana; PAVELKOVÁ, Drahomíra; ŠTEKER, Karel. Finanční analýza. *Komplexní průvodce s příklady. Praha*, 2010, s 174-176.

Strength - Silné stránky	Weaknesses - Slabé stránky
• většina zaměstnanců pracuje na úřadě déle než jeden rok • většina zaměstnanců pozná podvodné jednání v kyberprostoru • více než polovina zaměstnanců se účastní vzdělávání na bezpečnost v kyberprostoru • více než polovina zaměstnanců si doplňuje vzdělávání kybernetické bezpečnosti v rámci samostudia • zaměstnavatel nabízí více forem vzdělávání s akreditací • 66 % zaměstnanců se cítí být připraveno na přecházení kybernetickým hrozbám • schopnost odhalování kybernetických rizik • vyhovující kvalita informací v rámci vzdělávání	• 33, 3 % zaměstnanců má relativně nízkou motivaci k samostudiu • 6,7 % zaměstnanců neví o možnosti okamžité konzultace s IT technikem při vzniku rizikové události • 33 % zaměstnanců se cítí nepřipraveno na kybernetické hrozby • více než 30 % zaměstnanců není spokojeno se vzděláváním v oblasti kybernetické bezpečnosti • 40 % zaměstnanců není spokojeno s četností vzdělávání • rostoucí náklady na provoz úřadu
Opportunities - Příležitosti	Threats - Hrozby
• nové informační technologie • používání umělé inteligence • dotační programy na IT vybavení • vývoj a inovace softwaru • dostupnost odborných konzultací • zájem zaměstnanců o vzdělávání	• špatná ekonomická situace ve světě • 80 % zaměstnanců zaznamenává rizikové události v online prostoru • rychlost vývoje nových technologií a s tím i četnost kybernetických hrozeb • mnoho druhů kybernetických útoků • aktuálnost vzdělávání v oblasti kybernetických hrozeb • zneužití osobních údajů občanů

Tabulka 1 vlastní zpracování SWOT analýzy na základě výstupu z dotazníkového šetření

4.7 Vyhodnocení výsledků a možná doporučení

Cílem výzkumného šetření bylo zjistit, jestli si zaměstnanci samostatné městské části Praha – Dolní Chabry připadají dostatečně vzdělaní v oblasti kybernetické bezpečnosti. Dílčím cílem bylo identifikovat spokojenost zaměstnanců s průběhem a formami vzdělávání v oblasti kybernetické bezpečnosti.

Pro naplnění cíle výzkumu byly stanoveny tyto výzkumné předpoklady: **Výzkumný předpoklad 1:** Více než 50 % dotázaných respondentů potvrzuje, že jsou ve své profesi vystaveni různým kybernetickým hrozbám.

Výzkumný předpoklad 1 bylo možné potvrdit.

Celých 80 % dotázaných respondentů potvrdilo, že se ve svém povolání potýkají s různými kybernetickými hrozbami. Dokonce 13,3 % dotázaných odpovědělo, že s takovými hrozbami setkávají neustále, 20,0 % pak, že často.

Výzkumný předpoklad 2: Více než 50 % dotázaných respondentů se domnívá, že jsou dostatečně připraveni na to, aby dokázali kybernetické hrozby identifikovat a ubránit se jim.

Výzkumný předpoklad 2 bylo možné potvrdit.

Celých 66,6 % dotázaných respondentů potvrdilo, že absolvují vzdělávání v oblasti kybernetické bezpečnosti (školení od interního IT, předávání zkušeností od zkušenějších kolegů, externí školící firma apod.). Větší polovina dotázaných respondentů současně doplňuje, že si informace doplňují i samostudiem. Zřejmě na základě toho pak 66,7 % dotázaných potvrdilo, že by byli ochotni se spíše podílet na této formě vzdělávání vlastními prostředky. Konkrétně uvedlo 20 % dotázaných, že si spíše připadají dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s výkonem jejich povolání. Nejvíce dotázaných respondentů odpovědělo, že si určitě připadají dostatečně připraveni pro předcházení kybernetických hrozeb souvisejících s výkonem jejich povolání (46,7 %). Respondenti také potvrdili, že jsou po absolvování vzdělávání v oblasti kybernetické bezpečnosti lépe schopni odhalovat rizika a řešit je (73,3 %).

Výzkumný předpoklad 3: Více než 50 % dotázaných respondentů vyjadřuje spokojenost se vzděláváním v oblasti kybernetické bezpečnosti zajišťované úřadem.

Výzkumný předpoklad bylo možné potvrdit.

Celkem 66,7 % respondentů souhlasilo. Konkrétně 40 % dotázaných uvedlo, že jsou určitě spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem. Dalších 26,7 % dotázaných odpovědělo, že spíše jsou spokojeni se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno zaměstnavatelem. Více než polovina dotázaných respondentů také potvrdila, že jim vyhovuje četnost vzdělávání v oblasti kybernetické bezpečnosti, vyhovuje jim i kvalita a aktuálnost informací poskytovaných na školních v oblasti kybernetické bezpečnosti, rovněž respondenti vyjádřili i spokojenost s praktickým přesahem informací poskytnutých na školeních. Spokojení byli respondenti také s kvalitou a odborností lektora kurzů kybernetické bezpečnosti, vyhovující jsou podle všeho i používané metody vzdělávání.

Výzkumný předpoklad 4: Více než 50 % dotázaných respondentů vyjadřuje zájem o další vzdělávání v oblasti kybernetické bezpečnosti.

Výzkumný předpoklad bylo možné potvrdit.

Všichni dotázaní respondenti potvrdili, že by v budoucnu měli zájem o vzdělávání v oblasti kybernetické bezpečnosti. Konkrétně odpovědělo 66,7 % dotázaných respondentů a uvedlo, že by určitě v budoucnu měli zájem o další vzdělávání v oblasti kybernetické bezpečnosti. Zbylých 33,3 % dotázaných pak odpovědělo, že spíše mají v budoucnu zájem o další vzdělávání v oblasti kybernetické bezpečnosti. Konkrétně respondenti uváděli, že by měli zájem o informace ohledně podvodných emailů a zpráv. Dále měli zájem o rozpoznávání podvodných a rizikových programů, o bezpečný pohyb na internetu a jeho pravidla, zabezpečení mobilních telefonů, vzdělávání v bezpečnosti v internetovém bankovnictví. Více než polovina dotázaných respondentů by dokonce byla ochotna se finančně na tomto vzdělávání podílet.

Z uvedených výsledků vyplývá, že dotazovaní respondenti, ačkoli se často setkávají s kybernetickými hrozbami, absolvují v této oblasti různá školení a předávají si cenné informace i mezi kolegy a interním IT, který je jim k dispozici. Na základě těchto školení a pravděpodobně i vlastního samostudia si respondenti přijdou podle všeho dostatečně připraveni na přicházející kybernetické hrozby, ačkoli v dotaznících zaznívalo, že kybernetické hrozby a jejich vývoj je mnohdy rychlejší než probíhající školení a kurzy. Proto je na místě zajisté apelovat především na aktuálnost kurzů

a školení, k tomu je možné využít zejména interního IT technika, ale i externí, ověřenou firmu, která své kurzy pravidelně aktualizuje a připravuje kurzy podle toho, jak se na trhu objevují nové hrozby a ohrožení ideálně se zaměřením právě na veřejnou správu.

Z otázek zaměřujících se na kvalitu vzdělávacích aktivit valná většina respondentů potvrzovala jejich kvalitu, vyhovovala jim četnost školení, používané metody i kvalita lektorů. Ovšem na druhou stranu dotázaní respondenti potvrdili, že by měli o vzdělávání v oblasti kybernetické bezpečnosti v budoucnu ještě zájem. Z doporučení lze hlavní uvedená směřovat tímto směrem a naplánovat zaměstnancům další vzdělávání, a to ideálně s tímto zaměřením: podvodné emaily a zprávy, rozpoznávání podvodných a rizikových programů, bezpečný pohyb na internetu a jeho pravidla, zabezpečení mobilních telefonů, eventuálně bezpečnost v internetovém bankovnictví.

Závěr

Předkládaná práce se zaměřila především na problematiku vzdělávání ve veřejné správě. Vzdělávání v profesní kariéře je nezbytnou součástí jak v soukromé, tak i veřejné sféře, v každé zvlášť však má svá určitá specifika, která také byla vypíchnuta, zmíněna a popsána v této práci, stala se jejími součástmi. Cílem práce bylo mimo jiné přednostně identifikovat nedostatky v oblasti vzdělávání kybernetické bezpečnosti z pohledu zaměstnanců veřejné správy v samostatné městské části Praha – Dolní Chabry a navrhnout možná doporučení pro zlepšení situace. Dílčím cílem bylo pak zjistit spokojenost se vzděláváním zaměřeným na oblast kybernetické bezpečnosti.

Text této práce byl rozdělen na dvě části, část teoretickou a část praktickou. V první teoretické části práce byla pozornost věnována zejména kybernetické bezpečnosti, kybernetickým útokům, jejich specifikům ve vztahu k veřejné správě a možnostem prevence a obrany. Další část teoretické části se zaměřila už na oblast vzdělávání úřadníků. Tato část se zaměřila především na specifika vzdělávání v oblasti veřejné správy, používané metody a příslušnou legislativu. Poté navázala praktická část, jejíž součástí byla realizace dotazníkového šetření zaměstnanců vybraného úřadu se záměrem zjistit jejich zkušenosti, případná doporučení a názory na oblast vzdělávání v kybernetické bezpečnosti.

Z provedeného zkoumání vyplynulo, že zaměstnanci veřejné správy v samostatné městské části Praha – Dolní Chabry se pravidelně setkávají s kybernetickými hrozbami. Přesto se zaměstnanci cítili být připraveni těmto hrozbám čelit, a to pravděpodobně díky absolvování uváděných školení a vzdělávacích aktivit, které respondenti zmiňovali a formulovali (včetně samostudia). Při snaze identifikovat nedostatky bylo zjištěno, že zaměstnanci ve většině případů uvádějí se stávajícím stavem vzdělávání spokojenost a neidentifikovali žádné závažné nedostatky. S uvedeným pak souvisela rovněž zaměstnanci potvrzená spokojenost se vzděláváním zaměřeným na oblast kybernetické bezpečnosti, a to jak kvalitou lektorů, četností kurzů i používaných metod apod. Respondenti vyjádřili svůj zájem i o další vzdělávání v budoucnu, a dokonce by byli ochotni se na něm podílet i finančně. Proto doporučení v této práci směřovala především tímto směrem a navrhovala zejména témata dalších školení. Cíl práce i dílčí cíl byly tak splněny.

Přínos práce lze vidět především v souvislosti a ve spojitosti s výstupy a závěry pro samotné úředníky vybraného úřadu, neboť práce přesně popisuje a reflektuje situaci na daném pracovišti. Pro vedení tohoto úřadu se může stát zase východiskem při zajišťování dalších vzdělávacích programů a může být i potvrzením, že danou sledovanou a nejvíce ohroženou oblast státní správy správně monitoruje a zabezpečuje. Ovšem tím, že dotazníkové šetření bylo poměrně obecně pojaté, je možné ho s velkou pravděpodobností využít i pro jiné instituce v oblasti veřejné správy. Rovněž tak je možné využít práci s případnými úpravami i v soukromé sféře, kde kybernetické hrozby také ohrožují fungování firem.

Seznam použitých zdrojů

Literární zdroje

1. BAŠTA, P.; KROPÁČOVÁ, A.; KUNC, M. a kol. CyberSecurity. CZ.NIC. 2019. ISBN 9788088168324.
2. FARKAČOVÁ, L. Virtuální realita a další trendy ve vzdělávání zaměstnanců. Práce a mzda. 2023, (1): 36-40.
3. HRŮZA, P. Kybernetická bezpečnost. Brno: Univerzita obrany. 2012. ISBN 978-80-7231-914-5.
4. JIRÁSEK, P., NOVÁK, POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA. 2012. 93 s. ISBN: 978-80-7251-378-9.
5. KÁŇA, V. Základy veřejné správy. Montanex. 2007. 375 s. ISBN 80-722-5244-2.
6. KNÁPKOVÁ, Adriana; PAVELKOVÁ, Drahomíra; ŠTEKER, Karel. Finanční analýza. *Komplexní průvodce s příklady. Praha*, 2010, s.174-176.
7. KRÁKOROVÁ, Jaroslava. *Dolní Chabry*. Praha: Městská část Dolní Chabry, 2006. ISBN 80-239-7114-x.
8. MAREŠ, P. Kyberkultura, hackeři a digitální revoluce Informace chce být svobodná. Praha: Grada Publishing, a.s. 2022. ISBN 978-80-271-3358-1.
9. OECD. Přehled o stavu veřejné správy: Česká Republika. Česká republika na cestě k modernější a efektivnější veřejné správě. OECD Publishing. 2023. ISBN 9789264725751.
10. PEKOVÁ, J., JETMAR, M., PILNÝ, J. Veřejná správa a finance veřejného sektoru. Praha: ASPI. 2005. ISBN 80-7357-052-1.
11. SAK, P. Úvod do teorie bezpečnosti nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva. Petrklíč. 2018. ISBN 9788072297931.
12. ŠIKÝŘ, M. Personalistika pro manažery a personalisty: 2., aktualizované a doplněné vydání. Praha: Grada Publishing a.s., 2016. ISBN 978-80-271-9527-5.
13. ŠIMKOVÁ, E. Systémový přístup ke vzdělávání pracovníků veřejné správy. Olomouc: Univerzita Palackého v Olomouci, 2005, s. 142-147.
14. URBANCOVÁ, H. Vzdělávání zaměstnanců v českých organizacích. Práce a mzda, 2018, (7): 44-47.

15. URBANCOVÁ, H.; FAJČÍKOVÁ, A. Vzdělávání zaměstnanců. Je to aktivita managementu lidských zdrojů jen pro některé? Práce a mzda, 2019, (7): 46-50.
16. VALA, J. Celoživotní vzdělávání a dovednosti pro 21. století. Bezpečnost a hygiena práce. 2022, (2): 26-28.
17. WIRTZ, B. W. Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration. 2017, 40(13): 1085-1100.
18. ZORMANOVÁ, L. Obecná didaktika: Pro studium a praxi. Praha: Grada Publishing, a.s., 2014. ISBN 978-80-247-4590-9.

Elektronické zdroje

1. Deník veřejné správy. Kybernetická bezpečnost v obci – role starostů při jejím zajištění. [online]. 2022. [cit. 26-12-2023] Dostupné z WWW: <https://www.dvs.cz/clanek.asp?id=6824726>.
2. Deník veřejné správy. Vzdělávání úředníků územní samosprávy. [online]. 2023. [cit. 27-12-2023] Dostupné z WWW: <https://www.dvs.cz/clanek.asp?id=6883203>.
3. KADEŘÁBKOVÁ, M. Metody vzdělávání zaměstnanců: Víte, jaké lze použít? [online]. 2020. [cit. 28-12-2023] Dostupný z https://orangeacademy.cz/clanky/metody-vzdelavani-zamestnancu/.
4. MALÝ, Z. Kybernetické hrozby ve veřejné správě a zdravotnictví. Aktuální hrozby a legislativní změny (ZKB, GDPR). [online]. 2017. [cit. 26-12-2023] Dostupné z WWW: <https://www.systemonline.cz/clanky/kyberneticke-hrozby-ve-verejne-sprave-a-zdravotnictvi.htm?mobilelayout=false>.
5. NKÚ. Souhrnná zpráva o digitalizaci veřejné správy v ČR. [online]. 2019. [cit. 26-12-2023] Dostupné z WWW: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nku.cz/assets/publikace-a-dokumenty/ostatni-publikace/zprava-o-digitalizaci-verejne-spravy.pdf>.
6. STEM. Připravenost české společnosti na digitalizaci veřejné správy Přehledová studie vybrané teoretické a empirické literatury. [online]. 2023. [cit. 26-12-2023] Dostupné z WWW:<chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://osf.cz/wpcontent/uploads/2023/06/NadaceOSF_STEM_Pripravenost_ceske_spolecnosti_na_digitalizaci_verejne_spravy_2023.pdf>.

7. SVOBODA, C. Vzdělávání veřejné správy v soukromých rukách. [online]. 2021. [cit. 26-12-2023] Dostupné z WWW: <https://www.epravo.cz/top/aktualne/vzdelavani-verejne-spravy-v-soukromych-rukach-113834.html>.

Legislativní dokumenty

1. ČESKO. Vyhláška č. 512/2002 Sb., o zvláštní odborné způsobilosti úředníků územních samosprávných celků.
2. ČESKO. Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů.

Seznam zkratek

DDos	Distributed Denial-of-Service
E-banking	internetové bankovnictví
EMAS	Environmentální systém řízení
EU	Evropská unie
EVVO	Environmentální vzdělávání a výchova
ICT	informační a komunikační technologie
IPPCT	Integrovaná prevence a omezování znečištění
IT	informační technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OECD	Organizace pro hospodářskou spolupráci a rozvoj (1961)
RAF	Royal Air Forse
SWOT	Strengths –Weaknesses - Opportunities and Threats
TUR	Strategie udržitelného rozvoje
ŽP	životní prostředí

Seznam tabulek a grafů

Přílohy

https://www.survio.com/survey/d/B6O2C8E1K7G4N3V3C

Příloha 1: Dotazník pro úředníky.

Dobrý den,

ráda bych Vás požádala o účast na mém dotazníkovém šetření věnovaném oblasti kybernetického vzdělávání. Dotazník je naprosto anonymní, proto ho prosím vyplňte pravdivě. Pokud není u otázky uvedeno jinak, vyberte jen jednu odpověď a zřetelně ji označte. Výsledky dotazníku budou použity jen pro účely této práce.

Předem děkuji za Váš čas.

Jste:

a) žena
b) muž

Jak dlouho pracujete na úřadu samostatné městské části Praha – Dolní Chabry?

a) méně než rok
b) mezi 1 až 5 lety
c) déle

Zaznamenáváte ve svém zaměstnání různé hrozby a rizikové události v souvislosti s online či off-line prostorem využívaným v zaměstnání (podvodné emaily, hlášení antivirového systému aj.)?

a) ano, neustále
b) ano, často
c) ano, občas
d) ano, výjimečně
e) ne

Stalo se Vám už, že jste si neuvědomil/a nebo nevšiml podvodného či útočného jednání někoho skrze kyberprostor a ohrozil/a jste bezpečnost své práce?

a) ano, ale zabrzdil mě antivirový program
b) ano, ale naštěstí mi pomohl situaci vyřešit IT expert
c) ano a došlo k problému
   (vypište)……
   ……
d) ne

Absolvujete v rámci výkonu své profese vzdělávání zaměřené na bezpečnost v kybernetickém prostoru?

a) ano, pravidelně
b) ano, nepravidelně
c) ne

Doplňujete si vzdělávání v kybernetické bezpečnosti i v rámci samostudia?

a) ano, pravidelně
b) ano, nepravidelně
c) ne

Jaké formy vzdělávání v oblasti kybernetické bezpečnosti v rámci svého zaměstnání absolvujete (můžete zvolit více možností)?

a) jezdíme na kurzy a školení mimo pracoviště
b) absolvujete vzdělávací kurzy a školení na pracovišti s externím odborníkem
c) absolvujeme školení či přednášky našeho interního IT
d) máme k dispozici brožuru, příručku
e) využíváme na míru vytvořenou aplikaci
f) předáváme si navzájem zkušenosti s kolegy
g) jezdíme na stáže do firem
h) jiné……
……
i) žádné

Domníváte se, že jste na základě absolvovaného vzdělávání aktuálně dostatečně připraven/a pro předcházení kybernetických hrozeb souvisejících s výkonem Vašeho povolání?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Zaznamenáváte, že po absolvování vzdělávání v oblasti kybernetické bezpečnosti jste lépe schopni odhalovat rizika a řešit je?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Pokud ne, co je podle Vás důvodem?

a) nedostatečná aktualizace informací

b) kybernetické hrozby jsou rychlejší než vzdělávání
c) málo kurzů a školení
d) nedával/a jsem na kurzech pozor
e) špatně zaměřené kurzy
f) nudné kurzy
g) neabsolvoval/s jsem žádný kurz
h) jiný
důvod……
…….

Jste spokojen/a se vzděláváním v oblasti kybernetické bezpečnosti, které je zajišťováno Vašim zaměstnavatelem?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Vyhovuje Vám četnost vzdělávání v oblasti kybernetické bezpečnosti?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Vyhovuje Vám kvalita a aktuálnost informací v rámci vzdělávání v kybernetické bezpečnosti?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Jste spokojen/a s praktickým přesahem informací nabízených na kurzech?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Vyhovuje Vám kvalita a odbornost lektora?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Vyhovují Vám použité metody vzdělávání v oblasti kybernetické bezpečnosti?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

Máte na pracovišti možnost okamžité konzultace s odborníkem v oblasti kybernetické bezpečnosti, pokud byste si nevěděl/a rady při nějaké rizikové události?

a) ano, je vždy k dispozici
b) ano, ale ne vždy je k dispozici
c) ne
d) nevím

Měl/a byste zájem i v budoucnu o vzdělávání v oblasti kybernetické bezpečnosti?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne

V jaké oblasti konkrétně (můžete vybrat více možností)?

a) je mi to jedno
b) podvodné emaily a zprávy
c) bezpečný pohyb na internetu
d) rozpoznání rizikových programů apod.
e) bezpečné nakupování na internetu
f) bezpečí v oblasti internetového bankovnictví aj.
g) zabezpečení mobilních telefonů
h) jak chránit děti před kyberhrozbami
i) bezpečnost na sociálních sítích
j) antivirové programy
k) jiné……
……
l) nemám zájem

Byl/a byste eventuálně ochoten/na se i finančně podílet na takovém vzdělávání?

a) určitě ano
b) spíše ano
c) spíše ne
d) určitě ne