

Vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice

Kristýna Brůžová

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Kristýna Brůžová
Osobní číslo:	L22476
Studijní program:	B1032A020002 Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice

Zásady pro vypracování

- Vymezte základní pojmy a zpracujte teoretický vstup do dané problematiky.
- Proveďte analýzu současného stavu vzdělávání v kybernetické a informační bezpečnosti v České republice.
- Na základě provedené analýzy navrhněte opatření ke zvýšení kvality vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
3. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
4. SENANAYAKE, Tharindu a FERNANDO, Suchinhi. Information Security Education: Watching Your Steps in Cyberspace. Online. *The Online Journal of Science and Technology*. 2018, roč. 8, č. 2, s. 96-101. ISSN 2146-7390. Dostupné z: <https://www.tojsat.net/journals/tojsat/volumes/tojsat-volume08-i02.pdf>. [cit. 2024-10-27].
5. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **2. prosince 2024**
Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 25. 4. 2025

.....
podpis autora

ABSTRAKT

Bakalářská práce se věnuje problematice vzdělávání v kybernetické a informační bezpečnosti v České republice. V teoretické části práce je vymezen právní rámec včetně důležitých zákonů, vyhlášek a evropských směrnic. Dále jsou popsány instituce, které se danou problematikou v České republice zabývají. Důraz je rovněž kladen na vysvětlení základních pojmů, přehled významných kybernetických incidentů a na vzdělávání.

Praktická část se věnuje zhodnocení vybraných vzdělávacích kurzů v oblasti kybernetické a informační bezpečnosti v České republice prostřednictvím vícekritériální analýzy. Součástí praktické části bylo provedeno kvalitativní šetření formou strukturovaných rozhovorů se zaměstnanci státního a soukromého sektoru. Výsledkem práce je porovnání a návrh zvýšení úrovně vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice.

Klíčová slova: bezpečnost, informace, informační bezpečnost, kybernetická bezpečnost, vzdělávání

ABSTRACT

The bachelor thesis deals with the issue of education in cyber and information security in the Czech Republic. The theoretical part of the thesis defines the legal framework including important laws, decrees and European directives. Furthermore, the instructions dealing with this issue in the Czech Republic are described. Emphasis is also placed on the explanation of basic concepts, an overview of significant cyber incidents and on education.

The practical part is devoted to the evaluation of selected training courses in the field of cyber and information security in the Czech Republic through a multi-criteria analysis. The practical part included a qualitative investigation in the form of structured interviews with public and private sector employees. The result of the work is a comparison and a proposal to increase the level of education in the field of cyber and information security in the Czech Republic.

Keywords: safety, education, cyber security, information, information security

Tímto bych ráda poděkovala vedoucímu bakalářské práce, panu Ing. Petru Svobodovi Ph.D., za cenné rady a připomínky, které mi velmi pomohly při psaní bakalářské práce.

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

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 PRÁVNÍ RÁMEC A ORGANIZACE.....	13
1.1 DOKUMENTY, PRÁVNÍ NORMY VZTAHUJÍCÍ SE K PROBLEMATICE	13
1.1.1 Zákon o kybernetické bezpečnosti	13
1.1.2 Vyhláška o kybernetické bezpečnosti	13
1.1.3 Vyhláška o významných informačních systémech a jejich určujících kritériích	14
1.1.4 Směrnice NIS 1	14
1.1.5 Směrnice NIS2	15
1.1.6 Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti.....	15
1.1.7 Zákon o zpracování osobních údajů.....	16
1.2 VYBRANÉ ORGANIZACE ZABÝVAJÍCÍ SE KYBERNETICKOU BEZPEČNOSTÍ V ČESKÉ REPUBLICE	16
1.2.1 Národní bezpečnostní úřad.....	16
1.2.2 Národní úřad pro kybernetickou a informační bezpečnost	17
1.2.3 Národní centrum kybernetické bezpečnosti	18
1.2.4 Computer Security Incident Response Team (CSIRT).....	18
1.2.5 Computer Emergency Response Team (CERT)	19
1.2.6 Národní centrum kybernetických operací	19
2 ZÁKLADNÍ TERMINOLOGIE V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI.....	20
2.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ	20
2.2 KYBERNETICKÉ ÚTOKY	21
3 VÝZNAMNÉ UDÁLOSTI V OBLASTI KYBERNETICKÉ BEZPEČNOSTI.....	24
3.1 VYBRANÉ KYBERNETICKÉ BEZPEČNOSTNÍ INCIDENTY V ČESKÉ REPUBLICE	24
3.2 VYBRANÉ KYBERNETICKÉ BEZPEČNOSTNÍ INCIDENTY V ZAHRANIČÍ	25
4 PROBLEMATIKA VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI.....	29
4.1 POJEM, FORMY A METODY VZDĚLÁVÁNÍ.....	29
4.2 VZDĚLÁVACÍ AKCE PRO VEŘEJNOST	30
4.3 VZDĚLÁVÁNÍ ZAMĚSTNANCŮ	31
4.4 VZDĚLÁVÁNÍ VE ŠKOLÁCH	33
5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI	34
II PRAKTICKÁ ČÁST.....	35
6 VZDĚLÁVACÍ KURZY V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE	36

6.1	CHARAKTERISTIKA VYBRANÝCH KURZŮ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE	36
6.1.1	Placené kurzy	36
6.1.2	Neplacené kurzy	39
6.2	ANALÝZA VYBRANÝCH KURZŮ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE	41
7	STRUKTUROVANÉ ROZHOVORY	48
7.1	CÍL PRÁCE A VÝZKUMNÉ OTÁZKY	48
7.2	METODIKA VÝZKUMU	48
7.3	VÝBĚR A CHARAKTERISTIKA RESPONDENTŮ	50
7.4	PROVEDENÍ VÝZKUMNÉHO ŠETŘENÍ	51
7.5	SOUHRN ROZHOVORŮ	51
7.5.1	Respondenti ze státního sektoru	51
7.5.2	Respondenti ze soukromého sektoru	52
7.6	SHRNUTÍ A VYHODNOCENÍ ZÍSKANÝCH DAT	53
8	NÁVRH NA ZLEPŠENÍ VZDĚLÁVÁNÍ V KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE	57
	ZÁVĚR.....	60
	SEZNAM POUŽITÉ LITERATURY	61
	SEZNAM TABULEK.....	73
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	74
	SEZNAM PŘÍLOH.....	75

ÚVOD

V dnešním rychle se rozvíjejícím online světě, kdy je většina každodenních činností úzce spjata s informačními technologiemi, hraje vzdělávání v kybernetické a informační bezpečnosti důležitou roli při ochraně organizací, institucí i jednotlivců před rafinovanými hrozbami. Stále častěji jsme svědky situací, kdy dochází k narušení důvěrnosti, integrity nebo dostupnosti informací. Kybernetické hrozby se staly běžnou součástí každodenního života a zasahují do všech oblastí veřejného, ale i soukromého sektoru.

Ochrana před kybernetickými hrozbami už zdaleka není pouze otázkou technologií, ale také informovanosti a odpovědnosti lidí. Právě lidská chyba, nedostatečná informovanost nebo neznalost základů bezpečného chování na internetu často vedou ke vzniku kybernetických incidentů. Právě proto je vzdělávání v kybernetické a informační bezpečnosti velmi důležité. Zvyšování povědomí o hrozbách, rozvíjení základů bezpečného chování na internetu, jsou nezbytné pro všechny uživatele online prostředí. Vzdělání v této oblasti nabývá stále většího významu nejen ve firmách, ale také v institucích veřejné správy, které pracují s citlivými daty.

I přestože téma kybernetické bezpečnosti je čím dál více diskutované, úroveň vzdělávání je v této oblasti v různých institucích stále nerovnoměrná. Vědomosti v této oblasti jsou důležitým prvkem nejen ochrany pracovního prostředí, ale i důležitým prvkem pro bezpečné fungování jednotlivců v online světě.

Hlavním cílem bakalářské práce je na základě zjištěných informací navrhnout vhodné řešení vedoucí ke zlepšení vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice. K naplnění hlavního cíle práce je využito třech dílčích cílů. Prvním dílčím cílem je pojednat o teoretických východiscích řešené problematiky. Druhým dílčím cílem je analyzovat a provést komparaci za účelem porovnání vybraných kurzů poskytovaných v České republice. Třetím dílčím cílem je realizace strukturovaných rozhovorů s vybranými zaměstnanci státního a soukromého sektoru za účelem zmapování aktuální úrovně vzdělávání v oblasti kybernetické a informační bezpečnosti v České republice.

K dosažení stanovených cílů této bakalářské práce je využito rešerše, která slouží k vytvoření přehledu základních teoretických poznatků k danému tématu. Analýza a komparace je v práci využita k objektivnímu zhodnocení vybraných vzdělávacích kurzů. Strukturované rozhovory slouží ke zhodnocení stavu vzdělávání zaměstnanců ve státním a soukromém sektoru.

I. TEORETICKÁ ČÁST

1 PRÁVNÍ RÁMEC A ORGANIZACE

Kybernetická a informační bezpečnost v České republice je upravována řadou právních předpisů a je v kompetenci několika institucí. Následující kapitola se zaměřuje na právní rámec, který upravuje kybernetickou a informační bezpečnost a na instituce odpovědné za její zajištění.

1.1 Dokumenty, právní normy vztahující se k problematice

Tato kapitola se zaměřuje na klíčové legislativní předpisy platné na území České republiky, které se týkají oblasti kybernetické a informační bezpečnosti.

1.1.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. O kybernetické bezpečnosti definuje práva a povinnosti osob a pravomoc a působnost státních orgánů v oblasti kybernetické bezpečnosti. Zákon implementuje evropské předpisy, konkrétně však směrnici NIS, týkající se oblasti kybernetické bezpečnosti. Hlavním úkolem zákona je určit minimální úroveň bezpečnostních opatření, zlepšit identifikaci kybernetických bezpečnostních incidentů a zavést povinnost jejich hlášení. (ČESKO, 2014)

Nový zákon o kybernetické bezpečnosti plní požadavky dané evropskou směrnicí bezpečnostní NIS2. Podle nového zákona je poskytovatel regulované služby zařazen buď do režimu vyšších, nebo nižších povinností. Tento režim určuje rozsah povinností, které musí poskytovatel dodržovat. (Polák, 2024)

S účinností novely zákona vznikne organizacím povinnost registrace u Národního bezpečnostního úřadu pro kybernetickou a informační bezpečnost. Řídící orgány musí mít schopnost identifikovat a vyhodnocovat opatření pro řízení rizik kybernetické bezpečnosti. Novela zákona obsahuje přísnější pravidla pro řízení kybernetické bezpečnosti a také klade důraz na vzdělávání v této oblasti. Zákon taktéž ukládá povinnost lépe chránit data a infrastrukturu pro firmy poskytující klíčové služby. (ESET, 2024) Účinnost nového zákona by měla připadnout na druhou polovinu roku 2025. (Hanzel, 2025)

1.1.2 Vyhláška o kybernetické bezpečnosti

Na zákon o kybernetické bezpečnosti navazuje vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti, která se týká zejména informačních a komunikačních systémů kritické informační infrastruktury. Vyhláška definuje bezpečnostní opatření a jejich rozsah, obsah

bezpečnostní dokumentace, kategorie bezpečnostních incidentů, postup při likvidaci dat a provozních údajů. (Smejkal et al., 2019a)

1.1.3 Vyhláška o významných informačních systémech a jejich určujících kritériích

Dne 19. prosince 2014 nabyla účinnosti vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. Právní návrh vznikl ve spolupráci Národního bezpečnostního úřadu a Ministerstva vnitra. Tato vyhláška se zabývá určením významných informačních systémů a pravidel pro jejich určení. (KYBEZ, 2014)

1.1.4 Směrnice NIS 1

Směrnice NIS neboli Network Information Security má zásadní význam v oblasti kybernetické bezpečnosti. Směrnice vytvořila základ pro kybernetickou bezpečnost na úrovni Evropské unie. Cílem směrnice, která vstoupila v platnost v srpnu 2016, je zajistit bezpečnost sítí, informačních systémů a vytvořit požadavky, které budou plnit všechny státy Evropské unie. (Duračinská, 2016)

Mezi povinnosti každého státu EU patří přijetí strategie tzn., že každý stát EU má mít vytvořenou národní strategii zaměřenou na zajištění bezpečnosti sítí a informačních systémů, která bude obsahovat strategické cíle a opatření, které stát v brzké době přijme. Státy mají povinnost zřídit centrální orgán na řízení kybernetické bezpečnosti. Zřízený orgán by měl fungovat jako ústřední kontaktní místo pro přeshraniční spolupráci na úrovni Unie a měl by disponovat potřebnými technickými a finančními zdroji k plnění úkolů. (Duračinská, 2016)

Další povinností každého státu EU je zřízení CSIRT týmu (Cyber Security Incident Response Team) neboli Skupiny pro reakci na incidenty v oblasti počítačové bezpečnosti, jehož úlohou je spolupráce mezi všemi CSIRT týmy v daném státě. Další povinností je zřízení Skupiny pro spolupráci, jejíž úloha je strategická a bude složena ze zástupců centrálních orgánů. (Duračinská, 2016)

Směrnice se vztahuje na dvě skupiny povinných subjektů, a to na provozovatele základních služeb a provozovatele elektronických služeb. Do skupiny provozovatelů základních služeb spadají subjekty působící v odvětvích, jako jsou energetika, doprava, bankovníctví, zdravotnictví, infrastruktury a digitální infrastruktury. Do skupiny provozovatelů elektronických služeb řadíme online platformy typu tržišť, internetové vyhledávače a firmy poskytující cloudové služby. Na tuto skupinu se vztahuje méně povinností a státy by je

neměly zatěžovat dalšími, než které ukládá směrnice. Hlavním cílem je, aby nedocházelo k omezování trhu a provozovatelé se nedostávali do nepříznivého postavení vůči provozovatelům mimo EU. (Doucek et al., 2019)

1.1.5 Směrnice NIS2

Směrnice NIS2 vstoupila v platnost 16. ledna 2023, jejímž cílem je prohloubit a rozšířit předchozí směrnici NIS. Transpoziční lhůta, ve které členské státy musí směrnici začlenit do svého národního práva je stanovena na 21 měsíců. (NÚKIB, 2024a)

Směrnice NIS2 přinesla několik podstatných změn. Dle nové směrnice má každý členský stát povinnost určit jeden ze svých týmů CSIRT (CERT), který bude plnit roli národního koordinátora. Jeho úlohou bude koordinované zveřejňování zranitelností. Koordinátor *„usnadňuje interakci mezi fyzickou nebo právníkou osobou oznamující zranitelnost a výrobcem nebo poskytovatelem případných zranitelných ICT produktů nebo služeb.“* (NÚKIB, 2025a)

Další podstatnou změnou směrnice NIS2 je rozšíření počtu povinných osob, a to rozšířením regulovaných odvětví a rozšířením stávajících odvětví o regulované služby, anebo změnou metody identifikace povinných osob. Mezi další významnou změnu patří zvýšení pokut za nedodržení povinností. Za porušení povinností ve vyšším režimu hrozí pozastavení funkce statutára až na půl roku. Za porušení povinností základními subjekty hrozí pokuta s horní hranicí sazby nejméně 10 milionů Eur nebo 2 % celkového celosvětového ročního obrátu v předchozím roce. Při určení sankce záleží, která hodnota je vyšší. Za porušení povinností důležitými subjekty hrozí pokuta až do výše 7 milionů EUR nebo 1,4 % celkového celosvětového ročního obrátu za předchozí rok – přičemž se uplatní ta částka, která je vyšší. (NÚKIB, 2025a)

1.1.6 Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti

Zákon č. 412/2005 Sb. se zabývá pravidly pro nakládání s informacemi, které jsou považovány za utajované. Dále stanovuje podmínky pro přístup a nakládání s těmito informacemi. (ČESKO, 2005)

Zákon definuje stupně utajení informací:

- *„Přísně tajné – jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmu České republiky,*

- *Tajné – jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmu České republiky*
- *Důvěrné – jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmu České republiky,*
- *Vyhrazené – jestliže její vyjádření neoprávněné osobě nebo zneužití může být nevýhodné pro zájem České republiky“.* (ČESKO, 2005)

Cílem zákona je zajistit, aby tyto informace nebyly zneužity či zpřístupněny. Zveřejnění nebo neoprávněné využití informací může ohrozit nebo poškodit zájmy České republiky. (ČESKO, 2005)

1.1.7 Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., upravuje nakládání s osobními údaji v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679, nazývané GDPR neboli General Data Protection Regulation. Zákon stanovuje pravidla, za jakých okolností je možné osobní údaje shromažďovat, dále s nimi nakládat, zpracovávat a uchovávat. Zajišťuje odpovědnost organizací za správu a bezpečné zpracování osobních údajů. Dále stanovuje pokuty, které mohou být uloženy za porušení zákona. (ČESKO, 2019)

1.2 Vybrané organizace zabývající se kybernetickou bezpečností v České republice

Následující kapitola bude věnována organizacím zabývajícím se kybernetickou bezpečností v České republice.

1.2.1 Národní bezpečnostní úřad

Národní bezpečnostní úřad (dále jen „NBÚ“) byl založen dne 1. srpna 1998. NBÚ byl vytvořen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a změně některých zákonů. NBÚ je orgánem výkonné moci a plní funkci správního úřadu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. (NBÚ, 2025)

NBÚ je čistě civilní státní orgán, jehož zaměstnanci pracují v běžném pracovním poměru a nikoliv ve služebním. I přesto má na starosti vysoce citlivé úkoly související s národní bezpečností. Při plnění úkolů úzce spolupracuje se zpravodajskými službami a s ozbrojenými bezpečnostními složkami. Financování úřadu je zajišťováno výhradně

prostřednictvím státního rozpočtu. (Pavelka, 2018) Do čela úřadu je jmenován ředitel, kterého jmenuje předseda vlády na základě návrhu ministra vnitra. (NBÚ, 2024)

Hlavní činností úřadu je kontrola a ochrana utajovaných informací v orgánech statní správy i soukromých objektů. Dalším významným úkolem je vydávání utajovaných souborů pravidel, které stanovují postupy, technická opatření a organizační řešení pro zajištění minimální požadované úrovně ochrany utajovaných informací. NBÚ plní povinnosti v oblastech, které vycházejí z členství České republiky v EU, NATO a také z mezinárodních smluv. Provádí správní řízení a uděluje sankce za neplnění povinností souvisejících s ochranou utajovaných informací. (Pavelka, 2018)

Od října roku 2011 do 30. července 2017 spadal pod působnost NBÚ dohled nad kybernetickou bezpečností. Tuto oblast si ke dni 1. srpna 2017 převzal Národní úřad pro kybernetickou a informační bezpečnost. (Pavelka, 2018)

1.2.2 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vznikl dne 1. srpna 2017 na základě zákona č. 205/2017 Sb., který novelizoval zákon 181/2014 Sb., o kybernetické bezpečnosti. NÚKIB vystupuje jako ústřední správní orgán odpovědný za oblast kybernetické bezpečnosti, včetně zabezpečení utajovaných informací v rámci informačních a komunikačních systémů a za zajištění kryptografické ochrany. (NÚKIB, 2025b)

Úřad vede ředitel, který se pravidelně účastní jednání Bezpečnostní rady státu a zároveň je členem Výboru pro kybernetickou bezpečnost. (NÚKIB, 2025b)

Dne 1. července 2022 nastoupil do funkce ředitele a jejím i v současné době pan Ing. Lukáš Kintr. (NÚKIB, 2022a)

Úřad má své pobočky v Praze a Brně a je financován ze státního rozpočtu stejně, jako NBÚ. (NÚKIB, 2025c)

Dalšími důležitými úkoly je příprava zákonů a norem vztahujícím se ke kybernetické bezpečnosti a dále tvoří Národní strategii kybernetické bezpečnosti. Dalšími dokumenty vydávanými tímto úřadem je Zpráva o stavu kybernetické bezpečnosti České republiky a Akční plán k Národní strategii kybernetické bezpečnosti. NÚKIB dále zpracoval aktuální strategický dokument s názvem Národní politika kryptografické ochrany utajovaných informací v České republice pro období let 2024 až 2030, s výhledem

do roku 2040, který vymezuje klíčové směry rozvoje kryptografické ochrany utajovaných informací. Dokument byl schválen Bezpečnostní radou státu dne 14. listopadu 2024. V roce 2025 bude vypracován implementační plán, který transformuje stanovené cíle do konkrétních kroků a opatření. (NÚKIB, 2024b)

NÚKIB se taktéž věnuje vzdělávání a poskytuje e-learningové kurzy a přednášky z oblasti kybernetické bezpečnosti různým cílovým skupinám. Hlavní cílovou skupinou jsou zaměstnanci veřejné správy a úředníci. Do druhé skupiny spadají zejména žáci mateřských, základních a středních škol, u kterých se snaží rozvíjet návyky bezpečného zacházení s informacemi. Do další skupiny se řadí širší veřejnost a senioři, kterým kurzy pomáhají s bezpečným pohybem na internetu. (NÚKIB, 2025d)

1.2.3 Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti (dále jen „NCKB“) je výkonnou složkou NÚKIB. Jeho hlavním úkolem je řešení kybernetických bezpečnostních incidentů, mezinárodní spolupráce, osvětová a edukační činnost, výzkumná činnost v oblasti kybernetické bezpečnosti a analýza rizik. V neposlední řadě jeho úkolem je i činnost týmu CERT a ochrana prvků kritické infrastruktury před kybernetickými hrozbami prostřednictvím preventivních opatření. (NÚKIB, 2025e)

1.2.4 Computer Security Incident Response Team (CSIRT)

Computer Security Incident Response Team (dále jen „CSIRT“) je národní tým, který se zabývá řešením a monitorováním incidentů týkajících se kybernetické bezpečnosti v sítích vedených v České republice. (CZ.NIC, 2010)

Národní CSIRT České republiky je od 1. ledna 2011 provozován sdružením CZ.NIC. Tým má aktuálně 17 členů, kteří jsou zaměstnanci sdružení CZ.NIC. Hlavními cíli je udržování zahraničních vztahů a spolupráce v rámci České republiky s organizacemi, jako jsou banky, bezpečnostní složky, úřady státní správy a další organizace. (CSIRT, 2019a)

Jedním z mnoha projektů je projekt DNS Crawler, jehož úkolem je sběr dat z DNS a webových stránek všech domén druhé úrovně. Cílem projektu je zjištění bezpečnostních problémů, jako je odhalení falešných e-shopů či domén. Dalším známým projektem je penetrační testování, které *„slouží k hledání slabých míst v infrastruktuře zákazníka“*. (CSIRT, 2019b)

Testování organizací pomáhá odhalit a odstranit skryté hrozby, o kterých nemají často žádné povědomí. (CSIRT, 2019b)

1.2.5 Computer Emergency Response Team (CERT)

Vládní CERT (GovCERT.CZ) spadá pod Národní centrum kybernetické bezpečnosti. Hlavní činností vládního týmu CERT je řešení bezpečnostních incidentů a následná koordinace postupu jeho řešení. CERT dále zajišťuje penetrační testování sloužící k otestování průniku do systému, kde výsledkem je dokument obsahující nedostatky v zabezpečení daného subjektu. Další činností je pomoc při řešení incidentů, tvorba opatření a komunikace se zahraničními týmy. (NÚKIB, 2025f)

1.2.6 Národní centrum kybernetických operací

Národní centrum kybernetických operací (dále jen „NCKO“) je specializované pracoviště, které spadá pod Vojenské zpravodajství České republiky a bylo zřízeno na základě rozhodnutí vlády v roce 2015 s cílem zajistit kybernetickou obranu státu. (VOJENSKÉ ZPRAVODAJSTVÍ, 2018)

Jeho hlavním úkolem je vybudování obranného mechanismu v kybernetickém prostoru, který umožní České republice reagovat na kybernetické útoky, zabránit jim anebo je odvrátit, a tím zajistit bezpečnost civilního obyvatelstva a infrastruktury. (VOJENSKÉ ZPRAVODAJSTVÍ, 2025)

2 ZÁKLADNÍ TERMINOLOGIE V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

V následující kapitole budou popsány pojmy, které se vztahují ke kybernetické a informační bezpečnosti a jsou považovány za nejdůležitější z pohledu vypracování bakalářské práce.

2.1 Vymezení základních pojmů

Kybernetický prostor představuje digitální prostředí tvořené digitálními technologiemi, informačními systémy, komunikačními sítěmi a internetem, kde dochází ke vzniku, zpracování a výměně informací. (Sedlák a Konečný, 2021)

Kybernetická hrozba představuje možný zdroj bezpečnostního incidentu v kyberprostoru, který by mohl způsobit poškození systému, společnosti a organizací. (Jirásek et al., 2022)

Kybernetický bezpečnostní incident označuje situaci, kdy dojde k ohrožení nebo narušení zabezpečení informací v rámci informačních systémů, porušení důvěrnosti a integrity sítí. (Seyfor, 2024) Incidenty mohou vzniknout v důsledku lidského pochybení, selhání systému nebo narušením dostupnosti, důvěrnosti a integrity. (Doucek et al., 2019)

Kybernetická bezpečnostní událost je situace, kdy vzniká důvodné podezření, že došlo k ohrožení bezpečnosti informací, služeb nebo zásahu do správného a spolehlivého fungování sítí a elektronické komunikace. (Zákony pro lidi, 2024)

Pojem **bezpečnost** lze definovat jako stav, kdy jsou jednotlivci nebo skupiny chráněni před možnými hrozbami, riziky a necítí se být ohroženi. (Smejkal et al., 2019b)

Kybernetická bezpečnost je soubor metod, postupů a technologických opatření, jejichž cílem je zvýšit ochranu kritických systémů a sítí před kybernetickými hrozbami. (Microsoft, 2025)

Informační bezpečnost se soustředí na zabezpečení dat a informací ve všech fázích její existence bez ohledu na typ nosiče. (Kolouch a Bašta, 2019)

Triáda CIA je koncept používaný v oblasti informační bezpečnosti, který zajišťuje zásadu důvěrnosti, celistvosti a důslednosti informací. (Kolouch a Bašta, 2019)

Důvěrnost („confidentiality“) nám zajistí, že přístup k informacím, datům má pouze oprávněná osoba. **Celistvost** („integrity“) zaručuje, že informace nejsou neoprávněně změněny nebo zničeny. **Zásada dostupnosti** („availability“) označuje situaci, kdy má

uživatel možnost přistupovat k datům a informacím dle jeho požadavků. (Chowdhury et al., 2023)

Data jsou v knize CyberSecurity definovány jako „*jakékoli prvky s informační hodnotou, které jsou zpracovány počítačovým systémem, přičemž jsou zpracovány tak, aby následně utvořily informaci*“. (Kolouch a Bašta, 2019)

V literatuře existuje celá řada definic **pojmu informace**. Podle Smejkalů lze za informaci považovat: „*každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá*.“ (SMEJKAL, 2015)

Například podle Požára lze za informace považovat „*údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací*.“ (POŽÁR, 2005)

2.2 Kybernetické útoky

Kybernetické útoky představují rostoucí hrozbu nejen pro jednotlivce, ale i pro organizace a státní instituce, přičemž jejich sofistikovanost a četnost neustále narůstají. Útočníci využívají různé metody, jako jsou ransomware, malware, phishing, DDoS útoky a další k tomu, aby narušili provoz systémů a získali citlivá data.

Vybrané typy kybernetických hrozeb

Dle zprávy, kterou vydala Evropská agentura pro kybernetickou bezpečnost patří mezi nejčastější kybernetické hrozby v posledních letech:

- **Malware** – škodlivý software neboli škodlivý kód, jehož úkolem je odcizení dat, poškození systému, sledování uživatele. (Internetem BEZPEČNĚ, 2016)
- **Ransomware** – škodlivý systém, jehož cílem je zašifrovat, zablokovat nebo omezit přístup k datům, zařízením oběti, dokud není uhrazena požadovaná částka. (ESET, 2025a)
- **Spam** – představuje hromadné rozesílání nevyžádaných zpráv, které mohou v sobě skrývat malware, který se může snadno dostat do uživatelského zařízení s cílem ho poškodit. Z tohoto důvodu se doporučuje zprávy neotevírat, ale označit je jako spam a odstranit. (Sedlák a Konečný, 2021)

- **DDoS útoky** – typ útoku při kterém se útočníci snaží zahltit webovou stránku, síť velkým množstvím nevyžádaných požadavků. Cílem je způsobit zpomalení, omezení nebo úplný výpadek daného systému. (ESET, 2025b)
- **Phishing** – útok, jehož cílem je získat peníze a důvěrné údaje, například informace o platebních kartách, přihlašovací údaje nebo hesla. Útočníci se snaží oběť přesvědčit, aby informace zadala na falešné webové stránky, které se tváří zprvu důvěryhodně. (Khonji et al., 2013)

Phishing lze rozdělit na několik typů:

- **Smishing** – známý jako SMS phishing, je podvodná technika, při níž útočníci posílají falešné zprávy. Tyto zprávy obsahují odkaz na podvodnou webovou stránku nebo telefonní číslo, přes které se má oběť spojit s institucí, za kterou se útočníci vydávají. (ESET, 2025c)
- **Quishing** – poměrně nová a stále častější forma phishingu, která využívá QR kódy k přesměrování na falešné webové stránky a k následnému získávání citlivých informací. Tento typ útoku je obzvlášť nebezpečný, protože QR kódy jsou vnímány jako důvěryhodné. Jejich obsah není viditelný pouhým pohledem, což umožňuje útočníkům snadno skrýt nebezpečné odkazy. QR kódy lze jednoduše umístit na různá místa, což zvyšuje pravděpodobnost, že je nic netušící uživatel naskenuje. (WINTIP, 2024)
- **Whaling** – jedná se o druh phishingu, který je zaměřen na vedoucí pracovníky a majitele firem. Jedná se o oklamání obětí a přiměnění k poskytnutí citlivých informací nebo převodu peněz. (Vanitha et al., 2024)
- **Pharming** – funguje na principu změnění IP adresy, což vede k následnému přesměrování uživatele na falešné stránky, například e-mailu nebo internetového bankovníctví. Stránky bývají vizuálně téměř identické s originálními stránkami. (Jirásek et al., 2022)
- **Spear phishing** – specifický phishingový útok, při němž si útočník předem shromáždí veškeré dostupné informace o dané osobě či jednotlivci. Následně útočník vytvoří podvodnou zprávu přímo na míru. (ESET, 2025c)
- **Vishing** – neboli podvodné volání. K provedení útoků útočníci využívají předem nahrané zprávy. (ESET, 2025c) Během těchto hovorů se útočník představuje jako

zaměstnanec důvěryhodné společnosti. Útočnickovým úkolem je snaha získat zejména údaje k platební kartě nebo přihlašovací údaje do internetového bankovníctví. (MONETA BANK, 2025)

3 VÝZNAMNÉ UDÁLOSTI V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V posledních letech se díky počtu kybernetických útoků stala kybernetická bezpečnost klíčovým tématem v České republice. Významné bezpečnostní incidenty, jako jsou útoky na nemocnice, finanční instituce či vládní weby, poukazují na zranitelnost kritické infrastruktury. Tato kapitola se zaměřuje na vybrané kybernetické útoky v České republice a zahraničí.

3.1 Vybrané kybernetické bezpečnostní incidenty v České republice

Tato podkapitola se zaměřuje na vybrané kybernetické útoky na území České republiky.

Kybernetický útok na FN Brno

V roce 2020 došlo k největšímu kybernetickému útoku na česká zdravotnická zařízení, a to k útoku na Fakultní nemocnici Brno. Dle zjištění se jednalo o cílený phishingový útok, kde útočník k nabourání do systému využil kryptovir Defray, který je používán k šifrování dat a následnému požadování výkupného. Útok byl zahájen ve dvě hodiny ráno, kdy postupně docházelo k vyřazování jednotlivých částí IT systému nemocnice. Nemocnice reagovala na útok vypnutím všech počítačů. (HORÁK, 2020)

Došlo k zrušení plánovaných operací a akutní případy byly přesunuty do ostatních nemocnic v Brně a kraji. Základní chod nemocnice byl po útoku zachován. (IDNES.cz, 2020)

Nemocnice díky útoku přišla o mnoho dat, smluv či vědeckých podkladů. Odhadovaná výše škody dosahuje 150 milionů korun. (Service & Support, 2023)

Kybernetický útok na Psychiatrickou nemocnici v Kosmonosech

Pár dnů po útoku na FN Brno proběhl útok na psychiatrickou nemocnici v Kosmonosech. Jednalo se o ransomwarový útok, který využil nedostatečně chráněná místa na serverech. Cílem útoku bylo zašifrování dat v informačním systému a následné požadování výkupného. Rychlá reakce pracovníků nemocnice umožnila odhalení útoku v počáteční fázi. Včasným zásahem se podařilo škody na datech minimalizovat. (NCEZ, 2020)

Kybernetický útok na Univerzitu obrany

V září 2023 se Univerzita obrany v Brně stala terčem kybernetického útoku. V čele útoku dle dostupných informací stála ransomware skupina Monti, která pronikla do systému a odcizila zhruba 750 GB dat. Univerzita odmítla zaplatit výkupné požadované

útočníky, což vedlo k postupnému zveřejňování odcizených dat, mezi kterými byla e- mailová komunikace zaměstnanců, zápisy z porad, finanční výkazy a další citlivé informace, které se týkaly zejména Fakulty vojenského leadershipu. (IROZHLAS, 2023)

Kybernetický útok na Ředitelství silnic a dálnic

Ředitelství silnic a dálnic se potýkalo s ransomwarovým útokem, který tento podnik dočasně úplně ochromilo. Škoda se dle Ministerstva dopravy vyšplhala ke 30 milionům korun. (TOP SECURITY, 2025)

3.2 Vybrané kybernetické bezpečnostní incidenty v zahraničí

Tato podkapitola se zaměřuje na vybrané kybernetické útoky v zahraničí, jejich průběh a důsledky.

Ransomwarový útok WannaCry

Ransomware se začal šířit v květnu roku 2017 a během krátké doby infikoval více než 300 000 počítačů po celém světě. Využíval exploit EternalBlue, který využil chyby ve Windows. V napadených počítačích zašifroval soubory a od obětí požadoval výkupné ve výši 300 až 600 dolarů, jinak budou soubory trvale odstraněny. WannaCry zasáhl více než 150 zemí a postihl velké množství institucí, například britský National Health Service, španělskou společnost Telefonica nebo společnost FedEx. (Codreanu, 2021) Mezi nejvíce zasažené země se řadí: Rusko, Ukrajina, Indie, Thajsko, Rumunko a Pákistán. (KŘOUSTEK, 2017)

Útok na Equifax

Americká úvěrová společnost Equifax v roce 2017 čelila velkému hackerskému útoku. Hackeři z jejích systémů získali osobní údaje 148 milionů lidí, včetně jmen, adres, čísel sociálního pojištění a další citlivé údaje. (KRČMÁŘ, 2018)

Útočníci využili zranitelnosti v softwaru Apache Struts, kterou společnost nepodchytila pravidelnými aktualizacemi. Hackeři získávali data po dobu několika měsíců. Společnost následně čelila několika žalobám za odcizení dat a pozdní oznámení. V roce 2020 byli obviněni z útoku čtyři členové čínské armády. (FRUHLINGER, 2020)

Ransomwarový útok Petya

Ransomware Petya se šíří od roku 2016 a infikuje počítače s operačním systémem Windows. Tento typ ransomwaru znemožní přístup k celému pevnému disku tím, že zašifruje hlavní

tabulku souborů, díky čemuž nelze Windows spustit a bylo vynuceno restartování. Posléze se na obrazovce objeví lebka se zprávou obsahující informaci, že soubory jsou šifrovány a pro jejich odblokování je třeba zaplatit výkupné v Bitcoinech. Petya zasáhl instituce po celém světě. Nejvíce zasáhl Ukrajinu, kde bylo napadeno kyjevské metro, letiště a národní banka. Zasáhl i několik nadnárodních společností jako je Nivea, Mondelez a další. (Avast, 2025a)

Kybernetický útok NotPetya

V roce 2017 zasáhl Evropu a USA rozsáhlý kybernetický útok zvaný jako NotPetya, který byl zaměřený na počítače se systémem Windows a využíval zranitelnosti v EternalRomance v zastaralém protokolu SMBv1. Šířil se pomocí souborů a e-mailů obsahujících škodlivé odkazy. Po otevření infikovaného souboru se virus dostal do systému, vyčkal přibližně hodinu a následně vynutil restart počítače. Po restartu se na obrazovce zobrazila výzva k zaplacení částky v Bitcoinech. Platba výkupného neměla žádný smysl, data byla nenávratně zničena. (Juodytè, 2023)

NotPetya byl původně považován za novou variantu ransomwaru Petya z roku 2016, nakonec se ale ukázalo, že jeho cílem nebylo vydírání obětí, ale trvalé poškození dat. Zatímco klasický ransomware soubory pouze zašifroval a po zaplacení výkupného umožní jejich obnovení, NotPetya data nenávratně ničí. Jednalo se tedy o wiper převlečený za ransomware. (Juodytè, 2023)

Útok způsobil škody zejména na Ukrajině, kde zasáhl letiště, energetické podniky a finanční instituce. Ukrajinské úřady spekulují o tom, že šlo o řízený útok zaměřený na kritickou infrastrukturu. (Juodytè, 2023)

Kybernetický útok na SolarWinds

V roce 2020 došlo k významnému kybernetickému útoku na společnost SolarWinds. Tento útok měl dalekosáhlé důsledky pro mnoho organizací po celém světě. Útočníci využili metodu zvanou supply chain attack, neboli útok na dodavatelský řetězec, při které vložili škodlivý kód do softwaru Orion od firmy SolarWinds. Tento škodlivý kód byl součástí aktualizací, které byly poskytovány zákazníkům. Po instalaci aktualizace útočníci získali přístup k interním systémům napadených organizací. Aktualizace si nainstalovalo více než 18 000 zákazníků. Software Orion je používám pro monitorování IT infrastruktury. Napadeny byl společnosti jako FireEye, Microsoft či Intel. Došlo také k napadení vládních úřadů a ministerstev. Účel útoku není znám, ale jedním z mnoha důvodů útoku mohl být

přístup k plánům připravovaných produktů nebo k citlivým údajům zaměstnanců či zákazníků. Odborníci na kybernetickou bezpečnost se domnívají, že útok na SolarWinds byl součástí ruské špionážní akce. Ruská vláda tuto informaci popřela. (OLADIMEJI a KERNER, 2023)

Kybernetický útok Stuxnet na Írán

Stuxnet je sofistikovaný počítačový červ, který byl navržen k útokům na průmyslové řídicí systémy SCADA (Supervisory Control and Data Acquisition) používané k monitorování a řízení průmyslových systémů. Díky této schopnosti může být využit k neoprávněnému sběru dat a sabotáži v elektrárnách, průmyslových podnicích, letištích a dalších kritických infrastrukturách. Stuxnet se stal prvním kybernetickým útokem, který vedl k fyzickému poškození kritické infrastruktury. (Popelová, 2016)

Během útoku na elektrárnu v Natanzu, který probíhal mezi lety 2009 až 2010, byl Stuxnet navržen tak, aby manipuloval s provozem centrifug, používaných k obohacení uranu. Jeho hlavním cílem bylo měnit rychlost otáček a regulovat tlak uvnitř centrifug, což postupně vedlo k jejich poškození a následnému vyřazení z provozu. Odhaduje se, že došlo k zničení zhruba 1000 centrifug a tím mělo dojít ke zpomalení vývoje íránského jaderného programu až o několik let. Ačkoliv dodnes není oficiálně potvrzeno, kdo Stuxnet vytvořil, stopy vedou k americké CIA a izraelskému Mosadu. (O2, 2024)

V roce 2024 nizozemský deník Volkskrant uvedl, že za útokem měl stát nizozemský inženýr, kterému se podařilo vniknout do přísně střeženého pozemního íránského jaderného zařízení v Natanzu a infikoval tamní interní systém škodlivým malwarem Stuxnet. (O2, 2024)

Kybernetický útok na slovenský katastr nemovitostí

V lednu 2025 došlo na Slovensku k rozsáhlému kybernetickému útoku, který ochromil katastr nemovitostí. Útočníci použili ransomware k zašifrování dat katastru nemovitostí a po vládě požadovali výkupné ve výši desítek milionů dolarů za odblokování dat. Katastr nemovitostí a informační systémy byly po několik dní vyřazeny z provozu. (Novinky, 2025)

Krvavý kybernetický útok

V září 2024 zasáhl Libanon rozsáhlý kybernetický útok během něhož explodovala komunikační zařízení, a to zejména pagery a mobilní telefony využívané členy hnutí Hizbaláh. Do pagerů byly umístěny malé nálože plastické trhaviny, které se následně dostaly k členům Hizballáhu prostřednictvím falešných e-shopů. Výbušniny byly aktivovány na

dálku pomocí zpráv, které simulovaly komunikaci od vedení Hizballáhu. Následkem výbuchu zemřelo několik lidí a stovky utrpěly zranění. Podle dostupných informací za útokem stála izraelská zpravodajská služba Mossad, která provedla pečlivě naplánovanou operaci. (Armádny magazín, 2025)

4 PROBLEMATIKA VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

Zvyšování povědomí o kybernetické a informační bezpečnosti hraje zásadní roli v ochraně dat a systémů před stále častějšími kybernetickými hrozbami. Nízké vzdělání v této oblasti může vést k vzniku bezpečnostních problémům jak u jednotlivců, tak ve firmách. Následující kapitola je věnována problematice vzdělávání v České republice. V kapitole budou popsány metody a formy vzdělávání veřejnosti, zaměstnanců a dětí ve školách.

4.1 Pojem, formy a metody vzdělávání

Vzdělávání je proces, během kterého si jedinec osvojí určité poznatky a činnosti, které posléze přeměňuje na znalosti dovednosti a návyky. (Theimerová, 2023)

Vzdělávání lze rozčlenit do základních kategorií:

- **Formální** – realizuje se ve vzdělávacích zařízeních a je regulováno legislativními předpisy. Má přesně stanovené cíle, strukturu výuky a metody hodnocení a zohledňuje požadavky společnosti. (Theimerová, 2023)
- **Neformální** – se odehrává mimo standardní vzdělávací instituce a zpravidla nevede k získání oficiálního osvědčení. Probíhá například na pracovišti. (Theimerová, 2023)

Formy a metody vzdělávání určují způsoby, jakými jsou znalosti a dovednosti předávány studentům. Forma vzdělávání je konkrétní způsob předávání informací. Metoda ve vzdělávání slouží jako nástroj k rozvoji znalostí pod vedením lektora. (Theimerová, 2023)

Přednáška – je založena na jednostranném výkladu a patří mezi nejrozšířenější formy vzdělávání. V této formě výuky má hlavní roli přednášející a posluchači pasivně přijímají obsah výkladu. (Theimerová, 2023)

Seminář – je forma vzdělávání, která kombinuje výklad s aktivní účastí posluchačů. Mezi hlavní výhody semináře patří aktivní zapojení studentů a lepší pochopení probírané problematiky. (Theimerová, 2023)

E-learning – je v současnosti jednou z nejrozšířenějších metod vzdělávání, která probíhá prostřednictvím výpočetní techniky. Mezi hlavní výhody této metody řadíme cenovou dostupnost, flexibilitu a proškolení velkého množství účastníků bez nutnosti jejich přítomnosti. (Theimerová, 2023)

Workshop – krátkodobá vzdělávací metoda zaměřená na sdílení praktických zkušeností a aktivní spolupráci účastníků. Na rozdíl od tradičních přednášek nebo seminářů se zaměřuje na řešení konkrétních problémů, diskuzi a rozvoj dovedností prostřednictvím praktických úkolů. (Theimerová, 2023)

4.2 Vzdělávací akce pro veřejnost

Vzhledem k rostoucím kybernetickým hrozbám je důležité, aby se široká veřejnost v tomto směru pravidelně vzdělávala. Vzdělávací programy pro veřejnost pomáhají zvyšovat povědomí o bezpečném chování v online prostředí a tím pomáhají minimalizovat hrozbu kybernetických útoků. Útoky se nevztahují pouze na organizace spravující rozsáhlé databáze, ale mohou postihnout každého uživatele, který je připojen k síti. Každý uživatel by měl mít povědomí o bezpečnostních rizicích, jejich důsledcích a zejména způsobech, jak hrozbám předcházet. (Senanayake a Fernando, 2018)

V České republice existuje řada institucí a projektů, které poskytují školení, semináře, online kurzy a workshopy zaměřené na ochranu osobních údajů a bezpečné používání internetu. Osvětové kampaně přispívají k informovanosti veřejnosti o kybernetických hrozbách a poskytují rady pro bezpečné chování v digitálním prostředí. Kampaně by měly poskytovat praktické rady, jak se proti hrozbám aktivně bránit a chránit. Jejich cílem je zvyšovat povědomí lidí o rizicích a pomáhat jim lépe rozpoznávat potenciální nebezpečí. V České republice se na organizaci osvětových kampaní podílí řada subjektů, ať už neziskové organizace, soukromé společnosti nebo státní organizace.

V České republice probíhá hned několik kampaní zaměřených na zvyšování povědomí o kybernetické bezpečnosti. Mezi nejvýznamnější řadíme:

- **#KYBERŠTÍT** – osvětová kampaň, která byla spuštěna v roce 2022 pod záštitou NÚKIB, jejímž úkolem je informovat veřejnost o kybernetických hrozbách, jejich následcích a dále má za úkol veřejnosti ukázat, jak se hrozbám bránit a jak na ně reagovat. Kampaň se zabývá aktuálními tématy jako jsou škodlivé e-maily, nastavení hesel v zařízeních, zabezpečení mobilních zařízení aj. (NÚKIB, 2022b)
- **#nePINDEJ** – celonárodní vzdělávací kampaň, která se soustředí na edukaci uživatelů v oblasti kybernetických hrozeb, zejména rozpoznávání podvodných webových stránek a pokusů o získání citlivých údajů. (Pidrmnaová, 2022)

Kampaň je cílena na širokou veřejnost. Hlavní součástí kampaně je edukační www.kybertest.cz, který má za cíl informovat veřejnost o nejčastějších typech podvodů a naučit ji, jak je včas rozpoznat. Projekt je realizován pod záštitou České bankovní asociace. Do projektu se dále zapojila Policie České republiky, NÚKIB, Česká spořitelna, O2, ČEZ, České dráhy a další. (NÚKIB, 2023)

- **Týden pro digitální Česko** – projekt během kterého se v roce 2024 konaly osvětové akce zaměřené na kybernetickou bezpečnost. Centrum kybernetické bezpečnosti připravilo širokou škálu akcí, které se konají jak online, tak prezenčně, jejichž cílem je zvýšit povědomí o hrozbách na internetu. Jedná se o akci pořádanou Úřadem vlády ČR. (Centrum kybernetické bezpečnosti, 2025)
- **Kyberpohádky** – vzdělávací a osvětový projekt zaměřený na kybernetickou bezpečnost určený pro děti, mládež a učitele. Kyberpohádky využívají pohádkové příběhy k tomu, aby zábavnou formou upozornily na hrozby a rizika v online světě. Cílem pohádek je děti naučit se bezpečně orientovat v kyberprostoru. Tento projekt ve velkém využívají učitelé jako pomůcku k výuce. Kyberpohádky jsou dostupné nejen v online vydání, ale také v knižní podobě. V roce 2023 proběhla premiéra divadelního představení s tematikou kyberpohádek. Od této doby se divadelní představení v Žižkovském divadle v Praze koná pravidelně. Kyberpohádky v roce 2023 získaly mnoho národních i mezinárodních ocenění. Staly se vítězem European Cyber Security Month Awards 2023 nebo získaly ocenění IDEA AFCEA International. Partnerny projektu je NÚKIB a Vodafone. V říjnu 2024 byly oficiálně zveřejněny na portálu NÚKIB Kyberpohádky 2. (Centrum kybernetické bezpečnosti, © 2025)

Pro zajištění bezpečného pohybu v kybernetickém prostředí je důležité investovat do vzdělání a prevence.

4.3 Vzdělávání zaměstnanců

Pravidelné vzdělávání zaměstnanců pomáhá minimalizovat chyby, zvyšuje odbornost pracovníků a bezpečnost práce. Existuje mnoho metod vzdělávání, přičemž každá organizace si volí metody, které nejlépe vyhovují jejich potřebám. Efektivita vzdělávání závisí na povaze práce či podmínkách na pracovišti. Mezi základní způsoby vzdělávání

radíme samostudium, e-learning, interní školení a externě poskytované školení. Samostudium a e-learning patří mezi velmi efektivní a často používané metody s velkým přínosem pro rozvoj zaměstnanců. Další hojně využívanou metodou je školení vedené kvalifikovaným instruktorem. (Aptien, 2025)

Vzdělávání zaměstnanců v oblasti kybernetické a informační bezpečnosti je důležitým prvkem ochrany organizací před rostoucími kybernetickými hrozbami. Podle Světového ekonomického fóra se počet útoků na podniky za posledních 5 let zdvojnásobil, což zdůrazňuje potřebu zvýšení bezpečnostních opatření. Pro zlepšení ochrany organizací je důležité investovat do školení a neustálého vzdělávání zaměstnanců. Zaměstnanci jsou často hlavním cílem phishingových útoků, ransomwaru a malwaru. Tyto útoky se šíří zejména komunikačními kanály a jejich cílem je zaměstnance přimět k instalaci škodlivého systému nebo ke sdělení citlivých údajů. Útočníci se čím dál častěji zaměřují na zaměstnance, protože pro útočníky představují snadnější způsob, jak se nabourat do systému. Více než 90 % úspěšných útoků vzniká v důsledku neúmyslného sdělení informací ze strany zaměstnanců. (Noonan, 2024)

V České republice je hned několik organizací, které se zabývají vzděláváním v oblasti kybernetické a informační bezpečnosti. Jednou z nich je NÚKIB, který nabízí prezenční školení a semináře pro zaměstnance, preventisty a státní správu. NÚKIB připravil například e-learningový kurz Dávej v kyber!, který je určen pro zaměstnance státní správy nebo kurz Šéfuj v kyber!, který je vhodný pro manažery. (NÚKIB, 2025g)

Další organizací poskytující vzdělávání nejen zaměstnanců je CyberSecurityHub, která nabízí vzdělávání jak pro malé a střední podniky, tak i pro veřejné organizace. Veškeré vzdělávací kurzy jsou zdarma. (CyberSecurityHub, 2025)

Jednou z mnoha organizací poskytujících školení je i organizace Cybersec, která poskytuje e-learningové kurzy pro zaměstnance, které obsahují 6 témat ze všech částí kybernetické bezpečnosti. Každé téma obsahuje praktické příklady a zahrnuje závěrečný test.

(Cybersec, 2025)

S rostoucím počtem hrozeb narůstá i potřeba vzdělávání zaměstnanců. Na tuto situaci reaguje stále více organizací, které nabízejí kurzy zaměřené na tuto problematiku.

4.4 Vzdělávání ve školách

Kybernetická bezpečnost se stává nedílnou součástí vzdělávacího systému, neboť digitalizace zasahuje víc a víc do všech oblastí našeho života, včetně školního prostředí. Zmiňovaná problematika se ve školním systému prolíná různými předměty, jako jsou informatika, občanská výchova a další. Vzdělávání v této oblasti napomáhá žákům nejen bezpečně se pohybovat v online světě, ale také přispívá k prevenci kybernetických hrozeb a ochraně citlivých údajů.

Výuka na základních školách probíhá podle Rámcového vzdělávacího programu (dále jen „RVP“), jenž je vydáván Ministerstvem školství, mládeže a tělovýchovy. Dle aktuálního RVP, který byl aktualizován s účinností od 1.9.2023 se předmět informatika vyučuje od čtvrté až do deváté třídy. Žáci na prvním stupni si utváří základní představy o metodách zaznamenávání informací formou her, diskusí a experimentů. Základy bezpečného chování v digitálním prostředí jsou součástí učiva. Dle RVP se probírají témata týkající se pravidel bezpečné práce s digitálním zařízením, správa uživatelských účtů a hesel. Na druhém stupni jsou znalosti prohlubovány, žáci tvoří, navrhuji a rozvíjejí porozumění zásadám fungování digitálních technologií. Učivo se dle RVP věnuje tématu: *„bezpečnost – útoky – cíle a metody útočníků, nebezpečné aplikace a systémy; zabezpečení digitálních zařízení a dat – aktualizace, antivir, firewall, bezpečná práce s hesly a správce hesel, dvou faktorová autentizace, šifrování dat a komunikace, zálohování a archivace dat“*. (MŠMT, 2023)

Střední školy nabízejí mnohem větší možnosti pro začlenění výuky kybernetické bezpečnosti. Studenti mají již základní znalosti v tomto odvětví, tak jim mohou být rozšiřovány znalosti obtížnějšími tématy, jako je sexting nebo závislosti. Na středních školách NÚKIB vytvořil kolekci vzdělávacích materiálů pro učitele středních škol, které jsou vhodné jak pro studenty gymnázií se všeobecným zaměřením, tak i pro studenty informačních technologií. (NÚKIB, 2025h)

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část bakalářské práce se zaměřuje na představení vybraných legislativních dokumentů, které definují právní rámec kybernetické a informační bezpečnosti. Dále jsou v práci představeny hlavní organizace zabývající se kybernetickou bezpečností v České republice. Základní terminologie poskytuje potřebný základ k porozumění odborným pojmům, jako jsou kybernetické útoky, phishing, malware či ransomware.

V teoretické části bakalářské práce jsou také popsány významné jak národní, tak světové bezpečnostní incidenty. Tato kapitola nám ukázala, že kybernetické útoky jsou stále sofistikovanější a cílí nejen na jednotlivce, ale i na soukromé organizace, státní instituce a kritickou infrastrukturu. Tyto události zdůrazňují potřebu zdokonalování bezpečnostních opatření.

Poslední kapitola se zaměřuje na problematiku vzdělávání. Vzdělávání v této oblasti je stále důležitější, protože vývoj moderních technologií se vyvíjí velmi rychle. Spolu s tím narůstají i rizika spojená s hrozbami, které se dotýkají nejen jednotlivců, ale i organizací a kritické infrastruktury. Z výše uvedeného důvodu je důležité klást důraz na rozšiřování znalostí napříč celou společností.

Tato teoretická část vytvořila základ pro praktickou část práce, která se zaměří na analýzu vybraných kurzů kybernetické a informační bezpečnosti a na návrh zvýšení úrovně vzdělávání v České republice.

II. PRAKTICKÁ ČÁST

6 VZDĚLÁVACÍ KURZY V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE

Vzdělávání v kybernetické a informační bezpečnosti je neustále se vyvíjejícím procesem, který musí reagovat nejen na technologický pokrok, ale i na individuální potřeby jednotlivců a organizací. Při nastavování efektivních vzdělávacích programů je nutné zohlednit řadu faktorů, jako je věk, profesní zaměření, úroveň předchozích znalostí, časové možnosti nebo osobní motivace. Každá profesní skupina čelí jiným rizikům, a proto nelze ke školení přistupovat univerzálně. Obsah a forma vzdělávání by měly být přizpůsobeny konkrétní cílové skupině.

Kybernetické hrozby se neustále vyvíjejí, a proto je důležité, aby se vzdělávání přizpůsobovalo dnešním hrozbám a zůstalo tak aktuální. Klasická školení v podobě přednášek se čím dál častěji doplňují moderními formami výuky. Stále větší roli hrají e-learningové kurzy, praktické workshopy nebo různé simulace kybernetických útoků, které jsou pro zaměstnance velmi přínosné a pomáhají jim snadněji pochopit hrozby a naučit je na ně lépe reagovat.

V kapitole budou stručně představeny vybrané kurzy v oblasti kybernetické a informační bezpečnosti v České republice.

6.1 Charakteristika vybraných kurzů kybernetické a informační bezpečnosti v České republice

V této kapitole budou představeny vybrané kurzy, které jsou v ČR dostupné, přičemž se nejedná o kompletní přehled všech možností na trhu.

6.1.1 Placené kurzy

V této kapitole budou stručně představeny vybrané placené kurzy dostupné v ČR. Kurzy byly vybrány dle tematického zařazení, cílové skupiny a ceny. Tento přehled zahrnuje pouze vybrané placené kurzy relevantní pro účely bakalářské práce a nepokrývá veškeré dostupné možnosti na trhu.

Společnost ESET

Společnost ESET nabízí ucelené vzdělávací programy zaměřené na kybernetickou a informační bezpečnost, které je možné upravit dle požadavků jednotlivých organizací. Hlavním cílem těchto školení je posílit znalosti o možných bezpečnostních hrozbách a naučit

účastníky pracovat s citlivými informacemi. Školení se zaměřuje na vnitřní bezpečnostní hrozby, zabezpečení účtů silnými hesly, ochranu pošty a na odolnost vůči personalizovaným útokům. Společnost školení provádí pomocí e-learningových kurzů v délce 60–90 minut. Účastníci mají k dispozici video lekce a cvičení, na které navazuje závěrečný test. Osobě pověřené organizací jsou zasílány pravidelné přehledy o stavu proškolení zaměstnanců.

Školení lze také upravit dle specifických potřeb organizace, například začleněním interních směrnic a předpisů a je možné je připravit tak, aby šlo bez problémů začlenit do interního vzdělávacího systému. (ESET, © 1992 – 2025)

Školení BOZP.cz

Společnost BOZP.cz poskytuje online školení, které je zaměřeno na kybernetickou a informační bezpečnost a je určeno všem, kteří pracují s digitálními technologiemi, jako jsou počítače, mobilní zařízení a další. Hlavním cílem školení je zvýšit informovanost zaměstnanců o bezpečnostních rizicích a naučit je zásadám správného chování v kybernetickém prostoru. (BOZP, © 2025a)

Společnost kurzy nabízí formou výhodných balíčků obsahujících více kurzů z různých odvětví, kde cena se odvíjí od počtu školených osob. (BOZP, © 2025b)

Nezisková organizace Czechitas

Nezisková organizace Czechitas se zaměřuje na vzdělávání žen, dětí a mládeže v oblasti informačních technologií. Czechitas má ve svojí nabídce online kurz Úvod do kybernetické bezpečnosti, který je určen pro úplné začátečníky v rozsahu 7 hodin. Kurz je zaměřen na úplné základy, seznámení s pojmy kybernetická bezpečnost, zákony a normy a dále s příklady kybernetických hrozeb. Dále je možné absolvovat rozšiřující kurzy. (Czechitas, © 2016-2025a)

Organizace také nabízí půldenní či jednodenní vzdělávání zaměstnanců, které probíhá formou přednášek. (Czechitas, © 2016-2025b)

Společnost CYBERSEC

Společnost CYBERSEC má ve svojí nabídce e-learningový kurz, který je vhodný pro široké spektrum uživatelů a obsahuje komplexní základy bezpečnosti. Kurz se zabývá šesti tématy a to e-mailem a jeho používáním, zabezpečením počítače, bezpečným připojením, internetovými prohlížeči, zálohováním dat a právními důsledky. Kurz je zcela hrazený účastníky. (CYBERSEC, 2025)

Platforma KYBEZ

Platforma KYBEZ poskytuje vzdělávací kurzy zaměřené na kybernetickou bezpečnost. V nabídce je kurz Základy kybernetické bezpečnosti organizace, který se věnuje základním pojmům, právnímu rámci, kybernetickým útokům a ochranou před nimi. Tento kurz poskytne základní znalosti v této problematice. (KYBEZ, 2021a)

Platforma KYBEZ nabízí také workshop Řízení kybernetické a informační bezpečnosti, který poskytne zájemcům vzdělání v oblasti právního rámce, informace, jak evidovat hrozby, zranitelnost a opatření. Dále účastníci získají informace o správné reakci na bezpečnostní události a způsoby ochrany organizace. (KYBEZ, 2021b)

Společnost Blue Partners

Společnost Blue Partners nabízí Školení kybernetické bezpečnosti, které je navrženo tak, aby zvýšilo povědomí zaměstnanců o bezpečnostních hrozbách a naučilo je hrozbám předcházet. Kurz obsahuje 16 kapitol a 38 článků založených na reálných případech. Školení probíhá metodou chytrého vzdělávání, součástí jsou i kvízy. Školení je možné absolvovat prostřednictvím e-learningu systému společnosti nebo také přes platformu MS Teams nebo přímo ve firmě. Školení přináší pro organizace snížení ztráty informací, zvýšení znalostí o kybernetické bezpečnosti mezi zaměstnanci a další. (Blue Partners, 2024)

Společnost Seduo

Společnost Seduo nabízí tři kurzy zaměřené na vzdělávání v kybernetickém prostoru. Prvním a zároveň nejprodávanějším kurzem je kurz Digitální bezpečnost: naučte se chodit v online světě, který vede poradce pro digitální bezpečnost Karol Suchánek. Kurz je určen pro každého uživatele počítače nebo smartphonu. Zaměřuje se na prevenci hackerských útoků, bezpečné chování v online prostředí a ukazuje, jak předcházet nejčastějším chybám, které útočníci zneužívají. (Seduo, 2025a)

Druhým nabízeným kurzem je kurz Bezpečně v online světě: jak ochránit své peníze, data a identitu, který se zaměřuje na ochranu osobních údajů a cenných informací. Dále na to, jak bezpečně nakupovat na internetu a jak rozpoznat podvodné reklamy, weby a jak se na internetu pohybovat. Kurz je určen pro běžné uživatele využívající internet. (Seduo, 2025b)

Dále společnost nabízí webinář Připravte firmu na nové kybernetické výzvy, který se zaměřuje na regulaci NIS2 a jeho úkolem je provést účastníky celým procesem přípravy na NIS2. (Seduo, 2025c)

Společnost Pumpedu

Společnost Pumpedu má ve své nabídce plně hrazený kurz Kybernetické bezpečnosti, který probíhá buď to online ve virtuální učebně, kde je lektor připojen vzdáleně, anebo prezenčně v Praze. Kurz je vhodný pro zaměstnance, kteří pracují s informacemi společnosti a osobními údaji, ale také je vhodný pro běžné uživatele. Kurz je zaměřen na zvyšování povědomí v oblasti kybernetické a informační bezpečnosti. Kurz obsahuje názorné ukázky hrozeb, reálné praktiky útočníků a také se zabývá preventivními opatřeními. (Pumpedu, © 2025)

Společnost GORDIC

Společnost GORDIC zařadila do své nabídky také školení kybernetické bezpečnosti a GDPR, které je zaměřeno na seznámení se se základy kybernetické bezpečnosti, porozumění nejnovějším trendům v dané oblasti a příklady řešení kybernetických hrozeb. Školení lze přizpůsobit požadavkům dané organizace. (GORDIC, 2023)

6.1.2 Neplacené kurzy

V této kapitole budou stručně představeny vybrané neplacené kurzy dostupné v ČR. Tento přehled zahrnuje pouze vybrané neplacené kurzy relevantní pro účely bakalářské práce a nepokrývá veškeré dostupné možnosti na trhu.

Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost se věnuje nejen metodické podpoře, ale také vzdělávání veřejnosti, firem a institucí v oblasti kybernetické a informační bezpečnosti. NÚKIB provozuje vzdělávací portál, kde nabízí e-learningové kurzy zaměřené na různé úrovně znalostí a potřeby uživatelů zdarma. Kurzy se dělí na volně dostupné a ty, které vyžadují registraci. Kurzy jsou zakončeny závěrečným testem. Kurzy jsou vhodné nejen pro odborníky, ale také pro státní zaměstnance a veřejnost. (NÚKIB, 2025i)

NÚKIB má v nabídce několik kurzů, kde jedním z nejznámějších je kurz „Dávej kyber!“, který obsahuje osm okruhů, které účastníky seznamují s oblastmi kybernetické bezpečnosti, včetně bezpečného přihlašování, ochrany zařízení a důvěryhodné komunikace. Dále se věnují rizikům škodlivých souborů, ochraně soukromí a zabezpečení zařízení. Kurz je

volně dostupný a je zakončen testem, po jehož splnění účastníci získají certifikát platný dva roky. (NÚKIB, 2022c)

Pro zaměstnance škol byl připraven přímo na míru kurz „Dávej kyber pro učitele“. Kurz se zaměřuje na zásadní aspekty kybernetické bezpečnosti ve školním prostředí, včetně tvorby silných hesel, ochrany školních účtů a různým formám kybernetických útoků. Součástí kurzu je také téma digitální identity učitele a problematika kyberšikany, které mohou pedagogové čelit. (NÚKIB, 2025j)

Mezi další kurzy, které NÚKIB nabízí, řadíme kurzy, které jsou vhodné pro zaměstnance zdravotnictví. Jedná se konkrétně o Minimum kybernetické bezpečnosti pro zdravotnictví 25 a Základy kybernetické bezpečnosti pro zdravotnictví 25. Tyto kurzy jsou přístupné po přihlášení. (NÚKIB, 2025i)

Velmi známý je také kurz pro manažery kybernetické bezpečnosti „Šéfuj kyber!“. Plná verze je dostupná po registraci a zaměřuje se na systém řízení bezpečnosti informací a organizační bezpečnost. (NÚKIB, 2025k)

Mnoho dalších kurzů je uvedeno na vzdělávacím portálu „osveta.nukib.gov.cz“. (NÚKIB, 2025i)

Organizace CyberSecurityHub

Organizace CyberSecurityHub nabízí širokou škálu online kurzů zaměřených na kybernetickou bezpečnost. Jedním z nabízených kurzů je Úvod do kybernetické bezpečnosti nebo třeba Minikurz základů kyberbezpečnosti. Kurzy jsou určeny především pro malé a střední podniky a státní správu. Cílem školení je seznámit účastníky s hrozbami a možnostmi obrany proti kybernetickým útokům. Dále seznámit účastníky, jak správně zabezpečit počítače a jak chránit citlivé informace před jejich ztrátou. (CyberSecurityHub, © 2025a)

Díky podpoře z programů Evropské unie a Národního plánu obnovy jsou tyto kurzy dostupné zcela zdarma. (CyberSecurityHub, © 2025b)

Kurz Bud' safe online

Bud' safe online je interaktivní kurz, který byl vytvořený ve spolupráci influence Jiřího Krále, expertů z firmy Avast a projektu E-bezpečí. Cílem kurzu je naučit děti a dospívající, jak se bezpečně chovat v online prostředí. Kurz mohou učitelé snadno začlenit i do výuky. (Avast, 2025b)

6.2 Analýza vybraných kurzů kybernetické a informační bezpečnosti v České republice

Následující kapitola se zabývá analýzou vybraných kurzů kybernetické a informační bezpečnosti v České republice. Tato analýza se zaměřuje na srovnání pěti vybraných kurzů pomocí vícekritériálního rozhodování konkrétně bodovací metody. Tato metoda poskytne strukturovaný a přehledný způsob vyhodnocení jednotlivých vzdělávacích kurzů. Posouzení provedl hodnotitelský tým. Každý kurz byl hodnocen podle tří klíčových kritérií s přidělenou váhou a využitím bodové škály 1-5.

Na základě diskuse se specialistou na kybernetickou bezpečnost, který nesouhlasil se zveřejněním osobních údajů, proběhl výběr pěti kurzů kybernetické a informační bezpečnosti určených k analýze. Výběr proběhl na základě dostupných informací a recenzí účastníků kurzů. Seznam vybraných kurzů je uveden níže v tabulce.

Tabulka 1 - Seznam vybraných kurzů (vlastní zpracování)

Název kurzu	Společnost
Školení kybernetické a informační bezpečnosti	BOZP.cz
Základy kybernetické bezpečnosti 25	NÚKIB
Školení IT bezpečnosti pro zaměstnance	OKškolení
Úvod do kybernetické bezpečnosti	CZECHITAS
Školení kybernetické bezpečnosti	CYBERSEC

K tomu, aby mohly být vybrané kurzy posouzeny, byl sestaven tříčlenný hodnotitelský tým. Účastníkem hodnotitelského týmu je specialista na kybernetickou bezpečnost, který nesouhlasil s uvedením jména. Dalším členem hodnotitelského týmu je sama autorka práce. Posledním účastníkem je Emil. D., který působí v HZS ČR. Níže uvedená tabulka zachycuje složení hodnotitelského týmu.

Tabulka 2 - Složení hodnotitelského týmu (zpracování vlastní)

Hodnotitel č.	Jméno a příjmení	Pracovní pozice
H 1	Hodnotitel 1	Specialista na kybernetickou bezpečnost
H 2	Kristýna Brůžová	Autorka práce, studentka oboru Ochrany obyvatelstva
H 3	Hodnotitel 2	Respondent z řad HZS ČR

Pro účely objektivního posouzení jednotlivých kurzů byla stanovena tři hodnotící kritéria, která reflektují zásadní parametry z hlediska kvality a vzdělávání a jeho přínosu pro účastníky kurzu.

Největší váha (50 %) byla přidělena kritériu obsahu kurzu, které představuje maximalizační kritérium – parametr, jehož hodnota by měla být co nejvyšší, aby kurz dosáhl lepšího hodnocení. Druhým maximalizačním kritériem je praktický přínos (30 %), který vyjadřuje míru, do jaké lze získané znalosti uplatnit jak v profesním, tak osobním životě. Třetím zvoleným kritériem je cena (20 %), která představuje minimalizační kritérium – tedy takové, u kterého je nižší hodnota (nižší cena) považována za výhodnější. Proto byla cena převedena do bodové škály tak, aby nižší částka odpovídala vyššímu počtu bodů a bylo možné ji spravedlivě zahrnout do celkového hodnocení. Níže v tabulce jsou uvedena hodnotící kritéria a jejich váhy.

Tabulka 3 - Vybraná hodnotící kritéria (vlastní zpracování)

Kritérium	Váha (%)	Typ kritéria
Obsah kurzu	50 %	Maximalizační kritérium
Praktický přínos	30 %	Maximalizační kritérium
Cena	20 %	Minimalizační kritérium

První hodnocené kritérium je obsah kurzu, které bylo stanoveno jako maximalizační kritérium, tedy takové, u něhož vyšší hodnocení znamená lepší výsledek. Byla mu přiřazena

nejvyšší váha ze všech sledovaných kritérií a to konkrétně 50 %. Hodnotitelé přiřazovali hodnocení na škále 1-5, kde 1 představuje velmi slabou kvalitu. Zatímco 5 značí výbornou kvalitu kurzu. Hodnotící škála je uvedena v tabulce níže.

Tabulka 4 - Maximalizační kritérium kvalita a obsah (vlastní zpracování)

Maximalizační kritérium – obsah	
Stupeň hodnocení	Popis
1	Velmi nízká kvalita
2	Nízká kvalita
3	Průměrná kvalita
4	Dobrá kvalita
5	Výborná kvalita

Druhým hodnoceným kritériem je praktický přínos, který byl stanoven jako maximalizační kritérium s váhou 30 % v celkovém hodnocení. Toto kritérium udává, do jaké míry jsou získané znalosti využitelné v jak v pracovním, tak osobním životě. Hodnotitelé přiřazovali hodnocení na škále 1-5, kde 1 představuje nulovou využitelnost. Zatímco 5 značí výbornou využitelnost. Hodnotící škála je uvedena v tabulce níže.

Tabulka 5 - Maximalizační kritérium praktický přínos (vlastní zpracování)

Maximalizační kritérium – praktický přínos	
Stupeň hodnocení	Popis
1	Nulový přínos
2	Minimální přínos
3	Průměrný přínos
4	Dobrý přínos
5	Výborný přínos

Posledním hodnotícím kritériem je cena, která byla stanovena jako minimalizační kritérium s váhou 20 % v celkovém hodnocení. Na rozdíl od ostatních dvou kritérií, kde vyšší hodnota znamená lepší výsledek, je to u ceny naopak, tzn. nižší cena kurzu je považována za výhodnější, a tedy lepší z pohledu hodnocení. Hodnotící škála je uvedena v tabulce níže.

Tabulka 6 - Minimalizační kritérium cena (vlastní zpracování)

Minimalizační kritérium – cena	
Stupeň hodnocení	Popis
1	Velmi drahý (od 1500 Kč/osoba)
2	Dražší (1000-1500 Kč/osoba)
3	Přiměřená (500-1000 Kč/osoba)
4	Výhodná (do 500 Kč/osoba)
5	Velmi výhodná/zdarma

Tabulka č. 7 poskytuje souhrn cen jednotlivých kurzů, které byly zahrnuty do provedené analýzy.

Tabulka 7 - Ceny vybraných kurzů (vlastní zpracování)

Kurzy			Cena
K1	Školení kybernetické a informační bezpečnosti	BOZP.cz	240 Kč/osoba
K2	Základy kybernetické bezpečnosti 25	NÚKIB	Zdarma
K3	Školení IT bezpečnosti pro zaměstnance	OKškolení	975 Kč/osoba
K4	Úvod do kybernetické bezpečnosti	CZECHITAS	3190 Kč/osoba
K5	Školení kybernetické bezpečnosti	CYBERCSEC	180 Kč/osoba

Po seznámení členů hodnotitelského týmu s jednotlivými kurzy, jejich cenou, obsahem, ukázkami a recenzemi, přidělil každý hodnotitel bodové hodnocení sledovaným kritériím.

Tabulka 8 - Hodnocení vybraných kurzů (vlastní zpracování)

Kurz	Obsah			Přínos			Cena		
	H 1	H 2	H 3	H 1	H 2	H 3	H 1	H 2	H 3
K1: Školení kybernetické a informační bezpečnosti	4	5	4	5	4	4	4	4	4
K2: Základy kybernetické bezpečnosti 25	5	5	5	4	5	5	5	5	5
K3: Školení IT bezpečnosti pro zaměstnance	3	4	4	3	4	3	3	3	3
K4: Úvod do kybernetické bezpečnosti	2	2	3	2	2	2	1	1	1
K5: Školení kybernetické bezpečnosti	4	4	4	4	4	3	4	4	4

Nyní pro každý kurz a každé kritérium bylo vypočítáno průměrné hodnocení od všech tří hodnotitelů, které je znázorněno v tabulce níže.

Tabulka 9 - Průměrné hodnocení vybraných kurzů (vlastní zpracování)

Kurz		Průměrný obsah	Průměrný praktický přínos	Průměrná cena
K1	Školení kybernetické a informační bezpečnosti	4,3	4,3	4
K2	Základy kybernetické bezpečnosti 25	5	4,7	5
K3	Školení IT bezpečnosti pro zaměstnance	3,4	3,3	3
K4	Úvod do kybernetické bezpečnosti	2,3	2	1
K5	Školení kybernetické bezpečnosti	4	3,4	4

Nyní bylo vypočítáno vážené skóre pro každý kurz. Vážené skóre bylo vypočítáno pomocí vzorce:

$$\text{Vážené skóre} = (\text{Obsah} \times 0,5) + (\text{Praktický přínos} \times 0,3) + (\text{Cena} \times 0,2)$$

Hodnoty byly zapsány do tabulky níže, kde v posledním sloupci bylo dle výsledků určeno výsledné pořadí kurzů.

Tabulka 10 - Vážené skóre a výsledné pořadí kurzů (vlastní zpracování)

Kurz		Vážené skóre	Výsledné pořadí
K1	Školení kybernetické a informační bezpečnosti	4,24	2.
K2	Základy kybernetické bezpečnosti 25	4,56	1.
K3	Školení IT bezpečnosti pro zaměstnance	3,29	4.
K4	Úvod do kybernetické bezpečnosti	1,95	5.
K5	Školení kybernetické bezpečnosti	3,76	3.

Na základě bodovací metody vypracované hodnotitelským týmem se na první příčce umístil kurz **Základy kybernetické bezpečnosti 25**, který je pod záštitou NÚKIB. Kurz se zabývá osmi základními okruhy, mezi které patří například správa hesel a přihlašování, způsoby odemykání zařízení, metody sociální inženýrství, škodlivé zařízení a ochrana zařízení. Kurz je zaměřený na celkové zvýšení povědomí o kybernetické bezpečnosti mezi širokou veřejností. Kurz je vhodný jak pro zaměstnance státní správy, tak i pro zaměstnance soukromého sektoru a i pro širokou veřejnost. Tento online kurz je zcela bezplatný a umožňuje jeho absolvování odkudkoliv a kdykoliv. Kurz je navržen tak, aby byl přehledný a klade důraz na praktické využití získaných znalostí. Po absolvování kurzu mohou účastníci po registraci do vzdělávacího portálu získat certifikát, který dokládá jejich základní orientaci v problematice. Závěrečný test obsahuje 15 otázek a každý účastník má možnost využít tři pokusy k úspěšnému absolvování. (NÚKIB, 2025l)

Na druhém místě se umístil kurz **Školení kybernetické a informační bezpečnosti** od společnosti BOZP.cz. Tento kurz je zaměřen na zvyšování povědomí zaměstnanců o rizicích spojených s využíváním informačních technologií a na předcházení

bezpečnostním incidentům způsobených lidskou chybou. Dle hodnocení hodnotitelů kurz dosáhl dobrých výsledků, a to jak po stránce odborného obsahu, tak po stránce praktického využití s průměrným hodnocením 4,3, což vypovídá o jeho kvalitě a přínosu pro účastníky. Po stránce ceny spadá kurz do kategorie výhodná cena. Kurz je zakončen certifikátem a doporučuje se jej opakovat každý rok. (BOZP, © 2025a)

Na třetím místě se umístil kurz **Školení kybernetické bezpečnosti** od společnosti CYBERSEC. Jedná se online kurz, který je zaměřený na zabezpečení počítače, běžné chování v digitálním prostředí, na ochranu dat a zásady GDPR a další. Dle hodnotitelů kurz dosáhl průměrných výsledků. Po stránce kvality obsahu dosáhl dobrého průměrného výsledku, zatímco po stránce praktického přínosu to bylo o něco málo horší, tam se výsledky spíše schylovaly k průměrnému hodnocení. Po cenové stránce kurz spadá do kategorie výhodná cena. Při zakoupení jedné až padesáti licencí je cena za jednoho uživatele 180 Kč. Kurz je zakončen závěrečným testem, za jehož úspěšné splnění, a to minimálně 70 % správných odpovědí, účastník získá certifikát. Výhodou kurzu je časová flexibilita. Kurz je vhodný jak pro firmy, tak i pro jednotlivce, kteří si chtějí zvyšovat povědomí o kybernetické bezpečnosti. (CYBERSEC, 2025)

Díky bodovací metodě jsme dospěli k závěru, že na prvním místě se umístil kurz poskytovaný společností NÚKIB. Tato metoda byla zvolena kvůli svojí snadné použitelnosti a přehlednosti. Díky této metodě je možné systematicky porovnat dostupné kurzy a vybrat kurz, který nejlépe odpovídá zadaným kritériím.

7 STRUKTUROVANÉ ROZHOVORY

Pro realizace výzkumného šetření byla zvolena kvalitativní výzkumná metoda. K získání potřebných dat byly využity polostrukturované rozhovory s vybranými zaměstnanci státního a soukromého sektoru.

Kvalitativní výzkum se zaměřuje na hlubší porozumění zkoumaného problému. Jedná se o široký pojem, který zahrnuje různé přístupy k analýze. Kvalitativní výzkum je proces zkoumání lidských a sociálních jevů, různé metodologické tradice. Jeho hlavním cílem je nejen sběr dat, ale také jejich interpretace a pochopení souvislostí, které nelze kvantifikovat. Nejčastější metodou sběru dat v kvalitativním výzkumu jsou rozhovory. (Hendl, 2016)

Polostrukturované rozhovory jsou jednou z metod kvalitativního výzkumu, která je kombinací prvků strukturovaných a nestrukturovaných rozhovorů. Často bývá označován jako částečně řízený rozhovor. Tazatel si předem připravuje sadu otázek či tematických okruhů, kterým se chce věnovat, přičemž jejich pořadí není stanoveno. Důležité je, aby byla probrána všechna důležitá a potřebná témata. (Mindthegraph, 2023)

7.1 Cíl práce a výzkumné otázky

Výzkumné šetření bylo realizováno s cílem získat podrobnější informace o vzdělávání zaměstnanců ve státním a soukromém sektoru. Hlavním záměrem je porovnat přístup ke vzdělávání v této oblasti, dostupnost vzdělávacích programů a možnosti rozvoje zaměstnanců v obou sektorech. Pokud bude zjištěno nedostatečné vzdělávání v tomto odvětví, bude navrženo řešení ke zlepšení této situace.

Z tohoto cíle vyplývají tyto výzkumné otázky:

1. Je v rámci pracovní pozice respondenta realizováno školení v oblasti kybernetické a informační bezpečnosti a s jakou frekvencí?
2. Jakou formu školení respondenti upřednostňují?
3. Vnímá respondent školení jako přínosné pro svou práci a zlepšení povědomí o kybernetických hrozbách?

7.2 Metodika výzkumu

K získání potřebných dat byl vybrán polostrukturovaný rozhovor s vybranými zaměstnanci soukromého a státního sektoru. Otázky polostrukturovaného rozhovoru byly rozděleny

do dvou částí. První část otázek se týkala charakteristiky respondentů, jako je aktuální pracovní pozice a doba působnosti. Druhá část otázek byla zaměřena na vzdělávání v kybernetické a informační bezpečnosti v jejich zaměstnáních. V této části bylo respondentům kladeno 11 otázek týkajících se výše uvedené problematiky. Rozhovory s vybranými účastníky byly provedeny osobně nebo online formou.

Tabulka 11 - Otázky rozhovoru (Vlastní zpracování)

O. č.	Název otázky
1.	Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky a internetu?
2.	Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?
3.	Vztahují se školené v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?
4.	Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?
5.	Jakou formou školení probíhají? Prezenční školení s lektorem nebo e- learningový kurz? Jakou formu preferujete?
6.	Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?
7.	Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?
8.	Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému bezpečnostnímu incidentu? Pokud ano, jaká byla následná opatření?
9.	Víte, na koho se v případě incidentu obrátit?
10.	Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?
11.	Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

V tabulce č. 12 jsou uvedeny jednotlivé otázky, které tvořily součást polostrukturovaných rozhovorů.

7.3 Výběr a charakteristika respondentů

Výzkumný vzorek tvoří deset zaměstnanců, přičemž bylo vybráno pět pracovníků ze státního sektoru a pět ze soukromého sektoru. Respondenti se pohybují ve věkové hranici 32 až 70 let. Tento výběr umožňuje porovnat poznatky zaměstnanců v obou sektorech a analyzovat jejich přístup ke vzdělávání v oblasti kybernetické a informační bezpečnosti.

Tabulka 12 - Informace o respondentech ze státního sektoru (vlastní zpracování)

Respondent	Pracovní zařazení	Délka praxe	Datum realizace rozhovoru	Způsob provedení
1.	HZS	11 let	15. 03. 2025	Osobní
2.	PČR	8 let	15. 03. 2025	Online
3	AČR	10 let	15. 03. 2025	Online
4.	Sociální služby	7 let	15. 03. 2025	Online
5.	Veřejná správa	26 let	16. 03. 2025	Osobní

Tabulka 13 - Informace o respondentech ze soukromého sektoru (vlastní zpracování)

Respondent	Pracovní pozice	Délka praxe	Datum rozhovoru	Způsob provedení
1.	Účetní	23 let	16. 03. 2025	Osobní
2.	Vedoucí pobočky	15 let	16. 03. 2025	Osobní
3.	Obchodní zástupce	9 let	16. 03. 2025	Osobní
4.	Instruktor dopravy	1,5 let	17. 03. 2025	Online
5.	Servisní technik	9,5 let	17. 03. 2025	Online

7.4 Provedení výzkumného šetření

Sestavení otázek k rozhovorům a následný výběr respondentů proběhlo dne 11. 03. 2025. Následně proběhlo telefonické či písemné oslovení vybraných respondentů s žádostí o rozhovor. Shromažďování dat probíhalo od 15. 03. do 17. 03. 2025.

7.5 Souhrn rozhovorů

Respondenti byli před začátkem rozhovoru seznámeni s tématem bakalářské práce a s jeho hlavními cíli.

7.5.1 Respondenti ze státního sektoru

Pro výzkumné šetření bylo vybráno pět respondentů ze státního sektoru.

Respondent č.1 - Hasičský záchranný sbor České republiky

Respondent č. 1 je členem Hasičského záchranného sboru České republiky v kraji Vysočina, kde pracuje na pozici hasič – technik chemické služby. U hasičského záchranného systému působí 11 let. Respondent si doplňuje vzdělání na Univerzitě Tomáše Bati, kde studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 15. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P I.

Respondent č. 2 - Policie České republiky

Respondent č. 2 je členem Policie České republiky, kde pracuje jako policista při Krajském ředitelství policie Zlínského kraje, Územní odbor Vsetín, kde vykonává funkci vrchního inspektora. Jeho hlavní náplní práce je zejména zpracování a prověřování přečinů a vedení zkráceného přípravného řízení, tedy provádění úkonů v trestním řízení. U policie slouží osmým rokem a funkci vrchního komisaře zastává od roku 2023. Respondent si doplňuje vzdělání na Univerzitě Tomáše Bati, kde studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 15. března 2025. Transkripce rozhovoru v příloze P II.

Respondent č. 3 – Armáda České republiky

Respondent č. 3 je členem Armády České republiky, kde pracuje jako starší důstojník Skupiny virtuální simulace, Oddělení simulací taktické přípravy Skupiny simulačních a trenažerových technologií ve Vyškově. V armádě slouží desátým rokem. Respondent

zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 15. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P III.

Respondent č. 4 – Sociální služby a zdravotní péče

Respondentka č. 4 působí v příspěvkové organizaci zřízené krajem Vysočina. Pracuje v domově pro seniory, kde působí, jako zdravotní sestra již sedm let. Respondentka zvolila variantu anonymní. S respondentkou byl proveden online rozhovor dne 15. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P IV.

Respondent č. 5 – Veřejná správa

Respondent č. 5 působí ve veřejné správě, kde vykonává pozici uvolněného starosty obce v kraji Vysočina. Na této pozici působí již 26 let. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 16. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P V.

7.5.2 Respondenti ze soukromého sektoru

Pro výzkumné šetření bylo vybráno pět respondentů ze soukromého sektoru.

Respondentka č. 1 – Prodejna a servis elektromotorů

Respondentka č. 1 pracuje na pozici účetní v české společnosti zabývající se prodejem a servisem elektromotorů. Respondentka na této pozici působí již 23 let. Respondentka zvolila variantu anonymní. S respondentkou byl proveden osobní rozhovor dne 16. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P VI.

Respondentka č. 2 – Speciální prodejna střešních materiálů

Respondentka č. 2 pracuje v české společnosti zabývající se prodejem střešních materiálů. Respondentka působí ve společnosti jako vedoucí pobočky. Ve společnosti působí již 15 let. Respondentka zvolila variantu anonymní. S respondentkou byl proveden osobní rozhovor dne 16. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P VII.

Respondent č. 3 – Pneuservis a prodejna pneumatik pro osobní nákladní automobily a zemědělskou techniku

Respondent č. 3 pracuje ve společnosti na pozici obchodního zástupce. Tuto pozici vykonává devět let. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 17. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P VIII.

Respondent č. 4 – Dopravce sypkých hmot

Respondent č. 4 působí ve firmě zabývající se autodopravou sypkých hmot, ukládkou a recyklací stavebních odpadů. Respondent působí na pozici instruktora dopravy v segmentu stavitelství. V této firmě působí rok a půl. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 17. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P IX.

Respondent č. 5 – Prodejce nových a ojetých vozů

Respondent č. 5 působí ve společnosti zabývající se prodejem nových a ojetých vozů jako servisní technik. Tuto pozici zastává devět a půl roku. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 17. března 2025. Úplná transkripce rozhovoru je uvedena v příloze P X.

7.6 Shrnutí a vyhodnocení získaných dat

Vyhodnocení šetření proběhlo na základě předem určených výzkumných otázek. Vyhodnocení dat proběhlo ve dvou krocích, kde první krok byla analýza demografických údajů, kde byla zohledněna délka pracovního poměru. V druhém kroku byly vyhodnoceny výzkumné otázky. Vyhodnocení dat proběhlo zvlášť v státním sektoru a zvlášť v soukromém. Následně došlo k porovnání výsledků mezi sektory.

Vyhodnocení dat státního sektoru

Tabulka 14 - Státní sektor – délka výkonu pracovní pozice (vlastní zpracování)

Délka výkonu pracovní pozice	Absolutní četnost	Relevantní četnost
0-5 let	0	0 %
6-10 let	3	60 %
11-20 let	1	20 %
20 let a více	1	20 %
Celkem	5	100 %

Na základě provedených rozhovorů s respondenty ze státního sektoru bylo zjištěno, že celkem tři respondenti (60 %) působí ve funkci méně než 10 let a více let vykonává danou pozici 40 % respondentů.

Výzkumná otázka č. 1 - Je v rámci pracovní pozice respondenta realizováno školení v oblasti kybernetické a informační bezpečnosti a s jakou frekvencí?

Na základě provedených rozhovorů lze konstatovat, že školení v oblasti kybernetické a informační bezpečnosti je v rámci jejich pracovního zařazení ve většině případů realizováno. I když se přístup ke školení v některých organizacích liší, ve všech případech se potvrdilo, že určitá forma školení probíhá. U HZS probíhá školení jedenkrát ročně formou e-learningu a je určené pro všechny. U Policie České republiky je školení poskytnuto všem zaměstnancům v podobě e-learningu. Prezenční školení absolvují pouze pracovníci se specifickým zaměřením. V Armádě ČR a v domově pro seniory je školení povinné pro všechny zaměstnance s frekvencí jednou ročně. Školení probíhá prezenční formou. Zatímco ve veřejné správě dle rozhovoru školení probíhá v intervalu dvou let, přičemž frekvence školení se může lišit dle pracovní pozice.

Výzkumná otázka č. 2 - Jakou formu školení respondenti upřednostňují?

Prezenční formu školení preferuje 80 % respondentů, protože je vnímána jako srozumitelnější a přínosnější díky možnosti přímé interakce s lektorem než ve většině. Zbýlých 20 % preferuje e-learning z důvodu časové nezávislosti a pohodlí.

Výzkumná otázka č. 3 - Vnímá respondent školení jako přínosné pro svou práci a zlepšení povědomí o kybernetických hrozbách?

Všichni dotázaní respondenti vnímají školení jako přínosné a dostatečné pro svoje zaměstnání. Zároveň všichni oslovení respondenti uvedli, že získané znalosti využívají i v běžném životě. Dále uvedli, že díky informovanosti v dané problematice ví, na koho se v případě incidentu obrátit. Respondent z veřejné správy uvedl, že obsah školení by měl reflektovat aktuální dění v této oblasti, jako je například využití umělé inteligence nebo nové podvodné praktiky.

Celkově lze říct, že školení v oblasti kybernetické a informační bezpečnosti ve státním sektoru je vnímáno jako velmi důležité, ačkoliv se jeho frekvence a formy napříč organizacemi liší. Informace získané z těchto školení jsou respondenty považovány za užitečné.

Vyhodnocení dat soukromého sektoru

Tabulka 15 - Soukromý sektor – délka výkonu pracovní pozice (vlastní zpracování)

Délka výkonu pracovní pozice	Absolutní četnost	Relevantní četnost
0-5 let	1	20 %
6-10 let	2	40 %
11-20 let	1	20 %
20 let a více	1	20 %
Celkem	5	100 %

Na základě provedených rozhovorů s respondenty ze soukromého sektoru bylo zjištěno, že celkem tři respondenti (60 %) působí ve funkci méně než 10 let a více let vykonává danou pozici 40 % respondentů.

Výzkumná otázka č. 1 - Je v rámci pracovní pozice respondenta realizováno školení v oblasti kybernetické a informační bezpečnosti a s jakou frekvencí?

Na základě provedených rozhovorů lze konstatovat, že školení v kybernetické a informační bezpečnosti u 80 % respondentů neprobíhá. U zbylých 20 % respondentů školení probíhá. U respondentky pracující na pozici vedoucí pobočky školení probíhá dvakrát ročně, a to jak formou prezenční, tak formou e-learningu. U respondenta pracujícího na pozici servisního technika školení probíhá také jedenkrát až dvakrát ročně, ale formou e-learningového kurzu, který je zakončen výstupním testem.

Výzkumná otázka č. 2 - Jakou formu školení respondenti upřednostňují?

Prezenční formu školení preferuje respondentka působící na pozici vedoucí prodejny. Tuto formu preferuje z důvodu osobního kontaktu s lektorem a možnosti okamžitého vysvětlení nejasností. Respondent pracující na pozici servisního technika preferuje e-learningové kurzy z důvodu časové nezávislosti. U zbylých 40 % respondentů kurzy neprobíhají žádnou formou, jedná se o respondenty pracující na pozici účetní, obchodní zástupce a instruktora dopravy.

Výzkumná otázka č. 3 - Vnímá respondent školení jako přínosné pro svou práci a zlepšení povědomí o kybernetických hrozbách?

U 40 % respondentů bylo zjištěno, že vnímá školení v této oblasti jako přínosné pro svoje zaměstnání a svoje poznatky dále využívá i v běžném životě. Jedná se o respondenta pracujícího na pozici servisního technika a vedoucí pobočky. Zbýlých 60 % respondentů nemá dostatečné povědomí o hrozbách a možnostech incidentů v jejich zaměstnání a považuje vzdělávání v této oblasti za nedostatečné.

Celkově lze říct, že v rámci soukromého sektoru je patrná nízká úroveň povědomí o kybernetických hrozbách i bezpečnostních zásadách. U většiny oslovených respondentů nebylo školení v této oblasti dosud realizováno. Tato skutečnost naznačuje, že dané problematice není věnována dostatečná pozornost a v mnoha případech ze strany zaměstnavatelů chybí iniciativa k podpoře vzdělávání v této oblasti.

Komparace výsledků ve státním a soukromém sektoru

Na základě vyhodnocených dat byly analyzovány rozdíly a shody v přístupu ke vzdělávání v oblasti kybernetické a informační bezpečnosti mezi státním a soukromým sektorem.

V obou sektorech 80 % respondentů neabsolvovalo vstupní školení v oblasti kybernetické a informační bezpečnosti. Pouze 20 % respondentů v obou sektorech školení absolvovalo. Tudíž vstupní školení v obou sektorech je nedostatečné, jelikož většina zaměstnanců jej neabsolvovala.

Státní sektor má lepší systém vzdělávání, protože všichni zaměstnanci alespoň jedenkrát ročně navštíví školení. V soukromém sektoru se většina (60 %) zaměstnanců neškolí vůbec.

Ve státním sektoru je větší preference prezenčního školení, což naznačuje vyšší zájem o osobní výuku. Zatímco v soukromém sektoru je vyšší podíl zaměstnanců, kteří se neškolí vůbec.

Ve státním sektoru všichni respondenti považují školení jako přínosné, zatímco v soukromém sektoru většina (60 %) zaměstnanců nemá dostatečné povědomí o hrozbách a považuje vzdělávání za nedostatečné.

8 NÁVRH NA ZLEPŠENÍ VZDĚLÁVÁNÍ V KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE

Kvalitní a efektivní vzdělávání v oblasti kybernetické a informační bezpečnosti vede ke zvyšování odolnosti organizací vůči kybernetickým hrozbám. Vzhledem k rostoucímu počtu kybernetických útoků, úniků dat a zneužití informačních systémů je velmi důležité, aby zaměstnanci jak ve státním, tak soukromém sektoru měli základní znalosti a dovednosti, které jim umožní správně reagovat na vzniklé události a hrozby.

Na základě analýzy vybraných kurzů kybernetické a informační bezpečnosti provedené pomocí vícekriteriálního rozhodování, konkrétně bodovací metody a rozhovorů s vybranými zaměstnanci ze státního i soukromého sektoru, je zřejmé, že úroveň vzdělávání je značně odlišná jak v kvalitě, tak i v dostupnosti napříč jednotlivými sektory. Z těchto výsledků vyplývá potřeba navrhnout konkrétní kroky vedoucí ke zlepšení situace v této oblasti.

Na základě provedených rozhovorů bylo zjištěno, že ve státním sektoru je školení zavedeno, avšak se liší jeho kvalita, forma a i frekvence. V soukromém sektoru často školení neprobíhá vůbec nebo je realizováno nepravidelně. Vstupní školení, které by zahrnovalo základní seznámení s pravidly bezpečného chování na internetu u většiny respondentů ze soukromého sektoru chybělo.

Hlavním cílem navrhovaného řešení je vytvoření systematického a přístupného systému vzdělávání, který bude zaměřen na zvyšování povědomí zaměstnanců o kybernetických rizicích a na posilování jejich schopnosti bezpečně pracovat s citlivými informacemi. Jedním z důležitých kroků vedoucích ke zlepšení je zavedení pravidelných a systematických školení pro všechny zaměstnance. Zároveň je důležité sjednotit úroveň znalostí napříč sektory a předejít podceňování lidského faktoru, který často přispívá ke vzniku bezpečnostních incidentů. Školení by měla být povinnou součástí při nástupu do zaměstnání a měla by obsahovat témata jako je správa hesel, bezpečné používání e-mailu a předcházení bezpečnostním incidentům. Zároveň by měla probíhat i průběžná školení v rámci dalšího rozvíjení vědomostí. Optimální frekvence školení by měla být minimálně jedenkrát ročně z důvodu neustále se vyvíjejících forem kybernetických útoků.

Vzhledem k rozdílným preferencím respondentů by měla být školení poskytována v několika formách – prezenční, e-learningové i kombinované. Důraz by měl být kladen nejen na teoretickou část kurzu, ale zejména na praktickou část, kde budou ukázány reálné příklady útoků a ukázky z praxe. Jako efektivní forma se jeví prezenční výuka, z důvodu

možnosti kladení přímých otázek lektorovi. Prezenční výuka by mohla být případně doplněna o e-learningový kurz, který by umožnil zaměstnancům s odstupem času zopakovat si získané vědomosti.

Z rozhovorů dále vyplynulo, že respondenti by uvítali školení, které reflektuje aktuální vývoj v oblasti kybernetických hrozeb. Proto se navrhuje pravidelná aktualizace obsahu kurzů, a to minimálně jedenkrát ročně.

Dalším krokem vedoucím ke zlepšení úrovně vzdělávání je vytvoření vzdělávacího systému. Systém by měl být rozdělen do skupin podle pracovních pozic a úrovně vzdělání, aby byl obsah vždy přizpůsobený cílové skupině.

Z vyhodnocení bodovací metody jednoznačně vyplývá, že nejlépe hodnoceným kurzem je bezplatný online kurz Základy kybernetické bezpečnosti 25, který poskytuje NÚKIB. Předností tohoto kurzu je zejména dostupnost, ale také přehledná struktura, praktické zaměření. Kurz je vhodný pro širokou škálu uživatelů od zaměstnanců státní správy, přes pracovníky soukromých firem až pro běžné občany. Mezi hlavní výhody kurzu patří časová flexibilita, vysoká využitelnost v praxi a certifikace, která účastníkům poskytuje potvrzení o dosažených znalostech. Z výše uvedených důvodů lze kurz považovat za vhodný základní nástroj pro vzdělávání v kybernetické a informační bezpečnosti.

Vzhledem k výše uvedeným výhodám a k hodnocení kurzu Základy kybernetické bezpečnosti 25 od NÚKIB by bylo vhodné kurz implementovat do vzdělávacího procesu pro nové a stávající zaměstnance. Vzhledem k tomu, že kurz je dostupný a bezplatný pro všechny, tak by bylo možné ho zařadit pro všechny zaměstnance. Dále by měl být opakován minimálně jedenkrát ročně jako průběžná forma vzdělávání. Pro zvýšení efektivity je vhodné školení doplnit o praktické ukázky, jako jsou modelové situace nebo příklady z reálné praxe.

V soukromém sektoru by bylo užitečné podpořit zavádění školení například finančním zpřístupněním bezplatných vzdělávacích materiálů. Navázání spolupráce s institucemi, jako je NÚKIB či Ministerstvo školství, mládeže a tělovýchovy by mohlo přispět k větší osvětě v oblasti kybernetické bezpečnosti. Tyto subjekty zároveň mohou nabídnout metodickou podporu menším a středním podnikům, které si často nemohou dovolit budovat vlastní vzdělávací systém. Případně by mohl stát poskytnout jednotnou platformu pro vzdělávání, která by obsahovala pravidelně aktualizované kurzy rozdělené dle úrovně a zaměření.

Navrhovaná opatření mají za cíl posílit bezpečnostní povědomí zaměstnanců napříč sektory, snížit rizika incidentů způsobených lidskou chybou a tím posílit odolnost organizací vůči kybernetickým hrozbám. V dlouhodobém horizontu lze očekávat snížení počtu bezpečnostních incidentů, které jsou často způsobeny lidskou chybou. Díky lepší informovanosti zaměstnanců se zvýší schopnost včas rozpoznat rizikové situace a vhodně na ně reagovat. Organizace, které investují do pravidelného vzdělávání zaměstnanců budou také vnímány jako důvěryhodné, jak ze strany klientů, tak i obchodních partnerů. Investice do vzdělání se následně vrátí nejen v podobě bezpečnějšího prostředí, ale také ve stabilnějším fungování celé organizace.

ZÁVĚR

Vzdělávání v oblasti kybernetické a informační bezpečnosti se v dnešní online době stává předpokladem pro zajištění bezpečnosti informačních systémů, prevence hrozeb a ochrany dat.

Předmětem bakalářské práce bylo zhodnotit vybrané kurzy kybernetické bezpečnosti a zhodnotit vzdělávání v oblasti kybernetické a informační bezpečnosti v státním a soukromém sektoru. V návaznosti na provedenou analýzu vznikl návrh na zlepšení vzdělávání v oblasti kybernetické a informační bezpečnosti ve státním a soukromém sektoru.

Teoretická část se věnovala přehledu právních předpisů, vybraným organizacím a představení vybraných kybernetických útoků na území České republiky a v zahraničí.

Praktickou část bakalářské práce tvoří analýza kurzů kybernetické a informační bezpečnosti poskytovaných v České republice, které byly vybrány na základě diskuse se specialistou na kybernetickou a informační bezpečnost. U vybraných kurzů byly následně porovnány důležité aspekty a byla aplikována metoda vícekritériálního rozhodování, konkrétně bodovací metoda. Na základě provedení této metody se stal nejlépe hodnocený kurz Základy kybernetické bezpečnosti 25 pod záštitou NÚKIB. Posléze byly provedeny strukturované rozhovory s vybranými zaměstnanci ze státního a soukromého sektoru. V rámci šetření bylo zjištěno, že ve státním sektoru probíhá školení pravidelně, zatímco v sektoru soukromém je tato oblast mnohdy opomíjena.

Na základě zjištěných rozdílů v přístupu ke vzdělání mezi státním a soukromým sektorem a výsledků vícekritériální analýzy vzdělávacích kurzů bylo navrženo řešení vedoucí ke zlepšení stavu vzdělávání v této oblasti. Návrh zahrnuje implementaci bezplatného online kurzu Základy kybernetické a informační bezpečnosti 25 a jeho zařazení do vstupního školení, ale i jako součást pravidelného ročního školení. Návrh dále zdůrazňuje potřebu kombinace různých forem výuky včetně praktických ukázek a pravidelně aktualizovaného obsahu.

Práce přináší ucelený pohled na problematiku vzdělávání v oblasti kybernetické a informační bezpečnosti a nabízí realizovatelný návrh řešení, který může být využit jako inspirace. Na základě výše uvedeného, lze konstatovat, že hlavní i dílčí cíle práce byly naplněny.

SEZNAM POUŽITÉ LITERATURY

APTIEŇ, 2025. *Způsoby školení a rozvoje zaměstnanců*. Online. Aptien. 15. 01. 2025. Dostupné z: <https://aptien.com/cs/kb/articles/kinds-of-employee-training-and-development>. [cit. 2025-02-12].

ARMÁDNY MAGAZÍN, 2025. *Krvavý kybernetický útok: Izrael stovkám Libanončanův odpálil v rukách mobility a pagery*. Online. Armádní magazín. Dostupné z: <https://www.armadnymagazin.sk/2024/09/17/krvavy-kyberneticky-utok-izrael-stovkam-libanoncanov-odpalil-v-rukach-mobily-a-pagery/>. [cit. 2025-03-14].

AVAST, 2025. *Online kurz*. Online. Avast. Dostupné z: <https://www.avast.com/cz/besafeonline/online-kurz>. [cit. 2025-03-13].

AVAST, 2025. *Petya*. Online. Avast. Dostupné z: <https://www.avast.com/cs-cz/c-petya>. [cit. 2025-02-09].

BLUE PARTNERS, 2024. *Školení kybernetické bezpečnosti*. Online. Blue Partners. 13.11.2024. Dostupné z: <https://www.bluepartners.cz/sluzby-a-produkty/produkt/skoleni-kyberneticke-bezpecnosti>. [cit. 2025-03-11].

BOZP, © 2025. *Ceník*. Online. BOZP. Dostupné z: <https://www.skolenibozp.cz/cenik/>. [cit. 2025-03-10].

BOZP, © 2025. *Školení informační a kybernetické bezpečnosti*. Online. BOZP. Dostupné z: <https://www.skolenibozp.cz/skoleni-kyberbezpecnosti/>. [cit. 2025-03-10].

CENTRUM KYBERNETICKÉ BEZPEČNOSTI, © 2025. *Kyberpohádky*. Online. Centrum kybernetické bezpečnosti. Dostupné z: <https://www.kyberpohadky.cz/kyberpohadky/>. [cit. 2025-03-25].

CENTRUM KYBERNETICKÉ BEZPEČNOSTI, 2025. *DIGITÁLNÍ ČESKO - Osvěta kybernetické bezpečnosti*. Online. Centrum kybernetické bezpečnosti. Dostupné z: https://www.kybercentrum.cz/digitalnicesko.html?utm_source=chatgpt.com. [cit. 2025-02-12].

CODREANU, Claudiu Mihai, 2021. Exploring the need for human-centred cybersecurity. The WannaCry Cyberattack. Online. *The Romanian Journal of Society and Politics*. Roč. 15, č. 2, s. 87-94. ISSN 2393-3224. Dostupné z: <https://doaj.org/article/109b439bbefe45bd88d1ede8f48010d0>. [cit. 2025-02-13].

CSIRT, 2019. *O týmu CSIRT.CZ*. Online. CSIRT. Dostupné z: <https://csirt.cz/cs/o-nas/>. [cit. 2025-02-09].

CSIRT, 2019. *Projekty týmu CSIRT.CZ*. Online. CSIRT. Dostupné z: <https://csirt.cz/cs/projekty/>. [cit. 2025-02-09].

CYBERSEC, 2025. *Co se naučíte?* Online. Cybersec. Dostupné z: <https://www.cybersec.cz/obsah-skoleni/>. [cit. 2025-02-12].

CYBERSEC, 2025. *Obsah e-learningu*. Online. CYBERSEC. Dostupné z: <https://www.cybersec.cz/obsah-skoleni/>. [cit. 2025-03-10].

CYBERSECURITYHUB, © 2025. *Expertní služby, reálný dopad*. Online. CyberSecurityHub. Dostupné z: <https://www.cybersecurityhub.cz/services>. [cit. 2025-03-12].

CYBERSECURITYHUB, © 2025. *Katalog našich služeb*. Online. CyberSecurityHub. Dostupné z: <https://www.cybersecurityhub.cz/services/catalogue?type=SkillsAndEducation>. [cit. 2025-03-12].

CYBERSECURITYHUB, 2025. *Expertní služby, reálný dopad*. Online. CyberSecurityHub. Dostupné z: <https://www.cybersecurityhub.cz/services>. [cit. 2025-02-12].

CZ.NIC, 2010. *CZ.NIC OHLÍDÁ KYBERNETICKOU BEZPEČNOST ČESKÉ REPUBLIKY*. Online. CZ.NIC. 1. 4. 2012. Dostupné z: <https://www.nic.cz/page/830/cz.nic-ohlida-kybernetickou-bezpecnost-ceske-republiky/>. [cit. 2025-02-09].

CZECHITAS, © 2016-2025. *ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI*. Online. Czechitas. Dostupné z: <https://www.czechitas.cz/kurzy/uvod-do-kyberneticke-bezpecnosti>. [cit. 2025-03-10].

CZECHITAS, © 2016-2025. *VZDĚLÁVÁNÍ PRO FIRMY*. Online. Czechitas. Dostupné z: <https://www.czechitas.cz/vzdelavani-pro-firmy>. [cit. 2025-03-10].

ČESKO, 2005. Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2005-412>.

ČESKO, 2014. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2014-181>.

ČESKO, 2019. Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů. In: *Zákony pro lidi*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2019-110>.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DURAČINSKÁ, Zuzana, 2016. NIS Co přináší nová směrnice EU o síťové a informační bezpečnosti? Online. *IT Systems*. Roč. 2016, č. 10, s. 2 - 3. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf. [cit. 2025-02-02].

ESET, © 1992 – 2025. *Školení kybernetické bezpečnosti PREMIUM*. Online. ESET. Dostupné z: <https://www.eset.com/cz/firmy/eset-services/řízení-it-bezpecnosti/skoleni-kyberneticke-bezpecnosti/premium/>. [cit. 2025-03-10].

ESET, 2024. *Nový Zákon o kybernetické bezpečnosti bude reagovat na aktuální hrozby*. Online. ESET. 29. 2. 2024. Dostupné z: <https://digitalsecurityguide.eset.com/cz/jake-povinnosti-prinese-novy-zakon-o-kyberneticke-bezpecnosti>. [cit. 2025-02-11].

ESET, 2025. *Co je DDoS útok?* Online. ESET. Dostupné z: <https://www.eset.com/cz/ddos-utok/>. [cit. 2025-02-08].

ESET, 2025. *Ransomware*. Online. ESET. Dostupné z: <https://www.eset.com/cz/ransomware/>. [cit. 2025-02-09].

ESET, 2025. *Typy phishingu*. Online. ESET. Dostupné z: <https://www.eset.com/cz/phishing/>. [cit. 2025-02-09].

FRUHLINGER, Josh, 2020. *Equifax data breach FAQ: What happened, who was affected, what was the impact?* Online. CSO. 12. 2. 2020. Dostupné z: https://www.csoononline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html?utm_source=chatgpt.com. [cit. 2025-02-09].

GORDIC, 2023. *Školení kybernetické bezpečnosti*. Online. GORDIC. Dostupné z: <https://gordiccybersec.cz/skoleni-kyberneticke-bezpecnosti/>. [cit. 2025-03-11].

HANZEL, Petr, 2025. *NOVÁ PRAVIDLA KYBERNETICKÉ BEZPEČNOSTI: JAKÉ JSOU NEJČASTĚJŠÍ CHYBY PŘI SAMOIDENTIFIKACI?* Online. In: ARROWS. 20.1.2025. Dostupné z: <https://www.arws.cz/novinky-v-arrows/nova-pravidla-kyberneticke-bezpecnosti-jake-jsou-nejcastejsi-chyby-pri-samoidentifikaci>. [cit. 2025-02-06].

HENDL, Jan, 2016. *Kvalitativní výzkum: základní teorie, metody a aplikace*. Čtvrté, přepracované a rozšířené vydání. Praha: Portál. ISBN 978-80-262-0982-9.

HORÁK, Jan, 2020. *Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera*. Online. Aktuálně.cz. 20. 3. 2020. Dostupné z: <https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/>. [cit. 2025-02-09].

CHOWDHURY, MD Minhaz; RIFAT, Nafiz; AHSAN, Mostofa; LATIF, Shadman; GOMES, Rahul et al., 2023. *ChatGPT: A Threat Against the CIA Triad of Cyber Security*. Online. 2023 IEEE International Conference on Electro Information Technology (eIT).

2023-5-18, roč. 2023, s. 480. ISBN 978-1-6654-9376-5. Dostupné z: <https://doi.org/10.1109/eIT57321.2023.10187355>. [cit. 2025-02-13].

IDNES.CZ, 2020. *Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty*. Online. IDNES.cz. 13. 3. 2020. Dostupné z: https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313_071531_brno-zpravy_bur. [cit. 2025-02-09].

INTERNETEM BEZPEČNĚ, 2016. *CO TO JE MALWARE*. Online. Internetem BEZPEČNĚ. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/malware/co-to-je-malware/>. [cit. 2025-02-09].

IROZHLAS, 2023. *Univerzitu obrany napadli hackeři. Unikla data pracovníků a vyučujících včetně finančních výkazů*. Online. IROZHLAS. 27. 9. 2023. Dostupné z: https://www.irozhlas.cz/zpravy-domov/unob-univerzita-obrany-kyberneticky-utok-hackeri_2309271200_kac?utm_source=chatgpt.com. [cit. 2025-02-09].

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2022. *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA. ISBN 978-80-908388-4-0.

JUODYTĚ, Eglè, 2023. *NotPetya: A wiper disguised as ransomware*. Online. NordVPN. 20. 6. 2023. Dostupné z: <https://nordvpn.com/blog/notpetya-a-wiper-disguised-as-ransomware/>. [cit. 2025-03-07].

KHONJI, Mahmoud; IRAQI, Youssef a JONES, Andrew, 2013. *Phishing Detection: A Literature Survey*. Online. *IEEE Communications Surveys & Tutorials*. Roč. 15, č. 4, s. 2091. ISSN 1553-877X. Dostupné z: <https://doi.org/10.1109/SURV.2013.032213.00009>. [cit. 2025-02-13].

KOLOUCH, Jan a BAŠTA, Pavel, 2019. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-31-7.

KRČMÁŘ, Petr, 2018. *Úniku dat 148 milionů lidí bylo možné zabránit, kdyby fungovalo IT oddělení*. Online. ROOT. 13. 12. 2018. Dostupné z: <https://www.root.cz/clanky/uniku-dat-148-milionu-lidi-bylo-mozne-zabranit-kdyby-fungovalo-it-oddeleni/>. [cit. 2025-02-09].

KŘOUSTEK, Jakub, 2017. *Novinky o WannaCry: Nejhorší ransomwarový útok v historii*. Online. Avast. 17. 5. 2017. Dostupné z: <https://blog.avast.com/cs/novinky-o-wannacry-nejvetsi-ransomwarovy-utok-v-historii>. [cit. 2025-02-09].

KYBEZ, 2014. *Vyhláška o významných informačních systémech*. Online. KYBEZ. Dostupné z: <https://kybez.cz/vyhlaska-o-vyznamnych-informacnich-systemech/>. [cit. 2025-02-09].

KYBEZ, 2021. *Řízení kybernetické bezpečnosti (workshop)*. Online. KYBEZ. 9. 7. 2021. Dostupné z: <https://kybez.cz/sluzby/7228-2/>. [cit. 2025-03-10].

KYBEZ, 2021. *Základy kybernetické bezpečnosti organizace*. Online. KYBEZ. 9. 7. 2021. Dostupné z: <https://kybez.cz/sluzby/zaklady-kyberneticke-bezpecnosti-organizace/>. [cit. 2025-03-10].

MICROSOFT, 2025. *Co je kybernetická bezpečnost?* Online. Microsoft. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-cybersecurity?utm_source=chatgpt.com. [cit. 2025-02-09].

MINDTHEGRAPH, 2023. *Polostrukturované rozhovory v kvalitativním výzkumu*. Online. Mindthegraph. 20.12.2023. Dostupné z: <https://mindthegraph.com/blog/cs/polostrukturovane-rozhovory-v-kvalitativni-vyzkumu/>. [cit. 2025-03-20].

MONETA BANK, 2025. *Co je vishing?* Online. MONETA BANK. Dostupné z: <https://www.moneta.cz/caste-dotazy/odpoved/co-je-vishing>. [cit. 2025-02-09].

MŠMT, 2023. *Rámcový vzdělávací program pro základní vzdělávání*. 2. Praha. Dostupné také z: <https://edu.gov.cz/rvp-ramcove-vzdelavaci-programy/ramcovy-vzdelavacici-program-pro-zakladni-vzdelavani-rvp-zv/>.

NBÚ, 2024. *Nový ředitel Národního bezpečnostního úřadu se ujal funkce*. Online. NBÚ. 2. květen 2024. Dostupné z: <https://nbu.gov.cz/cs/aktualne/1297-novy-reditel-narodniho-bezpecnostniho-uradu-se-ujal-funkce/>. [cit. 2025-02-09].

NBÚ, 2025. *O NBÚ*. Online. NBÚ. Dostupné z: <https://www.nbu.cz/cs/o-nas/>. [cit. 2025-02-09].

NCEZ, 2020. *Úspěšné vyřešení následků kybernetického útoku na Psychiatrickou nemocnici Kosmonosy*. Online. NCEZ. 3. 4. 2020. Dostupné z: [datech minimalizovat. https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/uspesne-vyreseni-nasledku-kybernetickeho-utoku-na-psychiatrickou-nemocnici](https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/uspesne-vyreseni-nasledku-kybernetickeho-utoku-na-psychiatrickou-nemocnici). [cit. 2025-02-09].

NOONAN, Luke, 2024. *How to Promote Cyber Security Awareness and Improve Cyber Security at the Workplace*. Online. MetaCompliance. Dostupné z: <https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation>. [cit. 2025-02-12].

NOVINKY, 2025. *Hackeri napadli slovenský katastr nemovitostí a ochromili realitní trh. Žádají desítky milionů dolarů*. Online. Novinky. 9. 1. 2025. Dostupné z: <https://www.novinky.cz/clanek/zahranicni-evropa-hackeri-napadli-slovensky-katastr-nemovitosti-a-ochromili-realitni-trh-zadaji-desitky-milionu-dolaru-40503816>. [cit. 2025-03-14].

NÚKIB, 2022. *NÚKIB spouští aktualizovanou verzi on-line kurzu „Dávej kyber!“*. Online. NÚKIB. 1. červen 2022. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/1841-nukib-spousti-aktualizovanou-verzi-on-line-kurzu-davej-kyber/>. [cit. 2025-03-12].

NÚKIB, 2022. *Osvětová kampaň #KYBERštít*. Online. NÚKIB. 2. 3. 2022. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/1818-osvetova-kampan-kyberstit/>. [cit. 2025-02-11].

NÚKIB, 2022. *Vedení úřadu*. Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/vedeni-uradu/>. [cit. 2025-02-09].

NÚKIB, 2023. *Česká bankovní asociace opět spouští vzdělávací kampaň #nePINdej! Nově do ní zapojila i umělou inteligenci.* Online. NÚKIB. 5. 9. 2023. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/2002-ceska-bankovni-asociace-opet-spousti-kampan-nepindej-nove-do-ni-zapojila-i-umelou-inteligenci/>. [cit. 2025-02-12].

NÚKIB, 2024. *1. Obecné informace o směrnici NIS2.* Online. NÚKIB. 1. 10. 2024. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-obecne-informace-o-smernici-nis2>. [cit. 2025-02-09].

NÚKIB, 2024. *Bezpečnostní rada státu schválila Národní politiku kryptografické ochrany utajovaných informací.* Online. NÚKIB. 6. prosinec 2024. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/2195-bezpecnostni-rada-statu-schvalila-narodni-politiku-kryptograficke-ochrany-utajovanych-informaci/>. [cit. 2025-02-09].

NÚKIB, 2025. *„DÁVEJ KYBER“ PRO UČITELE.* Online. NÚKIB. Dostupné z: <https://osveta.nukib.gov.cz/course/view.php?id=121>. [cit. 2025-03-12].

NÚKIB, 2025. *01 - Obecné informace o směrnici NIS2.* Online. NÚKIB. Dostupné z: <https://osveta.nukib.gov.cz/mod/page/view.php?id=2582>. [cit. 2025-02-09].

NÚKIB, 2025. *Kybernetická bezpečnost.* Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/>. [cit. 2025-03-07].

NÚKIB, 2025. *Nabízené kurzy.* Online. NÚKIB. Dostupné z: <https://osveta.nukib.gov.cz/local/dashboard/>. [cit. 2025-03-12].

NÚKIB, 2025. *NÚKIB.* Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/>. [cit. 2025-02-09].

NÚKIB, 2025. *O úřadu.* Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/o-nukib/o-uradu/>. [cit. 2025-02-09].

NÚKIB, 2025. *Poskytované služby*. Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/>. [cit. 2025-02-09].

NÚKIB, 2025. *Státní správa*. Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/statni-sprava/>. [cit. 2025-02-12].

NÚKIB, 2025. *Střední školy*. Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/stredni-skoly/>. [cit. 2025-02-13].

NÚKIB, 2025. *ŠÉFUJ KYBER!*. Online. NÚKIB. Dostupné z: <https://osveta.nukib.gov.cz/course/view.php?id=220>. [cit. 2025-03-12].

NÚKIB, 2025. *Vzdělávání*. Online. NÚKIB. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/>. [cit. 2025-02-09].

NÚKIB, 2025. *Základy kybernetické bezpečnosti 25*. Online. NÚKIB. Dostupné z: <https://osveta.nukib.gov.cz/course/view.php?id=221>. [cit. 2025-03-25].

O2, 2024. *Stuxnet: Příběh malwaru, který narušil iránský jaderný program*. Online. O2cybernews. 31. 07. 2024. Dostupné z: <https://o2cybernews.cz/clanky/stuxnet-pribeh-malwaru-ktery-rozlozil-iransky-jaderny-program>. [cit. 2025-03-07].

OLADIMEJI, Saheed a KERNER, Sean Michael, 2023. *SolarWinds hack explained: Everything you need to know*. Online. TechTarget. 03. 10. 2023. Dostupné z: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know?utm_source=chatgpt.com. [cit. 2025-02-09].

PAVELKA, Ivan, 2018. *Správní právo: Institucionální zajištění ochrany utajovaných informací v ČR*. Online. Roč. LI, č. 3/2018. Praha: Ministerstvo vnitra. ISSN 0139-6005. [cit. 2025-03-25].

PIDRMNAOVÁ, Zuzana, 2022. *#nePINdej!*. Online. PČR. Dostupné z: <https://policie.gov.cz/clanek/nepindej.aspx>. [cit. 2025-02-12].

POLÁK, Ondřej, 2024. *Nová právní úprava kybernetické bezpečnosti*. Online. CYBERSECURITY. 7. února 2024. Dostupné z: https://cybersecurity.cz/data/polak_BS73.pdf. [cit. 2025-03-07].

POPELOVÁ, Lucie, 2016. *Zbraně budoucnosti: Stuxnet a jeho dopady na vývoj mezinárodních vztahů*. Bakalářská práce, vedoucí Mgr. et Mgr. Jakub Fučík. Brno: Masarykova univerzita. Dostupné také z: https://is.muni.cz/th/kklrr/Bakalarskaprace_LuciePopelova.pdf.

POŽÁR, Josef, 2005. *Informační bezpečnost*. Vysokoškolské učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 80-868-9838-5.

PUMPEDU, © 2025. *Kybernetická bezpečnost*. Online. Pumpedu. Dostupné z: <https://www.pumpedu.cz/kyberneticka-bezpecnost-c306#KT21010306-0001>. [cit. 2025-03-11].

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SEDUO, 2025. *Bezpečně v online světě: jak ochránit své peníze, data a identitu*. Online. Seduo. Dostupné z: <https://www.seduo.cz/bezpecne-v-online-svete-jak-ochranit-sve-penize-data-a-identitu>. [cit. 2025-03-11].

SEDUO, 2025. *Digitální bezpečnost: naučte se chodit v online světě bezpečně*. Online. Seduo. Dostupné z: <https://www.seduo.cz/digitalni-bezpecnost-naucte-se-chodit-v-online-svete-bezpecne>. [cit. 2025-03-11].

SEDUO, 2025. *Připravte firmu na nové kybernetické výzvy*. Online. Seduo. Dostupné z: <https://www.seduo.cz/pripravte-firmu-na-nove-kyberneticke-vyzvy>. [cit. 2025-03-11].

SENANAYAKE, Tharindu a FERNANDO, Suchintha, 2018. INFORMATION SECURITY EDUCATION: WATCHING YOUR STEPS IN CYBERSPACE. Online. *The Online Journal of Science and Technology*. Roč. 8, č. 2, s. 96-101. ISSN 2146-7390. Dostupné z: <https://www.tojsat.net/journals/tojsat/volumes/tojsat-volume08-i02.pdf>. [cit. 2024-10-27].

SERVICE & SUPPORT, 2023. *Útok na FN Brno po více jak dvou letech*. Online. Service & Support. Dostupné z: <https://www.sands.cz/utok-na-fn-brno-po-vice-jak-dvou-letech/>. [cit. 2025-02-09].

SEYFOR, 2024. *Kybernetický bezpečnostní incident – co to je a jaké druhy známe?* Online. Seyfor. 20. 6. 2024, 2024. Dostupné z: <https://www.seyfor.com/cs-cz/kyberneticky-bezpecnostni-incident-co-to-je-a-jake-druhy-zname>. [cit. 2025-02-09].

SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-501-2.

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

THEIMEROVÁ, Michaela, 2023. *Systém vzdělávání pracovníků odborného vzdělávání ve vězeňství*. Bakalářská práce, vedoucí Doc. Mgr. Ing. Krpálková Krellová Katarína, Ph.D. Praha: Univerzita Jana Amose Komenského Praha. Dostupné také z: https://theses.cz/id/8cz3c4/th76_1116220112.pdf.

TOP SECURITY, 2025. *Hackerské útoky v ČR v roce 2022*. Online. TOP SECURITY. Dostupné z: <https://www.topsecurity.cz/blog/clanek/hackerske-utoky-v-cr-v-roce-2022>. [cit. 2025-02-09].

VANITHA, J.; MALLIKA, C.; HEMA, A.; PARKAVI, K.; SHANDHOSH SHREE, K.K. et al., 2024. Detection System of Whaling Attack using Deep Learning Techniques. Online. *2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems*

(ICSSAS). 2024-10-23, s. 493. ISBN 979-8-3503-6841-3. Dostupné z: <https://doi.org/10.1109/ICSSAS64001.2024.10760478>. [cit. 2025-02-13].

VOJENSKÉ ZPRAVODAJSTVÍ, 2018. *NÁRODNÍ CENTRUM KYBERNETICKÝCH OPERACÍ VYPRACOVALO STRATEGII KYBERNETICKÉ OBRANY ČR*. Online. Vojenské zpravodajství. 06.08.2018. Dostupné z: <https://vzcr.gov.cz/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-97>. [cit. 2025-03-07].

VOJENSKÉ ZPRAVODAJSTVÍ, 2025. *VOJENSKÉ ZPRAVODAJSTVÍ SE PODÍLÍ NA ZAJIŠŤOVÁNÍ KYBERNETICKÉ OBRANY ČESKÉ REPUBLIKY*. Online. Vojenské ZPRAVODAJSTVÍ. Dostupné z: <https://vzcr.gov.cz/kyberneticka-obrana-46>. [cit. 2025-03-07].

WINTIP, 2024. *Co je to Quishing?* Online. Wintip. 26. 11. 2024. Dostupné z: <https://wintip.cz/4228-co-je-to-quishing>. [cit. 2025-03-07].

SEZNAM TABULEK

Tabulka 1 - Seznam vybraných kurzů (vlastní zpracování)	41
Tabulka 2 - Složení hodnotitelského týmu (zpracování vlastní)	42
Tabulka 3 - Vybraná hodnotící kritéria (vlastní zpracování).....	42
Tabulka 4 - Maximalizační kritérium kvalita a obsah (vlastní zpracování)	43
Tabulka 5 - Maximalizační kritérium praktický přínos (vlastní zpracování)	43
Tabulka 6 - Minimalizační kritérium cena (vlastní zpracování).....	44
Tabulka 7 - Ceny vybraných kurzů (vlastní zpracování).....	44
Tabulka 8 - Hodnocení vybraných kurzů (vlastní zpracování).....	45
Tabulka 9 - Průměrné hodnocení vybraných kurzů (vlastní zpracování).....	45
Tabulka 10 - Vážené skóre a výsledné pořadí kurzů (vlastní zpracování)	46
Tabulka 11 - Otázky rozhovoru (Vlastní zpracování)	49
Tabulka 12 - Informace o respondentech ze státního sektoru (vlastní zpracování).....	50
Tabulka 13 - Informace o respondentech ze soukromého sektoru (vlastní zpracování)	50
Tabulka 14 - Státní sektor – délka výkonu pracovní pozice (vlastní zpracování).....	53
Tabulka 15 - Soukromý sektor – délka výkonu pracovní pozice (vlastní zpracování).....	55

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR	Armáda České republiky
AFCEA	Armed Forces Communications Electronics Association
BOZP	Bezpečnost a ochrana zdraví při práci
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
EU	Evropská unie
GDPR	General Data Protection Regulation
HZS	Hasičský záchranný sbor
ICT	Informační a komunikační technologie
NATO	North Atlantic Treaty Organization
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NCKO	Národní centrum kybernetických operací
NIS 1, NIS 2	Směrnice o kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PČR	Policie České republiky
RVP	Rámcový vzdělávací program

SEZNAM PŘÍLOH

Příloha P I:	Státní sektor rozhovor č. 1
Příloha P II:	Státní sektor rozhovor č. 2
Příloha P III:	Státní sektor rozhovor č. 3
Příloha P IV:	Státní sektor rozhovor č. 4
Příloha P V:	Státní sektor rozhovor č. 5
Příloha P VI:	Soukromý sektor rozhovor č. 1
Příloha P VII:	Soukromý sektor rozhovor č. 2
Příloha P VIII:	Soukromý sektor rozhovor č. 3
Příloha P IX:	Soukromý sektor rozhovor č. 4
Příloha P X:	Soukromý sektor rozhovor č. 5

PŘÍLOHA P I: STÁTNÍ SEKTOR ROZHOVOR Č. 1

Respondent č. 1 je členem Hasičského záchranného sboru České republiky v kraji Vysočina, kde pracuje na pozici hasič – technik chemické služby. U Hasičského záchranného systému působí 11 let. Respondent si doplňuje vzdělání na Univerzitě Tomáše Bati, kde studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 15. března 2025

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano pravidelně využívám výpočetní techniku a firemní systémy.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Ne, vstupní školení neproběhlo.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Školení se v naší organizaci vztahují pro všechny.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Ano, pravidelná školení probíhají 1x ročně.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Školení probíhají pomocí e-learningových kurzů. Osobně preferuji e-learning z důvodu pohodlí, úspory času a časové nezávislosti.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Ano, považuji.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Rozhodně ochrana dat.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Nesetkal jsem se s žádným takovým případem.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Ano, obrátil bych se na IT specialisty.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Ano, využívám je i v běžném životě.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Ano, absolvoval jsem více kurzů zaměřených na tuto problematiku. Například kurz od NÚKIB a kurz od firmy Avast.*“

PŘÍLOHA P II: STÁTNÍ SEKTOR ROZHOVOR Č. 2

Respondent č. 2 je členem Policie České republiky, kde pracuje jako policista při krajském ředitelství policie Zlínského kraje, Územní odbor Vsetín, kde vykonává funkci vrchního inspektora. Jeho hlavní náplní práce je zejména zpracování a prověřování přečinů a vedení zkráceného přípravného řízení, teda provádění úkonů v trestním řízení. U policie slouží osmým rokem a funkci vrchního komisaře zastává od roku 2023. Respondent si doplňuje vzdělání na Univerzitě Tomáše Bati, kde studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 15. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Výpočetní techniky pochopitelně ano, ovšem internet vůbec. Svoji práci vykonávám prostřednictvím intranetu, kde není k internetu vůbec přístup.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Žádné vstupní školení na kybernetickou bezpečnost jsem vyloženě neabsolvoval.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Školení zaměřené na kybernetickou bezpečnost jsou přístupná pro všechny zaměstnance prostřednictvím interního portálu e-learning, školení ale není povinné. Vybraní policisté, zpravidla ti prověřující trestné činy, ovšem absolvují školení na toto téma prezenčně, já jsem jeden z nich.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Školení probíhají pravidelně, tedy alespoň jednou ročně, ovšem vždy pro nové policisty určené k prověřování méně náročné kybernetické kriminality. Pravdou tedy je, že se policisté takového školení zúčastní v podstatě pouze jednou. Zde ovšem nemohu mluvit za kolegy zařazené přímo na Oddělení analytiky a kybernetické kriminality, tito se možná školení účastní častěji.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Jak jsem již říkal, formy jsou dostupné obě, ale na prezenční školení se nedostane každý. Já preferuji školení prezenční.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Ano.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Nevybavuji si, že by školení mělo nedostatky.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*S tímto jsem se nesetkal.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Ano, vím.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*To určitě ano, i když můj názor je takový, že průměrně inteligentní člověk, který alespoň v základech ovládá výpočetní techniku, by měl vědět, jak se zde má chovat.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Vyloženě z vlastní iniciativy ne, vše bylo v zaměstnání, i když jsem se sám aktivně zajímal o možnost zúčastnit se takového školení.*“

PŘÍLOHA P III: STÁTNÍ SEKTOR ROZHOVOR Č. 3

Respondent č. 3 je členem Armády České republiky, kde pracuje jako starší důstojník Skupiny virtuální simulace, Oddělení simulací taktické přípravy Skupiny simulačních a trenažerových technologií ve Vyškově. V armádě slouží desátým rokem. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 15. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano. Výpočetní techniku využívám prakticky denně. Internet pouze výjimečně.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*V rámci vstupního školení bylo seznámení s problematikou kybernetické bezpečnosti. Byly nám vysvětleny jednotlivé pojmy z této oblasti (phishing, malware atd.) a ukázaný příklady.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Je to povinné školení pro všechny vojáky i občanské zaměstnance.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Probíhají jednou ročně.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Forma školení je prezenční s lektorem. Časová dotace je 90 minut. Tato forma mi přijde jako dostatečná.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Myslím si, že vzhledem k tomu, že náš organizační celek má přímo specialistu na kybernetickou bezpečnost, který nám může kdykoliv poradit, tak pravidelné jednoroční školení jsou naprosto dostatečná.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: *„Mělo by se vycházet ze současných trendů a reflektovat aktuální hrozby.“*

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: *„Ne, s tímto jsme se nikdy nesetkal.“*

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: *„Ano, na výše zmíněného specialistu.“*

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: *„Ano, znalosti získané v rámci školení se hodí i do běžného života.“*

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: *„Ne, stačí mi informace z pracovního školení nebo internetu.“*

PŘÍLOHA P IV: STÁTNÍ SEKTOR ROZHOVOR Č. 4

Respondentka č. 4 působí v příspěvkové organizaci zřízené krajem Vysočina. Pracuje v Domově pro seniory, kde působí, jako zdravotní sestra již sedm let. Respondentka zvolila variantu anonymní. S respondentkou byl proveden online rozhovor dne 15. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano, využívám.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Ne, vstupní školení neproběhlo.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Školení v této oblasti se vztahují pro všechny zaměstnance.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Školení probíhají pravidelně, a to jednou ročně.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Školení probíhají prezenční formou s lektorem. Já osobně preferuji prezenční formy.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Ano, považuji.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta:

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Nesetkala jsem se s žádným incidentem.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Ano, na IT vyhrazenou osobu.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Určitě ano.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Neabsolvovala jsem z vlastní iniciativy žádný kurz.*“

PŘÍLOHA P V: STÁTNÍ SEKTOR ROZHOVOR Č. 5

Respondent č. 5 působí ve veřejné správě, kde vykonává pozici uvolněného starosty obce v kraji Vysočina. Na této pozici působí již 26 let. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 16. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano, výpočetní techniku a internet používám denně.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Nebylo. V době, kdy jsem nastupoval, tak takové školení ještě nebyly.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Školení se vztahují pro všechny.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Ano, probíhají nejdéle jedenkrát za dva roky, ale záleží, jak u koho.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*U nás probíhají obě formy školení. Já osobně preferuji prezenční školení.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Ano, ale pořád je co zlepšovat a být aktuální.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Opakování základních věcí týkajících se kybernetické bezpečnosti, nakládání s citlivými údaji a v poslední době využití AI.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Zatím jsem se naštěstí s takovým případem nesetkal.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Ano, vím, obrátil bych se na IT.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Samozřejmě ano.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Ano, absolvoval jsem prezenční školení a e-learningový kurz na Institutu pro veřejnou správu v Praze. Kurzy byly zaměřené na kyberbezpečnost. Dále jsem absolvoval kurz od firmy Eset, také jsem se účastnil kurzu od Agentury Boya. Další informace čerpám z portálu NÚKIB.*“

PŘÍLOHA P VI: SOUKROMÝ SEKTOR ROZHOVOR Č. 1

Respondentka č. 1 pracuje na pozici účetní v české společnosti zabývající se prodejem a servisem elektromotorů. Respondentka na této pozici působí již 23 let. Respondentka zvolila variantu anonymní S respondentkou byl proveden osobní rozhovor dne 16. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano, denně využívám výpočetní techniku a internet.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*V době mého nástupu tyto školení nebyly.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Školení u nás vůbec neprobíhá.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Ne neprobíhají.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Žádnou formou neprobíhají.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Nepovažuji to rozhodně za dostatečné v dnešní době. Školení by mělo rozhodně probíhat.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Ochrana osobních údajů a dat.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Nesetkala.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Na externího IT specialistu.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Ne, protože žádné školení neproběhlo.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Ne.*“

PŘÍLOHA P VII: SOUKROMÝ SEKTOR ROZHOVOR Č. 2

Respondentka č. 2 pracuje v české společnosti zabývající se prodejem střešních materiálů. Respondentka působí ve společnosti, jako vedoucí pobočky. Ve společnosti působí již 15 let. Respondentka zvolila variantu anonymní. S respondentkou byl proveden osobní rozhovor dne 16. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondentka: „*Ano, naše společnost pracuje v programu K2 a jsme obchodní firma, takže e-mailová komunikace patří k dennodenní náplni práce.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondentka: „*Před patnácti lety se toto téma neřešilo.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondentka: „*Školení absolvují všichni zaměstnanci, kteří pracují s počítači. Skladníci školení neabsolvují.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondentka: „*Školení probíhají dvakrát za rok.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondentka: „*Školení probíhá jak formou prezentace, kterou nás provedl interní IT pracovník, tak máme toto téma i v e-learningových kurzech. Já osobně preferuji prezenční školení.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondentka: „*Naše IT oddělení udělalo několik kroků k ochraně naší společnosti, např. sledovač v telefonu proti stáhnutí nežádoucích souborů, probíhají phishingové testy. Myslím si, že to není dostačující. V běžném provozu nejsme schopni být vždy ve střehu.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Kybernetika všeobecně, hlavně, jak chránit osobní údaje.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*U nás naštěstí ne. Vím o případech konkurence a z řad dodavatelů, kde následky jsou hrozivé někdy nenahraditelné.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Ano, na naše IT oddělení.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Spíše ne.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Ne.*“

PŘÍLOHA P VIII: SOUKROMÝ SEKTOR ROZHOVOR Č. 3

Respondent č. 3 pracuje ve společnosti na pozici obchodního zástupce. Tuto pozici vykonává devět let. Respondent zvolil variantu anonymní. S respondentem byl proveden osobní rozhovor dne 17. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano využívám dennodenně.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Nebylo.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Neprobíhá v této oblasti žádné školení.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Neprobíhají.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Školení neprobíhají, ale kdyby preferoval bych prezenční.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Rozhodně v dnešní době nedostatečná.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Kdyby školení probíhalo, tak rozhodně ochrana osobních dat a příklady jednotlivých útoků.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*O žádném případě nevím.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Na ajťáka.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Nevyžívám.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Neabsolvoval jsem žádná školení.*“

PŘÍLOHA P IX: SOUKROMÝ SEKTOR ROZHOVOR Č. 4

Respondent č. 4 působí ve firmě zabývající se autodopravou sypkých hmot, ukládkou a recyklací stavebních odpadů. Respondent působí na pozici Instruktora dopravy v segmentu stavitelství. V této firmě působí rok a půl. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 17. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano, výpočetní techniku s připojením na síť využívám a potřebuji denně.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Neproběhlo žádné vstupní školení.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Bez rozdílu pracovní pozice nebo zařazení.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Neprobíhají vůbec.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Žádnou, školení nemáme.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Úplně ne, myslím si, že by školení měla aspoň jednou za čas probíhat.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Zabezpečení účtů a ochrana dat.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Doposud jsem se s ničím takovým nesetkal.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Správce sítě – IT služby.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Určitě bych je v běžném životě využil.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Neabsolvoval jsem žádné takové školení.*“

PŘÍLOHA P X: SOUKROMÝ SEKTOR ROZHOVOR Č. 5

Respondent č. 5 působí ve společnosti zabývající se prodejem nových a ojetých vozů, jako servisní technik. Tuto pozici zastává devět a půl roku. Respondent zvolil variantu anonymní. S respondentem byl proveden online rozhovor dne 17. března 2025.

1. Vyžaduje Vaše pracovní zařazení pravidelné využívání výpočetní techniky?

Odpověď respondenta: „*Ano.*“

2. Bylo součástí Vašeho vstupního školení při nástupu do organizace školení kybernetické bezpečnosti? Pokud ano, co školení zahrnovalo?

Odpověď respondenta: „*Ano, seznámení se základními pojmy, formami, bezpečností, jak se chovat v digitálním světě a jak snížit rizika.*“

3. Vztahují se školení v oblasti kybernetické bezpečnosti ve Vaší organizaci pro všechny nebo pouze pro určité skupiny zaměstnanců?

Odpověď respondenta: „*Vztahují se pro všechny zaměstnance, kteří využívají výpočetní techniku.*“

4. Probíhají ve Vaší organizaci pravidelná školení kybernetické a informační bezpečnosti? Pokud ano, jak často?

Odpověď respondenta: „*Ano, cca 1-2krát ročně.*“

5. Jakou formou školení probíhají? Prezenční školení s lektorem nebo e-learningový kurz? Jakou formu preferujete?

Odpověď respondenta: „*Probíhají formou e-learningového kurzu s výstupním testem. Preferuji e-learningové kurzy.*“

6. Považujete úroveň vzdělávání v oblasti kybernetické a informační bezpečnosti ve Vaší organizaci za dostatečnou?

Odpověď respondenta: „*Ano.*“

7. Jaká témata by podle Vás měla být ve vzdělávacích programech více akcentována?

Odpověď respondenta: „*Jak se bezpečně pohybovat v digitálním světě, procesy, technologické řešení a jak bránit síť před digitálními útoky.*“

8. Setkal/a jste se ve své organizaci s případem, kdy nedostatečné školení v této oblasti vedlo ke kybernetickému incidentu? Pokud ano, jaká byla následná opatření?

Odpověď respondenta: „*Ne.*“

9. Víte, na koho se v případě incidentu obrátit?

Odpověď respondenta: „*Máme vyhrazené osoby, včetně IT koordinátora.*“

10. Máte pocit, že znalosti získané během školení ve výše zmiňované oblasti využíváte i mimo pracovní prostředí?

Odpověď respondenta: „*Spíše ne, v digitálním světě se umím pohybovat.*“

11. Absolvoval/a jste z vlastní iniciativy nějaký kurz kybernetické, informační bezpečnosti?

Odpověď respondenta: „*Ano.*“