Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva

Bc. Kristýna Suchorová

Diplomová práce
2024

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: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Kristýna Suchorová**
Osobní číslo:	**L22387**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do dané problematiky.
2. Seznamte se s významnými kybernetickými bezpečnostními incidenty v České republice i v zahraničí.
3. Proveďte analýzu současného stavu vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva České republiky.
4. Na základě provedené analýzy navrhněte opatření ke zvýšení úrovně vzdělávání v oblasti kybernetické bezpečnosti.

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

Seznam doporučené literatury:

1. KREMLING, Janine. *Cyberspace, cybersecurity and cybercrime*. Los Angeles: SAGE Publications, 2017. ISBN 978-1-5063--4725-7.
2. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru.* Brno: CERM, akademické nakladatelství,2021. ISBN 978-80-7623-068-2.
3. SMEJKAL, Vladimír a Tomáš SOKOL a Jindřich KOPL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **1. prosince 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou 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 autorského zákona mohu užít své dílo – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 26.4.2024

Jméno a příjmení studenta: Bc. Kristýna Suchorová

.....
podpis studenta

ABSTRAKT

Diplomová práce se zaměřuje na problematiku vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Diplomová práce je rozdělena do dvou částí, které na sebe navazují. V první části, teoretické, je proveden rozbor právních norem v rámci řešené oblasti, jsou vysvětleny vybrané pojmy v oblasti kybernetické bezpečnosti, včetně institucí, které se zabývají kybernetickou bezpečností v České republice. Dále obsahuje teoretická část nejvýznamnější kybernetické bezpečnostní incidenty v České republice i v zahraničí.

Praktická část diplomové práce je zaměřena na zhodnocení aktuálního stavu vzdělávání v oblasti kybernetické bezpečnosti v České republice a v subjektech ochrany obyvatelstva. Metodou pro analýzu dat v rámci subjektů ochrany obyvatelstva je strukturovaný rozhovor. Součástí praktické části je rovněž analýza vybraných kurzů kybernetické bezpečnosti v České republice s výběrem optimální varianty kurzu. Výsledkem praktické části je návrh opatření ke zlepšení úrovně vzdělávání v subjektech ochrany obyvatelstva.

Klíčová slova: bezpečnost informací, informace, kybernetická bezpečnost, ochrana obyvatelstva, vzdělávání.

ABSTRACT

This diploma thesis focuses on the issue of cybersecurity education in population protection subjects. The thesis is divided into two parts, which follow each other. The first part, theoretical, provides an analysis of legal norms within the addressed area, explains selected concepts in the field of cybersecurity, including institutions dealing with cybersecurity in the Czech Republic. The theoretical part also contains the most significant cybersecurity incidents in the Czech Republic and abroad.

The practical part of the thesis is aimed at evaluating the current state of cybersecurity education in the Czech Republic and in subjects of population protection. The method for data analysis within the population protection subjects is structured interview. The practical part also includes an analysis of selected cybersecurity courses in the Czech Republic with the selection of the optimal course option. The result of the practical part is a draft for improving the level of education in population protection subjects.

Keywords: cybersecurity, education, information, information security, population protection.

Tímto bych ráda poděkovala vedoucímu mé diplomové práce, panu Ing. Petru Svobodovi Ph.D., za čas, který věnoval vedení mé diplomové práce a za poskytnutí cenných rad.

Děkuji rovněž mé rodině a přátelům, kteří mě podporovali po celou dobu mého studia.

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

OBSAH

ÚVOD

Dnešní digitálně orientovaná doba přinesla do našeho světa nebývalé možnosti a příležitosti spolu s významnými výzvami, zejména v oblasti kybernetické bezpečnosti. Den za dnem jsou subjekty ochrany obyvatelstva stále náchylnější ke kybernetickým hrozbám. S tím, jak se prohlubuje naše závislost na digitální infrastruktuře, roste i potenciál kybernetických útočníků využívat naše zranitelnosti a šířit chaos v rámci organizací.

Vzdělávání v oblasti kybernetické bezpečnosti představuje širokospektrální oblast s řadou složitostí a překážek. Tváří v tvář dynamickému prostředí hrozeb definovaných sofistikovanými protivníky se konvenční bezpečnostní metody ukazují jako nedostatečné. Důraz na vzdělání tedy nelze podceňovat. Předáváním znalostí a dovedností, které jsou nezbytné k pochopení principů kybernetické bezpečnosti, včetně identifikace hrozeb, může dojít k posílení naší odolnosti vůči stále sofistikovanější kybernetickým hrozbám.

Pro návrh řešení ke zlepšení současného stavu vzdělávání v oblasti kybernetické bezpečnosti je nezbytné analyzovat obsah vybraných vzdělávacích kurzů v řešené oblasti, posoudit současný stav v daných subjektech a nabídnout potencionální cesty, které inovují současné vzdělávací metodiky.

Nakonec cíl nás všech je zcela jasný: podniknout takové kroky, které posílí naši odolnost vůči hrozbám v kyberprostoru. Díky prosazování komplexního a proaktivního přístupu ke vzdělávání poskytneme všem zaměstnancům potřebné znalosti a dovednosti, zvýšíme jejich povědomí o dané problematice, čímž jim umožníme snazší orientaci v rámci kyberprostoru. Každé z těchto opatření nám tak dláždí cestu k bezpečnější budoucnosti pro každého z nás. Jelikož získané znalosti a dovednosti můžeme využít nejen v pracovním, ale i osobním životě.

CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Cílem diplomové práce je navrhnout opatření ke zlepšení současného stavu vzdělávání v oblasti kybernetické bezpečnosti v subjektu ochrany obyvatelstva. K tomu, aby mohlo dojít k naplnění cíle práce, je nutné si stanovit několik dílčích cílů:

- Pojednat o základních teoretických východiscích práce.
- Seznámit se s vybranými kybernetickými bezpečnostními incidenty v České republice a zahraničí.
- Analyzovat obsah vybraných vzdělávacích kurzů v České republice, provést komparaci a určit jejich vhodnost pro předmětnou oblast.
- Realizovat strukturované rozhovory se subjekty ochrany obyvatelstva s cílem zjištění současného stavu vzdělávání v oblasti kybernetické bezpečnosti a následnou identifikací případných nedostatků.
- Identifikovat nové postupy vzdělávání v oblasti kybernetické bezpečnosti.

Je potřeba provést rozbor dané problematiky za použití rešerše odborné literatury sloužící k objasnění vybraných pojmů zkoumané oblasti a výkladu legislativních norem, předpisů v oblasti kybernetické bezpečnosti. K výkladu právního rámce řešené problematiky budou využity vybrané legislativní dokumenty, normy a evropské směrnice. Pro kvalitní teoretický vstup do dané problematiky budou představeny české organizace, které se zabývají problematikou kybernetické bezpečnosti.

Pro výběr optimální varianty kurzu vzdělávání v oblasti kybernetické bezpečnosti je využita kvantitativní analýza vícekriteriálního rozhodování za využití zjednodušené bodovací metody se stanovením vah a určením pořadí. Pro zhodnocení aktuálního stavu vzdělávání v subjektech ochrany obyvatelstva je využito kvalitativní metody ve formě strukturovaných rozhovorů se zástupci z řad jednotlivých subjektů ochrany obyvatelstva. Pro posouzení stavu kybernetické bezpečnosti je využita Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022 a měsíční reporty o stavu kybernetické bezpečnosti za období listopad 2023 až únor 2024, obojí vydáno cestou Národního úřadu pro kybernetickou a informační bezpečnost.

V návaznosti na provedenou analýzu navrhnout opatření pro zvýšení úrovně vzdělávání v oblasti kybernetické bezpečnosti v subjektu ochrany obyvatelstva.

I. TEORETICKÁ ČÁST

1 LEGISLATIVA A ORGANIZACE

Následující kapitola diplomové práce bude věnována základním legislativním dokumentům, normám a směrnicím vztahujícím se k problematice kybernetické bezpečnosti. Níže uvedené dokumenty slouží nejen k ochraně jednotlivců, ale i k zabezpečení provozuschopnosti organizací. Je tedy žádoucí, aby lidé byli s touto legislativou seznámeni, a to tak, že díky této znalosti může být zvýšena úroveň jejich bezpečí. Zároveň jako u všech věcí je potřeba umět s danými nástroji správně zacházet a využívat je ke svému prospěchu a nikoli k neprospěchu jiných osob.

Druhá polovina uvedené kapitoly představuje vybrané organizace, které se na území České republiky zabývají kybernetickou bezpečností.

1.1 Legislativní dokumenty, normy a směrnice vztahující se k dané problematice

Následující kapitola je věnována nejvýznamnějším legislativním dokumentům na území České republiky ve vztahu k problematice kybernetické bezpečnosti.

1.1.1 Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., který upřesňuje zavedené nařízení Evropské unie (dále jen „EU“) o General Data Protection Regulation (dále jen „GDPR“) za pomoci zpracování Směrnice EU č. 2016/68O ze dne 26. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a Nařízení EU 2016/679, známé pod názvem nařízení GDPR. (Česko, 2019)

V rámci tohoto zákona jsou definována oprávnění ke zpracování a evidenci osobních údajů fyzických osob, které se nezabývají činnostmi soukromého nebo výlučně osobního charakteru. Rovněž je v tomto zákoně stanovena povinnost mlčenlivosti osob, které osobní údaje zpracovávají. Kromě toho zákon také stanovuje požadovaná opatření pro zabezpečení osobních údajů a předepisuje sankce, které hrozí za porušení tohoto zákona. (Česko, 2019)

1.1.2 Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti

V dnešní době, kdy je svět vystaven hrozbám pro vnitřní i vnější bezpečnostní prostředí získává ochrana utajovaných informací stále větší význam a míru důležitosti. V současnosti je potřeba krom správného pochopení informací, které je ve světe dezinformací čím dál více náročné, umět informace rozdělit dle jejich povahy citlivost a zvolit adekvátní míru ochrany.

Pro správné pochopení důležitosti ochrany informací je tak nezbytností každého z nás znát aktuální legislativu a také se jí řídit.

Zákon č. 412/2005 Sb. nám stanovuje, které informace spadají do utajovaných informací a jak utajované informace dělíme. Mimo to určuje druhy zajištění ochrany utajovaných informací. (Česko, 2005 a)

Informace můžeme dle povahy jejich ochrany rozdělit do několika skupin, a to (Česko, 2005 a):

- **Utajované informace.**
- **Určené neutajované informace.**
- **Informace volně publikovatelné na internetu.**

První dvě z výše uvedených skupin můžeme ještě podrobněji rozdělit. V oblasti utajovaných informací existuje rozdělení dle působnosti na (Česko, 2005 a; European Council, 2022; NATO, 2023):

- **Národní** – vyhrazené, důvěrné, tajné, přísně tajné.
- **Národní (zvláštní režim)** – vyhrazené krypto, důvěrné krypto, tajné krypto, přísně tajné krypto.
- **NATO** – nato restricted, nato confidential, nato secret, nato cosmic top secret.
- **EU** – eu restricted, eu confidential, eu secret, eu top secret.

Určené neutajované informace můžeme rozdělit do následujících tří skupin (Česko, 2005 a):

- **Osobní údaje** – citlivé osobní údaje.
- **Důvěrné informace** – veřejné zakázky, zájmy zaměstnavatele a zaměstnanců, NATO UNCLASSIFIED, EU RESTRICTED.
- **Neveřejné informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím** – trestní řízení, soudy, zpravodajské služby, obchodní tajemství, mlčenlivosti. (Česko, 1999)

Utajovanou informací se dle zákona č. 412/2005 Sb. rozumí „*informace v jakékoliv podobě, zaznamenaná na jakémkoliv nosiči, která musí být v souladu s výše uvedeným zákonem označená a jejichž vyzrazení nebo zneužití může způsobit újmu zájmu ČR nebo jejichž vyzrazení či zneužití může být pro tento zájem nevýhodné.*“ (Česko, 2005 a)

Zpracovatelem seznamu utajovaných informací je dle nařízení vlády č. 522/2005 Sb. Národní bezpečnostní úřad (dále jen „NBÚ“). (Česko, 2005 b)

Dle újmy vzniklé v důsledku vyzrazení můžeme utajované informace rozdělit do čtyř skupin (Česko, 2005 a):

- **Vyhrazené** – vyzrazení nebo zneužití může být nevýhodné pro zájmy ČR.
- **Důvěrné** – vyzrazení nebo zneužití může způsobit prostou újmu zájmům ČR.
- **Tajné** – vyzrazení nebo zneužití může způsobit vážnou újmu zájmům ČR.
- **Přísně tajné** – vyzrazení nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR.

V rámci zajištění ochrany utajovaných informací evidujeme níže uvedených šest úrovní bezpečnosti (Česko, 2005 a):

- **Personální bezpečnost** – hlavní důraz je kladen na výběr osob, které mají přístup k utajovaným informacím, ověřování podmínek pro přístup těchto osob k utajovaným informacím, výchovu a ochranu osob a povinnost osob majících přístup k utajovaným informacím účastnit se jedenkrát ročně školení.
- **Bezpečnost informačních nebo komunikačních systémů** – jedná se o systém opatření s cílem zajištění důvěrnosti, integrity a dostupnosti utajovaných informací, odpovědnost správy a uživatele informačního/komunikačního systému za jejich činnost v daném systému.
- **Kryptografická ochrana** – zavádí systém opatření, která slouží k ochraně utajovaných informací za použití kryptografických metod a materiálů při zpracování, přenosu a ukládání utajovaných informací.
- **Fyzická bezpečnost** – klade důraz na opatření, která slouží k zamezení nebo ztížení přístupu neoprávněných osob k utajovaným informacím, rovněž se zaměřuje na zamezení pokusu o přístup či zaznamenání utajovaných informací v případě neoprávněného vniknutí do objektu.
- **Administrativní bezpečnost** – jedná se o systém opatření, který mapuje proces tvorby, příjmu, evidence, zpracování, odesílání, přepravě, přenášení, ukládání, skartačního řízení, archivace a jiného případného nakládání s utajovanými informacemi.

- **Průmyslová bezpečnost** – zde je uplatňován systém opatření, který zkoumá a ověřuje podmínky pro přístup podnikatele k utajovaným informacím a sleduje nakládání s těmito informacemi.

Ve spojitosti se zákonem č. 412/2005 Sb. hraje důležitou roli i Národní úřad pro kybernetickou a informační bezpečnost, který je dle § 34 tohoto zákona určen jako oprávněný orgán pro provádění certifikace informačních systémů, které nakládají s utajovanými informacemi. Tyto informační systémy musí být schváleny odpovědnou osobou, která má za povinnost o tomto kroku NÚKIB informovat do 30 dnů. Požadavky na informační systémy se liší dle stupně utajení informací na nich zpracovávaných. Provádění certifikace je realizováno skrze Odbor bezpečnosti informačních a komunikačních technologií NÚKIB. (NBÚ, 2017)

Za právní normu spojenou s ochranou utajovaných informací můžeme označit zákon č. 40/2009 Sb., trestní zákoník, který nám upřesňuje skutkovou podstatu trestných činů, kterých se můžeme v souvislosti s ochranou utajovaných informací dopustit. Mezi tyto činy řadíme především vyzvědačství, ohrožení utajované informace a ohrožení utajované informace z nedbalosti. (Česko, 2009)

1.1.3 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. je přesně tou legislativní normou, která v České republice v oblasti kybernetické bezpečnosti chyběla. V souvislosti s rozvojem dnešního světa a moderních technologií bylo nutné vytvořit zákon, který bude tento pokrok na poli informačních a komunikačních technologií reflektovat. Mezi impulzy pro vznik zákona o kybernetické bezpečnosti můžeme zařadit požadavky organizací, kterých je Česká republika členem, a to především Severoatlantické aliance (dále jen „NATO“) a EU, posledním a rozhodně neméně důležitým impulzem pro vznik byl vzrůstající počet kybernetických útoků, především v roce 2013. (Sedlák a Konečný, 2021)

V tomto případě se tedy jedná o právní normu, která se zabývá působností správních orgánů v oblasti kybernetické bezpečnosti, rovněž řeší práva a povinnosti osob. Zákon o kybernetické bezpečnosti (dále jen „ZoKB“) reflektuje předpis EU – konkrétně se jedná o Směrnici NIS vztahující se k oblasti kybernetické bezpečnosti. (Česko, 2014 a)

Zákon rovněž popisuje rozdíl mezi kybernetickou bezpečnostní událostí, kterou můžeme vnímat jako hrozbu, která může mít za následek narušení bezpečnosti a celistvosti informační sítě, kdy, pokud se hrozba již projeví, hovoříme o kybernetickém bezpečnostním

incidentu. Pro laickou veřejnost můžeme definici těchto dvou pojmů zobecnit následujícím způsobem. Kybernetická bezpečnostní událost může být chápána jako „něco, co nám hrozí“ a musí to být detekováno. Oproti tomu kybernetický bezpečnostní incident lze chápat jako „něco, co už proběhlo“ a musí to být nahlášeno. (Česko, 2014 a)

Dle své působnosti jsou subjekty povinny hlásit kybernetické bezpečnostní incidenty dohledovým pracovištím. Do dohledových pracovišť řadíme národní CERT (Computer Emergency Response Team) a vládní CERT (též známý pod názvem CSIRT, Computer Security Incident Response Team), rovněž do této skupiny patří i armádní CIRC (Computer Incident Response Capabilty). V rámci svých povinností se dané instituce podílí na řešení kybernetických bezpečnostních incidentů, věnují se oblasti vzdělávání a prevence, provádí vyhodnocení získaných zkušení při řešení incidentů za účelem zvýšení efektivity a rychlosti reakce při dalších kybernetických bezpečnostních incidentech. (Sedlák a Konečný, 2021)

V současné době probíhá tvorba nového zákona o kybernetické bezpečnosti z důvodu začlenění aktualizované směrnice NIS 2. Novela ZoKB přinese především přísnější pravidla v systému řízení kybernetické bezpečnosti, kdy bude nově ze zákona povinná identifikace a evidence všech primárních aktiv v rámci dané společnosti, důkladnější systém řízení rizik a s tím spojená aktualizace bezpečnostní politiky daného podniku. Dále bude kladen větší důraz na osvětu a vzdělávání v oblasti kybernetické bezpečnosti, vzájemné sdílení informací v oblasti kybernetických hrozeb a zranitelností, tvorbu záloh a dodržování pokynů Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Všechny tyto změny musí být v novele ZoKB obsaženy nejpozději do 18. října letošního roku, i když je reálnější očekávat tyto změny na konci roku 2025. (ESET, 2024)

1.1.4 Vyhláška o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti má za úkol zapracovat do českého právního systému Směrnici Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016, známou též pod názvem NIS 1. Toto vyhláška se týká informačních a komunikačních systémů, prvků kritické informační infrastruktury, významných informačních systémů a také poskytovatelů základních služeb. Tato vyhláška řeší kybernetickou bezpečnost řekněme po praktické stránce věci, kdy dotčeným osobám upřesňuje *„obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení*

o provedení reaktivního opatření a jeho výsledku, vzor oznámení kontaktních údajů a jeho formu a způsob likvidace dat, provozních údajů, informací a jejich kopií.“ (Česko, 2018)

Součástí vyhlášky jsou i přílohy, kdy v první příloze můžeme nalézt stupnici pro hodnocení důvěrnosti, integrity a dostupnosti (dělení na nízkou, střední, vysokou a kritickou úroveň). Každá stupnice obsahuje obecný popis aktiv a příklady požadavků na jejich ochranu. V rámci druhé přílohy je řešeno hodnocení rizik, kdy krom základních informací k tomu hodnocení můžeme nalézt stupnici pro hodnocení hrozeb, jejíž součástí u každé úrovně je i doba předpokládané realizace hrozby. V příloze č. 2 této vyhlášky rovněž nalezneme stupnici pro hodnocení zranitelnosti a stupnici pro hodnocení rizik dle jejich míry akceptovatelnosti. Následující přílohy jsou věnovány příkladům zranitelností a hrozeb, likvidaci dat a příkladům likvidace dat dle míry důvěrnosti aktiv, bezpečnostní dokumentaci a fyzické bezpečnosti. Součástí přílohové části je rovněž i vzor formuláře pro hlášení kontaktních údajů na Národní centrum kybernetické bezpečnosti (dále jen „NCKB“). (Česko, 2018)

Důležitou částí této vyhlášky je § 9, který hovoří o povinnosti provádění školení a tvorbě bezpečnostního povědomí u zaměstnanců. Záznamy o provádění těchto aktivit musí mít uloženy určená odpovědná osoba. Tyto záznamy obsahují obsah školení a seznam osob, jež toto školení absolvovaly. (Česko, 2018)

1.1.5 Vyhláška o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích vstoupila v platnost dne 19. prosince 2014. Předmětem této vyhlášky je stanovení významných informačních systémů a kritérií pro určení těchto systémů. (Česko, 2014 b)

V rámci aktualizace legislativy byla v roce 2020 přijata novela, která více konkretizovala kritéria pro určení významnosti informačních systémů. (NÚKIB, 2020)

1.1.6 Normy ISO/IEC 27000

V níže uvedené kapitole budou blíže popsány normy ISO/IEC 27000 jakožto základní normy z oblasti kybernetické bezpečnosti.

Normy ISO/IEC 27000

Mezinárodní organizace pro normalizaci (dále jen „ISO“) a Mezinárodní elektrotechnická komise (IEC) vytváří celosvětový systém normalizace pomocí jimi vydávaných norem.

Organizace ISO sídlí v Ženevě a byla založena 23. února 1947. Prvním standardem této organizace byla norma ISO/R 1:1951. V současné době organizace sdružuje 170 národních normalizačních orgánů. (ISO, 2021)

Základní strukturu společnosti tvoří Valná hromada, která je nejvyšším orgánem organizace a setkává se každý rok, setkání se účastní ředitelé a členové organizace. Dalším orgánem je Rada ISO, kterou můžeme charakterizovat jako hlavní řídící orgán, jenž podléhá valnému shromáždění. Schází se třikrát ročně a tvoří ji 20 členských orgánů, úředníků a předsedů výborů. Členství v Radě je otevřené všem členským orgánům a funguje na principu rotace členů. Další součástí je Technická správní rada, která je odpovědná za technické komise, které mají na starost vývoj norem. Financování společnosti je zajištěno dvěma hlavními způsoby – výběrem členských poplatků, které hradí všichni členové, a prodejem norem. V čele společnosti stojí prezident ISO – Sung Hwan Cho. (ISO, 2023)

Do vydávání těchto norem jsou zapojeny i skrze své pracovní komise národní organizace zemí, jež jsou těchto organizací členové. V rámci oblasti informačních technologií byla zřízena společná komise pod názvem ISO/IEC JTC 1. (Sedlák a Konečný, 2021)

Zástupcem za Českou republiku je Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (dále jen „ÚNMZ“), který spadá do působnosti Ministerstva průmyslu a obchodu. Úkolem ÚNMZ je především zabezpečení úkolů plynoucích z příslušné legislativy ČR a EU. Činnosti spojené s tvorbou a distribucí norem zabezpečuje od 1. 1. 2018 Česká agentura pro standardizaci (dále jen „ČAS“). (Sedlák a Konečný, 2021)

Při procesu přebírání norem do českého prostředí došlo k přidání označení českých technických norem pomocí zkratky ČSN, kdy název dané normy je následně ve formátu ČSN + název přejímaného dokumentu. (Peková, 2020)

Pro skupinu norem ohledně bezpečnosti informací byla vytvořena skupina norem ISO 27000:

- **ČSN EN ISO/IEC 27000** Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Přehled a slovník: jedná se o základní normu z řady norem ISO 27000, v této normě nalezneme definice základních pojmů a terminologický slovník pro všechny normy z této série. (ČSN EN ISO/IEC 27000, 2020)

- **ČSN EN ISO/IEC 27001** Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky: tato norma se věnuje stanovení požadavků pro řízení bezpečnosti informací v organizaci, tak aby byla zabezpečena ochrana citlivých informací, norma klade důraz na plánování, realizaci, ověření a zlepšování postupů v rámci řízení informační bezpečnosti. (ČSN EN ISO/IEC 27001, 2014)
- **ČSN EN ISO/IEC 27002** Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření kybernetické bezpečnosti: nová aktualizovaná norma dělí opatření do 4 hlavních kategorií (organizační opatření, personální opatření, technologická opatření a fyzická opatření), kde v každé kategorii opatření můžeme nalézt nové ovládací prvky. (ČSN EN ISO/IEC 27002, 2022)
- **ČSN EN ISO/IEC 27003** Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Pokyny: v dané normě se nachází detailní pokyny pro zavedení ISMS. (ČSN EN ISO/IEC 27003, 2018)
- **ČSN EN ISO/IEC 27004** Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení: hlavním cílem směrnice je pomoc organizaci při splnění požadavků normy ČSN EN ISO/IEC 27001, rovněž norma pomáhá organizacím nastavením postupu hodnocení výkonnosti bezpečnosti informací. (ČSN EN ISO/IEC 27004, 2018)

1.1.7 Směrnice NIS 1

Směrnice NIS 1, celým názvem *„Směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii“* byla zapracována do našeho právního systému novelizace ZoKB. (EU, 2016)

Transpoziční lhůta pro zapracování Směrnice NIS byla stanovena do 9. května 2018. Mnohé povinnosti plynoucí ze Směrnice NIS 1 byly již zapracovány do původního ZoKB a jeho prováděcích předpisů, zbývající požadavky byly zapracovány v novele ZoKB č.205/2017 Sb. a nabyly účinnosti dne 1. srpna 2017. (NÚKIB, 2023)

Duračinská (2016) ve svém článku „Co přináší nová směrnice EU o síťové a informační bezpečnosti?“ charakterizuje Směrnici NIS 1 nejen jako ucelený, ale především unifikovaný dokument pro všechny členské státy EU, kdy před vydáním Směrnice měly pouze některé státy vyvinutou legislativu v oblasti kybernetické a informační bezpečnosti. Cílem NIS 1 je především ujednotit požadavky, které budou na všechny členské státy kladeny. Jak sama autorka ve svém článku tvrdí, bylo jen otázkou času, kdy se objeví oficiální doporučení ze strany EU v rámci řešení problematiky kybernetické bezpečnosti. (Duričanská, 2016)

Povinnosti plynoucí ze Směrnice můžeme rozdělit dle charakteru na organizační a legislativní, a dále povinnosti, které se vztahují k povinným subjektům, které jsou v rámci této Směrnice definovány. (Duričanská, 2016)

Mezi hlavní povinnosti organizačního a legislativního charakteru můžeme zařadit následující (Duričanská, 2016):

- **Přijetí strategie** – každému členskému státu EU je nově uložena povinnost mít národní strategii v oblasti kybernetické a informační bezpečnosti, kde budou zapracovány povinnosti a opatření plynoucí z NIS 1. Součástí tohoto dokumentu budou rovněž strategické cíle a konkrétní opatření, které daný stát v nejbližších letech přijme.
- **Zřízení centrálního orgánu** – v rámci ČR vznikl dne 1. srpna 2017 Národní úřad pro kybernetickou a informační bezpečnost, který se stal novým správním orgánem, kdy část svých kompetencí převzal od NBÚ.
- **Povinnost zřídit CSIRT tým** – na základě této povinnosti bylo zřízeno Ústřední kontaktní místo a CSIRT tým. Tyto týmy by měly v rámci ČR pokrýt poskytovatele základních služeb.
- **Ustanovuje Skupinu pro spolupráci a Skupinu CSIRT** – Skupina pro spolupráci má spíše strategický charakter a je tvořena především zástupci centrálních orgánů. Skupina CSIRT má za úkol koordinovat spolupráci napříč CSIRT týmy v rámci ČR.

Směrnice cílí především na následující dvě skupiny (Duričanská, 2016):

- **Provozovatelé základních služeb** – jedná se o provozovatele (soukromé či veřejné) základních služeb, kteří spadají do následujících kategorií odvětví: energetika, letecká doprava, železniční doprava, vodní doprava, bankovnictví, zdravotnictví, dodávky a rozvody pitné vody, bankovnictví, digitální infrastruktura a veřejná správa.
- **Provozovatelé digitálních služeb** – dle Směrnice NIS je poskytovatelem služby právnická osoba, která poskytuje služby v oblasti on-line tržiště, internetového vyhledávače a cloud computingu.

Provozovatel základních služeb je soukromý nebo veřejný subjekt, který poskytuje službu, kterou lze chápat jako základní z pohledu zachování kritických společenských nebo ekonomických činností. Zároveň pro poskytování dané služby je nezbytná funkčnost komunikačních a informačních technologií, kdy v případě narušení z důvodu kybernetického bezpečnostního incidentu může dojít k přerušení poskytování této služby. (Sedlák a Konečný, 2021)

1.1.8 Směrnice NIS 2

V návaznosti na dynamický vývoj aktuální bezpečnostní situace, která se dotýká i kybernetické a informační bezpečnosti, bylo potřeba aktualizovat stávající normy a přizpůsobit je současnému prostředí. Dalším důvodem pro vznik směrnice byl i čím dál vyšší výskyt kybernetických hrozeb a incidentů. (NÚKIB, 2022)

Nová Směrnice NIS 2 byla publikována 27. prosince 2022 v Ústředním věstníku Evropské unie, v platnost tato směrnice vstoupila 16. ledna 2023. Oproti předchozí NIS 1 věnuje nová směrnice větší pozornost zabezpečení v rámci oblasti kybernetické bezpečnosti. V procesu zavádění je stanovena lhůta 21 měsíců, během kterých musí být povinnosti a doporučení plynoucí z této směrnice začleněny do legislativy členských států EU. V případě ČR se jedná o zavedení nových povinností do 16. října 2024. (NÚKIB, 2022)

V souvislosti s NIS 2 je více než nezbytné provedení novely ZoKB, který bude požadavky této směrnice a zároveň poznatky získané v rámci činnosti NÚKIBu reflektovat. (NÚKIB, 2022)

V rámci nové NIS 2 bude v každém členském státě EU z týmu CERT vybrán jeden koordinátor, který bude mít za úkol zveřejňování zranitelností, díky čemuž bude

zjednodušena komunikace mezi fyzickou (dále jen „FO“) nebo právnickou osobou (dále jen „PO“) a poskytovatelem informačních a komunikačních služeb. Na stupni EU bude agenturou ENISA vytvořena Evropská databáze zranitelností. Díky této databázi bude možná větší informovanost členských států v oblasti možných kybernetických hrozeb. Členské státy také budou mít lepší podmínky pro přípravu na možnou hrozbu. (NÚKIB, 2022 b)

Další změnou bude rozšíření počtu organizací, které se budou muset novou směrnicí řídit. V rámci odhadů hovoříme o celkovém počtu nejméně 6 000 soukromých i veřejných subjektů. V rámci nové směrnice bude rozšířen výčet regulovaných odvětví a budou přidány regulované služby. Primárním kritériem pro zařazení organizace do skupiny povinných osob bude velikost organizace. (NÚKIB, 2022 b)

Mimo jiné přináší NIS 2 změnu rozdělení regulovaných subjektů, v rámci nové směrnice budou subjekty rozděleny na základní a důležité. Ve skupině základního subjektu budou všechny povinné osoby, které jsou v rámci regulace považovány na nejdůležitější a je u nich stanoven vyšší stupeň ochrany z důvodu vyšší míry rizika vzniku kybernetického incidentu. Do skupiny důležité budou patřit zbylé povinné osoby, u kterých je riziko vzniku kybernetického bezpečnostního incidentu nižší. U těchto skupin budou fungovat dva režimy povinností, a to režim vyšších povinností (essential) a režim nižších povinností (important). Tomuto režimu povinností říkáme tzv. princip dvourychlostní kybernetické bezpečnosti, který slouží k tomu, aby byly na organizace kladeny přiměřené nároky. (NÚKIB, 2022)

V rámci NIS 2 nastala změna i v systému sankcí, které se dělí podle druhu subjektu (NÚKIB, 2022):

- Při porušení povinnosti základním subjektem je stanovena horní hranice pokuty na nejméně 10 milionů EUR nebo alespoň 2 % celkového celosvětového ročního obratu v předchozím rozpočtovém roce, dle toho, co je vyšší.
- Při porušení povinnosti důležitým subjektem je stanovena horní hranice pokuty na nejméně 7 milionů EUR nebo alespoň 1,4 % celkového celosvětového ročního obratu v předchozím rozpočtovém roce, dle toho, co je vyšší.

1.2 České organizace zabývající se kybernetickou bezpečností

S nárůstem kybernetických bezpečnostních indentů jde ruku v ruce i nárůst organizací, které se problematikou kybernetické bezpečnosti v ČR zabývají. Právě těmto organizacím bude věnována následující kapitola.

1.2.1 Státní instituce

Národní agentura pro komunikační a informační technologie

Národní agentura pro komunikační a informační technologie (dále jen „NAKIT“) byla založena na základě usnesení vlády ze dne 21. prosince 2015 jako státní podnik. Tato agentura funguje jako servisní organizace pro ICT Ministerstva vnitra, která má zajistit dlouhodobý rozvoj komunikační infrastruktury, jež patří do majetku státu. Dále mezi její hlavní úkoly patří zajištění bezpečnosti této infrastruktury. (MV ČR, 2016)

Národní bezpečnostní úřad

Národní bezpečnostní úřad byl založen jako ústřední orgán státní správy (výkonná moc) 1. srpna 1998 a sídlí v ulici Na Popelce v Praze. V čele tohoto úřadu je ředitel, který je jmenován Vládou. Úřad je financován ze státního rozpočtu, ve kterém je jeho financování řešeno samostatnou kapitolou. V rámci své působnosti se NBÚ řídí zákonem č. 412/2005 Sb. o ochraně utajovaných informací a k jeho hlavním činnostem patří vydání a rušení osvědčení fyzických osob, zabezpečení ochrany utajovaných informací a kryptografické ochrany, řízení o bezpečnostní způsobilosti. (NBÚ, 2024)

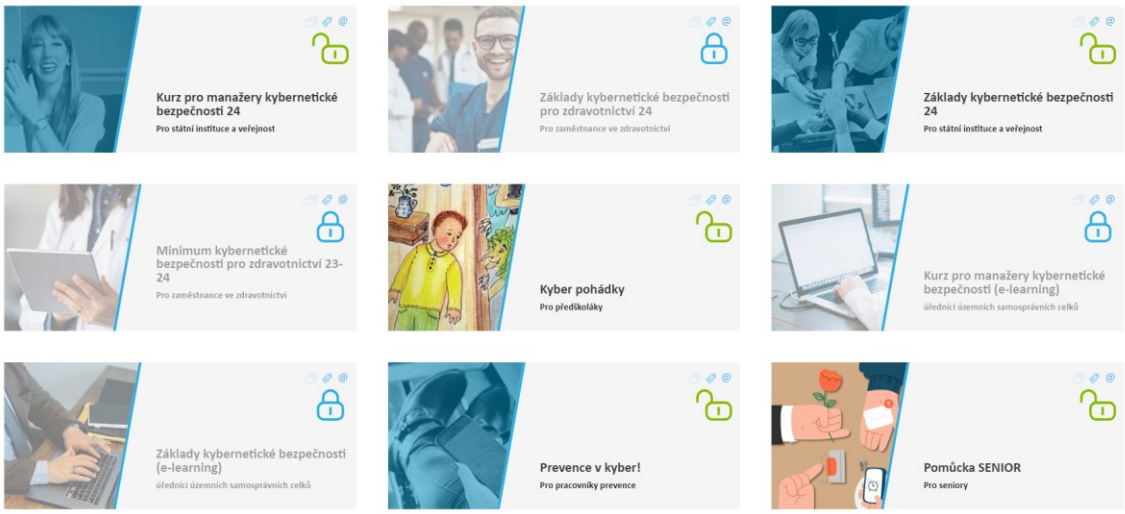
Specifikem tohoto úřadu je, že se jedná o civilní státní orgán, který ve svých řadách nemá zaměstnance ve služebním poměru. V rámci vedených úkonů spolupracuje NBÚ s ozbrojenými bezpečnostními sbory – především s Policií ČR a zpravodajskými službami. Díky citlivosti zpracovávaných informací byl Úřad zařazen do kategorie objektů se zvláštním významem pro vnitřní pořádek a bezpečnost a je trvale střežen příslušníky Policie ČR. (Pavelka, 2018)

Součástí NBÚ bylo dříve i Národní centrum kybernetické bezpečnosti, které následně přešlo v roce 2017 pod NÚKIB. V rámci tohoto odloučení přejal NÚKIB i některé úkoly v oblasti ochrany utajovaných informací a kryptografické ochrany. (NBÚ, 2024)

Národní úřad pro kybernetickou a informační bezpečnost

Stejně jako NBÚ je i NÚKIB ústředním správním úřadem, který při svém vzniku v roce 2017 převzal část povinností na úseku ochrany utajovaných informací (dále jen „OUI“) a kryptografické ochrany od NBÚ. Stejně jako NBÚ je Úřad financován ze státního rozpočtu. Své pobočky má NÚKIB v Praze a Brně. Současným ředitelem je od roku 2022 Lukáš Kintr, který do vedení nastoupil po Karlu Řehkovi. Kromě úkonů v rámci OUI a kryptografické ochrany připravuje NÚKIB kybernetická cvičení, připravuje zákony a zákonné normy a tvoří národní bezpečnostní standardy v dané oblasti. NÚKIB také šíří osvětu a vede vzdělávací kurzy v oblasti kyberbezpečnosti. (NÚKIB, 2023)

V oblasti vzdělávání vytváří NÚKIB e-learningové kurzy kybernetické bezpečnosti, které jsou rozdělené dle cílových skupin – například kurzy pro vedoucí manažery, státní úředníky, kurzy pro střední školy. Dále NÚKIB pořádá přednášky, webináře a odborné konference. Nelze opomenout ani tvorba příruček a informačních brožur. Všechny kurzy, které NÚKIB organizuje, můžeme najít na stránkách https://osveta.NÚKIB.cz/. Na obrázku níže můžeme vidět ukázku nabízených kurzů. (NÚKIB, 2024)



Obrázek 1 Nabídka kurzů NÚKIB k 14. 2. 2024 (NÚKIB, 2024)

Kromě výše zmíněné legislativy tvoří NÚKIB i Národní strategii kybernetické bezpečnosti, poslední je na období let 2021–2025. Mezi další dokumenty vydávané tímto úřadem řadíme Akční plán k Národní strategii kybernetické bezpečnosti, Zprávu o stavu kybernetické bezpečnosti České republiky, kdy poslední vydaná zpráva je z 19. července roku 2023, kde hodnotí stav kybernetické bezpečnosti za rok 2022. (NÚKIB, 2023)

Mezi aktivity NÚKIBu můžeme zařadit i podporu projektů, ať už na národní nebo mezinárodní úrovni. Za zmínku rozhodně stojí projekt KYBERCENTRUM – Centrum kybernetické bezpečnosti, které právě díky podpoře od NÚKIBu a dalších partnerů mohlo vzniknout. KYBERCENTRUM se podílí na šíření osvěty a vzdělávání v oblasti kybernetické bezpečnosti, kdy poskytuje podporu jak kantorům, tak studentům. Od roku 2016 pořádá toto centrum Národní soutěž ČR v kybernetické bezpečnosti, do které se mohou přihlásit žáci a studenti od 9 do 25 let. Centrum se rovněž zapojuje do vzdělávání nejmladší a zároveň i nejstarší generace skrze projekt KYBER POHÁDKY, ve kterém varuje o nebezpečí, které na člověka čeká v rámci kyberprostoru. (KYBERCENTRUM, 2023)

V rámci zapojení co největší části populace je od roku 2023 realizována soutěž KYBER CENA ROKU, která je určena k ocenění a propagaci nejlepších prací, projektů, činnosti pedagogů a žáků v oblasti kybernetické bezpečnosti. Cílem této soutěže je snaha poukázat na výjimečné případy a motivovat veřejnost k zájmu o danou problematiku. (KYBERCENTRUM, 2023)

Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti je výkonným orgánem NÚKIB a mezi jeho hlavní úkoly patří činnost týmu CERT, mezinárodní spolupráce v oblasti kybernetické bezpečnosti, prevence kybernetických hrozeb proti prvkům kritické informační infrastruktury, řešení kybernetických bezpečnostních incidentů, věda a výzkum, vyhodnocování rizik v oblasti kybernetické bezpečnosti a tvorba opatření k jejich nápravě. (NÚKIB, 2024)

Computer Security Emergency Response Team

Vládní tým CERT je provozován pod záštitou NCKB pod doménou GovCERT.cz. (NCKB, 2024)

Mezi hlavní činnosti a služby tohoto týmu patří koordinace a pomoc při řešení incidentů, která spočívá v poskytování pomoci po technické stránce, tvorba preventivních opatření či pomoc při zprostředkování kontaktu s českými/zahraničními bezpečnostními týmy. CSERT rovněž nabízí služby Penetračního testování ve formě interních (útočník je součástí vnitřní sítě společnosti) či externích (útočník pochází z vnějšího prostředí) testů. K dalším činnostem řadíme reakce na bezpečnostní incidenty, ochranu před nimi a efektivní využití dostupných možností k jejich předcházení. (NCKB, 2024)

Na rozdíl od týmu CSIRT má CSERT kompetenci zveřejňovat zjištění v oblasti kybernetických bezpečnostních hrozeb a incidentů, čímž pomáhá ke zvýšení bezpečnosti v rámci jednotlivých subjektů. (Sedlák a Konečný, 2021)

Computer Security Incident Response Team

Označení pochází z anglického názvu Computer Security Incident Response Team (dále jen „CSIRT“) a jedná se o tým, který má na starost řešení, monitoring a předcházení bezpečnostních incidentů na území České republiky. Při řešení bezpečnostních incidentů, které přesahují hranice našeho státu spolupracuje český CSIRT i se svými zahraničními kolegy. (CZ.NIC, 2019)

Od roku 2011 je Národní CSIRT provozován sdružením CZ.NIC. Mezi projekty týmu CSIRT řadíme například Penetrační testování, kdy tato služba hledá zranitelnosti zákazníka s cílem eliminace skrytých hrozeb a zvýšení zabezpečení společnosti. Dalším projektem je Malicious Domain Manager, který slouží k odhalení napadených webových stránek ať už druhem malwaru či phishingu. V případě indikace některé z hrozeb po sledování z různých zdrojů je vlastník domény informován. (CZ.NIC, 2024)

Velitelství informačních a kybernetických sil obrany

Velitelství informačních a kybernetických sil obrany (dále jen „VeKySiO“) vzniklo 1. července roku 2019. Jeho sídlo se nachází v Brně. (AČR, 2023)

VeKySiO působí samostatně, nezávisle na ostatních složkách, avšak aktivně spolupracuje s Vojenským zpravodajstvím a rozvíjí také civilně-vojenskou spolupráci. Jeho součástí je od 1. ledna 2020 Skupina Kybernetických sil a Informačních technologií, dále od 1. ledna 2021 bylo do struktury začleněno Centrum Computer Incident Response Capability (dále jen „CIRC“). (Havlík, 2020)

Mezi hlavní úkoly řadíme monitoring a identifikaci hrozeb, podporu strategické komunikace a podporu před kybernetickými hrozbami. (Havlík, 2020)

1.2.2 Ostatní organizace

Česká společnost pro kybernetiku a informatiku

Česká společnost pro kybernetiku a informatiku (dále jen „ČSKI“) je dobrovolná, výběrová organizace, která sdružuje vědecké, pedagogické a další odborné pracovníky, ale i studenty

oborů zaměřených na kybernetiku či informatiku. Společnost jako taková je nástupkyní Československé kybernetické společnosti, jež vznikla roku 1966. (ČSKI, ©2014-2024)

Mezi cíle ČSKI řadíme především rozšiřování znalostí v oblasti kybernetiky a informatiky jejich členů a popularizace tohoto dynamicky se rozvíjejícího vědního oboru. Výše uvedená společnost se rovněž zaměřuje na pedagogickou a vědeckou činnost. Například každoročně je pořádána Cena Antonína Svobody o nejlepší disertační práci roku. (ČSKI, ©2014-2024)

Mezi významné úspěchy této společnosti můžeme zařadit získání licence European Computer Driving Licence v roce 1999. Dnes je tato licence známá pod zkratkou ICDL, tedy International Computer Driving Licence. Tento projekt slouží jako celosvětově známý certifikační systém, který prohlubuje znalosti z oblasti digitálních technologií. (DigiKoalice, 2024)

Armed Forces Communications Electronics Association

Organizace Armed Forces Communications Electronics Association (dále jen „AFCEA“) vznikla v roce 1946 v USA a aktuálně sídlí ve Faifaxu ve Virginii. Evropskou centrálu můžeme najít v Bruselu. Česká pobočka AFCEA se zabývá především podporou a rozvíjením znalostí v oblasti informačních technologií u AČR. Založena byla 5. 5. 1993. Společnost se podílí na řadě akcí – například spolupracuje na veletrhu IDET, který je jedním z největších veletrhů obranných a bezpečnostních technologií, rovněž se podlí na organizaci Future Forces Forum, kde je tématem především propojení obrany a bezpečnosti. (AFCEA, 2024)

V roce 2021 pobočka založila Centrum kybernetické bezpečnosti, z. ú. (dále jen „KYBERCENTRUM“), které slouží ke zvýšení zájmu mladé generace o kybernetickou bezpečnost. KYBERCENTRUM se v rámci své osvětové činnosti podílelo na finále Národní soutěže ČR v kybernetické bezpečnosti, je tvůrcem projektu KYBERŘÍKANEK a spolu s českými vysokými školami se podílí na realizaci Letní školy kybernetické bezpečnosti. (AFCEA, 2021)

KYBEZ

Platforma KYBEZ.CZ slouží pro sdružování zástupců akademických institucí a představitelů soukromého sektoru. Cílem je především osvětová činnost, kde jsou informace předávány skrze odborné konference, semináře, přednášky a organizované soutěže. Mezi nabízené služby patří audity, kontrola zajištění bezpečnosti informací, kontrola dodržování GDPR a pořádání školení. (KYBEZ, 2024)

Národní centrum bezpečnějšího internetu

Národní centrum bezpečnějšího internetu (dále jen „NCBI“) slouží především k osvětové činnosti. Centrum funguje od roku 2007 a spolupracuje především se školami, knihovnami a orgány veřejné správy, kde provozuje přednášky a různé vzdělávací workshopy. Centrum je součástí evropských osvětových center INSAFE. Mezi nejvýznamnější projekty řadíme Safeinternet.cz, které se věnuje vzdělávání široké veřejnosti a informuje ji o rizicích spojených s pobytem v kyberprostoru. (NCBI, 2024)

2 ZÁKLADNÍ TERMINOLOGIE V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V rámci níže uvedené kapitoly budou popsány vybrané pojmy z oblasti kybernetické bezpečnosti, které jsou z hlediska zpracování diplomové práce brány jako nejvýznamnější. Výklad základních pojmů z řešené oblasti bude nápomocen k lepšímu pochopení řešené problematiky.

2.1 Vybrané pojmy z oblasti kybernetické bezpečnosti

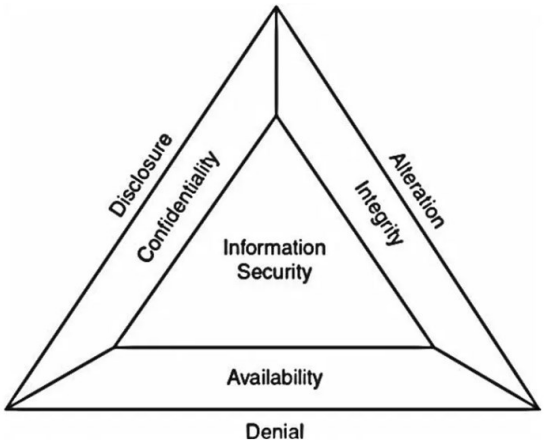
Pojem **bezpečnost** je charakterizován jako ochrana před hrozbami a riziky nebo jako stav, ve kterém se jednotlivci nebo skupiny necítí být ohroženy hrozbami a cítí se být dostatečně chráněny. (Smejkal et al., 2019)

Informační bezpečnost je chápána jako ochrana všech informací a dat na jakémkoliv nosiči před narušením jejich integrity, důvěrnosti a dostupnosti, a to po celý jejich životní cyklus. (Smejkal et al., 2019)

Triáda CIA je základní stavební kámen bezpečnosti informací, jedná se o zajištění důvěrnosti, integrity a dostupnosti informací ve fyzické i elektronické podobě (Hashemi-Pour, 2023):

- Zajištění **důvěrnosti** („confifentiality“) dosáhneme tak, že se k daným datům dostane pouze ten, kdo má. Ve fyzické podobě lze tohoto výsledku dosáhnout za pomoci pečlivého nakládání s dokumenty, kdy nejsou svěřeny do rukou třetích osob. Aby informace v elektronické podobě nepřišla do rukou nepovolané osobě, zabezpečíme informace za pomoci šifrování.
- Zajištění **celistvosti** informací („integrity“), tedy toho, že informace se dostanou k adresátovi celistvé a nezměněné, dosáhneme vy fyzické podobě za pomoci tzv. kolku a číslování stránek. V rámci elektronického dokumentu použijeme elektronický podpis, popřípadě elektronický otisk dokumentu.
- Pro zajištění **dostupnosti** („availibility“) daného dokumentu ve fyzické formě můžeme využít možnosti tvorby kopií, v případě elektronického dokumentu zvolíme možnost zálohy dat či tvorbu záložních tras.

Dále se můžeme setkat s pojmem **triáda DAD**, kdy se jedná o odhalení („disclousure“), modifikaci („alternation“) a zničení (destruction“). Můžeme říci, že vlastníkům informací slouží triáda CIA, kdežto útočníkům DAD, což je pravý opak CIA. (Yadav, 2021)



Obrázek 2 Triády CIA a DAD (Yadav, 2021)

Jedním ze základních pojmů je **kyberprostor**, jehož význam můžeme chápat jako digitální prostřední, skrze které může dojít ke vzniku, zpracování a výměně informací. Tento prostor je tvořen informačními systémy, službami a sítí elektronické komunikace. (Sedlák a Konečný, 2021)

Kybernetická bezpečnost v sobě obsahuje informační bezpečnost, jedná se o soubor právních a organizačních opatření, které řeší zařízení, stroje, sítě a jejich zabezpečení před hrozbami. (Kremling a Parker, 2017)

Smejkal a kol. (2019) charakterizují **hrozbu** jako událost, která může mít negativní vliv na naše aktiva, kdy může dojít k jejich poškození. V případě kybernetické bezpečnosti chápeme **kybernetickou hrozbu** jako možnou příčinu kybernetické bezpečnostní události nebo incidentu.

Kybernetická bezpečnostní událost – jedná se o takovou událost, při které může dojít k narušení kybernetické bezpečnosti daného subjektu. Kybernetická bezpečnostní událost se po jejím projevení/realizaci stává kybernetickým bezpečnostním incidentem. (Kremling a Parker, 2017)

Kybernetický bezpečnostní incident je takový incident, při kterém došlo k narušení kybernetické bezpečnosti. Jedná se o reálný incident, který nastal. (Kremling a Parker, 2017)

Častým pojmem, se kterým se můžeme v námi řešené oblasti setkat je **metodika budování bezpečnostního povědomí**. Tento proces je složen ze čtyř stupňů, které tvoří povědomí (awareness), výcvik a školení (training), vzdělávání (education) a profesní rozvoj (professional development). Toto vzdělávání je určeno pro skupiny uživatelů, kteří jsou rozděleni dle úrovně svých znalostí na začátečníky (beginners), středně pokročilé (intermediate) a pokročilé (advanced). Součástí toho procesu je testování po každém kurzu a předávání zpětné vazby mezi školitelem a posluchači tak, aby došlo k neustálému procesu zlepšování. (Sedlák a Konečný, 2021)

Sociální inženýrství je v současné době velmi rozšířenou podvodnou praktikou, která využívá manipulace s obětí za účelem získání citlivých informací či finančních prostředků. V obětech je často vyvoláván pocit strachu (například že přijdou o své úspory vlivem napadení svého bankovního účtu), tento strach je ještě umocňován časovým nátlakem a vyžadováním okamžité reakce za účelem minimalizace škod. Většina kybernetických útoků je provedena za pomoci praktik sociálního inženýrství, kdy mezi nejvíce známé útoky patří různé formy phishingu. (Požár et al., 2022)

2.2 Škodlivý software

Pro účely této diplomové práce je důležité charakterizovat jednotlivé druhy škodlivého softwaru (tzv. „**malware**“). Základní rozdělení škodlivého softwaru je do dvou hlavních skupin, a to dle způsobu šíření a dle efektu zaměření.

Do první jmenované skupiny, dle způsobu šíření, řadíme viry, červy a trojské koně. Každý z těchto škodlivých softwarů může mít pro uživatele fatální následky ať už v podobě ztráty kontroly nad zařízením nebo úniku či odcizení dat. (ESET, 2024)

Prvním zástupcem v rámci této skupiny je **počítačový virus**, kdy se jedná označení škodlivého programu, který je schopen se sám šířit bez vědomí uživatele daného zařízení. Jako způsob šíření využívá kopírování do jiných programů nebo dokumentů uvnitř napadeného zařízení. Rovněž může být virus v rámci počítačové sítě šířen za pomoci užití paměťových médií, jako jsou například USB flash disky. Tímto způsobem budou přeneseny zavirované soubory z jednoho zařízení do druhého. Mezi hlavní příznaky zavirování počítače řadíme zpomalení počítače, výpadky operačního systému a zvýšený výskyt chybových hlášek, deaktivace antivirového programu a náhlý nedostatek místa na disku. (ESET, 2024)

Na rozdíl od viru se může **počítačový červ** sám šířit do dalších počítačových systémů. Své vytvořené kopie je pak schopen na dálku aktivovat a spustit. Stejně jako virus si i počítačový červ klade za cíl co největší poškození daného uživatele skrze jeho data. (ESET, 2024)

Posledním uvedeným typem škodlivého softwaru je **trojský kůň**, v tomto případě je škodlivý kód vložen do programů, který na první pohled působí velmi věrohodně a bezpečně. Například může být součástí přílohy emailu, který se jeví jako email od antivirové společnosti. Právě tímto způsobem si získá důvěru daného uživatele, který jej častokrát v dobré víře spustí. Po spuštění takto infikovaného programu uživatelem dochází k převzetí kontroly nad napadeným zařízením, zašifrování dat a odeslání informací útočníkovi. Na rozdíl od předchozích škodlivých softwarů tak není jeho hlavním cílem další samovolné šíření. (Kouhout a Karchňák, 2016)

Dle efektu zaměření rozeznáváme tyto nejčastější druhy kybernetických hrozeb (Kouhout a Karchňák, 2016):

- Ransomware.
- Spam.
- Spyware.
- Adware.
- Phishing a jeho další formy.

Mezi hlavní znaky **ransomwaru** patří zašifrování souborů napadaného uživatele spojené s následným vydíráním a požadováním zaplacení výkupného nejčastěji ve formě kryptoměny. Uživateli je slíbeno, že po zaplacení výkupného dojde k opětovnému zpřístupnění daných souborů. (Kouhout a Karchňák, 2016)

Principem **spamu** je zasílání nevyžádané emailové pošty většinou ve formě reklamních sdělení, která jsou rozesílána hromadnou formou. Tyto emaily mohou často obsahovat malware, který se pak může snadno infiltrovat do uživatelova zařízení. Proto mezi doporučené rady v případě spamových emailů patří neotevření, nahlášení a přesunutí takového emailu do koše. (Sedlák a Konečný, 2021)

Při stahování filmů či instalaci her do našeho zařízení může snadno dojít k instalaci **spywaru**. Tento škodlivý software slouží ke sběru citlivých informací, který může vést až ke krádeži identity. Nástrojem, který hacker využívá při sběru informací, je především **key logger**, který sleduje stisknuté znaky na klávesnici. (Požár et al., 2022)

Méně škodlivým, avšak značně obtěžujícím typem škodlivého softwaru je **adware**, který sbírá informace o internetové aktivitě uživatele a následně zobrazuje velké množství reklam za pomoci vyskakovacích oken. Na rozdíl od spywaru, který je do zařízení instalován bez vědomí a souhlasu uživatele, je adware instalován do zařízení se souhlasem uživatele. (Požár et al., 2022)

2.3 Kybernetické útoky

Pod pojmem **phishing** rozumíme metodu, která usiluje o zcizení přihlašovacích údajů uživatele, jako jsou hesla do různých účtů, čísla bankovních karet apod. s cílem zneužití daných informací ve formě přihlášení do bankovního konta za účelem výběru peněžních prostředků nebo udělení neoprávněného přístupu k datům poškozené osoby. Nejčastější metodou pro získání těchto informací je zasílání podvodných emailů, které na první pohled působí velmi důvěryhodně, například se zdají být jako zpráva zaslaná bankou, která obsahuje žádost o zaslání čísla účtu a ověřovacího kódu pro přístup do internetového bankovnictví. (Požár et al., 2022)

V rámci běžné praxe rozlišujeme několik základních druhů phishingu (Požár et al., 2022):

- **Spear phishing** – forma cíleného phishingu, která míří na konkrétní skupinu uživatelů, případně i jednotlivce. Tento druh je aplikován především za účelem proniknutí do interních sítí daných společností. Vyznačuje se oproti ostatním druhům vysokou mírou propracovanosti.
- **Phishing za pomoci emailových zpráv** – nejčastější druh phishingu, kdy je zpráva zaměňována za email z důvěryhodného zdroje (například z banky), častým jevem je stejně jako v ostatních druzích phishingu tvorba nátlaku na oběť a vytváření časového limitu na reakci na daný podvodný email.
- **Vishing** – jedná se o druh phishingu, který je realizován skrze podvodné telefonáty, při kterých se útočník vydává za pracovníka banky. Cílem je vylákat z osoby přihlašovací údaje do internetového bankovnictví, popřípadě převod peněz na zdánlivě bezpečný účet, který je však účtem útočníka. Pro umocnění pocitu věrohodnosti jsou tyto hovory kombinovány s hovory osob, které se vydávají za příslušníka Policie České republiky, který potvrdí věrohodnost informací, které oběti sdělil údajný pracovník banky. Častokrát útočníci opravdu volají jménem banky, u které má oběť veden svůj bankovní účet.

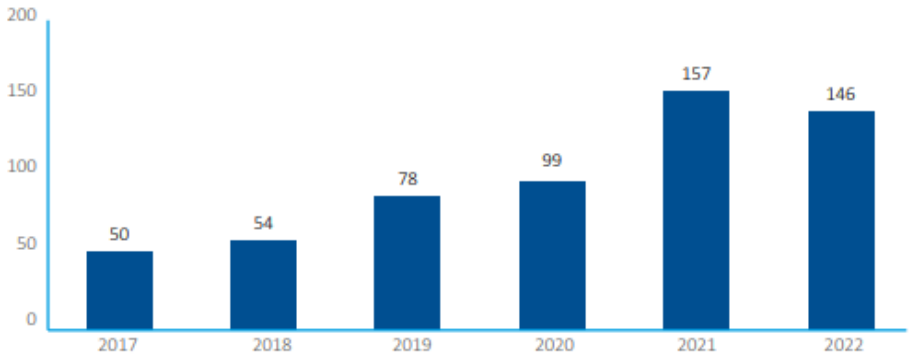
- **Smishing** – jedná se o druh phishingu, který je realizován formou zaslání SMS obětem. Tyto SMS obsahují zpravidla podvodné odkazy. Princip a cíle jsou stejné jako u ostatních forem phishingu.
- **Whaling** – jedná se o podvodné jednání za účelem odcizení citlivých informací a osobních údajů, které cílí na vedoucí zaměstnance daných společností.
- **Quishing** – druh phishingového útoku, který cílí především na mobilní zařízení, která umožňují čtení tzv. QR kódů, do kterých jsou vpraveny podvodné webové adresy a falešné přihlašovací brány do bankovních aplikací. Jde o poměrně nový druh phishingu, který ještě není mezi veřejností tak známý, a tudíž se může snáze šířit.
- **Pharming** – metoda, která využívá přesměrování IP adresy na falešné stránky, které se však tváří jako ty, jež oběť do prohlížeče zadala. Pro laickou veřejnost jsou tyto podvodné stránky jen velmi těžko rozpoznatelné. Klasickým případem přesměrování je například přesměrování na falešné stránky internetového bankovnictví.

Útoky na dostupnost vybraných služeb mohou probíhat za pomoci sítě infikovaných zařízení malwarem útočníka, kterou označujeme jako **botnet**. Tato síť zařízení se používá především k zesílení míry daného útoku. Jednotlivá infikovaná zařízení v rámci této sítě označujeme pojmem **zombie**. (Kremling a Parker, 2017)

V praxi rozlišujeme dva druhy útoků na dostupnost, a to **Denial of Servise** (dále jen „DoS“) a **Distributed Denial of Service** (dále jen „DDoS“). Rozdíl mezi těmito útoky je v počtu zařízení. V případě DoS útoku je útok veden z jednoho zařízení za pomoci velkého počtu požadavků na daný server nebo zařízení. Pro provedení DDoS útoku je potřebná velká síť ovládaných zařízení (botnet), skrze kterou je vedeno velké množství požadavků, které mají za následek přetížení daných webových stránek nebo aplikace a tím znemožněný přístup dalším uživatelům. (Požár et al., 2022)

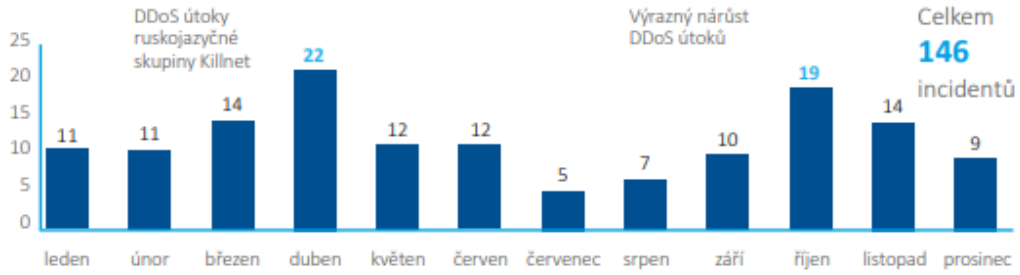
3 VÝZNAMNÉ KYBERNETICKÉ BEZPEČNOSTNÍ INCIDENTY

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2022 (NÚKIB, 2023) vyplývá, že v meziročním srovnání došlo ke snížení počtu kybernetických incidentů, které byly u NÚKIB evidovány, a to ze 157 na 146. Navzdory tomuto poklesu vzrostl počet kyberkriminálních aktivit, které jsou evidovány Policií České republiky (dále jen „PČR“) na dvojnásobek. (NÚKIB, 2023)



Graf 1 Vývoj počtu incidentů registrovaných NÚKIB (NÚKIB, 2023)

Je nutné si uvědomit, že iniciátorům kyberútoku nejde již jen o osobní informace, které mohou získat formou phishingových a ransomwarových útoků, ale i o znepřístupnění webů za pomoci DDoS útoků. (NÚKIB, 2023)



Graf 2 Počet řešených incidentů v průběhu roku 2022 (NÚKIB, 2023)

V roce 2022 byl zaznamenán nárust kybernetických bezpečnostních incidentů převážně v měsících březen a duben, což souvisí se sérií DDoS útoků ruskojazyčné skupiny Killnet. DDoS útoky byly rovněž v hojnější míře zaznamenány v měsíci říjen 2022. (NÚKIB, 2023)

Právě výše uvedená skupina Killnet stála v dubnu roku 2022 za rozsáhlými DDoS útoky, které ochromily především weby ministerstva vnitra, web NÚKIB nebo prodejní web Českých drah. (Český rozhlas, 2022)

Oproti roku 2021, kdy bylo procentuální zastoupení DDoS útoků v kybernetických incidentech 34 %, v roce 2022 tvoří DDoS útoky 58 % kybernetických incidentů. U ostatních kategorií hrozeb jako jsou škodlivé kódy došlo k poklesu z 25 % na 8 %, pokles rovněž hlásí pokusy o zneužití zranitelností. Mírného zvýšení dosáhly naopak phishingové útoky, které v roce 2021 tvořily 10 % incidentů, kdežto v roce 2022 již tvoří 11 % incidentů. (NÚKIB, 2023)

Mezi hlavní cíle kybernetických útoků můžeme zařadit kritickou informační infrastrukturu, kde útoky cílí především na dostupnost poskytovaných služeb, dále finanční sektor, průmysl a energetiku, zdravotnictví a školství. (NÚKIB, 2023)

Z Kybernetických incidentů pohledem NÚKIB za měsíc prosinec 2023 (NÚKIB, 2024) je patrné, že oproti roku 2022 Česká republika zaznamenala nárůst kybernetických incidentů. V průměru hovoříme o počtu 19 incidentů měsíčně. Lze očekávat, že ve Zprávě o stavu kybernetické bezpečnosti v České republice za rok 2023 bude rovněž patrný vzestup DDoS útoků a případů phisingových útoků. Například v měsíci prosinec 2023 tvořily DDoS útoky 83 % veškerých zaznamenaných incidentů. (NÚKIB, 2024)

Mezi nejčastějšími útoky zůstávají různé formy phishingu a DDoS útoky. Oproti předchozím letům jsou na ústupu ransomwarové útoky. Nejvíce útoků můžeme pozorovat ve veřejném sektoru, poté ve zdravotnictví a soukromém sektoru. Téměř dvojnásobně se zvýšil i počet útoků na kritickou informační infrastrukturu, kde hlavním cílem útoků byla dostupnost služeb. V rámci kybernetických útoků můžeme v roce 2022 pozorovat nárůst útoků, který je spojen s válkou na Ukrajině. (NÚKIB, 2023)

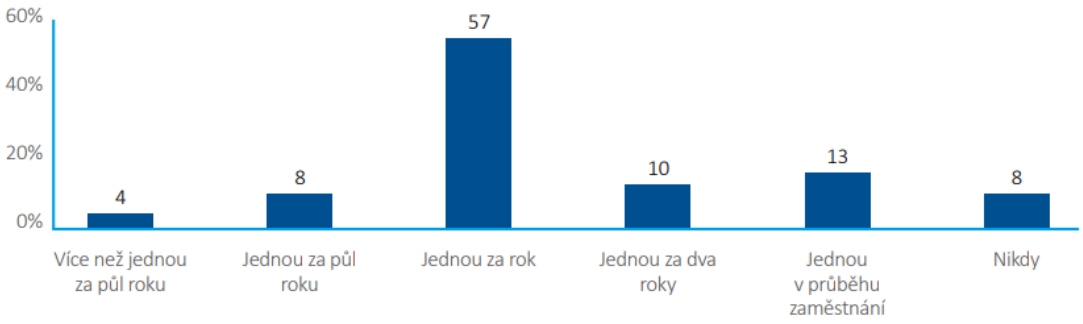
Součástí Zprávy o stavu kybernetické bezpečnosti je rovněž posouzení úrovně vzdělání v oblasti kybernetické bezpečnosti za pomoci dotazníkového šetření vytvořené NÚKIB. (NÚKIB, 2023)

Jak uvádí ve svém rozhovoru pro Hospodářské noviny Ing. Martin Bajer (2023), kybernetické útoky jsou nejčastěji směrovány na lidský faktor, přičemž jeho selhání stojí za většinou úspěšně provedených kybernetických útoků. (Dostalová, 2023)

Kolouch a Bašta ve své knize CyberSecurity (2019) uvádí následující tvrzení: *„Celý systém je tak silný, jak silný je jeho nejslabší článek. V tomto případě je oním nejslabším článkem, a největším nebezpečím pro zabezpečení informací, člověk.“* (Kolouch a Bašta, 2019)

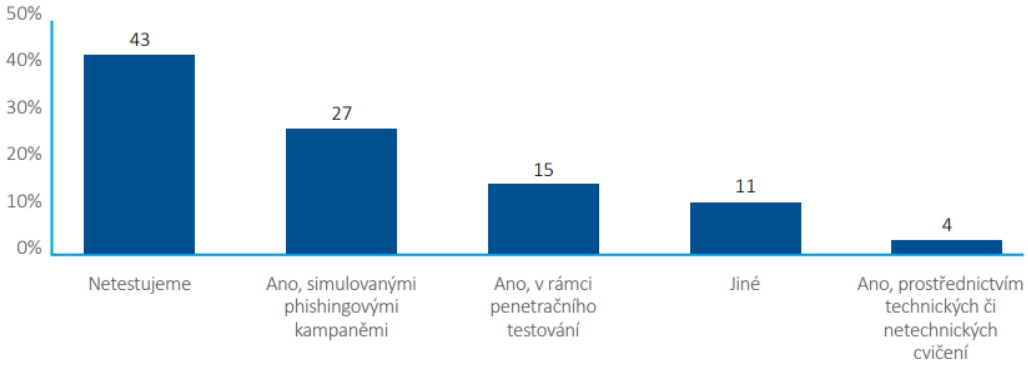
Jak můžeme vidět, vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti je dnes nezbytností. V rámci šetření NÚKIB, které bylo provedeno u náhodně vybraných regulovaných společností, vyplývá, že podíl organizací, které neprovádí žádné školení v oblasti kybernetické bezpečnosti, je velmi nízký a odpovídá pouze 5 % dotazovaných respondentů. (NÚKIB, 2023)

Z grafu (viz níže) vyplývá, že více než polovina dotazovaných organizací (57 %) provádí školení alespoň jednou za rok. V součtu u 69 % respondentů probíhá školení jednou a vícekrát ročně. (NÚKIB, 2023)



Graf 3 Frekvence školení uživatelů v oblasti kybernetické bezpečnosti v organizacích za rok 2022 (% respondentů) (NÚKIB, 2023)

V rámci provedeného šetření byly rovněž organizace dotázány na způsob testování v oblasti kybernetické bezpečnosti v rámci jejich společnosti. Z níže uvedeného grafu vyplývá, že méně než polovina dotazovaných neprovádí žádný druh testování kybernetické odolnosti, naopak 27 % dotazovaných testuje za pomoci simulovaných phishingových útoků a 15 % respondentů provádí testování pomocí penetračního testování. (NÚKIB, 2023)



Graf 4 Formy testování odolnosti zaměstnanců proti kybernetickým hrozbám v organizacích za rok 2022 (% respondentů) (NÚKIB, 2023)

Je tedy otázkou, jaké údaje o vzdělávání v oblasti kybernetické bezpečnosti budou obsažené ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2023. Dle mého názoru dojde k nárůstu počtu institucí, i těch neregulovaných, které do svého plánu činnosti zařadí alespoň jednu vzdělávací aktivitu na téma kybernetická bezpečnost.

3.1 Vybrané kybernetické bezpečnostní incidenty na území České republiky

V rámci popisu vybraných kybernetických bezpečnostních incidentů v České republice jsem se rozhodla pro rozdělení do sektorů, na které jsou útoky cíleny. Budou zde popsány útoky v rámci státního i soukromého sektoru.

3.1.1 Kybernetické útoky státní sektor

Níže uvedená podkapitola představuje vybrané kybernetické útoky na subjekty, které jsou součástí státního sektoru na území České republiky.

Kybernetický útok na nemocnici v Janově

Dne 23. června 2018 čelila kybernetickému útoku nemocnice v Janově, kde hacker zašifroval data o pacientech. Nenadálá situace neochromila léčbu úplně, avšak značně zkomplikovala práci zdravotnickému personálu, který například neměl přehled o datech propuštění jednotlivých pacientů. Nemocnice odmítla výkupné zaplatit a data obnovila ze záloh. (ČT24, 2018)

Kybernetický útok na nemocnici v Benešově

Během 11. prosince 2019 byl proveden kybernetický útok na nemocnici v Benešově, kde byl nemocniční systém infikován virem Ryuk (jedná se o ruský vyděračský vir), který plně ochromil chod nemocnice. V provozu nebyly přístroje, počítačové sítě, dostupná nebyla data o pacientech, plánované operace musely být zrušeny. Ztraceny byly informace například i o dárcích krve nebo data ekonomického charakteru. K úniku citlivých informací o pacientech nedošlo. Provoz nemocnice byl plně obnoven až 30. prosince 2029. Nemocnici byla způsobena škoda 59 milionů Kč, policii se pachatele nepodařilo dohledat, a tak byl případ odložen. (iDNES, 2020)

Kybernetický útok na Fakultní nemocnici v Brně

Další kybernetický útok na české nemocnice se odehrál 13. března 2020 ve Fakultní nemocnici v Brně, v době, kdy republika i svět bojoval s pandemii COVID-19, čelila nemocnice masivnímu útoku, který ochromil informační systém a přerušil veškeré plánované operace. V době útoku byli akutní pacienti převáženi například do Nemocnice u sv. Anny. Základní provoz nemocnice byl obnoven do tří měsíců od útoku. (iDNES, 2021)

Kybernetický útok na Ředitelství silnic a dálnic

V květnu 2022 byl proveden kyberútok na webové stránky Ředitelství silnic a dálnic (dále jen „ŘSD“), kde došlo k ransomwarovému útoku, při kterém byla zašifrována data a vyřazeny webové stránky ŘSD. Kromě znemožnění poskytování dopravních informací došlo například i k zrušení některých zakázek, kterým vypršela lhůta pro podání nabídky. (Echo24, 2022)

Kybernetické útoky hackerské skupiny NoName

Hackerská skupina NoName(057) zaměřující se na DDoS útoky proti zemím, které podporují Ukrajinu, provedla v letech 2022 a 2023 několik útoků i na území ČR. Skupina, která ke komunikaci využívá sociální síť Telegram, dokonce nabízí svým fanouškům za spoluúčast na DDoS útocích odměnu až do výše 25 000 Kč. V rámci Česka tato skupina provedla několik útok jak proti webům státních institucí v podobě stránek České obchodní inspekce, Poslanecké sněmovny Parlamentu ČR, Ministerstva vnitra, Úřad vlády, Policie ČR, tak i subjektům soukromého sektoru, jako jsou Letiště Praha, Air Bank, Fio banka nebo Komerční banka. Krom znepřístupnění daných serverů je rovněž jedním z cílů poškození dobrého jména dané společnosti. Proto jsou pro provedení útoku voleny organizace, které

jsou v rámci republiky známé a poškození dobrého jména může mít pro ně nemalý finanční dopad. (Zoulová, 2023)

Kybernetický útok na Českou národní banku

Terčem kybernetického útoku se stala dne 1. září 2023 Česká národní banka, na kterou byl proveden DDoS útok. Vlivem útoku byly některé služby nedostupné, avšak nedošlo k napadení vnitřního systému banky a úniku citlivých dat. (ČNB, 2023)

Kybernetický útok na Univerzitu obrany

V září 2023 provedla ransomware skupina Monti kyberútok na Univerzitu obrany v Brně. Cílem útoku bylo odcizit utajované informace, osobní údaje a dokumenty ekonomické povahy. Odcizené informace sahají dle webu irozhlas.cz až 10 let zpětně, což může představovat problém například pro absolventy univerzity, kteří jsou nadále aktivními příslušníky Armády ČR. (iRozhlas, 2023)

24. října 2023 zveřejnila skupina část zcizených informací, které se týkají Fakulty vojenského leadershipu. Celou věc vyšetřovala Vojenská policie. (Echo24, 2023)

Kybernetický útok na společnost CERMAT

Další institucí, kterou postil DDoS útok, byl web společnosti CERMAT s názvem DiPSy, který slouží k podávání přihlášek na střední školy. Útok byl proveden v sobotu 3. února 2024 a jeho nejsilnější část trvala od 12:35 do 12:45 hod., během této doby mohli uživatelé zaregistrovat problém s načítáním stránek. K dalšímu útoku již během podávání přihlášek nedošlo. (ČTK, 2024)

Kybernetické útoky na České dráhy

Během posledních let jsou rovněž na vzestupu kybernetické útoky kritickou infrastrukturu v podobě železniční sítě. V rámci České republiky jsou nejčastější kybernetické útoky vedeny na systémy národního dopravce – Českých drah. První větší útok byl zaznamenán již v březnu roku 2021. Tehdy došlo k ochromení interních systému, ale navzdory vlně útoků nebyl výrazně ovlivněn provoz na tratích ani bezpečnost zaměstnanců či cestujících. (RAILTARGET, 2021)

V rámci posledních měsíců stále sílící proruská hackerská kampaň má jako jeden z cílů vyřazení tuzemské železniční sítě jakožto důležité součásti kritické infrastruktury. Tyto útoky cílí na elektronické signalizační zařízení a počítačové sítě. Pod palbou útoků je rovněž systém prodeje jízdenek nebo aplikace Českých drah, která slouží k nákupu jízdenek

či k poskytnutí informací o spojích. Již v roce 2023 uvedla do provozu Česká správa železnic jako jedno z opatření specializované bezpečnostní centrum, které má ochránit citlivé informace a zamezit případným útočníkům průnik k ovládacím prvkům v rámci drah. (HN, 2024)

3.1.2 Kybernetické útoky na soukromý sektor

Níže uvedená podkapitola představuje vybrané kybernetické útoky na subjekty, které jsou součástí soukromého sektoru na území České republiky.

Kybernetický útok ransomwaru Avaddon

Ransomware známý pod názvem Avaddon v minulosti cílil na české firmy a organizace. Po infikování systému došlo k zašifrování souborů, obětem bylo vyhrožováno, že po nezaplacení výkupného budou jejich údaje uveřejněny na dark webu, což mělo oběti motivovat k platbě výkupného. Kromě zveřejnění citlivých dat v podobě účetnictví, smluv a osobních údajů bylo rovněž vyhrožováno provedením DDoS útoků. Dne 11. června 2021 byla uveřejněna informace o ukončení činnosti tohoto ransomwaru. Společnost Emsisoft následně uveřejnila návod, jak získat svá zašifrovaná data zpět. (NÚKIB, 2021)

Kybernetický útok na společnost O2

Cílem DDoS útoku se v pondělí 24. října 2023 stala společnost O2. V rozhovoru pro web zive.cz uvedl ředitel fixních služeb Tomáš Křešťálek, že se jednalo o velmi masivní útok, který trval tři dny, přičemž přicházel ve vlnách. Cíl útočníků byl více než jasný – odříznout české uživatele od internetu a telekomunikačních služeb. První známky přišly v podobě dvojnásobného provozu na internetu oproti obvyklému průměru. Pozitivně hodnotí Křešťálek především činnost krizového štábu a komunikaci se zákazníky, díky nimž se podařilo společnosti tento útok lépe zvládnout. (Živě.cz, 2022)

Kybernetický útok za pomoci škodlivého kódu Spy.Banker.BUL

V měsíci leden 2024 se Českem začal šířit škodlivý kód Spy.Banker.BUL napadající bankovní aplikace u zařízení s operačním systémem Android. Uživatel si daný škodlivý kód může jednoduše do svého zařízení nainstalovat spolu s programem pro čtení dokumentů ve formátu PDF. Při provádění aktualizace aplikace je do zařízení infiltrován malware Anatsa, který cílí na bankovní aplikace v daném zařízení. S výše uvedeným škodlivým kódem se potýkají uživatelé i v Německu, Velké Británii a USA.

Je tedy důležité při odsouhlasení aktualizace sledovat rovněž, které doplňky do svého zařízení spolu s aktualizací instalujeme. (Novinky.cz, 2024)

3.2 Vybrané kybernetické bezpečnostní incidenty v zahraničí

V rámci této kapitoly budou zmíněny některé z několika tisíc kybernetických bezpečnostních incidentů. Pro zpracování diplomové práce byly vybrány kybernetické bezpečnostní incidenty v rozmezí let 2017 až 2023.

Kybernetický útok malwaru Petya

Dne 27. června 2017 byl na Ukrajinu spáchán malwarový útok Petya. Dle bezpečnostních odborníků byl útok proveden skrze aktualizaci účetního systému MeDoc, který byl ve velké míře na Ukrajině používán. Po spuštění malwaru byly uživatelům zašifrovány hlavní soubory na pevném disku a bylo vynuceno restartování počítače, následně po tomto úkonu se objevilo sdělení, že jsou veškeré soubory zašifrovány a za jejich odblokování je požadováno výkupné v Bitcoinech. Útokem byla ochromena činnost ministerstev, státních podniků, systému metra a bank. Samotný útok proběhl v předvečer ukrajinského státního svátku, tedy v době, kdy byla většina uživatelů již doma, a tak se malware snáze šířil. Dne 28. června 2017 vydala ukrajinská vláda prohlášení, ve kterém uvedla, že byl útok zastaven a probíhají práce na obnově dat. (Polityuk a Prentice, 2017)

Po provedení kyberútoků na Ukrajině byl malware přejmenován na NotPetya či Nyetna, tento druh malware na rozdíl od původní Petyi soubory nejenže šifroval, ale rovnou mazal či trvale poškozoval. (NCKB, 2017)

Ukrajina byla však terčem velkého množství dalších kybernetických útoků, z nichž mezi ty významnější můžeme řadit například útok ze 14. ledna 2022, který vyřadil z provozu většinu ukrajinských vládních webů. (The New York Times, 2022)

Další útok na sebe nenechal dlouho čekat a 15. února téhož roku byl proveden DDoS útok na stránky ukrajinského ministerstva obrany, armády a bank. (Kelly, 2022)

Útok ransomwaru WannaCry

Ransomware WannaCry se šíří od května roku 2017 a napadá počítače s operačním systémem Microsoft Windows. Jedná se o typ ransomwaru, který se chová jako červ a šíří se skrze sítě, kde v napadených počítačích šifruje soubory. Po zašifrování souborů vyzve uživatele k zaplacení výkupného ve výši 300 USD, pokud uživatel odmítne zaplatit, je pod

výhružkou trvalého odstranění souborů výkupné navýšeno na 600 USD. Mezi nejvíce zasažené země patří Rusko, Čína a Ukrajina. (Latto, 2020)

Kybernetický útok na společnost Colonial Pipeline

V květnu roku 2021 byl proveden ransomwarový útok na společnost Colonial Pipeline, která je díky své rozvodné síti jedna z největších společností na přepravování ropných produktů v USA. Během dvou hodin se podařilo útočníkům odcizit společnost zhruba 100 GB dat, která byla následně uzamknuta a za jejichž odemknutí bylo požadováno výkupné. Samotný útok byl proveden skrze virtuální privátní síť (dále jen „VPN“), kterou používají zaměstnanci společnosti při práci z domova. V dané síti nebylo užíváno dvou faktorové autentifikace, tudíž útočníkům stačilo k infiltraci pouze jedno heslo. Společnost po útoku přešla do off-line režimu, aby zamezila šíření ransomwaru. S tímto krokem se však pojí zastavení všech operací v rámci rozvodné sítě, což u uživatelů vyvolalo paniku. Z důvodu zamezení větším škodám se rozhodla společnost zaplatit vyděračské skupině DarkSide výkupné ve výši 4,4 mil amerických dolarů (následně po ukončení vyšetření se společnosti podařilo získat část peněz zpět). Celý útok poukázal na nedostatečné zabezpečení v oblasti kybernetické bezpečnosti takto významného odvětví. (Turton a Mehrotra, 2021)

Kybernetický útok na Červený kříž

V lednu roku 2022 byl proveden kybernetický útok na servery Červeného kříže, ze kterých byly odcizeny informace o více než 515 000 osobách, které jsou v evidenci Červeného kříže z důvodu odloučení od rodiny kvůli válečnému konfliktu, přírodní katastrofě nebo z důvodu pohřešování. Právě citlivost těchto údajů je největší problém tohoto útoku. (ICRC, 2022)

Zneužití zranitelnosti nultého dne

Zranitelnosti nultého dne využili hackeři v červnu roku 2023, kdy pronikli do softwaru MOVEit transfer, který slouží k přenosu citlivých dat. Po infiltraci byla odcizena data obsahující citlivé osobní údaje včetně výpisů ze zdravotní dokumentace. Celkový počet obětí doposud není znám. (Tidy, 2023)

4 OCHRANA OBYVATELSTVA V ČESKÉ REPUBLICE

V následující kapitole jsou popsány vybrané pojmy z oblasti ochrany obyvatelstva, včetně rozdělení složek Integrovaného záchranného systému a vybraných legislativních dokumentů pro potřeby uvedení do kontextu této diplomové práce.

Pojmem **ochrana obyvatelstva** rozumíme dle zákona č. 239/2000 Sb. o Integrovaném záchranném systému *„plnění úkolů civilní ochrany, zejména varování, evakuace, ukrytí a nouzové přežití obyvatelstva a další opatření k zabezpečení ochrany jeho života, zdraví a majetku.“*. (Česko, 2000 a)

Za oblast ochrany obyvatelstva a integrovaného záchranného systému na území České republiky odpovídá Ministerstvo vnitra.

Škodlivé působení sil a jevů způsobených člověkem nazýváme pojmem **mimořádná událost**. Tento jev přímo ohrožuje život, zdraví a majetek osob nebo životní prostředí. Přítomnost tohoto jevu vyžaduje provedení záchranných a likvidačních prací. (Česko, 2000 a)

Integrovaný záchranný systém je chápán jako řízený postup jednotlivých složek v přípravě na mimořádnou událost, během mimořádné události a při provádění záchranných a likvidačních prací. (Česko, 2000 a)

Složky integrovaného záchranného systému dělíme na **základní** (skrze ně je zajištěna nepřetržitá pohotovost pro příjem informací o vzniku mimořádné události, následně je daná mimořádná událost vyhodnocena a je v místě jejího vzniku proveden zásah) a **ostatní** (tyto složky se podílí především na realizaci záchranných a likvidačních prací, kdy poskytují pomoc na vyžádání základní složkou). (Česko, 2000 a)

Mezi základní složky IZS řadíme (Česko, 2000 a):

- Hasičský záchranný sbor České republiky (dále jen „HZS“).
- Jednotky požární ochrany zařazené do plošného pokryté kraje jednotkami požární ochrany.
- Poskytovatele zdravotnické záchranné služby (dále jen „ZZS“).
- Policii České republiky.

Mezi ostatní složky IZS můžeme řadit následující (Česko, 2000 a):

- Vyčleněné síly a prostředky ozbrojených sil České republiky.
- Ostatní ozbrojené bezpečnostní sbory.
- Ostatní záchranné sbory.
- Orgány ochrany veřejného zdraví.
- Havarijní, pohotovostní, odborné a jiné služby.
- Záchranný tým Českého červeného kříže.
- Obecní/městskou policii.
- Zařízení civilní ochrany.
- Horskou službu ČR.
- Vodní záchrannou službu ČČK.
- Skalní záchrannou službu ČČK.
- Neziskové organizace, Bílý kruh bezpečí, Linku bezpečí.

Mezi subjekty ochrany obyvatelstva můžeme začlenit i obecní samosprávu v čele se starostou obce, který se podílí na řešení mimořádné události a krizové situace ve správním obvodu obce. (Česko, 2000 a)

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, vstoupil v platnost dne 1. ledna 2001. Zákon vymezuje „*integrovaný záchranný systém, rozdělení do jednotlivých složek včetně jejich působnosti, působnost a pravomoci státních orgánů a orgánů samosprávných celků. Dále součástí tohoto zákona jsou povinnosti právnických a fyzických osob př přípravě na MU a při provádění záchranných a likvidačních prací.“* (Česko, 2000 a)

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, vstoupil v platnost rovněž 1. ledna 2001. Předmětem tohoto zákona je „*stanovení působnosti a pravomocí státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením. Současně jsou v tomto zákoně vymezeny stavy nebezpečí, orgány krizového řízení a jejich činnosti.“* (Česko, 2000 b)

Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých dalších souvisejících zákonů nám charakterizuje *„hospodářská opatření pro stav nebezpečí, nouzový stav, stav ohrožení státu a válečný stav, rovněž hospodářská opatření při vyhlášení krizových stavů. Rovněž zákon vymezuje pravomoc vlády a správních úřadů při přípravě a přijetí hospodářských opatření pro krizové stavy. Součástí zákona je i popis systému nouzového plánování, systému hospodářské mobilizace, pravidla pro použití státních hmotných rezerv.“* (Česko, 2000 c)

5 PROBLEMATIKA VZDĚLÁVÁNÍ DOSPĚLÝCH

V rámci níže uvedené kapitoly budou popsány vybrané pojmy z oblasti vzdělávání dospělých, včetně základních metod a forem vzdělávání.

Pojmem **vzdělávání** rozumíme proces, při kterém získáváme vědomosti skrze poznatky a osvojujeme si různé dovednosti. Tento jev probíhá po celý lidský život, kdy nejvíce intenzivní je především v období dětství a dospívání, avšak se vzděláváním se setkáváme i v dospělosti v rámci pracovního života. (Plamínek, 2014)

Samotné vzdělávání můžeme rozdělit do následujících skupin (Velecká, 2019):

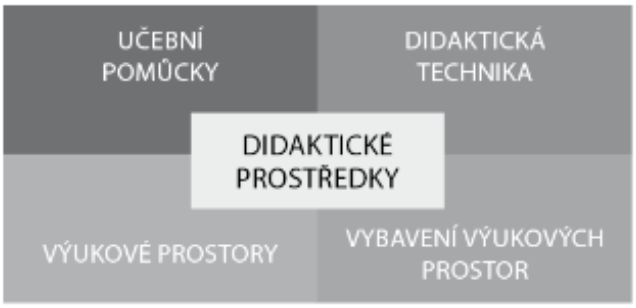
- **Vzdělávání formální** – toto vzdělávání probíhá přímo ve vzdělávacích institucích, výsledkem tohoto procesu je získání diplomu, certifikátu či potřebné úrovně kvalifikace. Mezi klasické instituce řadíme školky, základní, střední a vysoké školy, univerzity třetího věku.
- **Vzdělávání neformální** – tento druh vzdělávání je realizován mimo klasické vzdělávací instituce, nejčastěji se s tímto typem setkáváme v rámci pracovního zařazení nebo například při rekvalifikaci na úřadu práce.
- **Vzdělávání informální** – jedná se o celoživotní vzdělávání, které probíhá vědomou či nevědomou formou. Z příkladů lze namátkou uvést například muzea, knihovny, umělecké galerie.

Didaktickou metodou rozumíme druh a způsob vyučování. Pomocí této techniky dochází ke kontaktu mezi vyučujícím a posluchačem. (Plamínek, 2014)

Didaktické metody můžeme rozdělit do tří základních skupin (Plamínek, 2014):

- **Didaktické metody teoretické** – do této skupiny patří vzdělávání formou přednášek, cvičení a seminářů.
- **Didaktické metody teoreticko – praktické** – jedná se o kombinovanou skupinu, do které řadí metody diskuse nad určeným tématem, programovou výuku.
- **Didaktické metody praktické** – v této skupině metod je kladen důraz na co největší interakci mezi vyučujícím a posluchači, je zde očekáváno aktivní zapojení posluchačů. Mezi hlavní metody patří dnes velmi populární coaching, praktické stáže a exkurze, instruktáž.

Mezi **didaktické prostředky** řadíme veškeré prostředky, které nám napomáhají při vzdělávání a zlepšují jeho kvalitu. Rovněž tyto pomůcky pomohou daný proces vyučování zefektivnit. Základní rozdělení těchto pomůcek je na **materiální** a **nemateriální**. Do první zmíněné skupiny řadíme klasické učební pomůcky jako je tabule, tištěné učební materiály, učebny, audiovizuální technika. Nemateriální prostředky tvoří forma výuky, vyučovací zásady a organizace výuky. (Hladílek, 2009)



Obrázek 3 Didaktické prostředky (Šerák, 2009)

V dnešní době je čím dál více diskutovaným tématem **vzdělávání dospělých**, kdy pod tímto pojmem si můžeme představit vzdělávací aktivity spojené s osobami především v produktivním, ale i v postproduktivním věku. Jedná se o utužování a rozvíjení znalostí a dovedností u osob, které již ukončily vzdělávání v klasických školských zařízeních. Vědní disciplína, která se vzděláváním dospělých zabývá se nazývá **andragogika**. (Langer, 2016)

S rozvojem moderních technologií se mění jak forma vzdělávání, tak i obsah vzdělávání dospělých. Pryč jsou již doby, kdy pro vzdělávání stačila pouze tabule, přednášková místnost a školitel. V dnešní době, kdy se dostávají do popředí moderní technologie, je kladen čím dál větší důraz na interakčnost ve vzdělávacím procesu. Posluchači očekávají, že si budou moci probíranou látku prakticky vyzkoušet, pokud to dané téma umožňuje. Čím dál více je rovněž náročné upoutat pozornost posluchače a do výuky je potřeba zařazovat více příběhů z praxe, interakci mezi školitelem a posluchačem za pomoci diskuse, audiovizuální ukázky například v podobě krátkého videa. (Langer, 2016)

V rámci vzdělávání je možné využívat pravidlo **SMART**, které nám pomůže stanovit cíle a následně zpětně prozkoumat jejich formulaci.

Specifičnost	Vztah k určité konkrétní činnosti, specifikace cíle z hlediska jeho obsahu (množství, kvalita, čas).
Měřitelnost	Stanovení požadované kvality i kvantity (měřící jednotkou), cíl musí být měřitelný v kvantitě i kvalitě.
Akceptovatelnost	Soulad se zjištěnými potřebami i ztotožnění s přijetím cíle od všech, kteří jej budou naplňovat.
Reálnost	Musí existovat reálná šance pro účastníky, že dosáhnou cíle – musí být dosažitelný.
Termínovanost	Splnění cílů v potřebném (daném) čase i průběžně při dosažení jednotlivých etap.

Obrázek 4 Pravidlo SMART (Langer, 2016)

Pomocí tohoto pravidla, které je v managementu hojně využíváno, si tak každá společnost může před zahájením konkrétního vzdělávání jasně a přehledně stanovit své cíle. (Langer, 2016)

5.1 Příprava realizace vzdělávání

Příprava před zahájením vzdělávání je velmi důležitou součástí celého procesu. Zaměstnavatel si ve spolupráci s vyučujícím musí ujasnit jednotlivé klíčové oblasti, které můžeme rozdělit do následujících skupin (Langer, 2016):

- **Cílovou skupinu vzdělávání** – je potřeba charakterizovat skupinu, která bude vzdělávána, kdy poté je možno vytvořit vzdělávací program dle aktuálních potřeb a úrovní znalostí a dovedností. Klíčové je pro nás složení cílové skupiny (dosažené vzdělání, věk, pracovní zařazení), celkový počet posluchačů a jejich motivace (vnitřní nebo vnější), rozsah znalostí jednotlivých účastníků (mohou být rozřazeni do skupin dle úrovně svých znalostí).
- **Cíl vzdělávání** – jedná se o úroveň znalostí, kterou bude účastník po absolvování kurzu disponovat. Pro správnou formulaci cílů můžeme využít například výše popsané pravidlo SMART.

- **Obsah vzdělávání a jeho strukturu** – v rámci tvorby vzdělávací aktivity je potřebné stanovit si obsah výuky, určení informací, které jsou pro nás nezbytné, důležité. Dále informace a fakta, která prošla obměnou nebo jsou obtížněji pochopitelná a je nutné jim věnovat během výuky zvýšenou pozornost. Rovněž se v rámci výuky zaměřujeme na takové informace, které jsou pro posluchače užitečné a zbytečně je nezahlcujeme informacemi, které jsou pro ně nepotřebné. S obsahem výuky se úzce pojí i délka výuky, kdy si zaměstnavatel s vyučujícím stanoví časovou dotaci a počet lekcí. Základní rozdělení vzdělávacích aktivit je na jednorázové a mimořádné. Následně v rámci přípravy vytvoří lektor harmonogram jednotlivých výukových hodin.
- **Místo, kde bude vzdělávání probíhat** – nezbytný před zahájením výuky je výběr učebny s ohledem na počet posluchačů, vybavenost učebny prostředky pro posluchače (lavice, židle, potřebná psací plocha) a pro vyučujícího (dataprojektor, ozvučení, počítač, tabule, laserové ukazovátko, mikrofon). Důležité je také osvětlení místnosti, akustika a možnost větrání či klimatizace, odhlučnění, uspořádání míst v učebně.
- **Techniku, která bude k dispozici vyučující** – jedná se o veškeré prostředky, které může vyučující během výuky používat (tabule, fixy, dataprojektor, interaktivní tabule, reproduktor, mikrofon a další). Důležitou částí je zkouška funkčnosti veškeré techniky před zahájením výuky, aby nedocházelo k prodlevám či zhoršení kvality výuky.

5.2 Formy a metody vzdělávání

Při provádění konzultace mezi vyučujícím a zadavatelem dochází k volbě formy a metody vzdělávání. V následující podkapitole budou vysvětleny základní formy vzdělávání, dostupné metody, včetně možných výhod a nevýhod.

Formou vzdělávání rozumíme organizaci výuky z hlediska **času, počtu posluchačů a místa konaní výuky a formy realizace**. V případě, že hovoříme o časovém hledisku, rozlišujeme vzdělávání jednorázové a opakované, které následně dělíme na vzdělávání krátkodobé (jedná se o vzdělávání v řádu dnů či týdnů) a dlouhodobé (vzdělávání v řádu měsíců). Formou realizace je chápana prezenční nebo distanční forma výuky. Při volbě formy realizace je nutno brát zřetel na druh vzdělávací aktivity. Ne každá aktivita může být vyučována distanční formou. (Langer, 2016)

Místo konání výuky lze rozdělit na mimo pracoviště a na pracovišti. Specifikem dnešní doby je konání vzdělávací aktivity ve virtuálním prostředí (vzdělávání za pomoci e-learningového kurzu). (Langer, 2016)

Z hlediska počtu účastníků můžeme vzdělávací aktivity rozdělit do následujících tří skupin (Langer, 2016):

- **Hromadné vzdělávací aktivity** – charakterizovány velkým počtem účastníků, zpravidla více než 20 posluchačů.
- **Skupinové vzdělávací aktivity** – maximální počet účastníků je 20.
- **Individuální vzdělávací aktivity** – malý počet posluchačů, nejvíce 3. Blízká interakce posluchačů a vyučujícího.

Mezi nejčastější metody vzdělávání řadíme následující výčet (Langer, 2016):

- **Přednáška** – nejčastější varianta vzdělávání, pojme velké množství posluchačů v co nejkratším časovém úseku, jedná se o cenově přijatelnou variantu, nejedná se o prostorově náročnou metodu. Nevýhodou této metody je malá interakce posluchačů a vyučujícího, malá možnost zpětné vazby, obtížné udržení pozornosti posluchačů. Potřeba neustálého upoutání pozornosti formou praktických příkladů či videí.
- **Seminář** – jedná se o obdobu přednášky s větším zapojením posluchačů, soustředění semináře většinou na jedno hlavní téma se zaměřením na praxi. Výhodou této metody je větší zapojení posluchačů, naopak nevýhodou je kapacitní omezení a nutnost pravidelné přípravy posluchačů. V případě volby semináře skrze internet hovoříme o webináři.
- **E-learningové kurzy** – jedná se o efektivní variantu proškolení velkého počtu osob v určitém časovém období, výhodou této metody je snadný monitoring dosažených výsledků a finanční nenáročnost (v závislosti na společnosti, která bude kurz realizovat). Mezi další výhody řadíme časovou flexibilitu (posluchač kurz absolvuje dle svých pracovních možností během stanovené doby pro absolvování) a snadnou aktualizaci. Nevýhodou kurzu je nemožnost interakce se školitelem, nevěnování dostatečné pozornosti kurzu (posluchač si získá otázky a odpovědi ze závěrečného testu u svých spolupracovníků).

- **Workshop** – často bývá zaměňován za seminář, oproti kterému využívá vzdělávací aktivity k řešení aktuálních pracovních problémů dané společnosti. Výhodou je měřitelnost formou výstupu (tvorba koncepce řešení problému či tvorba výrobku).

Je zřejmé, že problematika vzdělávání jako taková je opravdu obsáhlou oblastí a k efektivní práci v této oblasti je zapotřebí pečlivě definovat vzdělávané oblasti, a to na základě složení posluchačů, časových a finančních možností dané společnosti. Veškerá tato specifika je nutné zhodnotit jak zadavatelem, tak školitelem. Pouze tak bude možné vybrat nejlepší formu vzdělávání pro konkrétní společnost.

6 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

První část diplomové práce je věnována rozboru vybraných legislativních dokumentů, norem a evropských směrnic a charakteristice vybraných pojmů z oblasti kybernetické bezpečnosti. Kapitola české organizace zabývající se kybernetickou bezpečností charakterizuje tuzemské organizace a jejich činnost na poli kybernetické bezpečnosti. V rámci teoretické části diplomové práce jsou rovněž popsány vybrané významné kybernetické bezpečnostní incidenty na území České republiky a v zahraniční.

Z uvedených zdrojů vyplývá, že oblasti vzdělávání je potřeba věnovat čím dál větší pozornost, jelikož vývoj moderních technologií jde dopředu mílovými kroky. Bohužel tento technologický pokrok s sebou přináší i značnou míru ohrožení pro lidskou společnost. Na denní bázi se dozvídáme o kybernetických útocích v rámci soukromého i státního sektoru, mnozí z nás se dokonce s některým z druhů kybernetických útoků mohli setkat v pracovním či osobním životě.

Proto je potřeba vzdělávání a prohlubování znalostí v oblasti kybernetické bezpečnosti pro lidskou společnost klíčová. Informovaný uživatel, který dodržuje zásady bezpečného chování na internetu a je obezřetný již pro případného útočníka nebude tak snadným cílem.

Potřebu vzdělávání svých zaměstnanců si v posledních letech uvědomuje čím dál více společností, proto v rámci praktické části bude provedena analýza vybraných kurzů kybernetické bezpečnosti za účelem volby vhodného kurzu. Ke zjištění současné úrovně vzdělávání bude použita metoda strukturovaných rozhovorů, kdy následně bude vytvořen návrh opatření ke zvýšení úrovně vzdělávání v subjektu ochrany obyvatelstva.

II. PRAKTICKÁ ČÁST

7 VZDĚLÁVACÍ KURZY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

V tak komplexní disciplíně, jakou je vzdělávání v oblasti kybernetické bezpečnosti, je potřeba brát v potaz hned několik faktorů. Mezi základní z nich řadíme věk, úroveň dosaženého vzdělání, sociální status jedince, pohlaví a pracovní zaměření (v rámci každého pracovního zařazení jsou kladeny na vzdělávání v oblasti kybernetické bezpečnosti jiné nároky). Zároveň nám do procesu vzdělávání vstupuje několik překážek, které je nutné při tvorbě vzdělávacího programu zohlednit. Mezi nejčastější řadíme ztrátu motivace k dalšímu vzdělávání, vysoké pracovní vytížení či závazky vůči rodině. Je potřeba pro konkrétní skupinu zaměstnanců zvolit adekvátní míru vzdělávání tak, aby byla využitelná v rámci zastávané pozice, ale i v jejich běžném životě.

Vzdělávání jako takové je komplexní, nikdy nekončící proces a takto je nutné k němu přistupovat. Potřeby společnosti se mohou v závislosti na čase a okolnostech měnit, a proto je nutné, aby vzdělávání bylo schopno na tyto změny dynamicky reagovat. Jiná byla situace před lety, kdy mezi největší hrozby patřily trojské koně, viry a červi a jiná situace je dnes, kdy vývoj na poli moderních technologií jde kupředu mílovými kroky a s tím ruku v ruce i vývoj hrozeb. Tomuto všemu se musí vzdělávací proces přizpůsobovat.

Zároveň s rozmachem technologií již nestačí pouze vzdělávání formou jedné přednášky s odborníkem a následný podpis prezenční listiny. Dnes se mnohem častěji v rámci vzdělávání volí e-learningové kurzy, tematicky zaměřené besedy a workshopy s odborníky.

V rámci níže uvedených kapitol diplomové práce bude provedena stručná charakteristika vybraných kurzů v oblasti kybernetické bezpečnosti v ČR. Zdaleka se však nejedná o všechny dostupné kurzy na našem území.

7.1 Charakteristika vybraných kurzů kybernetické bezpečnosti

V rámci této podkapitoly budou ve stručnosti představeny vybrané společnosti a jejich nabídka kurzů, kterou můžeme v rámci ČR nalézt. Nejedná se zcela o všechny kurzy, které jsou na našem území nabízeny. Vybráno bylo několik základních.

Vybrané kurzy jsou rozděleny do dvou skupin, a to dle své dostupnosti. První skupinu tvoří kurzy, které jsou poskytovány zdarma, kdežto v druhé skupině jsou kurzy placené.

Po seznámení s vybranou nabídkou bude vybráno několik kurzů, které v rámci provedené analýzy za pomoci expertního týmu zhodnotíme s cílem vybrat nejvhodnější z nich. Výběr optimální varianty kurzu bude proveden na základě vícekriteriálního rozhodování formou zjednodušené bodovací metody.

7.1.1 Bezplatné kurzy

Níže uvedená podkapitola je věnována popisu vybraných bezplatných kurzů kybernetické bezpečnosti, které jsou dostupné v České republice. Nejedná se o všechny dostupné kurzy, pouze vybraný vzorek pro účely zpracování diplomové práce.

Národní úřad pro kybernetickou a informační bezpečnost provozuje vlastní vzdělávací portál skrze doménu https://osveta.NÚKIB.cz/local/dashboard/.Na těchto stránkách jsou k dispozici e-learningové vzdělávací kurzy v oblasti kybernetické bezpečnosti jak pro širokou veřejnost, tak pro konkrétní skupiny dle odborností. Kurzy na tomto portálu jsou rozděleny do dvou základních skupin – kurzy volně přístupné a kurzy přístupné po registraci uživatele. Po prostudování všech témat v teoretické části většiny nabízených kurzů účastník vyplní povinný závěrečný test, kdy po jeho úspěšném absolvování obdrží na svou emailovou adresu certifikát o jeho absolvování. (NÚKIB, 2024)

V nabídce můžeme nalézt například Kurz pro manažery kybernetické bezpečnosti 24, který je v plné verzi dostupný po registraci a zabývá se ISMS, řízením aktiv a rizik a zajištěním organizační bezpečnosti. Součástí kurzu je i interaktivní workshop, v rámci kterého si může uživatel vyzkoušet zavádění ISMS ve fiktivně vytvořeném úřadu, čímž si může své nabyté teoretické znalosti ověřit v praxi. Dalším z nabízených kurzů je „DÁVEJ KYBER“, který je volně dostupný. Během tohoto kurzu si uživatel osvojí základy kybernetické bezpečnosti, jakou je například síla hesla a pravidla bezpečného přihlášení, uživatel se rovněž dozví základní informace o praktikách sociálního inženýrství, o druzích škodlivých souborů a možnostech jejich rozpoznání. (NÚKIB, 2024)

V rámci kurzů pro konkrétní skupiny osob můžeme zmínit „DÁVEJ KYBER“ pro učitele, který se rozděluje do dvou okruhů – okruh pro učitele a okruh pro třídu. V okruhu pro učitele jsou posluchačům kurzu předány základní informace o zabezpečení pracovních účtů, formách bezpečné on-line výuky a druzích kyberšikany, která je páchána na učitelích. Součástí okruhu pro třídu jsou témata zaměřena na sociální sítě a nástrahy zde se vyskytující, kyberšikanu, on-line sexuální chování a agresi. Další kurzy, které cílí na žáky základních a středních škol jsou například Jsem netvor na základce, Jsem netvor na střední

nebo Digitální stopa: Příběh Báry. Tyto kurzy jsou vedeny formou video příběhů a obrázkových příběhů tak, aby zaujaly širší vrstvu mladých posluchačů. Na těchto kurzech se podílelo Ministerstvo školství, mládeže a tělovýchovy. (NÚKIB, 2024)

Mezi kurzy určené pro zaměstnance ve zdravotnictví patří Minimum kybernetické bezpečnosti pro zdravotnictví 23-24, Základy kybernetické bezpečnosti pro zdravotnictví 24. Mezi kurzy pro státní instituce a veřejnost řadíme kurz Základy kybernetické bezpečnosti 24, který je rovněž určen pro úředníky územních samosprávných celků. (NÚKIB, 2024)

Kromě tvorby e-learningových kurzů pořádají zaměstnanci NÚKIB také odborné konference, semináře a workshopy. V případě zájmu a dostatečných kapacit pořádají pracovníci přednášky na půdě škol, firem či různých státních institucí. (NÚKIB, 2024)

Centrum kybernetické bezpečnosti, z.ú. nabízí v rámci svých aktivit i vzdělávání v oblasti kybernetické bezpečnosti skrze svoje projekty Kyberpohádky a Kyberříkanky. Rovněž byly tímto centrem organizovány přednášky a webináře na téma „Jak učit kybernetickou bezpečnost“, které se zaměřovaly na pomoc pedagogům při výuce kybernetické bezpečnosti. Této akce se zúčastnilo 20 vyučujících z jihočeského kraje. Kromě přednášek a seminářů pořádá KYBERCENTRUM projekt KYBER CENA ROKU. (KYBERCENTRUM, 2023)

Projekt **BUĎ SAFE ONLINE** pochází od bývalého youtubera a influencera Jiřího Krále, který spojil síly se společností Avast. Tento projekt je určen převážně pro mladší generaci, která díky tomuto kurzu získá povědomí o základech bezpečného chování na internetu, kybernetických hrozbách a o tom, jak se chovat v případě, že jsou svědky kyberšikany. (Avast, 2018)

7.1.2 Placené kurzy

Níže uvedená podkapitola je věnována popisu vybraných placených kurzů kybernetické bezpečnosti, které jsou dostupné v České republice. Nejedná se o všechny dostupné kurzy, pouze vybraný vzorek pro účely zpracování diplomové práce.

Nezisková organizace **Czechitas** se zaměřuje na vzdělávání v oblasti IT. Pořádá kurzy a semináře především pro ženy. V nabízených kurzech můžeme nalézt kurz Úvod do Kyberbezpečnosti, který je organizován formou webináře, je zdarma a poskytuje zúčastněným osobám základní orientaci v problematice kybernetické bezpečnosti. Kromě vzdělávacích kurzů pro jednotlivce nabízí tato organizace i kurzy pro firmy, které mohou proběhnout formou odborných přednášek či jednodenních kurzů. (Czechitas, 2023)

Společnost s více než 30letou praxí **ESET software spol. s.r.o** působící na území ČR se zaměřuje na digitální bezpečnost. Do její nabídky patří software pro domácnosti i firmy. Krom nabídky sotwaru pro zabezpečení můžeme na jejich webových stránkách nalézt taktéž školení kybernetické bezpečnosti pro zaměstnance či podniky. Vzdělávání realizuje pomocí e-learningových kurzů, které jsou zaměřeny na sociální inženýrství, druhy možných hrozeb, zabezpečení účtů a základní pravidla bezpečného chování na internetu. Součástí školení je i simulátor phishingového útoku. Samotné školení trvá 60–90 minut, součástí je i pravidelný report určenému zástupci ze strany zákazníka o seznamu účastníku a jejich plnění daného kurzu. V rámci doplňkových služeb je možné uzpůsobit školení konkrétním požadavkům zákazníka či jej organizovat v prezenční formě. (ESET, 2024)

Součástí nabídky společnosti je i možnost penetračního testování za účelem zjištění odolnosti firmy vůči hackerským útokům. Po ukončení testování je zákazníkovi poskytnuta podrobná zpráva, která může dané firmě pomoci ke zlepšení stavu kybernetické bezpečnosti. (ESET, 2024)

Společnost **CYBERSEC** nabízí školení kybernetické bezpečnosti pro širokou veřejnost. V tomto případě se jedná o plně placené kurzy. Vzdělávání je vedeno formou e-learningových kurzů se závěrečnou certifikací pomocí testu. Kurz obsahuje témata jako jsou email a jeho bezpečné použití, tipy, jak zabezpečit svá zařízení, bezpečné chování na internetu nebo zálohování dat a legislativní normy. (CYBERSEC, 2024)

Kurzy kybernetické bezpečnosti můžeme rovněž nalézt na platformě **KYBEZ**. Tato společnost nabízí workshop Řízení kybernetické bezpečnosti, který je organizován formou workshopu. Účastníci kurzu se dozví, jaká je základní legislativa KB, jak evidovat aktiva, hrozby a zranitelnosti v rámci své společnosti, co znamená plán kontinuity a jaká jsou potřebná nastavení ke zvýšení úrovně zabezpečení v oblasti kybernetické bezpečnosti. (KYBEZ, 2021)

Pro základní orientaci v rámci dané problematiky je určen kurz Základy kybernetické bezpečnosti organizace, který posluchačům přinese představení základních pojmů v oblasti KB, charakterizuje aktuálně platnou legislativu, uvede nejčastější kybernetické hrozby, součástí kurzu jsou i příklady z praxe a souhrn možných variant pro ochranu před kybernetickými útoky. (KYBEZ, 2021)

Plně hrazené kurzy kybernetické bezpečnosti nabízí společnost **Seduo**, která má ve své nabídce dva kurzy – Bezpečně v online světě a Digitální bezpečnost. Po vykonání obou kurzů obdrží posluchač certifikát absolventa. (Seduo, 2024)

V prvním z uvedených kurzů pod vedením Karola Suchánka, který je odborníkem v oblasti KB, získá uživatel přehled o zásadách bezpečného chování na internetu, a to včetně ochrany osobních dat a formě a druzích kybernetických útoků. Tento kurz je určen pro běžnou veřejnost a rovněž je vhodný pro děti od 15 let, není zde vyžadováno absolvování žádného předchozího kurzu. Kurz je rozdělen do 10 úseků, kde každý úsek se věnuje jednomu tématu z oblasti KB. Celková doba trvání kurzu je 45 minut a jako zakončení je zvolen test k ověření získaných znalostí. (Seduo, 2024)

Druhým a zároveň nejprodávanějším kurzem dané společnosti je Digitální bezpečnost: naučte se chodit v online světě bezpečně. Tento kurz předává posluchačům pravidla pro vytváření silných hesel, možnosti, jakými lze zabezpečit svá zařízení a naučí posluchače rozpoznat nejčastější typy hrozeb, se kterými se mohou v rámci každodenního života setkat. Kurz je určen pro všechny, kteří se setkávají v rámci svého života s IT technologiemi, vhodný je rovněž pro děti od 10 let. Kurz je tvořen 12 úseky a celková doba trvání je 52 minut. Rovněž je zakončen závěrečným testem. (Seduo, 2024)

Společnost **Next Generation Security Solutions** (dále jen „NGSS“) nabízí prostřednictvím svých webových stránek školení kybernetické bezpečnosti, školení normy ČSN ISO/IEC 27 000 a dále školení pro jednotlivé odbornosti – architekty, auditory, IT zaměstnance, bezpečnostní manažery. Kromě uvedených kurzů je možné vytvořit školení „na míru“ dané společnosti, kdy může školení trvat v řádu hodin až několika dní. Školení lze uskutečňovat formou čistě e-learningových kurzů nebo kombinovaně s účastí odborného školitele. V ceně školení jsou započítány i výukové materiály a příručka bezpečného chování. (NGSS, 2024)

Mezi další nabízené služby společností NGSS patří i penetrační testování ve 3 různých formách – test zranitelností (jsou identifikovány zranitelnosti informačního systému klienta, které by mohly být zneužity), penetrační test (simulace hackerského útoku) a analýza provozu (za pomoci analytických metod je zjišťováno, zda v daném informačním systému aktuálně neprobíhá hackerský útok). (NGSS, 2024)

Další z řady placených kurzů nabízí společnost **Kudrna Sobková** v podobě kurzu Kybernetická bezpečnost aneb Jak žít a přežít v kyberprostoru, tento kurz je určen pro laickou veřejnost k seznámení se se základními principy v dané oblasti, nabízený kurz je realizován jak online na platformě GoogleMeet, tak osobně za účasti školitele. V rámci tohoto kurzu je dbáno na zapojení účastníků a praktické ukázky. V případě online verze je odhadovaná cena dvouhodinového kurzu 8 000 Kč, u čtyřhodinového kurzu je cena 16 000 Kč. Pokud si vybereme prezenční variantu, je cena za čtyřhodinový kurz 23 000 Kč. (Kudrna Sobková, 2024)

Do své nabídky zařadila kurz kybernetické bezpečnosti i společnost **GORDIC**, která krom vzdělávání nabízí například i aplikaci pro řízení kybernetické bezpečnosti či aplikaci pro vzdělávání zaměstnanců GDPO, která nabízí ucelený soubor kurzů včetně reportingu za dané kurzy a sledování legislativních změn. V rámci nabízeného kurzu kybernetické bezpečnosti získají uživatelé základní teoretický i praktický vstup do dané problematiky obohacený o praktické ukázky. Další z nabízených možností je organizace školení pro konkrétní skupiny zaměstnanců dle jejich zaměření. Pro cenovou kalkulaci stačí vyplnit dotazník, kdy v řádu dní obdrží zákazník cenovou nabídku pro svou společnost. (GORDIC, 2023)

Vzdělávání v oblasti kybernetické bezpečnosti nabízí i společnost **T-SOFT**, která přichází s workshopy zaměřenými na nejčastější hrozby, obecné zásady bezpečnosti, možnosti zabezpečení zařízení a problematikou sociálního inženýrství. Tyto kurzy jsou rozděleny do dvou skupin – pro komerční sféru a pro veřejnou správu pod názvem Kybernetická bezpečnost ve veřejné správě. (T-Soft, 2017)

Společnost **BOZP.cz** nabízí školení informační a kybernetické bezpečnosti, v rámci tohoto kurzu jsou účastníci seznámeni se základní legislativou, pojmy a druhy hrozeb. Součástí tohoto kurzu jsou i zásady pro nastavení silného hesla, bezpečné používání webových stránek, zálohování dat a skartaci fyzických dokumentů. Cena kurzu se odvíjí od počtu zaměstnanců, kdy platí, že čím vyšší počet zaměstnanců, tím nižší cena za jednoho zaměstnance. Kurzy jsou prodávány v tzv. balíčcích, součástí balíčků jsou i další kurzy, jako například školení BOZP, PO a další. (BOZP, 2024)

Pravidla IT bezpečnosti pro zaměstnance je kurz nabízený společností **OKškolení**, který je určen pro všechny zaměstnance, kteří přichází do styku s IT technologií a internetem. Tento kurz není určen pro IT profesionály. Poskytuje účastníkům základní informace o sociálním inženýrství, fyzickém zabezpečení počítače, tvorbě silného hesla a základních druzích

kybernetických útoků. V tomto kurzu je rovněž pozornost věnována šifrování a elektronickému podpisu. Uživatelé jsou rovněž informování o tom, kam bezpečnostní incidenty hlásit. (OKškolení, 2023)

7.2 Analýza vybraných kurzů kybernetické bezpečnosti

Níže uvedená kapitola je věnována analýze vybraných kurzů kybernetické bezpečnosti za pomoci zástupce metod vícekriteriálního rozhodování – bodovací metody.

Za pomoci metody brainstorming s podplukovníkem Ing. Kamilem Halouzkou, Ph.D., z katedry informatiky a kybernetických operací Univerzity obrany, bylo vybráno pro účely hodnocení šest kurzů kybernetické bezpečnosti. Tyto kurzy byly za pomoci výše uvedené metody vybrány na základě dostupných informací, sylabů a referencí účastníků kurzů. Vybrané kurzy byly zpracovány v tabulce, kterou můžeme vidět níže (tabulka č. 1).

Tabulka 1 Vybrané kurzy pro provedení analýzy (Vlastní zpracování)

Název kurzu	**Společnost**
Základy kybernetické bezpečnosti 24	NÚKIB
Úvod do kybernetické bezpečnosti	CZECHITAS
Školení kybernetické bezpečnosti	CYBERSEC
Digitální bezpečnost: naučte se chodit v online světě bezpečně	SEDUO
Školení informační a kybernetické bezpečnosti	BOZP.cz
Pravidla IT bezpečnosti pro zaměstnance	OKškolení

U těchto vybraných kurzů byla provedena kvantitativní analýza za pomoci zjednodušené bodovací metody, kterou provedl tříčlenný hodnotitelský tým. Složení hodnotitelského týmu je znázorněno na níže uvedené tabulce.

Tabulka 2 Složení hodnotitelského týmu (Vlastní zpracování)

P. č.	**Jméno a příjmení hodnotitele**	**Označení**	**Funkce**
1.	pplk. Ing. Kamil Halouzka	H 1	Vyučující na katedře informatiky a kybernetických operací UO
2.	Bc. Kristýna Suchorová	H 2	Autorka diplomové práce
3.	Bc. Filip Krejčí	H 3	Účastník strukturovaných rozhovorů, respondent Policie České republiky

Mezi kritéria pro hodnocení byla zařazena cena, srozumitelnost a přínosnost kurzu. První uvedené kritérium – cena, bylo kritériem minimalizačním. Zbylá dvě kritéria byla naopak maximalizační. (Zapletal, 2023)

V tabulce č.3 můžeme vidět přehled cen u jednotlivých kurzů, které byly součástí analýzy.

Tabulka 3 Ceny vybraných kurzů (Vlastní zpracování)

Cena kurzu	
Základy kybernetické bezpečnosti 24 (NÚKIB)	zdarma
Úvod do kybernetické bezpečnosti (CZECHITAS)	3990 Kč/os
Školení kybernetické bezpečnosti (CYBERSEC)	150 Kč/os
Digitální bezpečnost: naučte se chodit v online světě bezpečně (SEDUO)	1290 Kč/os
Školení informační a kybernetické bezpečnosti (BOZP.cz)	240 Kč/os
Pravidla IT bezpečnosti pro zaměstnance (OKškolení)	770 Kč/os

Po zjištění ceny kurzů a seznámení se s jednotlivými sylaby kurzů, recenzemi a vyzkoušení demo verzí kurzu byla provedena samostatná bodovací metoda všech členů týmu. Každý člen týmu přidělil počet bodů kritériím srozumitelnost a přínosnost. Kritérium cena bylo hodnoceno pouze autorkou diplomové práce dle stanovené stupnice hodnocení, jelikož toto kritérium by bylo hodnoceno všemi hodnotiteli stejně.

Než přejdeme k samotným výsledkům a stanovení pořadí, je nutné popsat jednotlivá kritéria. Jak bylo zmíněno, první hodnocené kritérium je minimalizační. Tedy čím více je cena pro nás přípustná, tím více bodů daný kurz v rámci hodnocení obdrží. Rozpětí pro hodnocení můžeme vidět na níže uvedené tabulce.

Tabulka 4 Kritérium cena vlastní zpracování dle (Zapletal, 2023)

Cena – minimalizační kritérium	
1	**velmi vysoká** (od 2000 Kč/zaměstnanec)
2	**vysoká** (1000–2000 Kč/zaměstnanec)
3	**přiměřená** (do 500–1000 Kč/zaměstnanec)
4	**nízká** (do 500 Kč/zaměstnanec)
5	**zdarma**

Cenové rozpětí bylo v rámci slovního ohodnocení popsáno následujícím způsobem. Jedná-li se o kurz **zdarma**, bude danému kurzu přiděleno 5 bodů. Pokud se kurz nachází v cenové hladině do 500 Kč na jednoho zaměstnance, je cena kurzu považována za **nízkou** a bude takovýto kurz ohodnocen 4 body. V případě, že částka za provedení kurzu na jednoho zaměstnance vychází v rozmezí od 500 do 1 000 Kč, jedná se v případě našeho hodnocení o cenu **přiměřenou** a kurz bude ohodnocen 3 body. Je-li kurzovné na jednoho zaměstnance

v cenové hladině od 1 000 do 2 000 Kč, je takováto cena brána jako **vysoká** a daný kurz obdrží při hodnocení 2 body. Za situace, že cena za jednoho účastníka kurzu přesahuje 2 000 Kč, je cena hodnocena jako **velmi vysoká** a kurz bude ohodnocen 1 bodem.

Dalším kritériem při provádění hodnocení bylo kritérium srozumitelnosti daného školení či kurzu. Toto kritérium patří do kategorie maximalizačních kritérií, tedy čím více je kurz srozumitelný, tím více bodů v rámci daného hodnocení obdrží. Hodnotící stupni srozumitelnosti můžeme vidět znázorněnu v tabulce č. 5 níže.

Tabulka 5 Kritérium srozumitelnost vlastní zpracování dle (Zapletal, 2023)

Srozumitelnost – maximalizační kritérium	
1	**málo srozumitelný**
2	**méně srozumitelný**
3	**srozumitelný**
4	**více srozumitelný**
5	**absolutně srozumitelný**

Posledním kritériem pro námi zvolenou analýzu je kritérium přínosnosti daného kurzu. Toto kritérium stejně jako předchozí uvedené spadá do kategorie maximalizačních, tedy čím více přínosný kurz je, tím vyšší počet bodů od jednotlivých hodnotitelů obdrží. Stupnici hodnocení znázorňuje tabulka č. 6.

Tabulka 6 Kritérium přínosnost vlastní zpracování dle (Zapletal, 2023)

Přínosnost – maximalizační kritérium	
1	**málo přínosný**
2	**méně přínosný**
3	**přínosný**
4	**více přínosný**
5	**maximálně přínosný**

Po provedení hodnocení jednotlivými členy týmu došlo k výpočtu vah. Tento výpočet byl proveden jako geometrický průměr. Po provedení výpočtu vah u všech hodnocených kurzů bylo stanoveno pořadí daných kurzů. Kurz s nejvyšší váhou byl hodnocen jako nejvíce optimální. (Zapletal, 2023) Pořadí jednotlivých kurzů, včetně hodnocení a stanovených vah můžeme vidět v níže uvedené tabulce č. 7.

Tabulka 7 Hodnocení vybraných kurzů kybernetické bezpečnosti vlastní zpracování dle (Zapletal, 2023)

Hodnocení vybraných kurzů kybernetické bezpečnosti									
Název kurzu	Cena	Srozumitelnost			Přínosnost			Váhy	Pořadí
	H 2	H 1	H 2	H 3	H 1	H 2	H 3		
Základy kybernetické bezpečnosti 24	5	5	5	5	4	5	5	4,843	1.
Úvod do kybernetické bezpečnosti	1	2	3	2	2	2	1	1,738	6.
Školení kybernetické bezpečnosti	4	3	3	2	3	3	4	3,073	4.
Digitální bezpečnost: naučte se chodit v online světě bezpečně	2	2	4	3	2	3	2	2,479	5.
Školení informační a kybernetické bezpečnosti	4	4	4	3	5	4	2	3,589	3.
Pravidla IT bezpečnosti pro zaměstnance	3	4	5	4	5	5	4	4,224	2.

Na základě provedené bodovací metody sestaveným týmem se v pořadí na prvním místě umístil kurz **Základy kybernetické bezpečnosti 24** od NÚKIB. Tento kurz je nabízen zdarma široké laické veřejnosti a může být využit v soukromém i veřejném sektoru. Výhodou kurzu je, jak již bylo zmíněno, jeho bezplatnost. Rovněž zbylá dvě hodnocená kritéria jsou maximální. Samotný kurz je tvořen ze dvou částí – povinné a dobrovolné. (NÚKIB, 2024)

V rámci povinné části můžeme nalézt okruhy týkající se hesel a jejich tvorby, bezpečného odemykání zařízení, problematiky sociálního inženýrství, druhu škodlivých souborů a způsobů jejich šíření, možností soukromého připojení. Dobrovolné okruhy seznámí uživatele s pohledem na kybernetickou bezpečnost skrze média a osvětlí uživatelům vzdělávání dětí v oblasti kybernetické bezpečnosti. (NÚKIB, 2024)

Pro absolvování závěrečného testu a následné získání certifikátu je nutná registrace uživatele do tohoto portálu. Před spuštěním závěrečného testu je možné ověřit si své znalosti ve cvičné verzi testu. Absolvování cvičného testu není podmínkou pro vykonání závěrečného testu. Tento test slouží pouze ověření znalostí uživatele. Závěrečný test obsahuje 15 otázek, není zde stanoven časový limit a uživatel může využít dva pokusy pro jeho splnění. Po úspěšném absolvování testu obdrží uživatel certifikát. O tom, že je tento certifikát možné si uložit je uživatel informován skrze email, který zadal při registraci. Certifikát nalezne uživatel ve svém profilu, odkud si jej bude moci ve formátu PDF uložit do svého zařízení a následně vytisknout. (NÚKIB, 2024)

Na základě hodnocených aspektů se na druhém místě umístil kurz od společnosti OKškolení s názvem **Pravidla IT bezpečnosti pro zaměstnance**. Tento kurz řadíme do kategorie placených kurzů, kdy cena kurzu se odvíjí od počtu účastníků a typu námi zvolené varianty, při volbě varianty M, která je vhodná pro maximálně 50 účastníků vychází cena na jednoho posluchače 770 Kč. K Této ceně je nutné připočíst cestovní náklady školitele v případě, že školení nebude uskutečněno na území Prahy. Konkrétní varianty a cenové hladiny můžeme vidět na obrázku č. 5 níže. (OKškolení, 2023)

Cenová nabídka

	varianta S	varianta M	varianta L	varianta XL
počet zaměstnanců	< 20	< 50	< 100	> 100
počet běhů školení	1×2 hodiny	2×2 hodiny	4×2 hodiny	dle počtu účastníků
konzultace	2 hodiny	2 hodiny	4 hodiny	4 hodiny
příprava školení na míru	✓	✓	✓	✓
certifikát o absolvování kurzu	✓	✓	✓	✓
cena*	19 500 Kč	38 500 Kč	58 000 Kč	kontaktujte nás

* nezahrnuje DPH a cestovní a dopravní náklady mimo Prahu

Obrázek 5 Cenová nabídka společnosti OKškolení (OKškolení, 2023)

Součástí přípravy na školení je provedení konzultace mezi lektorem a IT manažerem dané společnosti, školení je uzpůsobeno na míru interním předpisům a rovněž díky provedení konzultace může řešit konkrétní problémy, které daná společnost řeší (např. špatné zálohování dát, neopatrné nakládání s osobními údaji a další). Školení je nabízeno online formou webináře nebo prezenčně za účasti odborného školitele v sídle zákazníka. V námi zvolené variantě M bude proškoleno celkem 50 osob, které budou rozděleny do dvou skupin. Časová dotace na jednu skupinu je dvě hodiny. Výhodou prezenčního způsobu provedení školení je přímá interakce účastníků kurzu se školitelem a uvedení praktických ukázek během provádění školení. (OKškolení, 2023)

V rámci školení se účastníci seznámí s typy škodlivého softwaru, pravidly pro fyzické zabezpečení počítače, tvorbu silného hesla, správného způsobu zálohování a skartace fyzických dokumentů. Rovněž jsou poskytnuty základní informace o šifrování dat a použití elektronického podpisu, metodách sociálního inženýrství. Po absolvování kurzu obdrží každý účastník certifikát. (OKškolení, 2023)

Třetí v pořadí se umístilo **Školení informační a kybernetické bezpečnosti** od společnosti BOZP.cz. Toto školení rovněž patří do kategorie placených, kdy však v rámci analýzy je jeho cena hodnocena jako nízká, přínosnost je hodnocena jako více přínosná a kurz je rovněž více srozumitelný. Tento kurz spadá do kategorie premium v rámci nabídky dané společnosti. Cena tohoto školení se odvíjí od počtu zúčastněných osob. Vezmeme-li v úvahu, že kurz využije do 50 zaměstnanců, bude cena za jednu osobu na rok 240 Kč (viz obrázek č. 6). S vyšším počtem účastníků cena za jednotlivce klesá. (BOZP, 2024)

Obrázek 6 Ceník kurzů společnosti BOZP.cz (BOZP, 2024)

Hodnocené školení je prováděno formou e-learningového kurzu. Obsah kurzu je obdobný jako u předchozího kurzu, avšak navíc jsou zde uživatelé proškoleni ohledně skartace tištěných dokumentů a zálohování dat. Účastníkům kurzu jsou rovněž předány způsoby, dle kterých lze poznat, zda daná webová stránka je podvodná či zda jejich email neobsahuje škodlivý soubor. Tento kurz je poskytován v českém a anglickém jazyce. Dle doporučení společnosti by měl být opakován jednou ročně. Po úspěšném složení závěrečného kurzu obdrží absolvent certifikát. (BOZP, 2024)

Tato zjednodušená bodovací metoda byla využita především pro svou srozumitelnost a přehlednost v případě užití laickou veřejností. Po průzkumu trhnu si hodnotitel stanoví hodnoticí kritéria pro dané kurzy dle svého uvážení. Touto efektivní metodou lze na základě provedené analýzy získat pro danou společnost nejvhodnější kurz.

8 STRUKTUROVANÉ ROZHOVORY SE SUBJEKTY OCHRANY OBYVATELSTVA ČESKÉ REPUBLIKY

Pro účely výzkumného šetření byla zvolena metoda kvalitativního výzkumu. Jako metoda pro sběr dat byl využit strukturovaný rozhovor, který byl s respondenty proveden osobně nebo formou emailové komunikace.

Pod pojmem kvalitativní výzkum rozumíme takový výzkum, který má za cíl popsat danou oblast pomocí perspektivy jednotlivých respondentů. Nejčastější metodou, jak můžeme provést tento výzkum, je skrze rozhovor.

8.1 Cíl výzkumného šetření

Cílem tohoto výzkumného šetření je získání informací o vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Výzkumné šetření je tedy zaměřeno na jednotlivé subjekty ochrany obyvatelstva, a to konkrétně na Policii ČR, Hasičský záchranný sbor, Zdravotnickou záchrannou službu, Armádu České republiky, Vězeňskou službu České republiky a na státní správu. V případě zjištění nedostačující úrovně vzdělávání bude navrženo opatření ke zvýšení dané úrovně, které bude aplikovatelné u jednotlivých složek dle jejich preferencí.

Před zahájením výzkumného šetření byly stanoveny následující výzkumné otázky:

1. Je v rámci pracovního zařazení respondenta prováděno školení kybernetické bezpečnosti?
2. Proběhne toto školení při nástupu nebo se jedná o periodické, nepravidelné školení?
3. Jak často školení probíhá?
4. Preferují respondenti spíše prezenční či online školení kybernetické bezpečnosti?

8.2 Charakteristika výzkumného vzorku

Do výzkumného vzorku byl zařazen vždy jeden zástupce konkrétního subjektu ochrany obyvatelstva. Věkové spektrum respondentů je do 22 do 50 let. Dotazníkové šetření bylo vedeno anonymní formou s užitím pseudonymu a v případě zájmu respondenta došlo k uvedení jeho osobních údajů na začátku transkripce konkrétního rozhovoru.

Tabulka 8 Záznamy o účastnících rozhovoru (Vlastní zpracování)

P. č.	Anonymní forma	Složka	Datum oslovení	Datum odpovědi	Realizace rozhovoru	Forma realizace rozhovoru
1.	NE	PČR	11.3.2024	11.3.2024	13.3.2024	Osobně
2.	ANO	HZS	11.3.2024	11.3.2024	14.3.2024	Email
3.	NE	ZZS	11.3.2024	11.3.2024	16.3.2024	Osobně
4.	ANO	Vězeňská služba	11.3.2024	11.3.2024	15.3.2024	Osobně
5.	ANO	Státní správa	11.3.2024	11.3.2024	18.3.2024	Osobně
6.	NE	AČR	11.3.2024	11.3.2024	12.3.2024	Osobně

8.3 Metodika

Jako forma výzkumného šetření byl zvolen strukturovaný rozhovor, který byl rozdělen na dvě části.

První demografická část nám přinesla základní údaje o vykonávané pracovní/služební činnosti respondenta včetně délky pracovního/služebního poměru na zastávané pozici.

V druhé části bylo respondentovi položeno 8 otevřených otázek týkajících se vzdělávání v oblasti kybernetické bezpečnosti v rámci jím zastávané pozice.

Tabulka 9 Otázky strukturovaného rozhovoru (Vlastní zpracování)

P. č.	Název otázky
1.	Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?
2.	Byl/a jste seznámen/a v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?
3.	Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?
4.	Setkal/a jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil/a?
5.	Absolvoval/a jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?
6.	Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?
7.	Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?
8.	Měl/a byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

Ve výše uvedené tabulce č. 9 můžeme vidět jednotlivé otevřené otázky, které byly součástí strukturovaných rozhovorů.

8.4 Realizace výzkumného šetření

Formulace otázek strukturovaného rozhovoru byla provedena v týdnu 4. 3.–10. 3. 2024, kdy byly rovněž vytvořeny formuláře pro informovaný souhlas pro každého respondenta. V rámci tohoto týdne byl proveden výběr respondentů, kteří byli telefonicky osloveni s žádostí o účast ve výzkumném šetření.

Dotazník byl následně distribuován respondentům formou emailu, kdy v případě osobní schůzky byl telefonicky sjednán termín setkání. Sběr dat probíhal od 11. 3. 2024 do 21. 3. 2024.

8.5 Transkripce strukturovaných rozhovorů

Před zahájením rozhovoru bylo provedeno s respondentem seznámení s tématem diplomové práce formou daného výzkumného šetření a cílem výzkumu.

8.5.1 Respondent Policie České republiky

Respondent č. 1 – Bc. Filip Krejčí, který je členem Policie České republiky, kde pracuje na pozici policejního potápěče, dále je jmenovaný také lektor/instruktor pro potřebu Police České republiky v oblastech vyplývající ze služebního zařazení, revizní technik, servisní technik, školitel servisních techniků vybavení pro potřebu Policie České republiky související se služebním zařazením. Na zastávané pozici je zařazen po dobu 16 let. Jmenovaný rovněž v rámci rozšíření své kvalifikace studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati. Respondent souhlasí s uveřejněním osobních údajů – jména, příjmení.

Se jmenovaným byl proveden osobní rozhovor dne 13. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Výpočetní technologii pro pracovní účely využívám ve dvou režimech. Intranet: interní vnitřní síť, pro zpracovávání činnosti související s náplní práce, komunikace v rámci PČR. Internet: za účelem komunikace mimo resort PČR, případně využíván k zjišťování informací souvisejících s výkonem služby.*

V rámci pracoviště není síť internet a intranet na jednom zařízení. Pro potřebu vykonávání činnosti v režimu homeoffice je některým pracovníkům umožněn přístup přes více faktorové ověření a token. Tento režim výpočetní techniky a systém přístupů jsem zatím nebyl nucen využít.“ (osobní rozhovor, dne 13.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ano, v rámci vstupního školení jsem byl seznámen. Jelikož PČR zpracovává citlivé údaje, proběhlo rovněž školení na neoprávněné nakládání s těmito údaji. K pravidelnému seznamování s hrozbami v oblasti kybernetické bezpečnosti dochází prostřednictvím interního komunikačního systému, v nedávné době bylo například provedeno školení, které se zaměřovalo na chování příslušníků PČR na sociálních sítích, kde bylo vysvětleno, co je a co není vhodné na těchto platformách sdílet a z jakých důvodů, rovněž byly rozebrány v rámci dalších školení i nejčastější kybernetické hrozby, se kterými se můžeme setkat. Školení probíhá jednou až dvakrát ročně“ (osobní rozhovor, dne 13.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„Přímo s mojí pozicí policejního potápěče ke školení v dané oblasti nedochází. K seznamovaní s kybernetickou bezpečností dochází plošně v rámci interního komunikačního systému PČR.“ (osobní rozhovor, dne 13.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Pokud by takový útok proběhl v souvislosti s mojí služební činností, obrátil bych se na IT oddělení PČR a informoval svého přímého nadřízeného, tak jak mi ukládají interní předpisy. U kolegů jsem zaznamenal útok zvaný ransomware, ale bylo to na soukromém zařízení nesouvisející se zaměstnáním.“ (osobní rozhovor, dne 13.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„V rámci svého služebního zařazení jsem žádný kurz neabsolvoval nebo si již nevzpomínám. Během studia jsem absolvoval kurz Bezpečně v kyber od NÚKIB.“ (osobní rozhovor, dne 13.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„Vzhledem k probíhajícímu studiu a vlastního soukromého zájmu o výpočetní technologie a kybernetickou bezpečnost nejsem schopen rozlišit, které informace jsem získal v rámci proškolení zaměstnavatelem, a které jsou získané soukromě. Určitě se jako v ostatních oblastech i zde najde prostor pro případné zlepšení.“ (osobní rozhovor, dne 13.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Za sebe mohu říci, že ideální je pro mě kombinace e-learningu a odborného školitele.“ (osobní rozhovor, dne 13.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„O rozšířené vzdělání nad rámec plošného informování v rámci zaměstnání bych zájem měl. Získané informace v rámci zaměstnání jsou mi prospěšné i v osobním životě. Rozšiřuje to povědomí, čemu se vyvarovat a na co si dát pozor.“ (osobní rozhovor, dne 13.3.2024)

8.5.2 Respondent Hasičského záchranného sboru České republiky

Respondent č. 2 je členem Hasičského záchranného sboru České republiky. Na zastávané pozici je zařazen po dobu 9 let. Jmenovaný zvolil variantu anonymního rozhovoru bez uvedení osobních údajů.

Se jmenovaným byl proveden emailový rozhovor dne 14. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Ano, výpočetní technologii pro pracovní účely každý den.“* (emailový rozhovor, dne 14.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ano.“ (emailový rozhovor, dne 14.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„Ano, získávání informací probíhá každý rok formou e-learningu.“ (emailový rozhovor, dne 14.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Ano, jednalo se o emailové útoky, incident byl řešen na příslušném oddělení KIS.“ (emailový rozhovor, dne 14.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„Ano, přesné znění kurzu již nevím.“ (emailový rozhovor, dne 14.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„Ano.“ (emailový rozhovor, dne 14.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Preferuji e-learning.“ (emailový rozhovor, dne 14.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„Nejspíše ne, v osobním životě téměř nevyužiji.“ (emailový rozhovor, dne 14.3.2024)

8.5.3 Respondent Zdravotnické záchranné služby

Respondent č. 3 – Bc. Jan Slánský, který je členem Zdravotnické záchranné služby, kde pracuje na pozici zdravotnický záchranář na oddělení ARO. Na zastávané pozici je zařazen po dobu jednoho roku. Jmenovaný rovněž v rámci rozšíření své kvalifikace studuje obor Ochrana obyvatelstva na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati. Respondent souhlasí s uveřejněním osobních údajů – jména, příjmení.

Se jmenovaným byl proveden osobní rozhovor dne 16. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Ano, v rámci svého zařazení využívám výpočetní technologie každý den.“* (osobní rozhovor, dne 16.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ano, je po nás požadováno absolvování online kurzu od NÚKIB a složení závěrečného testu.“ (osobní rozhovor, dne 16.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„Ano, za dobu mého pracovního poměru (1 rok) došlo k jednomu proškolení v oblasti kybernetické bezpečnosti prostřednictvím kurzu od NÚKIB.“ (osobní rozhovor, dne 16.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Doposud jsem se s žádným druhem útoku nesetkal. V případě, že by taková situace nastala, obrátil bych se na úsek výpočetní techniky.“ (osobní rozhovor, dne 16.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„Ano, absolvoval jsem Minimum kybernetické bezpečnosti pro zdravotnictví 24. Dále jsem během studia jsem absolvoval kurz Bezpečně v kyber od NÚKIB.“ (osobní rozhovor, dne 16.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„Ne, mnoho zaměstnanců ani netuší, že vůbec nějaké hrozby existují.“ (osobní rozhovor, dne 16.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Raději formou přednášek s odborným školitelem. E-learning nikoho nebaví a každý to jen prokliká.“ (osobní rozhovor, dne 16.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„Ano měl, přijde mi to jako zajímavé odvětví, ve kterém je důležité se orientovat v dnešní době.“ (osobní rozhovor, dne 16.3.2024)

8.5.4 Respondent Vězeňské služby České republiky

Respondent č. 4 je členem Vězeňské služby České republiky, kde pracuje na pozici dozorce. Na zastávané pozici je jmenovaný zařazen po dobu 16 let. Respondent č. 4 zvolil možnost anonymního rozhovoru bez uvedení osobních údajů.

Se jmenovaným byl proveden osobní rozhovor dne 15. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Ano, výpočetní technologie používám na denní bázi.“* (osobní rozhovor, dne 15.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ano, bylo provedeno vstupní školení.“ (osobní rozhovor, dne 15.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„Ano, probíhá periodické školení v oblasti kybernetické bezpečnosti. Školení je vedeno formou e-learningových kurzů, které jsou zakončeny testem.“ (osobní rozhovor, dne 15.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Osobní zkušenost s jakýmkoliv druhem útoku nemám. Pokud bych se stal obětí takového útoku, obrátil bych se na IT specialisty v naší věznici.“ (osobní rozhovor, dne 15.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„Ne, žádný volně dostupný kurz jsem doposud neabsolvoval.“ (osobní rozhovor, dne 15.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„V rámci mého služebního zařazení mi přijde úroveň dostačující.“ (osobní rozhovor, dne 15.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Preferuji možnost e-learningu.“ (osobní rozhovor, dne 15.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„Ne, zájem nemám. Myslím, že mi to do osobního života nedá žádný prospěch.“ (osobní rozhovor, dne 15.3.2024)

8.5.5 Respondent státní správy

Respondent č. 5 je zástupcem státní správy – samosprávy, kde zastává funkci starosta obce. V oblasti samosprávy se jmenovaný pohybuje po dobu 22 let. Respondent č. 5 zvolil možnost anonymního rozhovoru bez uvedení osobních údajů.

Se jmenovaným byl proveden osobní rozhovor dne 18. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Ano, v rámci mnou zastávané funkce využívám na denní bázi výpočetní technologie a internet.“* (osobní rozhovor, dne 18.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ano, v rámci vstupního školení při nástupu do funkce jsem byl seznámen se zásadami a riziky v rámci kyberprostoru.“ (osobní rozhovor, dne 18.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„V současné chvíli u nás žádné takové školení neprobíhá a není v současné chvíli plánováno.“ (osobní rozhovor, dne 18.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Doposud jsem se v rámci svého pracovního ani osobního života s žádným takovým incidentem nesetkal. V případě, že by tato situace nastala, obrátil bych se na Policii ČR.“ (osobní rozhovor, dne 18.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„Doposud jsem žádný volně dostupný kurz neabsolvoval.“ (osobní rozhovor, dne 18.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„Asi ne a budu zvažovat kroky ke zlepšení současného stavu.“ (osobní rozhovor, dne 18.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Vyhovují mi oba způsoby vzdělávání stejnou mírou.“ (osobní rozhovor, dne 18.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„V současné chvíli nevím, tuto variantu však v rámci budoucna nezavrhuji. Věřím, že vzdělávání by mohlo mít prospěch i v mém osobním životě.“ (osobní rozhovor, dne 18.3.2024)

8.5.6 Respondent Armády České republiky

Respondent č. 6 – podplukovník Ing. Martin Bursa je příslušníkem AČR a slouží na Univerzitě obrany jako zástupce velitele školního pluku. Jmenovaný je ve služebním poměru vojáka z povolání 25 let, na pozici zástupce velitele školního pluku je služebně zařazen po dobu čtyř let. Respondent souhlasí s uveřejněním osobních údajů – jména, příjmení.

Se jmenovaným byl proveden osobní rozhovor dne 12. března 2024.

O1 – Vyžaduje Vaše pracovní zařazení využívání výpočetních technologií a/nebo internetu?

K otázce jmenovaný uvedl: *„Ano, na mém pracovišti využívám výpočetní technologii včetně internetu.“* (osobní rozhovor, dne 12.3.2024)

O2 – Byl jste seznámen v rámci vstupního školení pro danou pozici se zásadami kybernetické bezpečnosti a riziky v kyberprostoru?

„Ne, v rámci vstupního školení na dané pozici jsem nebyl se zásadami kybernetické bezpečnosti a riziky v kyberprostoru seznámen či proškolen.“ (osobní rozhovor, dne 12.3.2024)

O3 – Probíhá v rámci Vaší pozice v nějaké formě vzdělávání v oblasti kybernetické bezpečnosti? Pokud ano, jak často a jakou formou je vedeno?

„Ano, v současné době probíhá cestou Národního úřadu pro kybernetickou a informační bezpečnost školení k základům kybernetické bezpečnosti, a to každým rokem.“ (osobní rozhovor, dne 12.3.2024)

O4 – Setkal jste se Vy nebo některý z Vašich kolegů někdy v rámci svého zařazení s kybernetickým bezpečnostním incidentem? Na koho byste se v takové situaci obrátil?

„Ano, v loňském roce cestou virtuálního profilu došlo k napadení složek na pracovišti mého zaměstnavatele. Řešila to součást, která má na starosti KIS v součinnosti s NÚKIB.“ (osobní rozhovor, dne 12.3.2024)

O5 – Absolvoval jste v rámci Vámi zastávané pozice některý z volně dostupných kurzů kybernetické bezpečnosti? V případě, že ano, o jaký kurz se jednalo?

„Ne, jiný, než kurz od NÚKIB jsem neabsolvoval.“ (osobní rozhovor, dne 12.3.2024)

O6 – Připadá Vám současná úroveň vzdělávání v oblasti kybernetické bezpečnosti na Vaší pozici jako dostačující?

„Ano, připadá.“ (osobní rozhovor, dne 12.3.2024)

O7 – Preferujete raději školení formou e-learningových kurzů nebo formou přednášek s odborným školitelem?

„Preferuji školení formou přednášek s odborným školitelem v případě malého kolektivu, pokud má pracoviště mnoho zaměstnanců, tak preferuji školení formou e-learningových kurzů.“ (osobní rozhovor, dne 12.3.2024)

O8 – Měl byste zájem o rozšíření vzdělávání v oblasti kybernetické bezpečnosti v rámci Vámi zastávané pozice? Přináší Vám toto vzdělávání prospěch i v rámci osobního života?

„Ano, zájem o rozšířené vzdělávání bych měl. Jakékoliv vzdělání využívám i v osobním životě.“ (osobní rozhovor, dne 12.3.2024)

8.6 Vyhodnocení a analýza získaných dat

Šetření bylo vyhodnoceno za pomoci námi stanovených výzkumných otázek. Nejdříve byla vyhodnocena demografická data, a to především délka služebního/pracovního zařazení na zastávané pozici.

Tabulka 10 Doba na zastávané funkci (Vlastní zpracování)

Doba na zastávané pozici	Četnost absolutní	Četnost relativní (%)
1–5 let	1	16,66 %
6–15 let	1	16,66 %
16–25 let	4	66,66 %
26 let a více	0	0 %
Celkem	**6**	**100 %**

Méně než 15 let jsou na zastávané funkci 2 respondenti (33, 32 %), 15 let a více vykonává danou pozici 66.6 % respondentů.
Po vyhodnocení demografických údajů můžeme přejít k zodpovězení výzkumných otázek.

VO č. 1 – Je v rámci pracovního zařazení respondenta prováděno školení kybernetické bezpečnosti?

U 100 % respondentů bylo/je prováděno školení v oblasti kybernetické bezpečnosti.

Nejčastěji se jedná o absolvování kurzu NÚKIB, ať už obecného kurzu pro širokou veřejnost nebo profesně zaměřeného kurzu (např. pro pracovníky ve zdravotnictví či státní správě).

VO č. 2 – Je toto školení při nástupu nebo se jedná o periodické, nepravidelné školení?

U 83, 33 % respondentů bylo provedeno vstupní školení kybernetické bezpečnosti, zároveň 83,33 % respondentů absolvuje školení periodicky alespoň jednou ročně a ve většině případů se jedná o školení formou e-learningového kurzu, které je ukončeno testem. U zástupce samosprávy bylo provedeno pouze vstupní školení, periodické školení neprobíhá a v současné chvíli není plánováno.

VO č. 3 – Jak často školení probíhá?

U respondentů č. 2, 3, 4 a 6 probíhá školení jednou ročně ve formě e-learningového kurzu. Respondent č. 1 uvedl, že školení u jeho složky probíhá jednou až dvakrát ročně. V rámci pracovního zařazení respondenta č. 5 nedochází k pravidelnému školení.

VO č. 4 – Preferují respondenti spíše prezenční či online školení kybernetické bezpečnosti?

Třetina respondentů uvedla, že za preferovanou formu vzdělávání považuje e-learningový kurz, a to především z důvodu úspory času. Druhá třetina volí raději formu přednášek. Zbylé třetině respondentů nejvíce vyhovuje kombinace e-learningu a přednášek odborného školitele.

9 NÁVRH OPATŘENÍ KE ZVÝŠENÍ ÚROVNĚ VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V rámci provedeného šetření bylo zjištěno, že alespoň jednou ročně probíhá školení v oblasti kybernetické bezpečnosti, kdy 50 % respondentů hodnotí úroveň vzdělávání jako dostačující, 33, 33 % považuje současný stav vzdělávání na své pozici jako nedostačující a 16,66 % respondentů uvádí, že v rámci vzdělávání je stále prostor pro zlepšení daného stavu.

Zároveň z provedeného šetření vyplývá, že 50 % respondentů by mělo zájem o rozšíření vzdělání v oblasti kybernetické bezpečnosti, druhá polovina respondentů považuje současné vzdělání za dostatečné a o jeho rozšíření nemá zájem, především z důvodu, že jim toto vzdělávání nepřijde potřebné a nevidí z něj užitek v rámci osobního života.

V rámci návrhů ke zlepšení současného stavu mi přijde jako vhodný návrh řešení vytvoření **Plánu vzdělávání v oblasti kybernetické bezpečnosti** na kalendářní rok (dále jen „plán“). Součástí tohoto plánu je výčet oblastí, které by bylo potřebné proškolit a následně bude popsána forma realizace jednotlivých školení (včetně jejich osnovy a časové dotace). Plán bude obsahovat sumarizaci hodin školení po jednotlivých čtvrtletích.

Odpovědnost za zpracování plánu bude dána do rukou bezpečnostnímu manažerovi daného subjektu (dále jen „BM“). Součinnost při zpracování plánu bude poskytnuta úsekem komunikačních a informačních technologií, rovněž oddělením bezpečnosti informací a vedoucími jednotlivých součástí.

Plánování jako takové je dlouhodobý proces, který vyžaduje součinnost a preciznost všech zainteresovaných osob. Tvorba daného plánu na rok 2025 započne již ve druhém čtvrtletí roku 2024, díky čemuž bude zajištěn dostatečný prostor na jeho připomínkové řízení a následný schvalovací proces skrze top management daného subjektu.

Samotný proces tvorby plánu bude probíhat následovně:

- Sumarizace proškolovaných oblastí skrze jednotlivé garanty.
- Tvorba harmonogramu a osnov školení, vyčlenění prostor pro školení.
- Připomínkové řízení plánu.
- Předložení plánu k posouzení a schválení.

Před tvorbou daného školení je potřebné vymezit si, pro jakou skupinu zaměstnanců je dané školení určeno. Pro účely návrhu plánu vzdělávání v rámci mé diplomové práce byli zaměstnanci rozděleni do následujících skupin:

- Zaměstnanci s přístupem k výpočetní technice.
- Vedoucí zaměstnanci.

Rovněž je důležité ujasnit si, jakým způsobem bude školení realizováno:

- Prezenčně za účasti interního školitele.
- Prezenčně za účasti externího školitele.
- Distančně formou přednášky za účasti interního školitele.
- Distančně formou přednášky za účasti externího školitele.
- Distančně formou samostudia v rámci vzdělávacího portálu.

Při procesu plánování vzdělávání musí být rovněž určena forma ověření znalostí posluchačů:

- Test na PC.
- Diskuse.

V případě testů je rovněž potřebné stanovit si počet pokusů na splnění daného testu a kritérium úspěšnosti daného ověřování (například minimální úspěšnost testu stanovena na 90 % správných odpovědí).

Rovněž bude v rámci daného subjektu určena osoba odpovědná za vedení dokumentace týkající se vzdělávání v oblasti kybernetické bezpečnosti. Nejčastěji je touto osobou BM nebo jím pověřená osoba.

V níže uvedené tabulce můžeme vidět přehled školení, která jsou potřeba v rámci kalendářního roku realizovat a určené čtvrtletí, ve kterém by bylo nejvhodnější dané školení absolvovat. Rovněž je součástí tabulky informace, zda je dané školení periodické – v tabulce označeno jako „P“ – či neperiodické – v tabulce označeno jako „N“.

Tabulka 11 Výčet témat školení (Vlastní zpracování)

Název školení	Vyčleněné čtvrtletí	Pravidelnost školení
Ochrana utajovaných informací	1. čtvrtletí	P
Nakládání se služebním zařízením a datovými nosiči, pravidla pro bezpečný pohyb na síti	1. čtvrtletí	P
Základy kybernetické bezpečnosti	1. čtvrtletí	P
Nejčastější kybernetické útoky	2. čtvrtletí	N
Kyberšikana, její formy a právní dopady	2. čtvrtletí	N
Šifrování a elektronický podpis	3. čtvrtletí	N

Problematiku, kterou je potřebné proškolovat periodicky, je nejvhodnější zařadit do prvního čtvrtletí, konkrétněji do měsíců leden a únor. Tímto krokem docílíme toho, že zaměstnanci snáze a rychleji získané znalosti a dovednosti aplikují do své každodenní praxe. Mezi periodická školení doporučuji řadit ochranu utajovaných informací, pravidla pro manipulaci se služebním zařízením (počítač, notebook, mobilní telefon) a pokyny pro použití služebních datových médií, jako jsou USB flash disky a paměťové karty, pevné disky a další. Rovněž je vhodné mezi periodická školení začlenit kurz základů kybernetické bezpečnosti.

Naopak rozšiřující školení, která nejsou prováděna každoročně (z důvodu obměny témat dle aktuálních potřeb společnosti), je vhodné integrovat do plánu v rámci druhého a třetího čtvrtletí roku 2025. Včlenění daných školení do této části roku je za mě vhodné především z toho důvodu, že již budou mít zaměstnanci absolvována veškerá povinná školení a úvod do problematiky kybernetické bezpečnosti, tedy základy, na kterých je možné stavět a které lze v rámci dalších školení rozvíjet. Po absolvování vzdělávání ve druhém čtvrtletí je z hlediska prověření získaných znalostí a dovedností vhodné realizovat simulaci phishingového útoku. Po realizaci simulace bude provedeno vyhodnocení, se kterým budou všichni zaměstnanci seznámeni a rovněž na základě tohoto vyhodnocení budou přijata opatření ke zlepšení stavu, v případě, že by došlo k velkému výskytu nedostatků.

Na závěr, v rámci čtvrtého čtvrtletí, dojde k vyhodnocení úkolů stanovených v plánu. Na základě tohoto vyhodnocení dojde k přijetí opatření, která budou zanesena do plánu na následující kalendářní rok.

Nyní budou popsány jednotlivé oblasti, které byly vybrány k proškolení, včetně osnovy školení, formy provedení, časové dotace a formy reportingu o průběhu plnění.

První oblastí určenou pro provedení periodického proškolení je **Ochrana utajovaných informací** určených dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tato oblast bude proškolena za pomoci absolvování e-learningového kurzu, jako výuková metoda bude zvoleno samostudium. Tvorbou daného kurzu bude pověřen BM subjektu. Školení se bude skládat z prezentací k dané problematice a závěrečného testu, na jehož splnění bude mít zaměstnanec 2 pokusy. Časová dotace pro dané školení je stanovena na 2 hodiny. Zaměstnanci budou povinni dané školení dokončit do poloviny února roku 2025. Díky volbě proškolení skrze e-learning bude zajištěn průběžný přehled o plnění daného školení pro jednotlivé vedoucí součástí.

V rámci tohoto školení budou posluchači seznámeni se základním členěním utajovaných informací, legislativou dané oblasti, druhy zajištění ochrany utajovaných informací s rozpracováním po jednotlivých oblastech.

V rámci prvního čtvrtletí bude rovněž proškoleno **Nakládání se služebním zařízením a datovými médii a pravidla pro bezpečný pohyb na síti**. Toto školení bude realizováno za pomoci přednášky zaměstnanců oddělení informačních technologií daného subjektu na platformě MS Teams. Tato přednáška nebude ukončena závěrečným testem, každý účastník stvrdí svou účast na proškolení podpisem do prezenční listiny uložené u vedoucího dané součásti nebo zápisem do elektronické třídní knihy. Přednáška bude realizována vybraný den v měsíci leden, kdy v případě nepřítomnosti zaměstnance na pracovišti bude možné si pustit záznam přednášky zpětně. Přednášku bude povinné absolvovat do konce února 2025. Doba trvání školení je stanovena na 2 hodiny.

Osnova přednášky bude znázorněna výčtem níže uvedených bodů:

- Fyzické zabezpečení počítače, zamezení odcizení zařízení a dat při opuštění kanceláře, bezpečnost dat na přenosových médiích.
- Možnosti bezpečného přihlášení, tvorba silného hesla a bezpečný pohyb na internetu a intranetu.
- Problematika vzdáleného přístupu.
- Pravidla pro použití služebních zařízení.

V neposlední řadě je žádoucí v rámci prvního čtvrtletí provést proškolení **Základů kybernetické bezpečnosti**. Pro tyto účely můžeme využít kurzy, které jsme si vyhodnotili za pomoci bodovací metody v kapitole 7.2. Pro účely tvorby plánu byl zvolen kurz Základy kybernetické bezpečnosti od NÚKIB, který je každoročně aktualizován tak, aby reflektoval nejnovější poznatky z oblasti kybernetické bezpečnosti. Pro využití všech funkcionalit, které kurz nabízí, je nutná registrace každého zaměstnance. Tu lze udělat hromadně, kdy následně každému zaměstnanci budou zaslány přihlašovací údaje pro vstup do vzdělávacího portálu.

Kurz základů kybernetické bezpečnosti je organizován pomocí e-learningu za využití samostudia. Kurz je zakončen testem, po jehož úspěšném absolvování je posluchači zaslán certifikát. Časová dotace pro splnění daného kurzu je 10 hodin.

Po splnění série periodických školení nastává čas na rozšíření získaných znalostí. Jako první bude v rámci druhého čtvrtletí realizována přednáška na téma **Nejčastější kybernetické útoky**.

Tuto přednášku provede odborný školitel prezenčně na adrese zákazníka. Jako vhodná společnost pro provedení vzdělávání v dané oblasti byla za pomoci bodovací metody zvolena firma okškolení.cz, která nabízí školení přímo na míru danému subjektu. Během vstupní konzultace budou požadavky předány školiteli skrze bezpečnostního manažera a vedoucího zaměstnance v úseku informačních technologií. Následně bude sestavena osnova dané přednášky a vytvořeny vzdělávací materiály, které obdrží každý účastník. Školení bude realizováno ve dvou rotacích, kdy každá rotace má stanovenou časovou dotaci 2 hodiny. Výhodou této formy vzdělávání je přímá interakce posluchačů se školitelem, možnost kladení dotazů, na které při volbě e-learningu není prostor a vyšší míra upoutání pozornosti posluchače skrze ukázky z praxe.

Součástí přednášky budou nejznámější typy kybernetických útoků včetně příkladů kybernetických bezpečnostních incidentů v ČR i v zahraničí. Rovněž do přednášky budou zahrnuty ukázky phishingových emailů, ukázka smishingu či škodlivých souborů přiložených v rámci emailové komunikace. V rámci přednášky budou posluchači seznámeni s praktikami sociálního inženýrství a získají základní povědomí o šíření dezinformací.

Realizace přednášky na téma **Kyberšikana, její formy a právní dopady** bude provedena rovněž během druhého čtvrtletí za pomoci přednášejícího z řad Policie České republiky. Přednáška bude prezenční formou s časovou dotací 2 hodiny.

Součástí přednášky je obecný úvod do problematiky šikany a kyberšikany, představení aktérů kyberšikany a jednotlivých druhů kyberšikany jako jsou kyberstalking, kybergrooming, sexting a další. Rovněž budou posluchači seznámeni s jednotlivými druhy právních postihů a možnostmi poskytnutí pomoci v případě, že se stanou oběťmi kyberšikany. V rámci této oblasti je osvětová činnost velmi důležitá, a to především z důvodu, že mezi zaměstnanci jsou i rodiče, kteří doposud neměli o kyberšikaně žádné povědomí a nemuseli ji tak u svých dětí rozpoznat. Tento fakt je důkazem, že vzdělávání v rámci zaměstnání může přinést využití i v osobním životě posluchačů.

Na období třetího čtvrtletí je plánováno školení na téma **Šifrování dat a elektronický podpis**, tato vzdělávací aktivita bude realizována formou e-learningu za využití samostudia. Jedná se o výběrové školení pro vedoucí zaměstnance, kteří s elektronickým podpisem přichází do kontaktu, toto školení nebude povinné pro běžné zaměstnance.

Účastníci kurzu budou seznámeni s úvodem do kryptografie, metodami šifrování dat, tvorbou elektronického podpisu a jeho ověřením, druhy elektronických podpisů, které jsou v rámci České republiky uznávány.

Během čtvrtého čtvrtletí dojde k ověření získaných znalostí a dovedností zaměstnanců formou **simulace phishingového útoku**, kde bude sledována schopnost reakce jednotlivých zaměstnanců. Simulaci útoku vytvoří zaměstnanci IT oddělení daného subjektu. V rámci časového rozmezí dvou až tří týdnů bude rozesláno několik phishingových emailů. Bude sledována reakce zaměstnanců – otevření daného emailu, kliknutí na přiložený odkaz a četnost hlášení podezřelého emailu pověřenému zaměstnanci/bezpečnostnímu manažerovi.

Po provedení bude simulace vyhodnocena a výsledky budou prezentovány nadřízeným, následně bude provedeno vyhodnocení i pro zaměstnance daného subjektu, kde budou phishingové emaily spolu se statistikou ukázány. Na základě vyhodnocení tohoto testování budou přijaty návrhy na zlepšení cestou BM ve spolupráci s vedoucím IT oddělení.

V rámci posledního čtvrtletí bude plán vzdělávání vyhodnocen odpovědnou osobou a dojde k vytvoření dílčích úkolů a úpravě plánu na následující kalendářní rok.

Tabulka 12 Časová dotace jednotlivých čtvrtletí (Vlastní zpracování)

Rok 2025				
1. čtvrtletí	**2. čtvrtletí**	**3. čtvrtletí**	**4. čtvrtletí**	**Celkem hodin**
14	4	2	0	**20**

Z výše uvedené tabulky je patrné, že největší časová náročnost je v rámci prvního čtvrtletí, kde budou provedena periodická školení tak, jak bylo uvedeno na začátku tvorby plánu. Naopak v rámci posledního čtvrtletí daného kalendářního roku je uveden počet hodin nula, a to z důvodu, že v rámci daného čtvrtletí dojde k provedení simulace phishingových útoků na dané uživatele a není tak možné časovou dotaci vyčíslit.

Tvorba plánu vzdělávání v oblasti kybernetické bezpečnosti se jeví jako vhodný návrh řešení ke zvýšení úrovně vzdělávání v jednotlivých subjektech. Jedná se o efektivní nástroj, který nám promítne přesný rozpis jednotlivých vzdělávacích aktivit, časovou náročnost a obsah jednotlivých kurzů. Díky součinnosti osob z různých součástí budou do tohoto plánu začleněny všechny stěžejní oblasti, které jsou určeny k proškolení.

Pro ověření aplikovatelnosti daného návrhu byl tento plán předložen ke zhodnocení Ing. Pavlovi Větrovskému, který pracuje jako Bezpečnostní manažer Univerzity obrany. Jmenovaný provedl celkové zhodnocení daného návrhu, které rozdělil do jednotlivých segmentů (cena, technická náročnost, obsah). Z hodnocení plyne, že daný návrh plánu se jeví jako aplikovatelný a využitelný v praxi. Podrobné hodnocení je obsaženo v příloze č. 3 této diplomové práce.

ZÁVĚR

Téma vzdělávání v oblasti kybernetické bezpečnosti díky rychlému rozvoji informačních a komunikačních technologií dostává stále větší míru významnosti. Skrze vzdělané a reakce schopné zaměstnance mohou dané společnosti mnohem lépe čelit vzrůstajícímu počtu kybernetických útoků.

Předmětem diplomové práce bylo posoudit a zhodnotit současný stav vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva a dále zhodnotit vybrané kurzy kybernetické bezpečnosti. Na základě provedených analýz byl vytvořen návrh opatření, které povede ke zvýšení úrovně vzdělávání v subjektu ochrany obyvatelstva.

Teoretická část této diplomové práce byla zaměřena na výklad právních norem, vymezení vybraných pojmů z oblasti kybernetické bezpečnosti a seznámení se s vybranými významnými kybernetickými bezpečnostními incidenty na území České republiky a v zahraničí.

Praktickou část diplomové práce tvoří analýza kurzů kybernetické bezpečnosti dostupných v České republice, kdy z daného množství bylo vybráno za pomoci metody brainstormingu šest kurzů, které byly následně podrobeny bodovací metodě za účelem volby optimální varianty kurzu. Bodovací metodu provedl tříčlenný expertní tým. V druhé polovině praktické části byly provedeny strukturované rozhovory s respondenty z jednotlivých subjektů ochrany obyvatelstva.

V rámci daného šetření bylo zjištěno, že u všech respondentů bylo provedeno alespoň vstupní školení kybernetické bezpečnosti. Zároveň 50 % respondentů by mělo zájem o rozšíření vzdělávání v rámci zastávané pozice.

Při realizaci návrhové části opatření byl jako návrh řešení zvolen Plán vzdělávání v oblasti kybernetické bezpečnosti na kalendářní rok. Součástí tohoto plánu byla sumarizace oblastí vhodných k provedení proškolení, přehled časové dotace potřebné k provedení školení po jednotlivých čtvrtletích a charakteristika realizovaných vzdělávacích aktivit. K realizaci vzdělávání byly využity jak kurzy, které v rámci bodovací metody vyšly jako nejvíce vhodné, tak vzdělávání zaměstnanců za využití interních školitelů. Na závěr byl kurz zhodnocen bezpečnostním manažerem Univerzity obrany.

Závěrem je zřejmé, že vzdělávání v oblasti kybernetické bezpečnosti je pro efektivní fungování společnosti opravu důležité. Proto je nezbytné tomuto procesu věnovat náležitou pozornost a důsledně usilovat o zlepšení současného stavu vzdělávacího prostředí. Díky tomuto shrnutí lze uvést, že cíle diplomové práce byly splněny.

Seznam použité literatury

AČR, 2023. *VELITELSTVÍ INFORMAČNÍCH A KYBERNETICKÝCH SIL*. Online. Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/. [cit. 2024-01-20].

AFCEA, 2021. *Centrum kybernetické bezpečnosti, z.ú*. Online. Dostupné z: https://www.afcea.cz/centrum-kyberneticke-bezpecnosti-z-u/. [cit. 2024-01-20].

AFCEA, 2024. *Česká pobočka AFCEA*. Online. Dostupné z: https://www.afcea.cz/ceska-pobocka-afcea1/. [cit. 2024-01-20].

AVAST, 2018. *Buď safe online.* Online. Dostupné z: https://www.avast.com/cz/besafeonline/online-kurz. [cit. 2024-02-20].

BOZP, 2024. *Školení informační a kybernetické bezpečnost*i. Online. Dostupné z: https://www.skolenibozp.cz/skoleni-kyberbezpecnosti. [cit. 2024-02-20].

ČNB, 2023. *Česká národní banka cílem kybernetického útoku.* Online. Dostupné z: https://www.ČNB.cz/cs/ČNB-news/tiskove-zpravy/Ceska-narodni-banka-cilem-kybernetickeho-utoku/. [cit. 2024-01-20].

CYBERSEC, 2024. *Online školení kybernetické bezpečnosti*. Online. Dostupné z: https://www.cybersec.cz/obsah-skoleni/. [cit. 2024-02-20].

CZ.NIC, 2019. *O nás.* Online. Dostupné z: https://csirt.cz/cs/o-nas/. [cit. 2024-01-20].

CZ.NIC, 2024. *Projekty týmu CSIRT.CZ.* Online. Dostupné z: https://csirt.cz/cs/projekty/. [cit. 2024-01-20].

ČESKO, 2000 a. *Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-239. [cit. 2023-12-12].

ČESKO, 2000 b. *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240. [cit. 2023-12-12].

ČESKO, 2000 c. *Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-241. [cit. 2023-12-12].

ČESKO, 2005 b. *Nařízení vlády č. 522/2005 Sb., Nařízení vlády, kterým se stanoví seznam utajovaných informací*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-522. [cit. 2023-11-17].

ČESKO, 2005 a. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412 . [cit. 2023-11-17].

ČESKO, 2009. *Zákon č. 40/2009 Sb., Trestní zákoník.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2023-11-17].

ČESKO, 2014 b. *Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317. [cit. 2023-11-17].

ČESKO, 2014 a. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-18. [cit. 2023-11-17].

ČESKO, 2018. *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82. [cit. 2023-11-17].

ČESKO, 2019. *Zákon č. 110/2019 Sb., o zpracování osobních údajů*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110. [cit. 2023-11-17].

ČESKÝ ROZHLAS, 2022. *Vnitro, hasiči i policie. Weby ministerstva čelily DDoS útoku, přihlásila se k nim ruská skupina.* Online. 2022-04_27. Dostupné z: https://www.irozhlas.cz/zpravy-domov/rusko-killnet-ddos-ministerstvo-vnitra_2204270856_pj. [cit. 2024-01-21].

ČSKI, ©2014-2024. *Česká společnost pro kybernetiku a informatiku*. Online. Dostupné z: https://www.cski.cz/homepage/cs. [cit. 2024-01-02].

ČSN EN ISO/IEC 27000, 2020. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Přehled a slovník*. 5. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN EN ISO/IEC 27001, 2014. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Požadavky*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369797.

ČSN EN ISO/IEC 27002, 2023. *Informační technologie – Bezpečnostní techniky: Soubor postupů pro opatření bezpečnosti informací.* 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369798.

ČSN ISO/IEC 27003, 2018. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Pokyny*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN ISO/IEC 27004, 2018. *Informační technologie – Bezpečnostní techniky: Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČT24, 2018. *Hacker napadl počítačovou síť v nemocnici na Rokycansku. Chtěl výkupné ve virtuální měně*. Online. Dostupné z: https://ct24.ceskatelevize.cz/clanek/regiony/hacker-napadl-pocitacovou-sit-v-nemocnici-na-rokycansku-chtel-vykupne-ve-virtualni-mene-78255. [cit. 2024-01-20].

ČTK, 2024. *Elektronický systém přihlášek na školy čelil útoku hackerů, díky ochraně funguje.* Online. 2024-02-03. Dostupné z: https://www.aktualne.cz/elektronicky-system-prihlasek-na-skoly-celil-utoku-hackeru-d/r~dd35696ac2a211ee9445ac1f6b220ee8/. [cit. 2024-02-20].

DIGIKOALICE, 2024. *Česká společnost pro kybernetiku a informatiku*. Online. Dostupné z: https://digikoalice.cz/organizace/ceska-spolecnost-pro-kybernetiku-a-informatiku/. [cit. 2024-04-16].

DOSTALOVÁ, Helena, 2023. *V bezpečnosti nejde jen o boj systémů, nejslabším článkem je člověk*. Online. In: HN. Dostupné z: https://hn.cz/c1-67257330-v-bezpecnosti-nejde-jen-o-boj-systemu-nejslabsim-clankem-je-clovek. [cit. 2024-01-21].

DURIČANSKÁ, Zuzana, 2016. *NIS: Co přináší nová směrnice EU o síťové a informační bezpečnosti?* Online. Nic.cz. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf.. [cit. 2024-04-16].

ECHO24, 2022. *Kyberútok na weby Ředitelství silnic a dálnic byl profesionální, zašifroval data.* Online. Dostupné z: https://echo24.cz/a/SdgLS/kyberutok-na-weby-reditelstvi-silnic-a-dalnic-byl-profesionalni-zasifroval-data. [cit. 2024-01-20].

ECHO24, 2023. *Univerzita obrany nezaplatila. Hackeři zveřejnili část jejích ukradených dat*. Online. 2023-10-23. Dostupné z: https://echo24.cz/a/H2a5D/zpravy-domov-hackeri-zverejnili-data-univerzity-obrany. [cit. 2024-01-20].

ESET, 2024. *Co je počítačový virus + druhy virů*. Online. Dostupné z: https://www.eset.com/cz/virus/. [cit. 2023-12-16].

ESET, 2024. *E-learning: Školení kybernetické bezpečnosti.* Online. Dostupné z: https://www.eset.com/cz/firmy/eset-services/rizeni-it-bezpecnosti/skoleni-kyberneticke-bezpecnosti-formou-e-learningu/. [cit. 2024-02-20].

ESET, 2024. *PENETRAČNÍ TESTY*. Online. Dostupné z: https://www.eset.com/cz/firmy/eset-services/penetracni-testy/. [cit. 2024-02-20].

EU, 2016. *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Online. EU. Eur-lex.europa. 2016-07-19. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016L1148#. [cit. 2023-12-16].

EUROPEAN COUNCIL, 2022. *Protection of European Union classified information (EUCI)*. Online. EUROPEAN COUNCIL. Consilium.europa. 2024-01-10. Dostupné z: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/. [cit. 2023-01-11].

Filip Krejčí. 13.3.2024.Strukturovaný rozhovor s respondentem Policie České republiky. Osobní komunikace.

GORDIC, 2023. *Školení kybernetické bezpečnosti.* Online. Dostupné z: https://gordiccybersec.cz/skoleni-kyberneticke-bezpecnosti/. [cit. 2024-02-20].

HASHEMI-POUR, Cameron, 2023. *CIA triad (confidentiality, integrity and availability)*. Online. 2023-12-21. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [cit. 2023-12-27].

HAVLÍK, Miroslav, 2020. *Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky.* Online. In: Vojenské rozhledy. 3. Brno: Univerzita obrany. Dostupné z: https://doi.org/10.3849/1210-3292. [cit. 2024-01-20].

HLADÍLEK, Miroslav, 2009. *Kapitoly z obecné didaktiky a didaktiky vzdělávání dospělých.* Praha: Univerzita Jana Amose Komenského. ISBN 978-80-86723-75- 4.

HN, 2024. *Rusko zkouší tisíce kybernetických útoků na evropské dráhy, tvrdí český ministr dopravy.* Online. 2024-04-05. Dostupné z: https://zahranicni.hn.cz/c1-67310740-rusko-zkousi-tisice-kybernetickych-utoku-na-evropske-drahy-tvrdi-cesky-ministr-dopravy. [cit. 2024-04-06].

ICRC, 2022. *A sophisticated cyber security attack against computer servers hosting information held by the International Committee of the Red Cross (ICRC) was detected this week.* Online. Dostupné z: https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people. [cit. 2024-01-20].

IDNES, 2020. *Hacker způsobil benešovské nemocnici škodu 59 milionů, policie ho nedopadla.* Online. Dostupné z: https://www.idnes.cz/praha/zpravy/kyberneticky-utok-policie-vysetrovani-benesovska-nemocnice.A200818_090949_praha-zpravy_pp. [cit. 2024-01-20].

IDNES, 2021. *Nemocnice se z kyberútoku otřepává celý rok, hrozbu hackerů bere vážněji.* Online. Dostupné z: https://www.idnes.cz/brno/zpravy/kyberutok-fakultni-nemocnice-hrozba-hackeri-NÚKIB.A210324_600537_brno-zpravy_krut. [cit. 2024-01-20].

IROZHLAS, 2023. *Univerzitu obrany napadli hackeři. Unikla data pracovníků a vyučujících včetně finančních výkazů.* Online. Dostupné z: https://www.irozhlas.cz/zpravy-domov/unob-univerzita-obrany-kyberneticky-utok-hackeri_2309271200_kac. [cit. 2024-01-20].

ISO, 2021. *About ISO*. Online. Dostupné z: https://www.iso.org/about-us.html. [cit. 2023-11-19].

ISO, 2023. *Structure and governance*. Online. Dostupné z: https://www.iso.org/structure.html. [cit. 2023-11-19].

Jan Slánský. 16.3.2024.Strukturovaný rozhovor s respondentem Zdravotnické záchranné služby. Osobní komunikace.

KELLY, Laura, 2022. *Ukraine Defense Ministry, banks hit by cyberattack amid tensions with Russia.* Online. In: The Hill. Dostupné z: https://thehill.com/policy/international/594330-ukraine-defense-ministry-banks-hit-by-cyberattack-amid-tensions-with/. [cit. 2024-01-24].

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

KOUHOUT, Roman a KARCHŇÁK, Radek, 2016. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary. ISBN 978-80-260-9543-9.

KREMLING, Janine a PARKER, Amanda M. Sharp, 2017. *Cyberspace, cybersecurity, and cybercrime.* Los Angeles: SAGE Publications. ISBN 978-1-5063-4725-7

KUDRNA SOBKOVÁ, 2024. *Kurz: Kybernetická bezpečnost aneb Jak žít a přežít v kyberprostoru.* Online. Dostupné z: https://kudrnasobkova.cz/kyberneticka-bezpecnost/#cenik. [cit. 2024-02-20].

KYBERCENTRUM, 2023. *Naše aktivity & projekty*. Online. Dostupné z: https://www.kybercentrum.cz/#nase-aktivity. [cit. 2023-12-20].

KYBEZ, 2021. *Řízení kybernetické bezpečnosti (workshop)*. Online. Dostupné z: https://kybez.cz/sluzby/7228-2. [cit. 2024-02-20].

KYBEZ, 2021. *Základy kybernetické bezpečnosti organizace*. Online. Dostupné z: https://kybez.cz/sluzby/zaklady-kyberneticke-bezpecnosti-organizace/. [cit. 2024-02-20].

KYBEZ, 2024. *O nás*. Online. Dostupné z: https://kybez.cz/o-nas/. [cit. 2024-01-20].

LANGER, Tomáš, 2016. *Moderní lektor: průvodce úspěšného vzdělavatele dospělých*. Praha: Grada. ISBN 978-80-271-0093-4.

LATTO, Nica, 2020. *What Is WannaCry?* Online. In: AVAST. 2020-02-27. Dostupné z: https://www.avast.com/c-wannacry. [cit. 2024-01-23].

Martin Bursa. 12.3.2024.Strukturovaný rozhovor s respondentem Armády České republiky. Osobní komunikace

MV ČR, 2016. *Vzniká Národní agentura pro komunikační a informační technologie*. Online. MV ČR. Dostupné z: https://www.mvcr.cz/clanek/vznika-narodni-agentura-pro-komunikacni-a-informacni-technologie.aspx. [cit. 2023-12-16].

NATO. *What's in a security classification?* Online. ©2023. Dostupné z: https://www.nato.int/cps/en/natohq/declassified_138449.htm. [cit. 2023-11-16].

NBÚ, 2017. *Bezpečnost informačních systémů.* Online. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/993-informace/. [cit. 2023-11-10].

NBÚ, 2024. *O NBÚ*. Online. Dostupné z: https://www.nbu.cz/cs/o-nas/. [cit. 2023-12-16].

NCBI, 2024. *O nás*. Online. Dostupné z: https://www.ncbi.cz/. [cit. 2024-01-20].

NCKB, 2017. *PETYA/PETRWRAP/NOTPETYA - NOVÁ HROZBA RANSOMWARU*. Online. 2017-06-27. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/2539-petrwrap-nova-varianta-ransomwaru/. [cit. 2024-01-21].

NCKB, 2024. *Poskytované služby.* Online. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/. [cit. 2024-01-20].

NCKB, 2024. *Vládní CERT*. Online. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/. [cit. 2024-01-20].

NGSS, 2024. *Bezpečnostní a penetrační testy*. Online. Dostupné z: https://www.ngss.cz/sluzba/19-penetracni-testy. [cit. 2024-02-20].

NGSS, 2024. *Školení kybernetické bezpečnosti*. Online. Dostupné z: https://www.ngss.cz/sluzba/13-skoleni-kyberneticke-bezpecnosti. [cit. 2024-02-20].

NOVINKY.CZ, 2024. *Českem se masivně šíří trojský kůň, který napadá bankovní aplikace.* Online. 2024-01-29. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-ceskem-se-masivne-siri-trojsky-kun-ktery-napada-bankovni-aplikace-40458843. [cit. 2024-01-30].

NÚKIB, 2023 a. *Legislativa KB*. Online. NÚKIB. Dostupné z: https://NÚKIB.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2023-12-01].

NÚKIB, 2020. *Nová pravidla pro určování významných informačních systémů*. Online. Dostupné z: https://NÚKIB.gov.cz/cs/infoservis/aktuality/1627-nova-pravidla-pro-urcovani-vyznamnych-informacnich-systemu/. [cit. 2023-11-16].

NÚKIB, 2021. *Ukončení činnosti ransomwaru Avaddon.* Online. 2021-06-11. Dostupné z: https://NÚKIB.gov.cz/cs/infoservis/aktuality/1722-ukonceni-cinnosti-ransomwaru-avaddon/. [cit. 2024-01-20].

NÚKIB, 2022. *Nová směrnice EU o kybernetické bezpečnosti „NIS2" a návrh NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI plánovaná platnost změn v kybernetické bezpečnosti od 2024.* Online. NÚKIB. Dostupné z: https://osveta.NÚKIB.gov.cz/course/view.php?id=145. [cit. 2024-04-16].

NÚKIB, 2022. *NÚKIB představuje evropskou směrnici NIS2.* Online. Dostupné z: https://NÚKIB.gov.cz/cs/infoservis/aktuality/1874-NÚKIB-predstavuje-evropskou-smernici-nis2/. [cit. 2024-04-16].

NÚKIB, 2023. *Dokumenty a Publikace*. Online. Dostupné z: https://NÚKIB.gov.cz/cs/infoservis/dokumenty-a-publikace/. [cit. 2023-12-20].

NÚKIB, 2023. *O úřadu.* Online. Dostupné z: https://NÚKIB.gov.cz/cs/o-NÚKIB/o-uradu/. [cit. 2023-11-20].

NÚKIB, 2023. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022.* Online. Dostupné z: https://NÚKIB.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetic ke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2024-01-13].

NÚKIB, 2024. *„DÁVEJ KYBER" PRO UČITELE*. Online. Dostupné z: https://osveta.NÚKIB.gov.cz/course/view.php?id=121. [cit. 2024-02-20].

NÚKIB, 2024. *Kybernetická bezpečnost.* Online. Dostupné z: https://NÚKIB.gov.cz/cs/kyberneticka-bezpecnost/. [cit. 2024-01-20].

NÚKIB, 2024. *Kybernetické incidenty pohledem NÚKIB - prosinec 2023*. Online. Dostupné z: https://NÚKIB.gov.cz/cs/infoservis/aktuality/2067-kyberneticke-incidenty-pohledem-NÚKIB-prosinec-2023/. [cit. 2024-01-13].

NÚKIB, 2024. *Nabízené kurzy.* Online. Dostupné z: https://osveta.NÚKIB.gov.cz/local/dashboard/. [cit. 2024-02-14].

NÚKIB, 2024. *Vzdělávání.* Online. Dostupné z: https://NÚKIB.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/. [cit. 2024-02-20].

NÚKIB, 2024. *Základy kybernetické bezpečnosti „DÁVEJ KYBER!" (verze pro rok 2024).* Online. Dostupné z: https://osveta.NÚKIB.gov.cz/course/view.php?id=169. [cit. 2024-02-20].

NÚKIB, 2024. *Základy kybernetické bezpečnosti pro zdravotnictví 24*. Online. Dostupné z: https://osveta.NÚKIB.gov.cz/enrol/index.php?id=186. [cit. 2024-02-20].

PAVELKA, Ivan, 2018. *Správní právo: Institucionální zajištění ochrany utajovaných informací v ČR.* Online. Roč. LI, č. 3/2018. Praha: Ministerstvo vnitra České republiky. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/clanek/spravni-pravo-cislo-3-2018.aspx. [cit. 2024-01-20].

PEKOVÁ, Andrea, 2020. *Co je užitečné vědět o normách a dalších dokumentech.* Online. Česká společnost pro jakost. Dostupné z: https://www.csq.cz/infocentrum/odborne-clanky/detail/co-je-uzitecne-vedet-o-normach-a-dalsich-dokumentech. [cit. 2024-01-05].

PLAMÍNEK, Jiří, 2014. *Vzdělávání dospělých: průvodce pro lektory, účastníky a zadavatele.* 2. rozšířené vydání. Praha: Grada. ISBN ISBN 978-80-247-4806-1.

POLITYUK, Pavel a PRENTICE, Aldssandra, 2017. *Ukrainian banks, electricity firm hit by fresh cyber attack.* Online. In: REUTERS. 2017-06-27. Dostupné z: https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ/. [cit. 2024-01-21].

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

Respondent Hasičského záchranného sboru. 14.3.2024.Strukturovaný rozhovor s respondentem Hasičského záchranného sboru. Emailová komunikace.

Respondent státní správy. 18. 3.2024.Strukturovaný rozhovor s respondentem státní správy. Osobní komunikace.

Respondent Vězeňské služby České republiky. 15. 3.2024.Strukturovaný rozhovor s respondentem Vězeňské služby České republiky. Osobní komunikace.

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

SEDUO, 2024. *Bezpečně v online světě: jak ochránit své peníze, data a identitu.* Online. Dostupné z: https://www.seduo.cz/bezpecne-v-online-svete-jak-ochranit-sve-penize-data-a-identitu. [cit. 2024-02-20].

SEDUO, 2024. *Digitální bezpečnost: naučte se chodit v online světě bezpečně.* Online. Dostupné z: https://www.seduo.cz/digitalni-bezpecnost-naucte-se-chodit-v-online-svete-bezpecne. [cit. 2024-02-20].

SEDUO, 2024. *Všechny kurzy – Kybernetická bezpečnost.* Online. Dostupné z: https://www.seduo.cz/vsechny-kurzy/nejsledovanejsi?kompetence=411. [cit. 2024-02-20].

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

THE NEW YORK TIMES, 2022. *Hackers Bring Down Government Sites in Ukraine.* Online. Dostupné z: https://www.nytimes.com/2022/01/14/world/europe/hackers-ukraine-government-sites.html. [cit. 2024-01-24].

TIDY, Joe, 2023. *MOVEit hack: BBC, BA and Boots among cyber attack victims.* Online. In: BBC. Dostupné z: https://www.bbc.com/news/technology-65814104. [cit. 2024-02-20].

T-SOFT, 2017. *Kybernetický workshop.* Online. Dostupné z: https://www.tsoft.cz/sluzby/bezpecnostni-workshop/. [cit. 2024-02-20].

TURTON, William a MEHROTRA, Kartikay, 2021. *Hackers Breached Colonial Pipeline Using Compromised Password.* Online. In: BLOOMBERG. Dostupné z: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. [cit. 2024-02-20].

VELECKÁ, Natálie, 2019. *Vzdělávání: formální, neformální a informální — a jaký je vlastně mezi nimi rozdíl?* Online. In: KISK MU. Dostupné z: https://medium.com/edtech-kisk/vzd%C4%9Bl%C3%A1v%C3%A1n%C3%AD-form%C3%A1ln%C3%AD-neform%C3%A1ln%C3%AD-a-inform%C3%A1ln%C3%AD-a-jak%C3%BD-je-vlastn%C4%9B-mezi-nimi-rozd%C3%ADl-80d3cfaa691b. [cit. 2024-04-17].

YADAV, Tejas, 2021. *CIA AND DAD TRIAD*. Online. Dostupné z: https://medium.com/@yadavtejas249/cia-and-dad-triad-ef84a94f9aee. [cit. 2024-01-16].

ZOULOVÁ, Lenka, 2023. *Masivní útoky proruských hackerů ochromily weby české policie i ministerstva vnitra.* Online. In: NOVINKY.CZ. 2023-10-24. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-masivni-utoky-proruskych-hackeru-ochromily-weby-ceske-policie-i-ministerstva-vnitra-40448168. [cit. 2024-01-21].

ŽIVĚ.CZ, 2022. *Česko zasáhl největší DDoS útok v historii. V čem byl specifický? Mohl být řízený z Ruska? Rozhovor s Tomášem Křešťákem z O2.* Online. 2022-12-03. Dostupné z: https://www.zive.cz/clanky/cesko-zasahl-nejvetsi-ddos-utok-v-historii-v-cem-byl-specificky-mohl-byt-rizeny-z-ruska-rozhovor-s-tomasem-krestakem-z-o2/sc-3-a-219591/default.aspx. [cit. 2024-01-20].

Seznam použitých symbolů a zkratek

AČR	Armáda České republiky
AFCEA	Armed Forces Communications Electronics Association
ARO	Anesteziologicko-resuscitační oddělení
BM	Bezpečnostní manažer
BOZP	Bezpečnost a ochrana zdraví při práci
CERT	Computer Emergency Response Team
CIRC	Computer Incident Response Capabilty
CSIRT	Computer Security Incident Response Team
ČAS	Česká agentura pro standardizaci
ČSKI	Česká společnost pro kybernetiku a informatiku
ČSN	České technické normy
DDoS	Distributed denial of service
DoS	Denial of servise
ENISA	Evropská agentura pro bezpečnost sítí a informací
EU	Evropská unie
FO	Fyzická osoba
GDPR	General Data Protection Regulation
HZS ČR	Hasičský záchranný sbor České republiky
ICDL	International Computer Driving Licence
ICT	Informační a komunikační technologie
IDET	Mezinárodní veletrh obranné a bezpečnostní techniky
IEC	Mezinárodní elektrotechnická komise
INSAFE	Evropská síť informačních center propagujících bezpečnější a lepší používání internetu
IP adresa	Číslo jednoznačně identifikující síťové rozhraní v počítačové síti
IT	Informační technologie
ISMS	Systém řízení bezpečnosti informací
ISO	Mezinárodní organizace pro normalizaci
ISO/IEC JTC 1	Komise pro informační technologie
IZS	Integrovaný záchranný systém
JPO	Jednotky požární ochrany
KB	Kybernetická bezpečnost

KIS	Agentura komunikačních a informačních systémů Armáda České republiky
KYBERCENTRUM	Centrum kybernetické bezpečnosti
NAKIT	Národní agentura pro komunikační a informační technologie
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NCBI	Národní centrum bezpečnějšího internetu
NCKB	Národní centrum kybernetické bezpečnosti
NIS 1 a NIS 2	Směrnice o kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OUI	Ochrana utajovaných informací
PČR	Policie České republiky
PO	Právnická osoba
QR kód	Čtvercový obrazec přenášející data
Triáda CIA	Confidentiality, Integrity, Availability
Triáda DAD	Disclosure, Alteration, Denial
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
VeKySiO	Velitelství informačních a kybernetických sil obrany
VPN	Virtuální privátní síť
ZoKB	Zákon o kybernetické bezpečnosti
ZZS	Zdravotnická záchranná služba

Seznam obrázků

Seznam tabulek

Seznam příloh

PŘÍLOHA P I: INFORMOVANÉ SOUHLASY RESPONDENTŮ

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent **chci/nechci** uvést své jméno a pracovní pozici a **souhlasím/nesouhlasím** s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 12. 3. 2021

Účastník: [illegible]

Podpis účastníka: .....

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent ~~**chci**~~/**nechci** uvést své jméno a pracovní pozici a **souhlasím**/~~**nesouhlasím**~~ s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 14. 3. 2024

Účastník: Tomáš Kadlec

Podpis účastníka: .....

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent **chci/nechci** uvést své jméno a pracovní pozici a **souhlasím/nesouhlasím** s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 14.03.2024

Účastník: Jan Stánský

Podpis účastníka: .....

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent ~~chci/nechci~~ uvést své jméno a pracovní pozici a **souhlasím/~~nesouhlasím~~** s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 12-03-2024

Účastník: Komisař npor. Mgr. Tomáš Kratochvíl sl. č. 24483 zástupce vedoucího OVT

Podpis účastníka: .....

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent **[redacted]/nechci** uvést své jméno a pracovní pozici a **souhlasím/[redacted]** s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 14. 3. 2024

Účastník: ZAČEŠÁK PETR

Podpis účastníka: .....

Příloha č. 1

Informovaný souhlas s účastí ve výzkumném šetření

Vážený pane,

ráda bych Vás požádala o souhlas s účastí ve výzkumném šetření pro účely zpracování mé diplomové práce s název Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Cílem tohoto šetření je provést rozhovor s příslušníky jednotlivých subjektů ochrany obyvatelstva. Rozhovor se bude týkat úrovně vzdělávání v oblasti kybernetické bezpečnosti a bude probíhat online přes MS Teams či formou emailové komunikace, dle preferencí a časových možností. Výsledná data budou zpracována a interpretována v rámci uvedené diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na výzkumném šetření studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Rozhovor bude zpracovaný v souladu s pravidly pro ochranu osobních údajů.

Jako respondent **chci/~~nechci~~** uvést své jméno a pracovní pozici **~~a souhlasím~~/nesouhlasím** s užitím pseudonymu. *(nehodící se škrtněte)*

Byl jsem informován, že

- mám právo požadovat přístup k osobním údajům týkajícím se mé osoby, jejich opravu nebo výmaz,
- popřípadě omezení zpracování, mám právo vznést námitku proti zpracování osobních údajů týkajících se mé osoby,
- mám právo podat stížnost dozorovému orgánu (Úřad pro ochranu osobních údajů) v případě, že se domnívám, že zpracování mých osobních údajů probíhá v rozporu s právními předpisy;
- mám právo tento souhlas se zpracováním osobních údajů kdykoliv odvolat, aniž by mi za to hrozila jakákoliv sankce či znevýhodnění, a to oznámením na elektronickou adresu k_suchorova@utb.cz, případně jinou formou na kontaktní údaje správce osobních údajů. Zákonnost zpracování údajů před odvoláním souhlasu tím není dotčena.

Datum: 12.3.2024

Účastník: Beran Martin

Podpis účastníka: .....Beran Martin.....

PŘÍLOHA P II: PROTOKOLY O HODNOCENÍ VYBRANÝCH KURZŮ HODNOTITELSKÝM TÝMEM

Příloha č. 2

Formulář pro hodnocení vybraných kurzů kybernetické bezpečnosti

Vážený pane doktore,

ráda bych Vás požádala o hodnocení vybraných kurzů kybernetické bezpečnosti jako součást praktické části mé diplomové práce na téma Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Během přípravy na provedení hodnocení jednotlivých kurzů budete seznámen se s jejich obsahem, strukturou, formou provedení, volně dostupnou ukázkou a recenzemi účastníků. Na základě tohoto seznámení a za využití Vašich znalostí z praxe, bude provedeno hodnocení daných kurzů za použití bodovací metody, která Vám bude před započetím daného hodnocení vysvětlena. Tato analýza je vytvořena za účelem výběru optimální varianty kurzu kybernetické bezpečnosti na základě předem stanovených kritérií hodnocení. Výsledná data budou zpracována a interpretována v rámci mé diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na hodnocení vybraných kurzů kybernetické bezpečnosti studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Hodnocení vybraných kurzů kybernetické bezpečnosti		
Název kurzu	**Srozumitelnost**	**Přínosnost**
	H 1	**H 1**
Základy kybernetické bezpečnosti 24	5	4
Úvod do kybernetické bezpečnosti	2	2
Školení kybernetické bezpečnosti	3	3
Digitální bezpečnost: naučte se chodit v online světě bezpečně	2	2
Školení informační a kybernetické bezpečnosti	4	5
Pravidla IT bezpečnosti pro zaměstnance	4	5

Datum: 8.4.2024
Hodnotitel: prof. Ing. Karel Hájovský, Ph.D.
Podpis hodnotitele: .....

Příloha č. 2

Formulář pro hodnocení vybraných kurzů kybernetické bezpečnosti

Vážený pane,

ráda bych Vás požádala o hodnocení vybraných kurzů kybernetické bezpečnosti jako součást praktické části mé diplomové práce na téma Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Během přípravy na provedení hodnocení jednotlivých kurzů budete seznámen se s jejich obsahem, strukturou, formou provedení, volně dostupnou ukázkou a recenzemi účastníků. Na základě tohoto seznámení a za využití Vašich znalostí z praxe, bude provedeno hodnocení daných kurzů za použití bodovací metody, která Vám bude před započetím daného hodnocení vysvětlena. Tato analýza je vytvořena za účelem výběru optimální varianty kurzu kybernetické bezpečnosti na základě předem stanovených kritérií hodnocení. Výsledná data budou zpracována a interpretována v rámci mé diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na hodnocení vybraných kurzů kybernetické bezpečnosti studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Hodnocení vybraných kurzů kybernetické bezpečnosti		
Název kurzu	**Srozumitelnost**	**Přínosnost**
	H 3	**H 3**
Základy kybernetické bezpečnosti 24	5	5
Úvod do kybernetické bezpečnosti	1	1
Školení kybernetické bezpečnosti	1	4
Digitální bezpečnost: naučte se chodit v online světě bezpečně	3	2
Školení informační a kybernetické bezpečnosti	3	2
Pravidla IT bezpečnosti pro zaměstnance	4	4

Datum: 8.4.2024

Hodnotitel Bc. Filip Krejčí

Podpis hodnotitele .....

PŘÍLOHA P III: HODNOCENÍ NÁVRHU PLÁNU VZDĚLÁVÁNÍ BEZPEČNOSTNÍM MANAŽEREM

Příloha č. 3

Žádost o provedení hodnocení návrhu Plánu vzdělávání v oblasti kybernetické bezpečnosti na kalendářní rok

Vážený pane inženýre,

ráda bych Vás požádala o hodnocení návrhu Plánu vzdělávání v oblasti kybernetické bezpečnosti na kalendářní rok jako součást praktické části mé diplomové práce na téma Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva. Samozřejmostí v rámci přípravy na hodnocení je zaslání návrhu daného plánu s dostatečnou časovou rezervou pro jeho prostudování. Na základě tohoto hodnocení bude možné posoudit možnou přínosnost implementace daného plánu do běžné praxe. Výsledná data budou zpracována a interpretována v rámci mé diplomové práce.

Prohlášení

Svým podpisem dávám souhlas s účastí na hodnocení návrhu plánu vzdělávání v oblasti kybernetické bezpečnosti studentky Kristýny Suchorové pro účely diplomové práce s názvem Vzdělávání v oblasti kybernetické bezpečnosti v subjektech ochrany obyvatelstva na Ústavu ochrany obyvatelstva Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

Datum: 15. dubna 2024
Hodnotitel Ing. Pavel Větrovský.
Podpis hodnotitele .....

Příloha č. 3

Zhodnocení návrhu Plánu vzdělávání v oblasti kybernetické bezpečnosti

Na základě žádosti o zhodnocení návrhu Plánu vzdělávání v oblasti kybernetické bezpečnosti Kristýny Suchorové jsem provedl hodnocení za pomoci zkušeností z mé dosavadní praxe, vybraných pracovníků oddělení bezpečnosti informací a oddělení komunikačních a informačních technologií. V současné době pracuji na pozici Bezpečnostní manažer Univerzity obrany. Součástí mých pracovních činností a povinností je i plánování vzdělávacích aktivit na kalendářní rok. V období let 2023 a 2024 byla do procesu vzdělání zaměstnanců začleněna i edukace v oblasti kybernetické bezpečnosti. Po seznámení se s obsahem plánu jsem rozdělil své hodnocení do jednotlivých kategorií dle obsahu.

Výběr formy vzdělávání

Vzdělávání za využití kombinace metod e-learningových kurzů, přednášek lektora a simulace phishingových útoků se z mého pohledu jeví jako efektivní metoda k dosažení žádaného cíle. Výhodou způsobu výuky skrze e-learningové je především využití jednoduchého a uživatelsky přívětivého softwaru, menší finanční náročnost na realizaci a úspora času zaměstnanců v závislosti na aktuálních pracovních úkolech. Při přednáškách s vyučujícím spatřuji výhodu v možnosti přímé interakce s vyučujícím, kdy opadá ostych posluchačů v kladení otázek (zeptají se na to, co je zajímá a co chtějí vědět v případě, že to nebylo v rámci přednášky řečeno). Naopak negativem v případě přednášky může být náročnost na udržení pozornosti posluchačů.

Vzdělávací aktivity

Výčet jednotlivých témat vzdělávání se zdá být dle mého názoru logicky provázaný s potřebnou tematickou návazností, kdy je postupováno od základů problematiky k postupnému rozšíření získaných znalostí.

V rámci prostředí UO rovněž provádíme periodické proškolení ochrany utajovaných informací formou e-learningového kurzu v prostředí Moodle, jehož součástí jsou i pravidla pro manipulaci se služebním zařízením a paměťovými nosiči.

K proškolení základů kybernetické bezpečnosti dochází formou bezplatného kurzu od NÚKIB, který je každoročně aktualizován. Rozšíření znalostí o možnost odborných přednášek zaměřených na konkrétní problematiku (kybernetické útoky či kyberšikana) vnímám jako přínosnou. Posluchačům přiblíží danou oblast podrobněji a přinese tím lepší znalost dané oblasti.

Své místo má rovněž odůvodněně v plánu vzdělávání i školení na téma šifrování dat a elektronický podpis, kdy je dobré toto školení provádět pouze u osob, které jej aktivně využívají a bude pro ně mít potřebný přínos do praxe.

Na závěr vyjádření k simulaci phishingových útoků, kterou vnímám jako potřebnou a v mém zaměstnání je v rámci posledních let úspěšně realizována, kdy z interních statistik vyplývá zvýšení obezřetnosti uživatelů při obdržení podezřelého emailu. Tato technika je rovněž vhodná pro stanovení postupu, jak v případě nastání takové události postupovat.

Technická, časová a finanční náročnost realizace

Realizaci po technické stránce značně ulehčuje fakt, že většina institucí již dnes vlastní některou z variant vzdělávacích portálů, rovněž v zázemí většiny společností můžeme nalézt místnosti, které jsou určeny jako školící či k pořádání porad, kdy součástí technického vybavení běžně bývá tabule, dataprojektor i počítač. Tím pádem lze hovořit o nízké technické náročnosti v případě realizace vzdělávání.

Otázka finanční náročnosti je velmi ožehavé a diskutabilní téma, kdy finanční možnosti vždy závisí na stanoveném rozpočtu dané organizace. V rámci hodnoceného plánu jsou využity jak bezplatné možnosti, tak i placené, kdy je možno očekávat snížení výsledné ceny v závislosti na počet účastníků. S vyšším počtem účastníků lze očekávat snížení ceny. Kombinace obou možností kurzů mi přijde jako vhodně řešená, v případě minimalizace nákladů lze také využít určenou osobu uvnitř instituce, která danou přednášku realizuje na základě své dosavadní praxe.

Časový harmonogram hodnoceného plánu je uzpůsoben potřebám zaměstnavatele i zaměstnanců dobrým způsobem. Je logické, že většina školení musí být realizována začátkem roku, naopak menší časová náročnost během posledních dvou čtvrtletí zabezpečí nepřetěžování zaměstnanců a plnou soustředěnost na pracovní úkoly.

Závěr

Potenciál efektivního využití navrhovaného plánu v praxi vnímám jako existující. Je patrný přínos z hlediska zkvalitnění výuky i jako opatření pro zvýšení současné úrovně vzdělání. Vzhledem k přehlednosti jej lze využít u různých druhů organizací, kdy je možnost přizpůsobení plánu aktuálním potřebám.

Datum: 16. dubna 2024
Hodnotitel Ing. Pavel Větrovský
Podpis hodnotitele .....