**UNIVERZITA PALACKÉHO V OLOMOUCI**

**FILOZOFICKÁ FAKULTA**

# Možnosti vzdělávání dospělých v oblasti kyberbezpečnosti v ČR

Magisterská diplomová práce

Olomouc 2024 Bc. Jaroslav Compeľ

**UNIVERZITA PALACKÉHO V OLOMOUCI**

**FILOZOFICKÁ FAKULTA**

**KATEDRA SOCIOLOGIE, ANDRAGOGIKY A KULTURNÍ ANTROPOLOGIE**

# MOŽNOSTI VZDĚLÁVÁNÍ DOSPĚLÝCH V OBLASTI KYBERBEZPEČNOSTI V ČR

Magisterská diplomová práce

Studijní program: andragogika

**Autor:** Bc. Jaroslav Compeľ

**Vedoucí práce:** Karger Tomáš, Mgr. Ph.D.

Olomouc 2024

Prohlašuji, že jsem magisterskou diplomovou práci na téma „Vzdělávání dospělých v oblastech kyberbezpečnosti“ vypracoval samostatně a uvedl v ní veškerou literaturu a ostatní zdroje, které jsem použil.

V Olomouci dne 18. března 2024 Podpis ……

# Anotace

| | |
|---|---|
| **Jméno a příjmení:** | Bc. Jaroslav Compeľ |
| **Katedra:** | Katedra sociologie, andragogiky a kulturní antropologie |
| **Studijní program:** | Andragogika |
| **Studijní program obhajoby práce:** | Andragogika |
| **Vedoucí práce:** | Karger Tomáš, Mgr. Ph.D. |
| **Rok obhajoby:** | 2024 |

| | |
|---|---|
| **Název práce:** | Možnosti vzdělávání dospělých v oblasti kyberbezpečnosti v ČR |
| **Anotace práce:** | Tato diplomová práce má za cíl analyzovat možnosti vzdělávání dospělých v oblasti kybernetické bezpečnosti v České republice a navrhnout případný alternativní vzdělávací program v této oblasti. |
| **Klíčová slova:** | Kybernetická bezpečnost vzdělávání veřejnosti, Kybernetická bezpečnost – online kurz, Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti, Školení kybernetické bezpečnosti |
| **Title of Thesis:** | Opportunities for adult education in the field of cybersecurity in the Czech Republic |
| **Annotation:** | This master's thesis aims to analyze the possibilities of adult education in the field of cybersecurity in the Czech Republic and propose a potential alternative educational program in this area. |
| **Keywords:** | Cybersecurity Public Education, Cybersecurity Online Course, Public Education in the Field of Cybersecurity, Cybersecurity Training |
| **Názvy příloh vázaných v práci:** | Kurzy a školení na českém trhu nabízené českými společnostmi |
| **Počet literatury a zdrojů:** | 186 |
| **Rozsah práce:** | 94 s. (150.454 znaků s mezerami) |

# Obsah

# ÚVOD

Nacházíme se v rychle se vyvíjejícím světě, ve kterém získávají na významu nové moderní technologie. Počítače, laptopy, mobilní telefony, internet a mnoho dalších výdobytků této doby fungujících v tzv. kyber-doméně ovlivňují nejen každého jedince, ale i společnost, státy, organizace a celý systém tak, jak je známe. Digitální technologie přináší mnoho výhod, ale také vystavují uživatele spoustě rizikům. S jejich rostoucí důležitostí a se závislostí lidstva na jejich existenci tudíž roste možnost jejich potenciálního zneužití, které může vést k destabilizaci a ohrožení všeho, na co jsme zvyklí a co již nyní bereme jako samozřejmost.

Kybernetická bezpečnost proto představuje stále důležitější téma, které se dotýká prakticky všech oblastí lidského života. A nejkritičtějších zranitelnost představuje právě člověk samotný. Aby se uživatelé byli schopni v digitálním prostředí bezpečně a eticky orientovat, potřebují ovládat nejen základní technické znalosti a dovednosti, ale také chápat širší kontext, ve kterém se kybernetická bezpečnost odehrává. Toto porozumění ovlivňuje rozhodování, jednání, ale i život, práva a bezpečnost každého jedince pohybujícího se v tzv. kyberprostoru.

Zcela zásadním aspektem pro zachování bezpečnosti České republiky (ČR) se tak stává vzdělávání a osvěta v oblasti kybernetické bezpečnosti, jakožto obrovská výzva pro náš stát i společnost. Základní motivace pro tuto práci spočívá v otázce, v jakém stavu se nachází vzdělávání kybernetické bezpečnosti v ČR a jaké jsou aktuální možnosti v dané oblasti. Tento obor se na první pohled zdá nedynamický, neúčinný, víceméně čistě technologicky zaměřený a reakce neschopný s ohledem na překotný technologický vývoj a s tím související společenské, institucionální a systémové změny. Cílem této diplomové práce je proto analyzovat možnosti vzdělávání dospělých v oblasti kybernetické bezpečnosti v ČR a navrhnout případný alternativní vzdělávací program této oblasti.

Hypotéza zní: *Aktuální možnosti vzdělávání veřejnosti v kybernetické bezpečnosti v České republice neodpovídají žádoucímu stavu*, který je možné chápat jako odpovídající *množstevní pokrytí* dospělých vzdělávacími alternativami v daném oboru, a zároveň *obsahové zaměření* kurzů, které obsahuje technické i netechnické aspekty kybernetické bezpečnosti.

Pro její potvrzení, nebo vyvrácení bude v této práci použito části výzkumu klíčových slov vybraných na základě individuálního brainstormingu a zobrazených v přehledu pomocí myšlenkové mapy. Bude se jednat se o termíny spojené s probíranou tematikou, tedy o:

- *Kybernetická bezpečnost vzdělávání veřejnosti, Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti, Kybernetická bezpečnost – online kurz, Školení kybernetické bezpečnosti, Hry kybernetická bezpečnost, Kybernetická bezpečnost simulátory, Kybernetická bezpečnost pomůcky*.

S jejich užitím dojde k identifikaci a deskripci nabídky konkrétních soukromých a státních organizací, které poskytují osvětové aktivity v kybernetické bezpečnosti na českém trhu a budou primární zkoumanou skupinou této práce. Základem pro komparativní analýzu, která bude spočívat v identifikaci přítomnosti indikátorů „ideální“ podoby vzdělávacích a osvětových aktivit u jednotlivých společností, budej jejich rozdělení do kvantitativní tabulky podle parametrů vycházejících z teorií:

- Mgr. Bruce Schneiera, Ph.D. (*srozumitelnost, motivace, názornost, logičnost, důslednost, rozvoj a inovace*)
- Kybernetického indexu gramotnosti (*postoje, dovednosti a znalosti*),
- Rámce cambridgeských životních kompetencí (*kreativní myšlení, sebe-reflexe, komunikaci, spolupráci, sociální odpovědnost*),
- autorem nastavených hodnot neboli uživatelské motivace (*dostupnost, uživatelsky přívětivé, doba licence, bonus, zdarma, cena*).

# KONCEPTUALIZACE

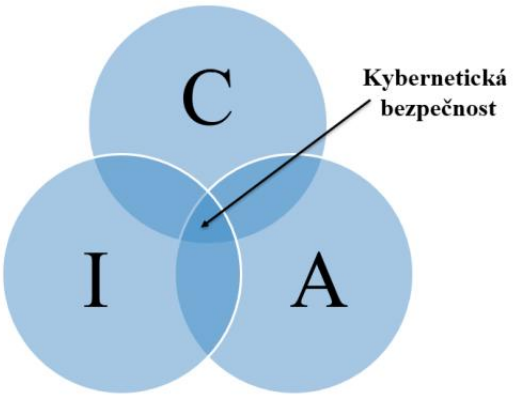
## Kyberprostor a kybernetická bezpečnost

Chápání ***kyberprostoru*** není jednotné. Jeho konceptualizace se neustále vyvíjí, stejně jako fenomén a jeho rozsah samotný. Dle výkladu D. Kuehla se jedná o „globální doménu uvnitř informačního prostředí, jejíž osobitý a unikátní charakter je zarámován užitím elektroniky a elektromagnetického spektra k vytváření, skladování, modifikaci, změnám a využívání informací skrze vzájemně závislé a provázané sítě užívající informační a komunikační technologie“ (Kuehl, 2009). V §2a zákona č. 181/2014 Sb. o kybernetické bezpečnosti je pak kyberprostor definován jako „[…] digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.“

Pokud se bavíme o čemkoli souvisejícím se slovem ***kyber***, má to návaznost na prvky informačních a komunikačních technologiích (ICT) a kyberprostor jako takový (Kolouch 2019: 40). ***Bezpečnost*** pak referuje ke stavu, kdy jsou limitovány hrozby na nejnižší možnou míru (Mareš, 2002: 13).

Dle *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* (2015) je pak ***kybernetická bezpečnost*** (KB) „souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru […] pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem […] je pak ochrana prostředí k realizaci informačních práv člověka.“ Jednoduše řešeno, zajišťování KB je proces, který vede k ochraně prvkům ICT a tzv. CIA triády před hrozbami v kyberprostoru, a zároveň k navýšení odolnosti, robustnosti a integrity informační infrastruktury, systémů a sítí.

Zmíněná ***CIA triáda*** odkazuje na charakteristiky dat a informací, které jsou přenášeny, zpracovávání a uchovány ICT prvky, jež chceme v rámci zajišťování KB zachovat. *Důvěrnost (confidentiality)* odkazuje na stav, kdy k datům, informacím a ICT mají přístup jen k tomu oprávněné subjekty. *Celistvost (integrity)* neboli platnost znamená, že data nebyla změněna, systém vykonává svou funkci nenarušeným způsobem bez manipulace se systémem nežádoucím aktérem. *Dostupnost (availability)* značí stav, kdy má uživatel zajištěn přístup k datům, ICT a informacím dle vlastní potřeby (Kolouch, 2019: 45-54).




*Obrázek 1: Triáda CIA a kybernetická bezpečnost (Kolouch, 2019: 56).*

## Kybernetické bezpečnostní hrozby a rizika

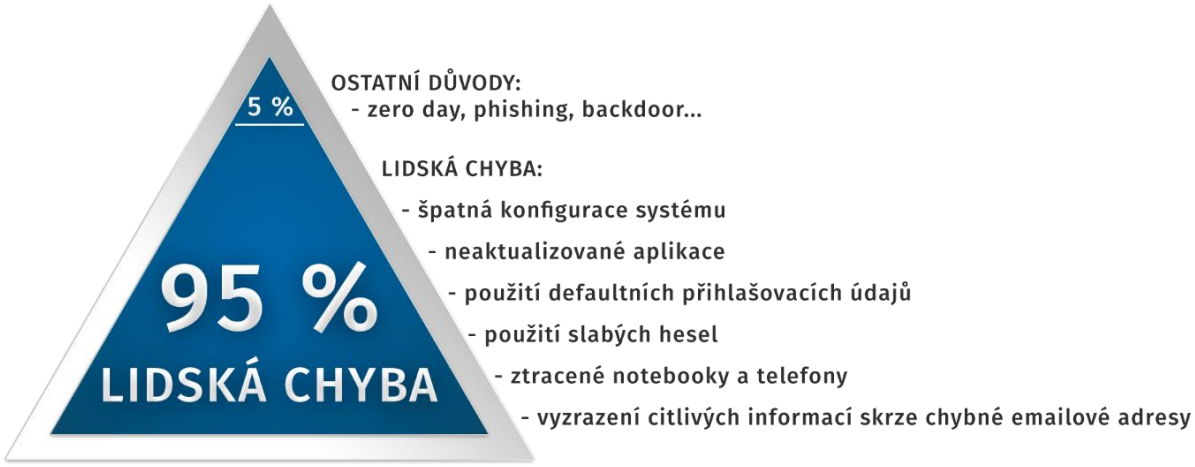
***Hrozby a rizika v kyberprostoru*** cílí primárně na triádu CIA a na prvky KB, které jsou blíže popsány a definovány v zákoně č. 181/2014 Sb. o kybernetické bezpečnosti, který nabyl účinnosti 1. ledna 2015. Hrozbu lze: „definovat jako něco, co je ze své podstaty schopné narušit běžný či řádný stav věcí a zasáhnout do práv jiných subjektů“ (Kolouch, 2019: 74).

Naplnění hrozby může vést např. ke ztrátě citlivých dat, osobních informací, přihlašovacích údajů. Případní útočníci či ti, co se k nim dostanou, je mohou prodat, požadovat po uživateli výkupné nebo, v případě že dojde k úniku dat firmy, obtěžovat na organizaci napojené zákazníky a dodavatele. Zisk přístupových dat do internetového bankovnictví může vést k „vyčištění“ účtu jedinců i organizací. Dále je možné ukrást identitu osob čili útočník se začne vydávat za okradenou oběť, což pro ni může mít negativní finanční (ztráta peněz), právní (nezákonná činnost), regulační (pokuty), reputační a psychologické (deprese) dopady. Údaje lze také použít k nákupu nelegálních a nechtěných produktů nebo umožňují získat přístup k citlivým

informacím. Kyberútoky také mohou narušit klíčové obchodní aktivity firem (např. DDoS útoky a zaplavení firemního webu) (Tunggal, 2022).

### Typy a povaha kybernetických hrozeb

Nejčastějším faktorem (95 %), který ohrožuje chod a bezpečnost kyberprostoru nejen uživatelů, ale i firem a institucí, je lidská chyba. Ať už se jedná o špatnou konfiguraci systému, neaktualizované aplikace, používání slabých hesel (81 %) či defaultních přihlašovacích údajů, ztráty notebooků a telefonů či vyzrazení citlivých informací, nejčastěji se vyskytující hrozbou je sám uživatel (NÚKIB, 2021).




*Obrázek 2: Hrozby v kyberprostoru (NÚKIB, 2021).*

U zbylých 5 % může potenciální útočník využívat nejrůznější kybertechniky. Probíhají ovšem ruku v ruce s představenými 95 %, které značně ulehčují zločineckou činnost.

Dle statistik KYBEZ ([nedat.]b.), platformy zaměřující se na efektivní spolupráci akademických institucí a komerčních firem pro zajištění bezpečnějšího digitálního prostoru a kvalitního života v něm, představují nejčastější typy útoků:

| Typ | Informace | Zdroj |
|---|---|---|
| Malware | Jedná se o několik variant kybernetických útoků. Instalaci škodlivého softwaru většinou spouští sám uživatel skrze klik na infikovanou přílohu či odkaz. Do systému se tak dostává lidskou chybou a je zneužíván pro průnik do zařízení uživatele. | (DATA SYS 2022; KYBEZ [nedat.]b). |
| Spyware | Neboli špionážní software, který sbírá „statická" citlivá data a informace a následně je bez vědomí uživatele odesílá útočníkovi. | (ESET [nedat.]b). |
| Adware | Neboli reklamní software, který je určený k nežádoucímu vyvolání a zobrazování reklam na ploše zařízení nebo sleduje internetovou aktivitu uživatele pro podklad pro cílené reklamy. | (ESET [nedat.]c). |
| Ransomware | Neboli vyděračský malware mající za cíl narušit dostupnost systému a dat (zamyká přístup k zařízení a jeho obsahu) do doby, než je útočníkovi zaplaceno za jejich obnovu (po zaplacení ovšem nemusí dojít k zpřístupnění a odšifrování). Může se šířit skrze phishing, spam, infikované weby či zneužití zranitelností. | (ESET [nedat.]e; Tunggal 2022). |
| Trojské koně | Jedná se o malware, který mystifikuje uživatele o svém skutečném záměru a tváří se jako legitimní software. Následně vytváří „zadní vrátka" pro potenciální zneužití, nicméně sám se šířit neumí. Do systému se dostává s užitečně vypadajícím programem, zranitelností systému, sociálním inženýrstvím aj. | (ESET [nedat.]d; Tunggal 2022). |
| Viry | Infikují zranitelné systémy, pokouší se získat kontrolu a ukrást data uživatelů. Po spuštění nakažené přílohy (např. e-mailové, z USB) se bez vědomí uživatele stáhnou a spustí. Následně se replikují kopírováním do jiných programů. | (ESET [nedat]a.). |
| Červi | Tento typ škodlivého softwaru se sám replikuje a infikuje další počítače. Zároveň zůstává aktivní v již infikovaných systémech. | (Tunggal 2022). |
| Botnet | Prověřuje velké množství síťových adres, následně infikuje zranitelné počítače, čímž útočník přebere kontrolu nad více počítači najednou. Poté je promění v „roboty", kteří vytvoří síť. Ta je zneužitelná např.pro DdoS útok. | (ESET [nedat.]h). |
| Cryptominer | Neboli nelegální těžba kryptoměn. Těžařský vir se k těžbě kryptoměny snaží využít výpočetní výkon zařízení. Úkon probíhá skrytě bez vědomí a souhlasu uživatele. | (ESET [nedat.]i). |
| Phishing | Útočník se vydává za důvěryhodnou autoritu (např. banka, práce, škola) a pokouší se získat citlivá data oběti (např. informace o kreditní kartě, přístupových údajů do internetového bankovnictví). Probíhá to především prostřednictvím komunikačních nástrojů. | (ESET [nedat.]ch; KYBEZ [nedat.]b). |
| SQL Injection | Na server je vložen škodlivý kód pomocí jazyka SQL, čímž nutí server doručit chráněné informace. Následně lze také vytvořit, upravit či odstranit data. Primárně cílí na databáze, kde je velké množství citlivých informací. | (KYBEZ [nedat.]b; DATA SYS 2022). |

| | | |
|---|---|---|
| Cross-site scripting XSS | Na webovou stránku je vložen škodlivý kód, který se spustí jako infikovaný skript v prohlížeči uživatele. Cílem je zisk citlivých informací. Nejčastěji je cílen na webová fóra, blogy a stránky, kde uživatelé sdílí vlastní obsah. | (KYBEZ [nedat.]b; DATA SYS 2022). |
| DDoS útoky | Dochází k zaplavení sítě falešnými požadavky. Výsledkem bývá narušením dostupnosti služby a znepřístupnění stránek ostatním uživatelům. Často se využívá botnetu (několika stovek tisíc počítačů, které žádosti šíří). | (KYBEZ [nedat.]b; DATA SYS 2022). |
| Man-in-the-Middle | Útočník odposlouchává konverzaci mezi webovou aplikací a uživatelem sítě. Cílí na jednotlivce, podniky i organizace. | (DATA SYS 2022). |
| Hijacking | Útočník získá ID uživatele a vydává se za něj při komunikaci s ostatními webovými stránkami. | (KYBEZ [nedat.]b). |
| DNS spoofing | Uživatelé jsou posíláni přes pozměněné DNS záznamy na falešné webové stránky, které se jeví jako legitimní. Alternativu představuje vytvoření falešného webu určité společnosti s pobuřujícím obsahem, což poškozuje značku firmy. | (DATA SYS 2022). |
| Zero-day exploit | Tzv. „zneužití nultého dne“ referuje ke zneužití zranitelností objevených v určité verzi softwarových aplikací a operačních systémů. | (DATA SYS 2022; Tunggal 2022). |
| Sociální inženýrství | Využívá lidskou psychologii a manipuluje oběti, aby vyzradily důvěrné informace a citlivá data nebo provedly akci, která naruší obvyklé bezpečnostní standardy (např. klikly na infikovaný soubor) – mezi nejčastější techniky je řazeno vyvolání strachu, využívání chamtivosti, vzbuzení zvědavosti, žádost o pomoc či zneužití empatie a soucitu. | (Bičíková 2022; Tunggal 2022). |
| Vishing | Neboli hlasový phishing (či podvodné volání) je podvod, kdy skrze se útočník pokouší z oběti vylákat peníze skrze telefonní hovor. | (ESET [nedat.]g). |
| Hacking | Jedná se o záměrnou změnu běžného chování či o pokus o zneužití a zisku kontroly nad sítí nebo počítačovým systémem nepovolanou osobou za nezákonným účelem. | (Avast [nedat.]; The Economic Times [nedat.]). |
| Spam | Neboli nevyžádané reklamní e-maily a zprávy (vč. řetězových zpráv a hoaxů). | (ESET [nedat.]f). |
| Sniffing | Neboli odposlech datové komunikace (tzv. „čenichání“) je technika, při níž dochází k ukládání a čtení komunikace. Používá se např. při diagnostice sítě. Může suplovat činnost spywaru či keyloggeru (zjištění hesel). Jednou z jejích forem je již zmíněný Man-In-the-Middle. | (Itbiz.cz 2009; aira [nedat.]). |
| APT | Neboli Advanced Persistent Threat, jakožto sofistikované hackerské techniky zaměřené na konkrétní cíle. | (AEC [nedat.]). |
| Kyberterorismus | Teroristické aktivity zaměřené proti či prováděné skrze kyberprostor a počítačové sítě | (MV [nedat.]). |

*Tabulka 1 – Nejčastější typy kyberútoků dle KYBEZ*

## Principy kybernetické bezpečnosti

V rámci vzdělávání jsou uživatelům převážně předávány informace o základních preventivních principech souvisejících s kybernetickou bezpečností jednotlivců, organizací i států v jejich technické rovině. Mluví se o:

| **Typ** | **informace** |
|---|---|
| Osobních údajích | GDPR, nesdělovat data z občanského průkazu, pasy, platebních karet aj. |
| Bezpečných heslech | Pravidla: délka (alespoň 12 znaků), velká a malá písmena, číslice a speciální znaky. Zásady: nesdílet – nepsat – měnit – střídat. |
| Dvoufaktorovém ověřování | Po vyplnění přihlašovacích údajů zadáváme kód, jenž dostaneme do mobilního telefonu. |
| Elektronických podpisech | Potřeba mít certifikát, nicméně se jedná o ověření identity odesílatele e-mailu a zajištění toho, že obsah nebyl „po cestě“ změněn. |
| Zabezpečování zařízení | PIN kód, otisk prstu (nejsilnější varianta), gesto (nejslabší), odemykání obličejem. |
| Veřejných wi-fi sítích | Otevřené wi-fi sítě jsou otevřené každému – nepracujte na nich s citlivými informacemi a službami. Zvažujte, kam se připojíte a proč, hlídejte HTTPS a vypínejte wi-fi až skončíte. |
| Mobilních datech | Bezpečná varianta u standardních mobilních operátorů. Stále dbejte na HTTPS a další principy bezpečného chování na internetu. |
| VPN | Šifruje vše, co odesíláme i přijímáme. Nepovolaným zrakům skryje naši aktivitu na internetu. |
| Platbách na internetu | Nutnost velké opatrnosti: nastavit vždy dvoufaktorové ověřování, opatrně na phishing, rozumný výběr prostředníka, 3D Secure. |
| Infikovaných webech | Překlepy a přesmyčky, o zneužitelnosti přesměrovávacích odkazů, zkracovače. |
| Přílohách | Opatrně se soubory typu ZIB, přípony .docm, .xlsm,, .pptm., .exe, .iso. Neotvíráme nic bezhlavě. |
| Aplikacích | Stahujte z oficiálních obchodů, čteme recenze, podmínky přístupu aplikace, omezíme jejich množství. |
| HTTPS | Především důležité v momentě, kdy pracujeme s citlivými údaji či pracujeme v internetovém bankovnictví. |
| Aktualizacích | Jedná se o zalepení bezpečnostních problémů, „děr“. |
| Firewallech | Kontrolní vstupní brána do našeho počítače, systému. |
| Antivirech | Stráže kontrolující a chránící náš počítač, systém – zabraňují vstupu nežádoucích prvků do našeho systému. |
| Zálohách | Podstatné pro obnovu dat v případě, že o ně přijdeme. |

*Tabulka 2 – Principy kybernetické bezpečnosti*

## Aktéři zajišťující a ovlivňující kybernetickou bezpečnost v ČR

Přestože na zajišťování KB by se měl podílet každý jedinec, přední roli hrají speciální bezpečnostní týmy (CERT pro identifikaci útoků a CSIRT pro řešení kybernetických incidentů) a další mezinárodní, státní (např. MZV, MO, MPO) i soukromé instituce. I kvůli neexistenci fyzických hranic kyberprostoru (tzn. případná rizika nemají územně lokalizovaný charakter) je zcela zásadní spolupráce všech sfér, kterou lze vidět např. ve společných cvičeních a projektech (Polčák – Harašta – Stupka 2016: 89-90).

O národní KB v ČR se primárně stará Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), jeho výkonná sekce a specializované pracoviště Národní centrum kybernetické bezpečnosti (NCKB) a její součást Vládní CERT ČR (GovCERT.CZ). Podstatnou roli v zajišťování KB v ČR také hraje Národní CERT a CSIRT (CSIRT.CZ), který je provozován ze strany CZ.NIC. Rozdíly mezi ním a GovCERT.CZ jsou definovány zákonem o KB, přičemž Vládní CERT a CSIRT se věnuje primárně sítím státní správy, KII a VIS, zatímco Národní CERT a CSIRT.CZ se soustředí na ostatní (v komerční a akademické sféře) bezpečnostní incidenty (NBÚ 2015; Polčák – Harašta – Stupka 2016: 90-93).

CSIRT týmy obecně mohou vznikat na úrovni jednotlivých organizací, jejichž hlavní činnost je situovaná na internetu. Můžeme zmínit například bezpečnostní tým Masarykovy univerzity CSIRT-MU či interní CZ.NIC-CSIRT. Hlavní náplň jejich činnosti představuje kooperace při řešení incidentů, které jsou spojeny s jejich vlastní síťovou infrastrukturou. Národní CSIRT pak zprostředkovává kontakt a kooperaci CSIRT týmů ve státě (Peterka 2011).

V soukromé a komerční sféře funguje také řada organizací a firem zaměřujících se (nejen) na KB, antivirovou ochranu a osvětu v této oblasti, jako je např. Avast, ESET, Microsoft, CyberSec, MyCom Solution, Cyber Security Complience, CyberSecurity.cz a mnoho dalších.

Z mezinárodních institucí, které ovlivňují zajišťování KB v ČR, je možné zmínit např. Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) a Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), na jejichž činnosti se přímo zástupci našeho státu podílí. KB představuje jednu z klíčových oblastí kolektivní obrany a jednotného přístupu mezinárodních organizací (ČR v EU, NATO, OBSE, OSN, OECD).

# VZDĚLÁVÁNÍ V KYBERNETICKÉ BEZPEČNOSTI V ČR

Vzdělání je více než investice do lidského kapitálu, jelikož otevírá také možnosti osobního rozvoje. Jedná se o celoživotní, nikdy nekončící proces získávání a rozvoje vědomostí, intelektových schopností a praktických dovedností, rozvoje rozumové stránky osobnosti, jejího myšlení a paměti. Zároveň přispívá ke zlepšování vybavenosti člověka pro život, práci a další studium (Palán, 1997, s. 131; Grecmanová, Holoušová, Urbanovská, 2002, s. 64).

Navyšování povědomí o důležitosti KB a povaze kybernetických hrozeb a jak se proti nim bránit, napomáhá uživatelům adekvátně a bezpečně se v kyberprostoru pohybovat. Jednoduše řečeno, vzdělávání a osvěta představuje základní faktor, jak snižovat vliv a počet rizik a narušeních souvisejících s nepoučenými a nepozornými uživateli. Tím dochází k podpoře zajišťování KB (NÚKIB 2021).

V ČR má vliv na vzdělávání v této oblasti státní, soukromá (školící centra), komerční („dobročinné“ projekty u antivirových společností) sféra i neziskový sektor. Ze státních organizací se jedná o MŠMT, která ji a kybernetickou hygienu ukotvuje v nových rámcových vzdělávacích programech, dále MV, jenž hraje roli při vzdělávání úředníků, policistů a metodiků prevence, MPSV, jakožto orgán vzdělávající metodiky prevence, a především NÚKIB. Ten vydává a připravuje různé vzdělávací a osvětové materiály, kampaně a kurzy. Primárně cílí na pracovníky státní správy a samosprávy, zaměstnance strategických podniků, entity dle ZKB a NIS, sekundárně pak na žáky a učitele, pracovníky prevence, policii, zdravotníky, armádu a seniory. Také umožňuje absolvovat kurzy KB pro jednotlivé skupiny (např. Dávej kyber!, Šéfuj kyber!, Bezpečně v kyber!, Kyber nemocnice!, Startuj kyber!), videokurzy (Jsem netvor, který žije na netu!, Jsem netvor na střední!), spustil sérii vzdělávacích příspěvků na Instagramu a mnoho dalšího (NÚKIB 2021; NÚKIB 2022).

Mezi další konkrétní aktéry, kteří se věnují vzdělávání, lze zařadit již zmíněný CZ.NIC a KYBEZ, Českou národní koalici pro digitální pracovní místa a dovednosti

(DigiKoalice), Centrum kybernetické bezpečnosti aj. V akademické sféře se KB např. zabývá Masarykova univerzita, Univerzita obrany, ČVUT, VUT a další VŠ (a nově i SŠ) zaměřené na ICT a IT.

Kvalifikační standardy relevantní pro kybernetickou bezpečnost v Národní soustavě kvalifikací zatím nejsou stanoveny.

## Vzdělávání dospělých

Palán (1997, s. 130) definuje vzdělávání dospělých jako obecný pojem pro vzdělávání dospělé populace a zahrnuje veškeré vzdělávací aktivity, které jsou realizovány jako řádné školské vzdělávání dospělých (tj. získání určitého stupně vzdělání) nebo jako další vzdělávání a vzdělávání seniorů. „Vzdělávání dospělých je cílevědomé a systematické zprostředkování, osvojování a upevňování schopností, dovedností, návyků, znalostí, hodnotových postojů i společenských forem jednání a chování osob, které ukončily školní vzdělání a přípravu na povolání a vstoupily na trh práce“ (Palán 1997, s. 131).

Jedná se tedy o organizovanou, cílevědomou, systematickou, plánovanou a více či méně institucionalizovanou pomoc dospělému člověku, skupinám licí nebo organizacím, týkající se zvládání určitých problémů pomocí učení či uspokojování potřeb po poznání. „Vzdělávání dospělých je (…) proces, ve kterém se dospělý člověk aktivně, systematicky a kontinuálně učí za účelem změny znalostí, názorů, hodnot, schopností a dovedností. (…) Od vzdělávání dospělých je očekáván určitý přínos pro stabilizaci či rozvoj společnosti“ (Beneš, 2003, s. 15, 43).

### Motivace ve vzdělávání dospělých

Motivace zaměřuje chování jedince, dynamizuje ho a udržuje jeho aktivitu do okamžiku dosažení stanoveného cíle. V literatuře rozlišujeme mezi motivací vnitřní a vnější.

Vnitřní je poháněna osobními přesvědčeními, potřebami, zájmy a hodnotami jedince, který ve vzdělávací aktivitě nalézá potěšení. Ovlivňují ji faktory, které si lidé tvoří sami, nechávají se jimi ovlivňovat, aby se mohli nasměřovat za určitým cílem a přizpůsobit tomu své chování. Mezi ně patří např. pocit zodpovědnosti, díky němuž máme vše pod kontrolou a stále se koncentrujeme pouze na důležité věci. Vnitřní motivace, která ovlivňuje náš pracovní život, mívá dlouhodobý charakter, jelikož je naší součástí a vyplývá z našich vlastních potřeb a přání (Armstrong, 2007, s. 221).

Vnější motivace je ovlivňována faktory z vnějšího prostředí a vede k motivování lidí, aby vykonávali to, co je potřeba. Jsou při ní používány prvky jako finanční odměna, povýšení v pracovním zařazení, pochvala. Na druhé straně se používají i tresty, lidé jsou kritizováni, nejsou jim přiznány odměny, jsou postiženi snižováním platu. Vnější motivátory nepůsobí dlouhodobě, nicméně v krátkodobém horizontu mívají výrazný účinek (Armstrong, 2007, str. 221). Může se jednat například o ztrátu nebo změnu zaměstnání či mateřskou dovolenou.

Podle Beneše (2003, s.133-135) většinou nepůsobí při vzdělávání dospělých pouze jeden motiv, ale jejich komplex, který se vyvíjejí a mění. Motivy jednotlivých skupin se navzájem liší. Motivační rozdíly najdeme ve věku, v socioekonomickém statusu, v úrovni dosaženého vzdělání, v pohlaví a životních okolnostech jako je počet dětí, život na vesnici nebo ve městě, rodinný stav.

### Překážky ve vzdělávání dospělých

Ve vzdělávání dospělých existuje několik bariér, které mohou ovlivnit jejich schopnost a touhu získávat nové znalosti a dovednosti. Kromě vlivu motivace, která velkou měrou přispívá k učení a zájmu o další vzdělávání, je potřeba věnovat pozornost i dalším překážkám. Některé z nich může být časové omezení, kdy dospělí mají mnoho závazků, jako je práce, péče o rodinu a domácnost, což jim ztěžuje nalézt čas na vzdělávání. Finanční bariéry jsou pak spojené s náklady na vzdělávání, studiu na univerzitě, úhrady kurzů nebo nákup učebních materiálů. Někteří dospělí mohou mít

také pocit, že již mají dostatečné znalosti a dovednosti pro svou kariéru, nebo nemají jasné cíle, které by je motivovaly ke vzdělávání. Další z překážek je strach z neúspěchu. Podle Rabušice a Rabušicové (2008, s. 105) je to zcela pochopitelné, protože dospělí mohou mít strach, že nebudou schopni splnit očekávání nebo se nebudou schopni vyrovnat s náročností vzdělávacího procesu.

Podle Beneše (2008, s. 145) je pro odstranění překážek a podporu motivace dospělých k dalšímu vzdělávání důležitá společenská atmosféra a míra v jaké vláda a sociální partneři podporují profesní i zájmové vzdělávání dospělých.

### Formy vzdělávání dospělých

Pojem organizační forma vzdělávání dospělých vyjadřuje vnější uspořádání vzdělávacího procesu s dospělými z hlediska času, prostoru a vztahu k jednotlivým aktérům a systému vzdělávání. Forma nám určuje podmínky, okolnosti, organizaci, způsob uspořádání, v němž probíhá proces učení (Bednaříková, 2006, s. 47-48).

Vzdělávání dospělých tvoří součást celoživotního vzdělávání. Dle Ivety Bednaříkové (2006, s. 51) je členěno do několika typů forem vzdělávání, a to:

- *školské vzdělávání dospělých,*
- *občanské vzdělávání dospělých,*
- *zájmové vzdělávání dospělých,*
- *profesní vzdělávání dospělých,*
- *vzdělávání seniorů*.

Proces celoživotního učení v sobě zahrnuje:

- *formální vzdělávání*, institucionalizované vzdělávání v subjektech školského systému,
- *neformální vzdělávání*, vzdělávání realizované různými subjekty vně školského systému,
- *informální učení*, ostatní vzdělávání, neinstitucionalizované, nesystematické.

Dospělý člověk má možnost si doplnit vyšší úroveň vzdělávání než tu, jež nabyl v mladším věku. Podle Bednaříkové (2006, s. 51) se školské vzdělávání dospělých týká lidí, kteří využijí možnost, aby si doplnili vzdělání ve formách:

- *prezenční studium*, které se koná pravidelně, každý den ve vyučovacím týdnu (přednášky, konzultace, semináře).
- *dálkové studium*, kdy se jedná o samostatné studium při zaměstnání spojené s konzultacemi. Při tomto studiu se studující připravuje převážně mimo školu na základě studijního plánu. Nabízejí ho střední nebo vyšší odborné školy.
- Velmi podobnou formou vzdělávání je *večerní forma studia*. Uplatňuje se nejčastěji na středních školách, kde se realizuje v odpoledních a večerních hodinách.
- *kombinované studium*, které je nabízeno zvláště vysokými školami je kombinací distančního studia a prezenční výuky. Tato forma vznikla ze snahy zvýšit podíl individuálního studia na celkovém objemu vzdělávání.

U seniorů může být vzdělávání poskytováno akademií nebo univerzitou třetího věku (U3V). V současnosti možnost studia na U3V nabízí většina českých veřejných vysokých škol. Na každý kraj vychází minimálně jedna univerzita třetího věku, takže možnost studovat i v pozdějším věku mají skutečně všichni.

### Profesní vzdělávání

Profesní vzdělávání se zabývá získáváním a rozšiřováním odborných dovedností, znalostí a kompetencí potřebných pro vykonávání konkrétního povolání. Je zaměřeno na rozvoj a zdokonalení odborných schopností jednotlivců, aby byli schopni lépe plnit požadavky a výzvy svého pracovního prostředí.

Může být poskytováno prostřednictvím různých forem a metod, včetně tradičního školního vzdělávání, kurzy, semináři, stážemi, online výukou a dalšími odbornými školeními. Cílem je rozvíjet konkrétní dovednosti, jako je technická zručnost, manažerské dovednosti, komunikační schopnosti nebo odborné znalosti v dané oblasti.

Profesní vzdělávání je důležité jak pro jednotlivce, kteří chtějí zlepšit své pracovní příležitosti a kariéru, tak i pro zaměstnavatele, kteří hledají kvalifikované pracovníky s potřebnými schopnostmi pro své podnikání. Je také důležité pro ekonomiku a společnost jako celek, protože kvalifikovaní pracovníci přispívají k inovaci. Zároveň přispívá k osobnímu růstu a sebeuspokojení dospělých jedinců, kteří mají možnost neustále se rozvíjet a posilovat své kompetence.

### Občanské vzdělávání

Občanské vzdělávání se zaměřuje na kultivaci člověka jako občana. Podle Bartáka (2008) se specializuje na formování vědomí práv a povinností osob v jejich občanských, politických, společenských a rodinných rolích.

Jedná se o proces, který se zaměřuje na osvojování znalostí, dovedností a postojů, které jsou nezbytné pro aktivní a informovanou účast občanů ve společnosti. Cílem je rozvíjet občanské kompetence a povědomí, aby jednotlivci mohli lépe porozumět a účastnit se demokratického procesu, a přispívat tak jako informovaní, odpovědní a participující občané ke společenskému rozvoji. Zahrnuje řadu témat, které se týkají společnosti, politiky, lidských práv, sociální spravedlnosti, udržitelnosti, mezikulturního porozumění a dalších aspektů současného života.

Ve vzdělávacím procesu občanského vzdělávání se používají různé metody, včetně diskuzí, skupinové práce, simulací, prezentací, výzkumu a praktických aktivit.

### Zájmové vzdělávání

Zájmové vzdělávání lze vymezit jako „souhrn krátkodobých i dlouhodobých forem, které umožňují edukační, tvůrčí i organizační volnočasové aktivity účastníků, směřující k saturaci jejich zájmů“ (Šerák, 2009 str. 50).

Zaměřuje se na rozšíření znalostí a dovedností v oblastech, které jsou mimo tradiční akademické kurikulum. Jedná se o vzdělávání, které je prováděno mimo formální školské prostředí a je založeno na zájmech, koníčcích a osobním rozvoji jednotlivce. Poskytuje lidem možnost naučit se nové dovednosti, objevovat nové

oblasti zájmu a rozvíjet své schopnosti. Často se týká neformálního vzdělávání, které probíhá prostřednictvím kurzů, dílen, seminářů, klubů, online platforem nebo prostřednictvím samostudia.

Existuje široká škála oblastí, ve kterých se lidé mohou v rámci zájmového vzdělávání rozvíjet. Patří sem umělecké a řemeslné dovednosti (malování, fotografie, hrnčířství, řezbářství), jazykové kurzy, hudební a taneční lekce, sportovní aktivity (jóga, plavání, lezení), kulinářské dovednosti, programování, osobní rozvoj aj.

Zájmové vzdělávání má mnoho výhod. Pomáhá lidem objevovat své skryté talenty, poskytuje možnost seznámit se s novými lidmi se stejnými zájmy, a může sloužit jako forma relaxace a vyrovnání se se stresem. Také přispívá k rozvoji kreativity a sebevědomí. V dnešní době je zájmové vzdělávání často dostupné online, což umožňuje lidem získávat nové dovednosti a znalosti v pohodlí vlastního domova.

### Vzdělávání seniorů

Toto vzdělávání představuje vzdělávání lidí v poproduktivním věku, zejména kulturně společenského charakteru. Starší lidé si tak uspokojují potřeby, kterým se v produktivním věku nemohli věnovat. (Barták, 2008)

Zatímco v minulosti bylo vzdělávání často považováno za oblast pro mladší generace, vzdělání seniorů získává stále větší důležitost a uznání. Má funkci z pohledu samotného seniora, kdy pomáhá člověku oddalovat negativní projevy stárnutí, pomáhá k udržování duševní a intelektuální aktivity, dovedností a adaptace na technologický pokrok nebo zvyšuje jeho samostatnost při rozhodování, ale také i z pohledu společnosti.

# METODOLOGIE

## Cíl práce, hypotéza a zvolená metoda výzkumu

Cílem této diplomové práce je analyzovat možnosti vzdělávání dospělých v oblasti kybernetické bezpečnosti v České republice a případně navrhnout alternativní vzdělávací program pro tuto oblast. Výzkumná otázka je stanovena: *Jaké jsou aktuální možnosti vzdělávání veřejnosti v kybernetické bezpečnosti v České republice?*

S ohledem na zkušenosti autora, který se v oboru pohybuje několik let, představenou konceptualizaci a fakt, že například volně dostupný online kurz NÚKIB *Dávej kyber!*, jakožto vzdělávací nástroj zdarma představující základy kybernetické bezpečnosti, absolvovalo v roce 2022 pouze 40 592 osob (NÚKIB, 2023) a v roce 2021 26 146 osob (NÚKIB, 2022)[1], lze předpokládat, že v současnosti vzdělávání kybernetické bezpečnosti v ČR neodpovídá požadavkům a potřebě vzdělávání veřejnosti, jakožto uživatelů kyberprostoru. Také je možné předpokládat, že dostupné kurzy a školení jsou zaměřeny primárně na technické aspekty kybernetické bezpečnosti.

Hypotéza řídící tuto práci proto zní: *Aktuální možnosti vzdělávání veřejnosti v kybernetické bezpečnosti v České republice neodpovídají žádoucímu stavu.*[2] Žádoucí stav je možné chápat jako odpovídající *množstevní pokrytí* demografického rozložení populace a počtu dospělých vzdělávacími alternativami v daném oboru, a zároveň *obsahovým zaměřením* kurzů, které by měly obsahovat technické i netechnické aspekty kybernetické bezpečnosti.

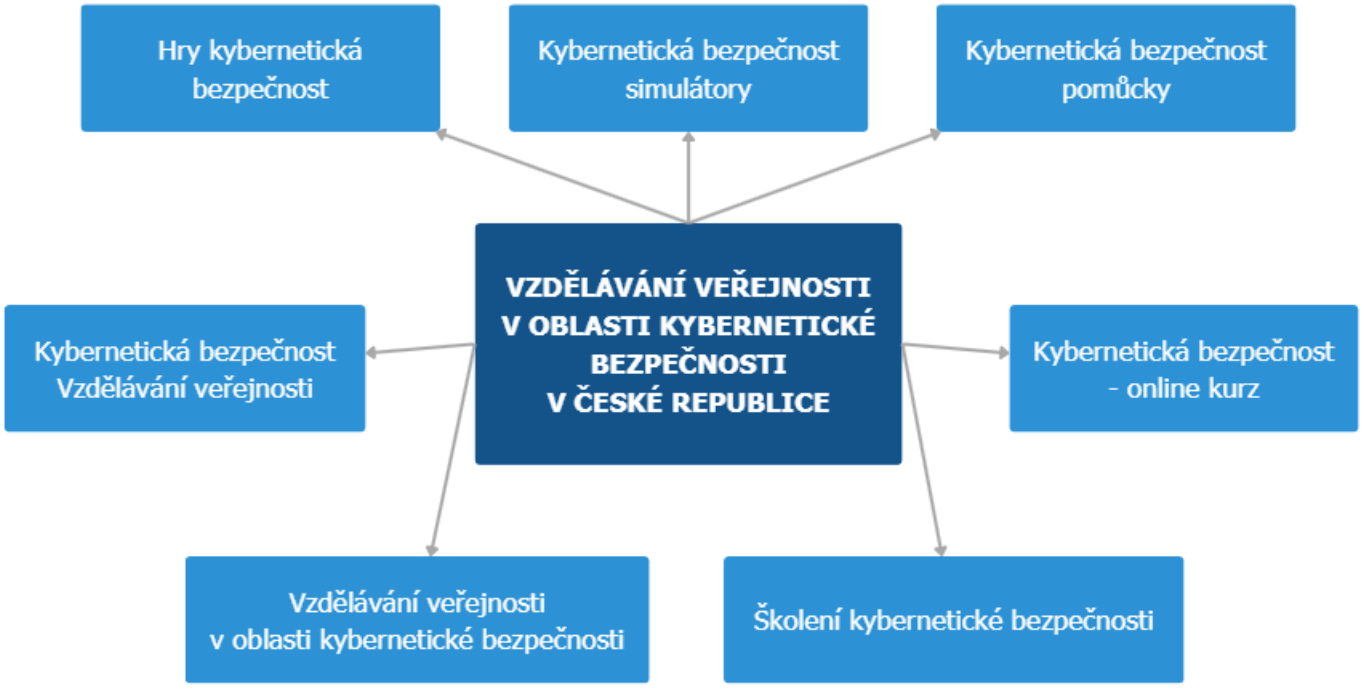
V případě, že by byla stanovená hypotéza potvrzena, dojde k navržení alternativního vzdělávací kurzu pro dospělé, který bude reflektovat vybrané

[1] Produktivní složka obyvatelstva (15-64 let) tvoří přibližně 64 % populace, tedy 6,82 mil. obyvatel (ČSÚ [nedat.]).
[2] Proměnnými jsou: (1) Aktuální možnosti vzdělávání veřejnosti v kybernetické bezpečnosti v ČR – (2) žádoucí stav.

parametry vzdělávání v kybernetické bezpečnosti, jež vyplynou z představených teorií (viz podkapitola *Teorie vzdělávání kybernetické bezpečnosti, nastavení parametrů a operacionalizace žádoucího stavu*).

Primární zkoumanou skupinu zastávají soukromé společnosti a státní organizace, které poskytují kurzy a školení a nabízejí osvětu v kybernetické bezpečnosti pro veřejnost. K vyhledávání jejich přítomnosti na českém trhu dochází na základě části výzkumu klíčových slov, kdy se při jejich stanovení využívá shromažďování návrhů (Stein, 2022) na bázi individuálního brainstormingu zabývajícího se tématem práce čili *vzděláváním veřejnosti v kybernetické bezpečnosti v České republice*. Vybraná klíčová slova jsou formulována tak, aby co nejvíce odrážela relevanci dat týkajících se výzkumu a byla úzce spojena se zkoumanou problematikou. Jejich přehled je zaznamenán na str. 26 (Obrázek 3) za užití myšlenkové mapy (Stein, 2022). Pro vyhledávání relevantních informací jsou využita slovní spojení v jejich heslovité podobě:

1. *Kybernetická bezpečnost vzdělávání veřejnosti*
2. *Kybernetická bezpečnost – online kurz*
3. *Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti*
4. *Školení kybernetické bezpečnosti*
5. *Hry kybernetická bezpečnost*
6. *Kybernetická bezpečnost simulátory*
7. *Kybernetická bezpečnost pomůcky*




*Obrázek 3: Myšlenková mapa pro identifikaci klíčových slov výzkumu (Autor, 2024).*

Sběr dat, jakožto informačně orientovaný záměr vyhledávání, jehož hledaný obsah tvoří zástupci primárně zkoumané skupiny (Stein, 2022), je pak prováděn prostřednictvím online vyhledávání představených klíčových vložením do vyhledávacího nástroje Google. V případě, že se některá organizace objevuje ve vyhledávání vícekrát, dochází k jejímu zaznamenání pouze jednou, čímž se zabraňuje zdvojení informací. Každá identifikovaná společnost je popsána.

Tímto způsobem jsou získány relevantní informace poskytující základ pro analytickou fázi. Komparativní analýza obsahu nabídky vzdělávacích možností v oblasti kybernetické bezpečnosti v českém prostředí je řízena porovnáním získaných dat, která jsou členěny do tabulky kvantitativního charakteru dle stanovených parametrů (Tab. 3). Indikátory zástupců zkoumané skupiny čili organizací nabízejících kurzy a školení v oblasti kybernetické bezpečnosti v ČR jsou členěny za užití kategorií vyplývajících z relevantních teorií (viz podkapitola *Teorie vzdělávání kybernetické bezpečnosti, nastavení parametrů a operacionalizace žádoucího stavu*).

## Teorie vzdělávání kybernetické bezpečnosti, nastavení parametrů a operacionalizace žádoucího stavu

Pro měření způsobu vzdělávání populace v kybernetické bezpečnosti neexistuje jediná univerzální teorie. Některé z nich ovšem stanovují, jaké základní komponenty by měl obsahovat nebo jakými dovednostmi by měli „studenti“ kybernetické bezpečnosti, a tedy nezbytně všichni uživatelé kyberprostoru, disponovat.

Mezi teorie věnující se vzdělávání kybernetické bezpečnosti patří přístup doktora Bruce Schneiera, Kybernetický index gramotnosti Centra pro kybernetickou bezpečnost z Tel Aviv či Rámec cambridgeských životních kompetencí dle Cambridge University, Cambridge Assessment English a Cambridge University Press. Autor vidí jako klíčovou pro vzdělávání v dané oblasti také roli uživatelské motivace.

### Vzdělávání podle Schneierova přístupu (Click Here to Kill Everybody, 2019)

Mgr. Bruce Schneier, Ph.D je americký kryptograf, odborník na počítačovou bezpečnost, specialista na soukromí a spisovatel. Přednáší veřejnou politiku na Harvard Kennedy School a spolupracuje s Berkman Klein Center for Internet & Society. Vzdělávání považuje za klíčový prvek pro zajištění bezpečnosti a přežití v hyper-propojeném světě, v němž se technologický vývoj nedá zastavit a přináší nové hrozby i příležitosti.

"Musíme lidi naučit, jak být v bezpečí, stejně jako je učíme, jak být v bezpečí ve fyzickém světě. Musíme je naučit, jak rozpoznat phishingové e-maily a škodlivé adresy URL, jak bezpečně nakonfigurovat svůj počítač, jak rozpoznat příznaky malwaru atd. […] Musíme učit inženýry, jak vytvářet bezpečné systémy. Musíme učit programátory, jak bezpečně kódovat. Musíme naučit správce systémů, jak bezpečně konfigurovat systémy. A musíme naučit manažery, jak řídit bezpečnost […] Potřebujeme více technologů veřejného zájmu: lidí z našeho oboru, kteří pracují na mnoha místech, kde se tvoří politika. Potřebujeme je v zákonodárných orgánech, ve

výkonných agenturách, na soudech, v nevládních organizacích a jinde" (Schneier, s. 211-213).

Tato citace ukazuje, že Schneier považuje vzdělávání za klíčový prvek pro zajištění bezpečnosti a přežití v hyper-propojeném světě, kde se technologický vývoj nedá zastavit a přináší nové hrozby i příležitosti. Schneier ale zdůrazňuje, že nejde jen o technické dovednosti, ale také o schopnost chápat sociální a politické důsledky technologie a ovlivňovat její směr a regulaci. Systematické vzdělávání má tedy pozitivní vliv na rozvoj dovedností, protože podporuje kritické myšlení, kreativitu, spolupráci a sociální odpovědnost u studentů, jimiž by měli být uživatelé kyberprostoru.

Pro hodnocení poskytovaného vzdělávání a kurzů v kybernetické bezpečnosti bude pro indexování využito, zda vzdělávací program zohledňuje priority, kterým Schneier přikládá velkou váhu, tedy *srozumitelnosti, motivaci, logičnosti, důkladnosti, rozvoji*.

### Kybernetický index gramotnosti (Digital Humanities at the Sourasky Central Library, Cyber Literacy)

Kybernetický index gramotnosti (Cyber Literacy Index) byl vyvinut Centrem pro kybernetickou bezpečnost na Univerzitě Tel Aviv ve spolupráci s firmou Check Point Software Technologies. Základem pro něj byla převzatá úroveň vzdělání v oblasti STEM (věda, technologie, inženýrství a matematika).

Tento index je jedním z prvních pokusů o měření úrovně znalostí, dovedností a postojů obyvatel ke kybernetické bezpečnosti na celosvětové úrovni. Index hodnotí 12 indikátorů, které se týkají tří hlavních aspektů kybernetické gramotnosti: znalostí, dovedností a postojů. Těmito indikátory jsou:

- Znalosti:
    - *Znalost základních pojmů kybernetické bezpečnosti.*
    - *Znalost základních opatření kybernetické bezpečnosti.*

- *Znalost základních práv a povinností v kyberprostoru.*
- *Znalost základních hrozeb a rizik v kyberprostoru.*

- Dovednosti:
  - *Schopnost používat silná hesla a spravovat je.*
  - *Schopnost používat antivirový software a aktualizovat ho.*
  - *Schopnost rozpoznat a vyhnout se phishingu a podvodům.*
  - *Schopnost zálohovat a obnovovat data.*

- Postoje:
  - *Opatrnost při sdílení osobních informací online.*
  - *Důvěra v online služby a instituce.*
  - *Zodpovědnost za vlastní bezpečnost a bezpečnost ostatních.*
  - *Zájem o vzdělávání se novým věcem v kybernetické bezpečnosti.*

Zajímavostí může být, že Česká republika má nižší skóre v Kybernetickém indexu gramotnosti, než je průměr Evropské unie.

Pro hodnocení poskytovaného vzdělávání a kurzů v kybernetické bezpečnosti bude využito toto indexování, tedy zda vzdělávací program zohledňuje *postoje, dovednosti a znalosti*, jakožto základní indikátory reflektující technologickou i netechnologickou rovinu problematiky.

### Rámec cambridgeských životních kompetencí (Cambridge Life Competencies Framework)

Rozsáhlý výzkum Cambridge University, Cambridge Assessment English a Cambridge University Press vedl k vytvoření příručky pro učitele a manažery vzdělávání o digitální gramotnosti. Vzniklý Rámec cambridgeských životních kompetencí tak poskytuje mapu nejdůležitějších dovedností, které studenti potřebují rozvíjet. Digitální gramotnost je zde propojena s dalšími vrstvami Cambridge Life Competencies Framework a podporuje jejich rozvoj.

Skládá se ze šesti kompetencí, s kterými jsou spojeny tři základní vrstvy. Těmito kompetencemi jsou:

- *Kreativní myšlení*: schopnost generovat nové a originální nápady, řešit problémy a inovovat pomocí různých zdrojů inspirace a technik.
- *Kritické myšlení*: schopnost analyzovat, hodnotit a interpretovat informace, argumenty a důkazy z různých perspektiv a zdrojů.
- *Sebe-reflexe*: schopnost plánovat, organizovat, monitorovat a regulovat vlastní učení, využívat různé strategie a zdroje a reflektovat nad vlastním pokrokem a výsledky.
- *Komunikace*: schopnost sdílet a vyměňovat informace, názory a emoce s různými lidmi, v různých situacích, pomocí různých jazyků a médií.
- *Spolupráce*: schopnost pracovat efektivně s ostatními na společném cíli, respektovat rozdílnosti, přispívat k týmové práci a řešit konflikty.
- *Sociální odpovědnost*: schopnost chápat a ovlivňovat dopad vlastních akcí na sebe, ostatní, společnost a životní prostředí.

Pro hodnocení poskytovaného vzdělávání a kurzů v kybernetické bezpečnosti bude využito indexování, tedy zda vzdělávací program zohledňuje šest základních životních kompetencí podle cambridgeského rámce: *kreativní myšlení, sebe-reflexi, komunikaci, spolupráci, sociální odpovědnost*.

### Uživatelská motivace

Uživatelská motivace vzdělávacího kurzu je klíčovým faktorem pro efektivní vzdělávání, jelikož ovlivňuje zájem a úspěch jeho účastníků. Ovlivňují ji různé aspekty, jako potřeba, zvídavost, cíle, preference a podmínky vzdělávání. Kurz by měl také naplňovat potřeby a očekávání v oblastech uživatelské přívětivosti, dostupnosti, doby licence, bonusu a ceny, čímž se zvýší zájem, motivace, spokojenost a úspěch účastníků vzdělávání.

Vzdělávací kurz by tedy měl mít parametry, které odpovídají potřebám a očekáváním účastníků:

- *Dostupnost* – kurz by měl být dostupný za jasně stanovených a přívětivých podmínek, týkajících se ceny i časové dotace.
- *Uživatelská přívětivost* – kurz by měl být srozumitelný, zajímavý, interaktivní a přizpůsobený úrovni a stylu učení účastníků, což se dá ověřit s pomocí zpětné vazby.
- *Doba licence* – kurz by měl mít jasně stanovenou dobu platnosti licence, která umožňuje účastníkům opakovat nebo aktualizovat své znalosti a dovednosti.
- *Bonusy* – kurz by měl nabízet nějakou přidanou hodnotu pro účastníky, například certifikát, slevu, zpětnou vazbu nebo další možnosti vzdělávání.
- *Zdarma / placené* – kurz by měl být cenově dostupný a konkurenceschopný, měl by reflektovat kvalitu, náročnost a obsah kurzu.

Zohlednění těchto parametrů v přípravě kurzu je důležité pro zvýšení motivace a spokojenosti účastníků vzdělávání.

Z představených rámců a přístupů nám vyvstává řada parametrů, s nimiž je pracováno v praktické části diplomové práce. Konkrétně se jedná o faktory, které vyvstávají ze:

1. *Vzdělávání podle Schneierova přístupu ke KB*: srozumitelnost, motivace, názornost, logičnost, důslednost, rozvoj a inovace.
2. *Kybernetický index gramotnosti*: postoje, dovednosti a znalosti.
3. *Rámec cambridgeských životních kompetencí*: kreativní myšlení, sebe-reflexe, komunikaci, spolupráci, sociální odpovědnost.
4. *Uživatelská motivace*: dostupnost, uživatelsky přívětivé, doba licence, bonus, zdarma, cena.

Z vybraných teorií a stanovených parametrů jednoznačně vyplývá, že vzdělávání kybernetické bezpečnosti by mělo pokrývat *technické i netechnické aspekty* (viz stanovené parametry), což také odpovídá tzv. žádoucímu stavu stanovenému hypotézou této práce. Již vysvětlená důležitost vzdělávání veřejnosti, jakožto uživatelů pohybujících se v kyberprostoru, také přidává žádoucí aspekt přístupu dospělé populace k dostupným možnostem vzdělávání v dané oblasti.

## Limity a omezení práce

V rozsahu práce nelze určit a analyzovat veškeré dodavatele a poskytovatele vzdělávání v oblasti kybernetické bezpečnosti pro veřejnost. Jelikož se jedná o dynamicky se vyvíjející trh, jejich existence a funkčnost stejně jako počet se neustále mění.

Výsledky a rozsah analyzovaných společností je také limitován metodou individuálního brainstormingu a povahou klíčových slov. Případné doplnění o další charakteristiky a specifikace či klíčová slova (např. kyberbezpečnost nebo počítačová bezpečnost) by mohlo vést k rozšíření analyzovaných proměnných. Jedná se o limit, ale zároveň potenciál pro budoucí rozšíření, využití a nakládání s prezentovanými daty. Stejný princip platí pro omezení související s vyhledávacím nástrojem, tedy Googlem a absencí užití dalších webů, jako je Bing, Seznam či Yahoo.

S tím souvisí také obecnost zkoumaných parametrů, která se může zdát nevhodná pro hlubší výzkum. Jejich užití do jisté míry ospravedlňuje fakt, že vychází z relevantní literatury a užívaných a respektovaných teorií. I s ohledem na předchozí limit není zkoumání případných jednotlivostí konkrétních parametrů v rozsahu diplomové práce možné a opět se jedná o aspekt potenciálního rozšíření výzkumu.

V práci také nelze analyzovat kompletní kurikula jednotlivých nabízených kurzů, jelikož ta nejsou volně dostupná, stejně jako konkrétní počty absolventů jednotlivých kurzů. Bylo by třeba je veškeré absolvovat a dané údaje si vyžádat, což

ale vyžaduje značnou časovou i finanční dotaci. Nejedná se tak o faktor zvládnutelný v rámci rozsahu diplomové práce, ale o potenciál pro případné rozšíření a doplnění analýzy. V práci je proto pracováno s volně dostupnými informacemi o obsahu a zaměření jednotlivých kurzů, které je možné identifikovat z nabídek na webových stránkách organizací.

Dle zákona má zaměstnavatel povinnost v oblasti kybernetické bezpečnosti vzdělávat své zaměstnance, proto je otázkou, zda občané ČR považují separátní edukaci za logickou, a tedy zda je pro osvětové firmy výhodné nabízet kurzy, školení a jiné vzdělávací materiály pro veřejnost. Případný negativní vliv na poptávku po specializovaných kurzech může mít také velké množství volně dostupných edukačních materiálů online, často dostupných zdarma. Cílem této práce ovšem není analyzovat poptávku po daných kurzech, ale zjistit stav jejich nabídky.

# KURZY A ŠKOLENÍ NA ČESKÉM TRHU NABÍZENÉ ČESKÝMI SPOLEČNOSTMI

V následující části dojde k představení nabízených kurzů v českém prostředí na základě jejich vyhledávání dle stanovených klíčových slov:

1. *Kybernetická bezpečnost vzdělávání veřejnosti*
2. *Kybernetická bezpečnost – online kurz*
3. *Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti*
4. *Školení kybernetické bezpečnosti*
5. *Hry kybernetická bezpečnost*
6. *Kybernetická bezpečnost simulátory*
7. *Kybernetická bezpečnost pomůcky*

### 1. KLÍČOVÉ SLOVO: Kybernetická bezpečnost vzdělávání veřejnosti

**Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**

„Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany“ (NÚKIB, [nedat.]a). Jeho činnost a role i vztah ke vzdělávání jsou řízeny zákonem o č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB).

Přestože se jedná o gestora a nejvyšší autoritu KB v České republice, nespadá do primární činnosti NÚKIB vzdělávání široké populace, ale především se soustředí na zaměstnance veřejné správy, úředníky a další osoby stanovené ZKB (jejich činnost je zásadní pro chod České republiky). Osvětu mezi žáky a studenty, seniory stejně jako u širší veřejnosti rozšiřuje spíše sekundárně (NÚKIB, [nedat.]e), a proto je nabídka pro ně množstevně a rozsahově omezená (nikoli však kvalitativně).

I tak ale nabízí řadu zajímavých možností, které jsou jednoduše dostupné online a zdarma na stránkách https://osveta.nukib.cz/. Je možné tam najít e-learningové kurzy (např. ***Základy kybernetické bezpečnosti – Dávej kyber!, Bezpečně v kyber!, pro úředníky, preventisty, zdravotníky, zaměstnance škol***) a vzdělávací materiály pro jednotlivé cílové skupiny. Zaměstnanci NÚKIB se také osobně účastní konferencí, seminářů, workshopů a dalších vzdělávacích aktivit. Na požádání (pokud mají prostor dostupný lidský kapitál) připravují přednášky a školení věnující se dílčím tématům kybernetické bezpečnosti (NÚKIB, [nedat.]e; NÚKIB, 2022). Jednotlivci v případě dotazů mohou kontaktovat oddělení vzdělávání. Je důležité zopakovat, že úkolem (a ani v silách) NÚKIB není masová osvěta a výše zmíněné aktivity, jelikož se nejedná o klasickou vzdělávací instituci, ale o správní orgán soustředící se spíše na rozvoj systému vzdělávání (NPI, [nedat.]).

### Buď Safe Online

Zdarma dostupný online kurz od YouTubera Jiřího Krále a Avast Foundation (specializuje se na globální zabezpečení) velice jednoduchým a lidským způsobem vysvětluje, jak se chovat na internetu a online světě. Nejrůznější témata představuje tím, že uživatel může sledovat chat dvou lidí, kteří řeší hry, celebrity, výhružky, ukradení účtu, podezřelé zprávy, soutěže a další klasické triky, s nimiž se každý z nás na internetu může každý den setkat (Buď Safe Online, [nedat.]).

### COM PLUS CZ a.s.

„Přes 80 % všech hackerských útoků využívá chyb lidí.“ S tímto odůvodněním nabízí **placené e-kurzy** a školení kybernetické bezpečnosti (od užívání počítačového software až po odborná školení) společnost COM PLUS CZ a.s. Jedná se o českou společnost, která se zaměřuje na komplexní ICT řešení, outsourcingové služby s důrazem na kybernetickou bezpečnost a služby v oblasti telekomunikací. Na trhu

působí více než 30 let. Její služby využívá soukromý i státní sektor (COM PLUS, [nedat.]a). Reference může na společnost poskytnout řada měst (Velké Hamry, Kroměříž aj.), AV Media, Sportisimo, Povodí Moravy a další (COM PLUS, [nedat.]b).

Naneštěstí se tyto kurzy zaměřují primárně na zaměstnance firem. V tří hodinovém e-learningovém kurzu (videa, opakovací krátké testy) se COMPLUS Security pokouší zvyšovat povědomí o hrozbách a trendech, stejně jako seznamovat se základy kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti č. 181/2014 Sb. (ZKB). Nutnost absolvování kurzů staví na počtu probíhajících útoků a na možných postizích pro firmy stanovených legislativou, pokud své zaměstnance neproškolí (COM PLUS, [nedat.]b). Naneštěstí není jasné, zda a za kolik peněz je možné kurz koupit pro jednu osobu. Využitelnost pro vzdělávání veřejnosti je tedy spekulativní.

**Centrum kybernetické bezpečnosti, z.ú. (KYBERCENTRUM)**

Tato společnost se plně zaměřuje na šíření osvěty, vzdělávání v oblasti kybernetické bezpečnosti a kybernetické obrany. Svou činností primárně cílí na mládež, studenty a učitele. Některé její výstupy jsou volně dostupné na internetu (např. Kyberpohádky, Kyber říkanky) a lze je libovolně využít. Zároveň připravuje řadu akcí, soutěží (Cyber Security Competition), konferencí, festivalů, letních škol a kurzů. Na druhou stranu nenabízí volně dostupné kurzy a spíše má užší zaměření, které je časově omezené na jednotlivé jí organizované události.

„Naše cíle vychází z potřeb moderní společnosti závislé na informačních a komunikačních technologiích. Z potřeby vyhledávat, motivovat a připravovat mladé lidi se zájmem o kybernetickou bezpečnost a obranu, a poskytovat celoživotní vzdělávání a podporu lidem pohybujících se v oblasti kybernetické bezpečnosti“ (Centrum kybernetické bezpečnosti, [nedat.]).

Mezi partnery Kybercentra patří společnosti AFCEA, npi (Digi Koalice), Jhk.cz, Jihočeská hospodářská komora a v případě projektu národní soutěže NSKB a týmu

ECSC 2022 pak MŠMT, Skupina ČEZ, NAKIT, DELL, ČD, Microsoft, Škoda, Corpus Solutions a mnoho dalších (Centrum kybernetické bezpečnosti, [nedat.]).

### ESET software spol. s.r.o.

ESET je globální společností již 30 let se zaměřující na digitální zabezpečení uživatelů. Nabízí ochranu a podporu pro PC domácnostem, firmám i dalším organizacím z nejrůznějších sektorů (ESET, [nedat.]i). Má stovky partnerů z celé republiky (ESET, [nedat.]j).

Nabízí také několik forem online školení kybernetické bezpečnosti zaměřené na zaměstnance a podniky. Probírá v nich základní prvky a principy, jako je ochrana e-mailu, webu, hesla, homeoffice, sociální inženýrství a kybernetické hrozby. Cena není uvedena, nicméně se odvíjí od počtu školených zaměstnanců. V nabídce je možné poptat školení i pro jednu osobu (ESET, [nedat.]k), tudíž, přestože se jedná o zaměření na firmy, je možné předpokládat dostupnost i pro klasickou veřejnost.

### MyCom Solutions, s.r.o.

Velice lidský přístup a pokus představit se jako mladá dynamická IT skupina zaujímá poměrně malá společnost MyCom Solutions, s.r.o. Původně se věnovala virtualizaci a dodávkám serverů, nyní se výhradně soustředí na outsourcing služeb, KB, cloudové služby, hardware a software (StartupJobs, [nedat.]). Mezi jejich partnery patří společnosti jako je ESET, Microsoft, HP Development, Veeam, VMware, Safetica, Fortinet, Dell a další (MyCom Solutions, [nedat.]a).

Co se šíření osvěty týče, poskytují placené školení kybernetické bezpečnosti, kdy za pomocí praktických příkladů uživatelům vysvětlují, na co si dát pozor a co dělat pro zajištění bezpečnosti dat a prostředí (bezpečně na internetu, viry, bezpečná pošt@, silné a slabé heslo, poznání podvržených e-mailech, stránek, firemní data aj. (MyCom

Solutions, [nedat.]b). Školení je naneštěstí také zaměřeno na firmy a její zaměstnance, nikoli přímo na veřejnost a dospělé.

### Novicom, s.r.o. – Novicom Academy

Poměrně nové produkty v oblasti vzdělávání kybernetické bezpečnosti (z podzimu 2022) nabízí společnost Novicom, s.r.o., český výrobce nástrojů pro síťovou správu, monitoring a bezpečnost, působící na IT trhu od roku 1994. V rámci Novicom ACADEMY nabízí osvětu formou seminářů, přednášek, interních školení, pracovními úkoly, případovými studiemi a předáváním zkušeností z praxe o bezpečnosti IT a komunikací. Nejčastěji koncipují kurzy na vyžádání zákazníka, které se věnují úvodu do KB, KB ve firmách a zaměstnanců. Tato společnost se primárně zaměřuje na střední a velké zákazníky, navíc opět chybí možnost vzdělávání veřejnosti (Novicom, [nedat.]a; Novicom [nedat.]b; Novicom Academy, [nedat.]).

Partnery společnosti Novicom jsou například organizace dns, SECTEC, O2, Caleum, ANECT, T-SOFT, TOTAL SERVICE a další (Novicom, [nedat.]c).

### T-SOFT, a.s.

Společnost T-SOFT je IT společností, která se primárně zaměřuje na speciální informační systémy, integraci a bezpečnost. Její zákazníci pochází z veřejné správy, bank, velkých podniků i mezinárodních institucí. Funguje od roku 1991 (T-SOFT, [nedat.]a). Mezi partnery má společnosti jako je GORDIC spol. s.r.o., ICZ a.s., Microsoft, O2, Siemens IT Solutions and Services a mnoho dalších organizací (T-SOFT, [nedat.]b).

Raritou je její jednodenní interaktivní školení zaměřené na to, jak se běžný uživatel IT může starat o svou kybernetickou bezpečnost, jaké se v kyberprostoru objevují hlavní hrozby, jak zabezpečit telefon, jak nenaletět sociálnímu inženýrství apod. Kurz je

postaven na základě aktivní diskuse. Primárně směřuje na podnikatele, majitele firem, úředníky a zaměstnance škol. Tento workshop se liší oproti jiným nabídkám svým rozsahem. Pojme max. 25 lidí najednou, tudíž je v něm kladena větší pozornost na fungování jedince. Kybernetický workshop je součást programu „KB ve veřejné správě“. Nelze však určit jeho cenu, protože ta není na stránkách organizace uvedena (T-SOFT, [nedat.]c). Navíc se nezdá pravděpodobné, že by tento kurz byl volně dostupný veřejnosti či by jej bylo možné objednat sám za sebe nebo v malém měřítku bez opakování pro více skupin.

**Acresia Consulting s.r.o.**

Základním mottem společnosti Acresia zní: „Knowledge is power“. Sama se tedy profiluje jako firma propagující a uznávající znalosti, vědomosti a zkušenost. Primárně poskytuje řešení v oblasti GDPR pro korporace a malé i velké podniky (Acresia, [nedat]a; Evropská databanka, [nedat.]). Nabízí ale také školení a e-learning (kurzy na platformě Moodle), video learning, screancasting a webináře spojené s IT bezpečností pro uživatele, phishingem a ransomwarem. Velice fádně tedy také „naťukává“ KB a nabízí specializovaná školení „šitá na míru“ organizacím. Na stránkách nejsou uvedeny ceny za daná školení. Nabídka explicitně nezahrnuje jedince a veřejnost (Acresia, [nedat.]b).

Mezi její partnery patří Walmark, Fortuna, Generální finanční ředitelství, Český statistický úřad a několik dalších (Acresia, [nedat.]a).

## 2. KLÍČOVÉ SLOVO: Kybernetická bezpečnost – online kurz

**ITnetwork.cz**

Velice zajímavou nabídku e-learningových kurzů a dalších materiálů pro nejrůznější IT profese a veřejnost poskytuje zcela zdarma (nebo za nejnižší cenu na trhu) největší

IT akademie v ČR - ITnetwork.cz, která se sama prezentuje jako sociální síť IT. Nabízí také školení s lektorem (prezenční výuka ve skupinách s cca 10 lidmi) a má akreditací pro rekvalifikační kurzy (hrazené úřadem práce) pro obory, jako je programování, vývojářství mob. aplikací, AI a big data, tester (ITnetwork.cz, [nedat.]a) aj. Na jejích stránkách je možné studovat jednotlivé technologie, jako např. Java, PHP, JavaScrypt, C#.NET, SQL a další (ITnetwork.cz, [nedat.]b).

V rámci své nabídky má společnost ITNetwork.cz také lekce kybernetické bezpečnosti. Zcela zdarma si mohou uživatelé internetu projít její základní pojmy a zásady, hesla a biometrickou ochranu, tematiky spojené s kryptografií, operačními systémy (vč. antiviru), základů šifrování, pravidla bezpečného zálohování, zásady práce s maily a weby (ITnetwork.cz, [nedat.]c) aj.

### ALEF Training Center

Společnost nabízející ICT řešení – od základní infrastruktury, pokročilé síťové technologie pro vývoj aplikací, až po poskytování ucelených služeb, funguje od roku 1994 (ALEF, [nedat.]a). Poskytuje rozsáhlá školení, on site, online kurzy, konzultace, e-learning, webináře a semináře a vzdělávací programy v oblasti IT. Některé produkty jsou placené, jiné zdarma. Většinou se jedná o osvětové akce pro více pokročilé uživatele, nikoli veřejnost (ALEF, [nedat.]b).

Jedno z volně dostupných školení se nazývá Základy kybernetické bezpečnosti a jeho cílem je uvést školeného do bezpečnosti informací, technických nástrojů a řízení informační bezpečnosti. Referuje k „základům“ a je nabízen „komukoli, kdo se v bezpečnosti informací neorientuje a měl by zájem o obecný přehled“, nicméně jedná se o více pokročilý kurz s požadavky na orientaci v ICT prostředí (porozumění pojmům jako je server, SAN, LAN aj.) (ALEF, [nedat.]c) a je otázkou, zda by úplný lajk daný kurz zvládl. Zároveň stojí 7 500 Kč a svou náplní spadá spíše pod informační

bezpečnost, nikoli kybernetickou, tudíž se nejedná o vzorek zhodnotitelný jako relevantní prvek vzdělávání veřejnosti o KB v ČR.

Obdobně je na tom kurz Kybernetický útok a obrana v praxi, který trvá dva dny a má účastníky naučit realizovat základní testy, odhalovat zranitelnosti, analyzovat síťový provoz apod. Zároveň kurz stojí 36 000 Kč a je určen pracovníkům ICT, nikoli veřejnosti (ALEF, [nedat.]d).

Mezi partnery ALEF patří Cisco, Microsoft, vmware partner, aws, f5, paloalto a CompTIA (ALEF, [nedat.]e).

### Kyber školení.cz

Společnost Advis Consulting s.r.o. se primárně zaměřuje na zajištění služeb v oblasti PO a BOZP, prevenci rizik a požární ochranu aj. V rámci svého projektu pak nabízí proškolení zaměstnanců o bezpečném chování v kyberprostoru. Cílem e-learningového kurzu a interaktivní výuky je pak seznámit uživatele se základními principy a pravidly informační bezpečnosti. Věnují se v něm např. elektronické poště, malware, spamu, phishingu, heslům, antivirům aj. základním bezpečnostním prvkům a vědomostem (Kyber školení, [nedat.]). Cena ani více informací není uvedeno.

### Knowspread.cz s.r.o.

Knowspread.cz s.r.o. se prezentuje jako nástroj a platforma pro e-learning v organizacích. Zároveň za peníze (od 120 přes 240 do 324 Kč / licenci) nabízí pro organizace a firmy z nejrůznějších oblastí (např. zdravotnictví) již existující kurzy. Zaměstnavatel si má možnost sám vygenerovat obsah a jednoduše dle vlastních preferencí zaměstnancům poslat soubor online školení. Jejich zaměření většinou směřuje na BOZP, PO, první pomoc a školení řidičů (Knowspread.cz, [nedat.]a; Knowspread.cz, [nedat.]b).

Jeden z kurzů je přímo určen „Kybernetické bezpečnosti“. Zaměřuje se na úplné základy, představení pojmů, legislativy, hrozeb a zabezpečením. Obrovskou výhodou je, že jej lze zakoupit za 290 Kč samostatně, mimo firemní balíčky (Knowspread.cz, [nedat.]c). Můžeme jej tedy považovat za nástroj osvěty KB pro veřejnost.

### BOZP.cz

Jedná se o komplexní online školící systém využívající e-learningový nástroj BOZP-SYSTEM.cz, který se dá využít pro školení zaměstnanců, primárně v oblasti BOZP, PO první pomoci a řidičů, nicméně se dá využít také interaktivních kurzů zaměřených na rizika spojená s konkrétními profesemi (BOZP, [nedat.]a). Osvětové online materiály a školení je možné zakoupit (za poměrně nízkou cenu) v nejrůznějších balíčcích (Mini – Basic – Standard – Premium). Jsou dostupná i jednotlivcům (90 – 160 – 200 – 240 Kč) (BOZP, [nedat.]b).

V rámci nabízených služeb a produktů v balíčku Premium má společnost připraveno Školení informační a kybernetické bezpečnosti, jenž má navýšit povědomí zaměstnanců s pojmy a základními principy kybernetické bezpečnosti. Například se v něm mohou dozvědět, jak správně pracovat s hesly, e-maily, vzdáleným obsahem, jak poznat podvodné webové stránky a potenciální kybernetické útoky, stejně jako jak zálohovat data (BOZP, [nedat.]c) aj. Jelikož lze balíček Premium zakoupit pro jednu a více osob, dá se toto školení považovat za dostupné a potenciálně vzdělávací pro veřejnost.

Mezi její klienty patří např. Wolt, Národní památkový ústav, Dedoles, Arriva, Vinted, LG, Peugeot, neeco, productboard, Wikimedia a mnoho dalších (BOZP, [nedat.]d).

### Hikvision

Kurz kybernetické bezpečnosti lze také absolvovat online na webu společnosti Hikvision, poskytovatele IoT řešení pro video, který vznikl v roce 2010 a nyní slouží na trzích ve více než 150 zemích a zahrnuje 66 dceřiných společností a poboček. Nabízí širokou škálu produktů pro fyzické zabezpečení, jež zahrnují video zabezpečení, kontrolu přístupu a poplašné systémy, smart cities atd. Poskytuje také integrovaná bezpečnostní řešení využívající technologii umělé inteligence, robotiky, inteligentních úložišť aj. a rozvíjí mnoho dalších klíčových technologií (Hikvision, [nedat.]a).

Za jeden ze svých předních závazků prezentuje podporu a dodržování mezinárodně uznávaných standardů a postupů v oblasti kybernetické bezpečnosti. Pokouší se také podpořit úsilí zvýšení schopnosti obrany sítě. Na svých stránkách vydávají novinky a aktuality z této oblasti (Hikvision, [nedat.]b). V šesti online přednáškách také mluví o kybernetické bezpečnosti v bezpečnostním průmyslu, které probírají počítačový hacking, kyberbezpečnosti produktů, zranitelnosti, IP kamerách, GDPR a implementaci kybernetické bezpečnosti v praxi. Kurz lze shlédnout pouze pomocí Hikvision ID, ke kterému se je nutné přihlásit (Hikvision, [nedat.]c). S ohledem na zaměření přednášek se navíc nejedná přímo o základy kybernetické bezpečnosti, ale o úzce specializovaný okruh témat. Nedá se tedy tato nabídka považovat za příliš přínosnou ve spojitosti se vzděláváním veřejnosti o této problematice.

### Učímeonline.cz

Zajímavý kurz také je volně a zdarma k najití online na webových stránkách ucimeonline.cz a nese název Kybernetická bezpečnost ve vzdělávání. Přestože je primárně určen učitelům, přínosný může být také pro rodiče a děti na začátečnické či pokročilé užívání počítače a internetu (Učímeonline.cz, [nedat.]a). Jeho cílem je seznámit účastníky s hrozbami na internetu, jako je phishing; deep a dark webem; zabezpečením v online světě a dětem v něm se pohybujícím. Zároveň dává praktický návod, jak se chránit a nabízí tipy na filmy spojené s danou problematikou (Suchánek,

[nedat.]). Jedná se o velmi přívětivý nástroj poskytující základní kyberbezpečnostní rady. Zároveň jednoduše a dostupně některá základní pravidla kybernetické bezpečnosti pro všechny uživatele.

Samotný projekt Učíme online vznikl jako iniciativa dobrovolníků neziskové organizace Česko.Digital, komunity specialistů z mnoha oborů (vč. IT), jejich partnery jsou Google, Avast, PPF nadace a Livesport (Česko.Digital, [nedat.]). Projekt samotný pak funguje za spolupráce s Googlem, Microsoftem, GUG.cz a dalšími partnery. Nyní jej realizuje Národní pedagogický institut ČR. Jeho cílem je rozvoj digitálních kompetencí a zlepšování užití digitálních technologií ve školách, inspirace a vzdělávání učitelů v této oblasti (Učíme online.cz, [nedat.]b).

## Czechitas

Nezisková organizace, která otevírá svět IT ženám a dětem. „Motivujeme ženy, vzděláváme je a pomáháme jim najít vysněnou práci v oboru. Propojujeme je s partnerskými firmami, které vítají různorodost v pracovních týmech.“ (Czechitas, [nedat.]a) Tak se prezentuje společnost Czechitas, která poskytuje řadu kurzů zaměřených na IT, programování, robotiku a moderní technologie.

Mezi partnery Czechitas jsou společnosti jako Google.org, ČSOB, Škoda, Microsoft, IBM, Inco Academy Work in Tech, AT&T, Barclays, CISCO, Brno, Nestlé, Notino, Siemens a řada dalších (Czechitas, [nedat.]b). Tato společnost také získala řadu titulů a národních i mezinárodních cen (Czechitas, [nedat.]c).

Czechitas nabízí kurz nesoucí název Úvod do kybernetické bezpečnosti. Je plánován pro úplné začátečníky prezenční formou v rozsahu 8 hodin za 990 Kč a probíhá jednou za pár měsíců. Školené má provést základy KB tedy vysvětlit, co je kybernetická bezpečnost, jak vypadají základní kybernetické útoky, jak je detekovat a nahlásit. Krátce také představuje téma kryptografie a přehled pozic v této oblasti (Czechitas, [nedat.]d). Jedná se o způsob, jak se k informacím může dostat de facto kdokoli. Na

druhou stranu není tolik frekventovaný, nicméně stále lze považovat kurz Czechitas za podstatnou možnost, jak vzdělávat veřejnost v oboru KB a IT.

### Instructor by Prevent

Instructor by Prevent je vzdělávací platformou, jež přináší interaktivní online kurzy a poradenství pro zákonná a jiná firemní školení zaměstnanců (Instructor, [nedat.]a).

Její nabídka obsahuje také praktický online kurz Informační a kybernetická bezpečnost, jenž představuje zásady ochrany informací, bezpečného používání ICT prostředků. Také seznamuje s riziky, hrozbami (jako je phishing) a bezpečnostními incidenty a jak se jim bránit. Jedná se o velmi přívětivý a sympaticky působící kurz poskytující základní informace o zásadách KB (Instructor, [nedat.]b).

Společnost sice má na svých stránkách uvedenou cenu za kurzy, ale upravuje ji podle požadavků zájemce (počet proškolených, balíčky Jeden kurz – zvýhodněný balíček – Vlastní balíček aj.). Z webu je patrné, že přestože jeden kurz stojí 90 Kč/osoba/rok, minimální cena nákupu je 1800 Kč, tedy musí být zájem pro minimálně 20 účastníků (Instructor, [nedat.]c). Naneštěstí tento faktor působí, že není přístupný jednotlivcům, tudíž pro veřejnost by byl použitelný pouze v případě větší skupiny.

Školení této společnosti užívají např. Allianz, IBM, DHL, ŘSD ČR, Sazka, Kiwi.com, NAKIT Porsche, PPF, KPMG, Deloitte a další.

### eÚředník

Další variantou vzdělávání zaměstnanců je elektronický portál eÚředník, který nabízí interaktivní e-learningové kurzy. Prezentuje se jako estetický, efektivní a finančně výhodnější s ohledem na jeho online podobu. Jako součást lekce nabízí také řadu příloh s různými detaily (eÚředník, [nedat.]a). Cenová relace kurzů není uvedena, ale údajně se odvíjí dle délky licence a počtu zájemců. Je možné je zakoupit i pro

jednotlivce (eÚředník, [nedat.]b). Kurzy na tomto portálu prošla řada úředníků z několika městských částí Prahy (eÚředník, [nedat.]c).

Na webu lze objednat také kurz Kybernetická bezpečnost. Představuje útoky a jejich znaky v kyberprostoru a jak je identifikovat. Také probírá základní pojmy a principy kyberprostoru, hesel, informačních systémů, počítačových sítí, elektronické pošty, USB, e-mailu aj. Cílem má být posílení vnímání bezpečnostních zásad, jenž chrání jedince i organizaci (eÚředník, [nedat.]d).

## SOVA STUDIO

Vzdělávací společnost sídlící v Brně vznikla již v roce 2002. Jejím smyslem je pořádat osvětové kurzy z nejrůznějších oblastí, které pokrývají potřeby odborné firemní edukace pro soukromý, veřejný i neziskový sektor. Školení, workshopy a další formy vzdělávání probíhají v učebnách a školících centrech v Brně a Praze (Educity, [nedat.]).

Na poptání lze u lektorů SOVA STUDIO prezenčně absolvovat kurz Kybernetická bezpečnost, jehož cena se pohybuje kolem 4 000 Kč. Je možné jej objednat i pro jednotlivce. Věnuje se pojmům kybernetické a informační bezpečnosti (vč. kyberválky, ransomware, sociální inženýrství) a mnohému dalšímu. Jeho cílem je, aby se účastník orientoval v dané problematice a byl schopný nově nabyté znalosti uplatnit v každodenním životě (SOVA Studio, [nedat.]). Tento kurz je tedy využitelný pro veřejnost, nicméně limitující může být jeho cena.

## DOXO LOGIC s.r.o.

Poměrně mladá firma (vznik roku 2016) prezentující se velmi lidským a přívětivým způsobem, zaměřující se na kybernetickou a informační bezpečnost komplexním způsobem. Za pomocí etických hackerů nabízí nejen hledání slabých míst sítí, ale také jejich zacelení a možnost naučení se útokům předcházet. Součástí jejich činnosti jsou

tedy také školení a pořádání tréninkových her Capture the flag (DOXO LOGIC, [nedat.]a). Mezi partnery společnosti patří např. Check Point Software Technologies, Trend Micro, Bitdefender a RESPECT (DOXO LOGIC, [nedat.]b).

Jedním z kurzů, jejž dříve společnost nabízela, byl online kurz nesoucí název Chraňte se před hackery: kybernetická bezpečnost polopatě. Ten byl určen pro jakéhokoli uživatele počítače a internetu a bylo možné jej zakoupit za 2990 Kč (v případě akce za 990 Kč). Obsahoval čtyř týdenní přednášky a živé webináře zaměřené na hesla a jejich principy v kyberprostoru, nejčastější hackerské techniky vč. sociálního inženýrství, poznání falešných webů, dále na Wi-Fi a hrozby související se vzdáleným připojením a Free Wi-Fi, dále na soukromí na internetu a zda je možné jej vůbec v dnešní době mít. Jako alternativu také společnost nabízela osobní konzultace v kybernetické bezpečnosti za 1500 Kč/hod (DOXO LOGIC, [nedat.]c). Obecně tento kurz vypadal jako ideální řešení vzdělávání veřejnosti a jednotlivců online. Naneštěstí v době psaní této práce přiložené odkazy na přihlášení nebyly plně funkční a skutečná užitelnost a současný stav zůstává otázkou také proto, že momentálně se firma vyhraňuje spíše na školení zaměstnanců menších a větších firem (DOXO LOGIC, [nedat.]d).

### Počítačová škola GOPAS

Společnost GOPAS představuje největšího poskytovatele školení v oblasti ICT na českém i slovenském trhu. Pořádá konference, semináře, organizuje veřejné i privátní kurzy z oblasti IT, testuje dovednosti skrze certifikační zkoušky, poskytuje e-learning a samostudijní interaktivní kurzy (GOPAS, [nedat.]a).

Jedním z nabízených školení od této společnosti jsou Základy kybernetické bezpečnosti. Jedná se o představení bezpečnosti informací, vysvětlení jejich řízení a technických nástrojů, ISMS, procesů a dokumentací. Je určen také pro veřejnost se zájmem o moderní trendy. Lze jej objednat na vyžádání a probíhá pravidelně prezenčně v Praze a Brně. Cena se pohybuje přibližně kolem 7 500 Kč / den. Naneštěstí

je třeba již určitá znalost ICT prostředí (porozumění serverům, SAN, LAN aj. pojmům), nejedná se tedy o kurz určený pro klasickou veřejnost a začátečníky (GOPAS, [nedat.]b).

### 3. Klíčové heslo: vzdělávání veřejnosti v oblasti kybernetické bezpečnosti

**Next Generation Security Solutions s.r.o.**

Poměrně mladá (vznik 2016) česká společnost NGSS poskytuje služby specialistů v oblasti informační a kybernetické bezpečnosti – ať už se jedná o penetrační testování, analýzu rizik, SIEM, SOC, bezpečnostní audity, SMC či outsorcing bezpečnostních rolí. Dále je také možné u nich udělat mezinárodně uznávané certifikace (ISMS, CISA, CISM, ITIL aj.) (NGSS, [nedat.]a). Jejich služby využívá např. Fakultní nemocnice Ostrava, Lesy ČR, ČZÚ Praha, voestaline aj.

Společnost NGSS nabízí několik školení kybernetické bezpečnosti. Taktéž primárně cílí na firmy a jejich zaměstnance, nicméně např. v Kurzu kybernetické a informační bezpečnosti těm se pokouší vštípit zásady bezpečného chování na internetu, v interní síti a zvýšit tak obranyschopnosti firem. Využívá k tomu praktické postupy, teoretickou i praktickou část a výukové materiály dle požadavků poptávajícího. Základní školení trvá 2 hodiny nebo lze objednat několikadenní intenzivní kurzy. Umožňují také vytvoření e-learningových kurzů, které cílí na individuální učení zaměstnanců (většinou o tématech jako je phishing a techniky sociálního inženýrství) (NGSS, [nedat.]b). Problémem je fakt, že se skutečně jedná primárně o školení pro zaměstnance firem, tudíž dosah k dalším segmentům veřejnosti je omezen.

**TOTAL SERVICE a.s.**

Od roku 1997 v ČR také působí společnost Total Service. Jejich specialisté spravují datová centra, zajišťují KB, nabízí inovativní řešení v prostředí ICT a zajišťují kybernetickou bezpečnost pro malé, střední podniky, nadnárodní korporace i státní správu (TOTAL SERVICE, [nedat.]a). Zároveň tato firma poskytuje služby, produkty, ale také know-how v oblasti ICT. Lze si od nich nechat připravit prezenční i online školení dle požadavků zákazníka. Její služby využilo např. město Praha, VZP, KONE, ÚZIS, Biocev, Česká televize, Globus a další.

Konkrétně nabízí Kurz kybernetické bezpečnosti, kde zaměstnance seznamuje s principy KB a postupy jejího dodržování a trendy. Poskytují jej pro běžné uživatele IT i pokročilé kybernetické pracovníky. Témata se liší dle cílové skupiny, ale lze objednat školení např. o sociálním inženýrství, phishingu, malwaru a soukromí uživatelů, OWASP TOP 10 zranitelností (TOTAL SERVICE, [nedat.]b). Cena ani možnost využití širokou veřejností není uvedena.

### CyberSec Online školení kybernetické bezpečnosti

Společnost CyberSec nabízí online školení kybernetické bezpečnosti pro firmy nejrůznějších velikostí a jejich zaměstnance. Za cenu 180 Kč je u ní možné získat licenci pro jednu osobu/rok, zbytek cen určuje počet vydaných licencí. Na webu jednoduše tvůrci CyberSec vysvětlují, proč je školení v této podobě důležité a jaké přináší výhody: ať už mluvíme o ceně, lidské chybě nebo nebezpečích v kyberprostoru (CyberSec, [nedat.]a; CyberSec, [nedat.]b).

Tento e-learning byl vytvořen odbornými garanty IDC-softwarehouse, s.r.o. (specializace na budování a správy IT infrastruktury od roku 2000, připravili obsah kurzu), ATOM Digital s.r.o. (přes více než 10 let vyvíjí webové stránky a nabízí digitální služby, zajišťuje technickou podporu a grafickou podobu kurzu) a legislativním garantem Stuchlíková & Partners, advokátní kancelář, s.r.o. (právní poradentství a právní stránka kurzu) (CyberSec, [nedat.]c).

Jedná se o poměrně přívětivé školení skládající se z 6 certifikovaných kurzů, využívajících jednoduchou formu a ilustrativní příklady. Jejich obsah tvoří vývojáři, právníci a další odborníci na kybernetickou bezpečnost (CyberSec, [nedat.]d; CyberSec, [nedat.]e). Školení je přímo zaměřeno na předání komplexních základů a zásad kybernetické bezpečnosti. Účastníci se tak mohou dozvědět o e-mailu a jeho bezpečném používání, zabezpečení počítače a telefonu, bezpečném připojování, internetových prohlížečích, zálohování dat, právních důsledcích či GDPR (CyberSec, [nedat.]f). Opět se jedná o společnost zaměřující se primárně na firmy a její zaměstnance, nicméně je možnost zakoupit také menší množství licencí, tudíž se zde nachází potenciál vzdělávání jednotlivců v rámci společnosti.

## 4. Klíčové slovo: školení kybernetické bezpečnosti

### Integra

Česká soukromá společnost Integra nabízí od roku 2012 řadu služeb v oblasti informační bezpečnosti (např. vývoj SW na míru) a outsourcingu IT specialistů (Integra, [nedat.]a). V rámci její specializace také poskytuje školení a kurzy pro základní i pokročilé uživatele (např. UX design, React pro pokročilé, Základy pythonu) (Integra, [nedat.]b). Prezentují se primárně jako dodavatel firem. Spolupracuje s nimi více než 60 společností (např. Člověk v tísni, Komerční banka, Notino, Avast, Home Credit, Allianz, air bank, Equa bank) (Integra, [nedat.]c).

Zajímavé může být prezenční (připravuje se individuálně) či online školení Vzdělávání uživatelů v oblasti kybernetické bezpečnosti, které je dedikováno podvrženým e-mailům, citlivým údajům, phishingu, ochraně proti hrozbám. Pro online verzi využívá 45 speciálních testovacích a školících modulů zaměřených na tuto problematiku. Každý z nich obsahuje kurz, který uživatele vzdělává v uvedené oblasti KB. Je sestaven z vysvětlení pojmů, následují doporučení, jak se chovat a končí testem

(testuje, zda školený rozpozná podvrh či validní zprávu) (Integra, [nedat.]d). Cena kurzu ani možnost využití pro veřejnost není na webu uvedena.

### Scenario Informační Technologie

Poměrně mladá firma (cca 5 let) působící v oboru IT, dodává HW a SW, stejně jako informační systémy, služby a vývoj SW svým zákazníkům pocházejícím ze soukromé i státní správy. Na jejím webu lze najít základní přehled a laické vysvětlení hrozeb kyberprostoru. Službami se zaměřuje primárně na velké podniky, státní instituce, malé a střední firmy, školky, školy a univerzity, ale také města, kraje a obce. Mezi její zákazníky patří např. Česká pošta, ALEFT Nula, CCC, Český rozhlas, Tatra a další. Zároveň je partnerem společností DELL, EMC, Lenovo, ESET, Konica Minolta, Fujitsu (Scenario, [nedat.]a; Scenario, [nedat.]b) aj.

V rámci své nabídky také zařizuje dvouhodinové školení zaměřené na zvyšování povědomí v oblasti KB v několika formách: prezenčně, e-learning s lektorem online, e-learning. Má tak přispět k zajištění bezpečnosti organizací, splnit povinnost zaměstnavatelů vzdělávat zaměstnance v této oblasti a naučit je chovat se v dnešním ICT světě bezpečně. Představuje základní pojmy, legislativu KB, útoky a sociální inženýrství, bezpečné chování na sítích a internetu, práci s hesly, online, elektronickou poštu, webové stránky a vše prověřuje závěrečným testem. Primárně je určeno pro zaměstnance společností, firem a státní správy, a nikoliv veřejnosti (Scenario, [nedat.]c).

### KEY Trainings s.r.o.

Jednou ze společností zaměřujících se čistě na školení v IT odvětví, je firma KEY Trainings. Nabízí široké portfolio kurzů např. o IT dovednostech, soft skills a připravených na míru. Je možné u nich objednat také odborné poradenství (KEY

Trainings, [nedat.]a; SKOLENI.cz, [nedat.]). Disponují akreditací Ministerstvem školství, mládeže a tělovýchovy.

KEY Trainings je partnerem předních dodavatelů IT produktů, jako je Microsoft, ATO of ITIL Prince2 Agile, CompTIA, DASA Training Partner, Elastic, IT preneurs aj. Své služby dodává mezinárodním i českým firmám, jako např. CGI, Microsoft, O2, Generali, pwc, Ministerstvo obrany, makro, Kooperativa, Česká pošta, Česká spořitelna, T-Mobile (KEY Trainings, [nedat.]b) a dalším.

Jedním z nabízeních kurzů je také školení základů kybernetické bezpečnosti, jež přibližuje problematiku různých druhů útoků na domácí i firemní infrastrukturu. Má zvýšit bezpečnostní povědomí uživatelů v kybernetické a informační bezpečnosti, tedy o sociálním inženýrství, spamu, phishingu, malwaru, heslech, webech, online identitě, Wi-Fi, hackingu aj. Užívá teoretické i praktické ukázky reálných praktik a rady, jak se útokům bránit. Nabízí jej v pravidelných intervalech v českém i anglickém jazyce za cenu 6900 Kč online i prezenčně. Trvá jeden den (KEY Trainings, [nedat.]c). S ohledem na možnost koupě se tato varianta dá považovat za způsob, jak jedinec může získat školení v oblasti kybernetické bezpečnosti. Na druhou stranu odrazujícím faktorem je cena, která spíše odpovídá zájemcům z malých a středních firem.

### BEPOR.eu

Další společností věnující se školení BOZP a PO, která také zajišťuje kurz informační a kybernetické bezpečnosti, je e-learningový BEPOR.eu. Jejich online verzi vzdělávání lze získat pro jednu osobu za 150 Kč. Mezi klienty patří např. VOX, ČIA News, FitInn, GB, GML, inveo (BEPOR.eu, [nedat.]a) a další.

Konkrétně Školení informační a kybernetické bezpečnosti tvoří sled témat a testových otázek zaměřených na bezpečnost informací. Je zaměřeno na běžné uživatele PC a dalších koncových zařízení. Poskytne znalosti rizik napadení zařízení, počítačových systémů, technik útočníků a případné obrany proti nim (BEPOR.eu, [nedat.]b).

Přestože je zaměřeno na zaměstnance firem a jejich naplnění zákona a povinnosti vzdělávat svůj personál, lze jej objednat pro jednu osobu.

### GORDIC

Firma Gordic funguje na českém trhu od roku 1993. Pokouší se poskytnout nástroj pro komunikaci mezi lidmi a organizacemi, navíc zajišťuje řadu školení. Jedná se také o předního českého tvůrce a dodavatele informačních systémů a komplexní uživatelské podpory. Zároveň je to provozovatel a iniciátor již představené platformy KYBEZ.

Společnost spolupracuje s ministerstvy ČR (MO, MV, MPSV, MZdrav, MPO atd.), Českou inspekcí, Českým telekomunikačním úřadem, Ombudsmanem a řadou dalších státních institucí, měst, krajů, letišť, stejně jako firem ze soukromého sektoru apod. Mezi jejich partnery patří také O2, Ness, Power Systems (GORDIC, [nedat.]a) aj.

Jedno z nabízených online školení jsou i Základy kybernetické bezpečnosti, které stojí 1500 Kč./osobu Věnují se v něm důležitosti KB, legislativě, hrozbám a zranitelnostem, kybernetickým útokům a jak jim čelit, proč se před nimi chránit a jak na ně reagovat. Součástí je také cvičení modelových situací a závěrečný test (GORDIC, [nedat.]b). Jedná se o alternativu použitelnou pro veřejnost a jednotlivce.

### ASSIST Intelligence Solutions

Další českou firmou dodávající softwarové služby a řídící aplikace na různých platformách. Jedná se o Europe Digital Hub, specialisty na IBM Power Systems a další technologie. Tato společnost taktéž nabízí vzdělávací aktivity – komerční kurzy pro firmy, školení pro zaměstnance, projekt Akademie ASSIST (ASSIST, [nedat.]a) apod. Softwarové služby poskytuje např. firmám Renault, NN, Uniqua aj., vzdělává a další činnost pak zajišťuje pro Komerční banku, NN, Generali, Panasonic, MONETA, ČMSS, IBM, Deloitte (ASSIST, [nedat.]b) atd.

Součástí její nabídky je také prezenční školení Kybernetická bezpečnost pro uživatele. Jedná se o kurz s časovou dotací jednoho dne, který stojí 2 000 Kč/osobu. Je určeno všem zájemcům, tedy i komukoli ze široké veřejnosti. Zaměřuje se na principy kybernetické bezpečnosti pro běžné uživatele, motivaci útočníků, bankovní identitu, GDPR, faktory bezpečnosti, malware, sociální inženýrství, hesla, zabezpečení OS Windows, prohlížečů, sociálních sítí, messengerů, dále také představuje Cookies, domácí routery, problematiku dětí na internetu, informační hygienu a digitální závislost (ASSIST, [nedat.]c). Rozhodně se jedná o školení použitelné širokou veřejností.

### Cyber Security Comliance

Komplexní řešení kybernetické bezpečnosti pro firmy nabízí společnost Cyber Security Compliance: Audit kybernetické bezpečnosti. Věnuje se právním, technickým i organizačním aspektům této problematiky. Čili auditem identifikují slabiny, navrhnou a implementují opatření, osvětlí problematiku KB zaměstnancům. Připravuje tak zájemce na kybernetické hrozby. Mezi její partnery patří česká kancelář KPMG, dále LPP a advokátní kancelář Toman & Partneři (Cyber Security Compliance, [nedat.]a).

Jak již bylo zmíněno, součástí nabídky je také online nebo prezenční Školení kybernetické bezpečnosti (pro zaměstnance a pro management), které trvá 4 hodiny. Jeho cílem je uvést uživatele do základů kybernetické bezpečnosti a bezpečnosti informací. Osvětluje technické i organizační nástroje, stejně jako techniky a taktiky kybernetického útoku a obrany. Jeho projití tak zvyšuje kybernetickou odolnost společnosti. Přestože se na první pohled zdá, že je určeno primárně zaměstnancům firem, není tomu tak. Mohou jej absolvovat i jednotlivci z řad široké veřejnosti (Cyber Security Compliance, [nedat.]b). Jedná se tedy o školení použitelné širokou veřejností. Naneštěstí na stránkách Cyber Security Compliance není uvedena cena jejích služeb.

## Pavel Lorenc

Pavel Lorenc je jedinec věnující se tvorbě webových stránek a online kurzů e-learningových systémů. Historicky již navrhl celou řadu těchto produktů na míru žadatelům (Lorenc, [nedat.]a).

Jedním z e-learningových veřejně nabízených kurzů, který navrhl je také Informační a kybernetická bezpečnost, který je zaměřen na KB ve smyslu ZKB. Využil k tomu speciální interakce a gamifikační prvky čili simulátor spamových a phishingových e-mailů, messenger, simulátor internetového prohlížeče, sociálního hackingu. Zároveň v něm podával tipy pro silná hesla a další. Nabízí jej ve formátu SCORM, přičemž obsah lze customizovat dle přání klienta (Lorenc, [nedat.]b). Jeho cena a přístupnost v současnosti není zcela jasná, nicméně dle profilu webu by byl možný případný zájem vykomunikovat přímo s panem Lorencem. Tato forma se tedy dá považovat za potenciální vzdělávací prvek pro veřejnost.

## DATA SYS

Česká společnost, která na trhu poskytuje řadu IT služeb již od roku 1994. Zaměřuje se především na podniky všech velikostí, státní správu, samosprávu, subjekty z oblasti vzdělávání a vědy, neziskové organizace i nemocnice (DATA SYS, [nedat.]a). Mezi její zákazníky patří např. MZV, Justice.cz, McDonalds, MV, ICOM transport a.s. či Česká pošta (DATA SYS, [nedat.]b). Jejími partnery je řada společností nejen z oblasti IT, přesto je na tomto resumé mnoho předních firem věnující se právě kyberprostoru, např. tedy ESET, CISCO, DELL, HITACHI, FORTINET, Microsoft, Kaspersky, Red Hat, SOPHOS (DATA SYS, [nedat.]c).

Na vyžádání nabízí také e-learningové kurzy zaměřené na kybernetickou bezpečnost – základy IT bezpečnosti, fyzická bezpečnost, sociální inženýrství a phishing, práce na

dálku, elektronická pošta a bezpečnost na webu (DATA SYS, [nedat.]d). Na stránkách naneštěstí nelze dohledat více informací o těchto kurzech, tudíž jejich použitelnost, a především aplikovatelnost pro veřejnost a jednotlivce je čistě spekulativní. I s ohledem na výčet charakteristik DATA SYS výše lze předpokládat, že se nejedná o společnost zajišťující osvětu společnosti, ale spíše o aktéra důležitého pro státní správu a soukromé subjekty.

### ReNTEL a.s.

ReNTEL je firma fungující na trhu od roku 1999. Nabízí multijazykové a multimediální e-learningové kurzy, webináře, s prezenční i kombinovanou formou z širokého spektra oblastí. Její služby využívají především úřady a firmy (ReNTEL, [nedat.]a).

Jedním z nabízených kurzů je Úvod do kybernetické bezpečnosti. Ten má účastníky uvést do světa kyberprostoru a naučit je základním pravidlům a principům kybernetické bezpečnosti. Zdůrazňuje také důležitost této problematiky. Školení vyžaduje časovou dotaci 4 hodin a stojí 370 Kč (ReNTEL, [nedat.]b). Dle podmínek lze předpokládat, že jej lze zakoupit i jako jedinec, tudíž jej můžeme považovat za způsob osvěty pro veřejnost.

### Chráním data, s.r.o.

Chráním data tvoří skupina odborníků na problematiku KB, vzdělávání dospělých, marketingu a online formu rozvoje. Nabízí 37 kurzů a testů zaměřujících se na informační bezpečnost, GDPR nebo vytváří kurzy na míru. Existuje po 25 let (Chranimdata, [nedat.]a).

Jejich kurz je určen primárně pro zaměstnance a učí pravidla bezpečného zacházení s informacemi. Obsahuje témata jako jsou internetové hrozby, sociální sítě, zabezpečení telefonů, veřejné počítače a Wi-Fi sítě. Obsahuje 17 videí po 5-10 minutách

ve 4 jazycích. Jeho cena se liší podle počtu účastníků, většinou se pohybuje mezi 396-250 Kč/osobu. Nejmenší počet potenciálně přihlašovaných účastníků je ale 5 ks (Chranimdata, [nedat.]b). Z toho vyplývá, že kurz by byl veřejnosti dostupný pouze v případě, kdy by se domluvilo více jedinců se zájmem o školení, nelze jej tedy považovat za dostupnou variantu všem.

### Trigama.eu

Trigama.eu je moderní a inovativní společnost věnující se IT, digitalizaci, poradentství a modernímu designu od roku 2013. Zároveň se specializuje na e-learning a vzdělávání (Trigama.eu, [nedat.]a). Mají podíl na vzniku Bankovní identity, webové aplikace Bingo, grafice Kooperativa Helpdesk, O2 a mnoha dalších (Trigama.eu, [nedat.]b). Mezi její partnery patří BankID, ecolytiq, mojeID a Vocalls a mezi zákazníky společnosti jako je Komerční banka, xmarton, Avenier, Home Credit, ČZÚ Praha, Česká spořitelna (Trigama.eu, [nedat.]c) a řada dalších.

V rámci e-learningu nabízí firemní vzdělávání o BOZP, PO a kybernetické bezpečnosti (Trigama.eu, [nedat.]d). Naneštěstí neposkytuje více informací a lze předpokládat, že kurz není možné absolvovat jako jednotlivec.

### Edject Courses

Další ze společností nabízejících primárně kurzy BOZP, PO a školení řidičům, tedy zaměřující se primárně na firmy, je česjý Edtech firma Edject s globální působností, přední dodavatel e-learningových řešení. Vyvíjí vlastní produkty, aplikace a řešení pro e-learningový průmysl, které pomáhají organizacím s digitálním vzděláváním a vzdělávacími technologiemi již od roku 2010 (Ejdet Courses, [nedat.]a). S jejími kurzy je spojena řada firem, jako např. Fortuna, AAA Auto, Skupina ČEZ, VZP, Veřejný ochránce práv, Raiffeisen BANK, Lidl, Just a další (Edjet Courses, [nedat.]b).

Nabízí také e-learningový kurz informační a kybernetické bezpečnosti dle zákona č. 181/2014 Sb. Trvá 45 minut a má seznámit účastníky s nejrůznějšími kyberhrozbami a kyberútoky, malwarem a ransomwarem, phishingem, riziky sociálních sítí, kyberšikanou, hoaxy a fake news, ale také s problematikou a důležitostí kybernetické bezpečnosti, zákonem o kybernetické bezpečnosti, NÚKIB, tipy pro bezpečnost hesel, zabezpečení zařízení (Edjet courses, [nedat.]c) aj. Jedná se o komplexní školení, které lze zakoupit i pro jednotlivce za 100 Kč/rok (Basic varianta) či v balíčcích s dalšími školeními za ceny vyšší (Edjet courses, [nedat.]d).

Školení a vzdělávání kybernetické bezpečnosti u zaměstnanců malých, středních i velkých firem se věnuje i celá řada dalších organizací, jako např. Network Security Monitoring Cluster, Arion IT Solutions, CyberG Europe, SECURU, Verlag Dashöfer a její kursy.cz. Jiné se zase specializují na vzdělávání pedagogů v této oblasti, jako např. npi, či na jiné cílové skupiny. Více se jim nebudeme věnovat, jelikož nenabízí varianty pro jednotlivce a klasickou veřejnost.

#NePinDej

Česká bankovní asociace (ČBA) odstartovala v září 2022 rozsáhlou vzdělávací kampaň, která má upozornit na sílící nebezpečí podvodů na internetu. Pod názvem #nePINdej! (kreativní tvorba ze slov PIN nedej) představuje nejčastější kybernetické útoky a formou hravého testu na www.kybertest.cz (Kybertest, [nedat.]) se snaží naučit, jak jim nenaletět. Kybertest má několik variant, které simulují nejčastější podvodné praktiky dle různých věkových skupin. Cílovou skupinou jsou mladistvé od 12 let, dospělí a senioři. Celý projekt vznikl za podpory Policie ČR a NÚKIB, tím získává na důvěryhodnosti.

**5.-7. Klíčová slova: hry kybernetická bezpečnost, kybernetická bezpečnost simulátory, kybernetická bezpečnost pomůcky**

Alternativou pro online kurzy a školení jsou také vzdělávací hry či simulátory, které pomáhají (nejen) veřejnost učit jinými způsoby.

## Clashing

Jako zářný příklad můžeme uvést Clashing: Cyber Security Awareness Training, vzdělávací online nástroj, jenž fixuje a vytváří návyky bezpečného chování v kyberprostoru, ať už při práci z domova či kanceláře na firemní síti. Snižuje tak bezpečnostní rizika spojená s útoky hackerů.

Jeho principem je, že zaměstnanci cca 15 min hrají proti sobě v pozici hackera-útočníka a obránce či mohou hrát proti počítači. Jedná se o cloudovou službu, tudíž ke spuštění potřebuje uživatel pouze webový prohlížeč.

Učení tak staví na tom, že je třeba, aby lidi daná věc bavila, což pak vede k lepšímu zapamatování a automatizaci správných reakcí v případě bezpečnostních hrozeb. Zároveň pro hru využívá reálné situace, jež většina lidí zažila a umožňuje hráči také nahlédnout na druhou stranu, tedy si zahrát z pohledu útočníka. To jim pak pomáhá pochopit, jak a co lze v kyberprostoru zneužít.

Přestože je primárně určena firmám všech velikostí, počet účtů, které lze zřídit, není nijak omezen. Cena se pak odvíjí od počtu přístupů do hry (Clashing, [nedat.]). Lze proto předpokládat, že ji mohou využít i lidé mimo společnosti, tudíž i zástupci veřejnosti.

# KOMPARACE A VYHODNOCENÍ KURZŮ A ŠKOLENÍ NABÍZENÝCH NA ČESKÉM TRHU

| Σ HODNOCENÍ KURZU | Uživatelská motivace | | | | | | Rámec cambridgeských životních kompetencí | | | | | | Kybernetický index gramotnosti | | | | | | | | | | Vzdělávání podle Schneierova přístupu k KB | | | | | | Hodnocení vzdělávání v ČR<br>KYBERNETICKÁ BEZPEČNOST | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | zohledňuje | | | | | | postoje | | | dovednosti | | | znalosti | | | | | | | | | | | | |
| | placené | zdarma | bonus | doba licence | uživatelsky přívětivé | dostupnost | sociální odpovědnost | spolupráce | komunikace | sebe reflexe | kritické myšlení | kreativní myšlení | zájem o vzdělávání | zodpovědnost | důvěra v online služby | sdílení osobních informací | záloha a obnovovat data | rozpoznat hrozbu | antivirový software | silná hesla / správa | hrozby a rizika v KB | práva a povinnosti v KB | opatření v KB | pojmy v KB | rozvoj / inovace | důslednost | logičnost | názornost | motivace | srozumitelnost | | |
| | Index30 | Index29 | Index28 | Index27 | Index26 | Index25 | Index24 | Index23 | Index22 | Index21 | Index20 | Index19 | Index18 | Index17 | Index16 | Index15 | Index14 | Index13 | Index12 | Index11 | Index10 | Index09 | Index08 | Index07 | Index06 | Index05 | Index04 | Index03 | Index02 | Index01 | | | |
| 11 | 1 | | | | | 1 | | | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K01 | Acresia Consulting | školení, vzdělávání zaměstnanců (veřejný, státní, komerční sektor) |
| 18 | 1 | 1 | | 1 | 1 | 1 | | 1 | | | | 1 | | 1 | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K02 | ALEF training center | |
| 18 | 1 | | | 1 | 1 | 1 | | | | | 1 | | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K03 | ASIST Intelligence Solutions | |
| 16 | 1 | | | 1 | 1 | 1 | | | | | | | | 1 | | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K04 | BOZP.cz | |
| 14 | 1 | | | | 1 | 1 | | | | | 1 | | | 1 | 1 | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K05 | ComPLus CZ | |
| 10 | 1 | | | | 1 | | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K06 | Centrum kybernetické bezpečnosti | |
| 20 | 1 | | | 1 | 1 | 1 | | | | 1 | 1 | | | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K07 | CyberSec | |
| 14 | 1 | | | 1 | 1 | 1 | | | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K08 | Cyber Security Comliance | |
| 21 | 1 | | 1 | 1 | 1 | 1 | | | | | 1 | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | K09 | Czechitas | |
| 13 | 1 | | | | 1 | 1 | | | | | | | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K10 | Data SYS | |
| 12 | 1 | | | | 1 | 1 | | | | | | | | | 1 | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K11 | DOXO LOGIC | |
| 11 | 1 | | | | 1 | 1 | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K12 | Edject Courses | |
| 14 | 1 | | 1 | 1 | 1 | 1 | | | | | | | | | | | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K13 | eÚředník | |
| 14 | 1 | 1 | | | 1 | 1 | | | | | | | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K14 | GOPAS | |
| 16 | 1 | | | 1 | 1 | 1 | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K15 | Gordic Cyber Security | |
| 14 | | 1 | | | | | | 1 | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | | 1 | K16 | HIK Vision | |
| 18 | 1 | | 1 | 1 | 1 | 1 | | | | | | | 1 | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K17 | Chráním data | |
| 19 | 1 | | | 1 | 1 | 1 | | | | | 1 | | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K18 | Integra | |
| 11 | 1 | | | | 1 | 1 | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K19 | Instructor by Prevent | |
| 20 | | 1 | | 1 | 1 | 1 | | | | | 1 | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | K20 | Itnetwork | |
| 14 | 1 | | | 1 | 1 | 1 | | | | | | 1 | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K21 | KEY Trainings | |
| 13 | 1 | | | 1 | 1 | 1 | | | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K22 | Knowspread | |
| 13 | 1 | | | | | 1 | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K23 | Kyber školení | |
| 15 | 1 | | | | 1 | | | | | | 1 | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K24 | MyCom Solution | |
| 18 | 1 | 1 | | 1 | 1 | 1 | | | | | 1 | | | | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K25 | NGSS Next Generation Security Solution | |
| 10 | 1 | | | | 1 | | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K26 | Novicom Academy | |
| 23 | | 1 | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 | K27 | NÚKIB e-learning | |
| 13 | 1 | | | | 1 | 1 | | | | | | | | | 1 | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | 1 | 1 | K28 | Pavel Lorenc | |
| 11 | 1 | | | | 1 | 1 | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K29 | ReNTEL | |
| 14 | 1 | | | 1 | 1 | 1 | | | | | | | | | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | | 1 | K30 | Scenario Informační technologie | |
| 11 | 1 | | | | 1 | 1 | | | | | | | | | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K31 | SOVA STUDIO | |
| 13 | 1 | | | 1 | 1 | 1 | | | | | | | | 1 | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K32 | Školení BOZP | |
| 14 | 1 | | | | 1 | | | | | | 1 | | | 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K33 | Total Service | |
| 12 | 1 | | | | 1 | | | | | | | | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | 1 | | 1 | K34 | Trigama.EU | |
| 15 | 1 | | | | | | | 1 | | | 1 | 1 | | 1 | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | 1 | 1 | 1 | | 1 | K35 | T-soft | |
| 18 | 1 | | | 1 | 1 | 1 | | 1 | 1 | | | 1 | | 1 | | | | 1 | | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K36 | Clashing / Online hra | Online kurzy, rady a tipy |
| 22 | | 1 | | 1 | 1 | 1 | | | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | 1 | 1 | 1 | 1 | K37 | Buď safe online | |
| 16 | | 1 | | 1 | 1 | 1 | | | | 1 | | | | 1 | | 1 | | 1 | | 1 | 1 | | | 1 | | 1 | 1 | 1 | 1 | 1 | K38 | NePinDej / ČBA | |
| 16 | | 1 | | | | 1 | | | | 1 | 1 | | 1 | 1 | 1 | 1 | | | | 1 | | 1 | 1 | | 1 | 1 | 1 | | 1 | K39 | Učíme online – KB ve vzdělávání | |
| Σ | 33 | 9 | 3 | 20 | 34 | 32 | 0 | 5 | 2 | 5 | 13 | 5 | 3 | 21 | 13 | 23 | 8 | 38 | 12 | 39 | 38 | 38 | 38 | 38 | 1 | 7 | 19 | 39 | 10 | 39 | Σ za Index | | |



*Tabulka 3 – Hodnocení vzdělávacích institucí v České republice (Autor, 2024).*

Vyhledávání jednotlivých společností na českém trhu nabízejících osvětu kybernetické bezpečnosti proběhlo na základě zadání klíčových slov (*Kybernetická bezpečnost vzdělávání veřejnosti, Kybernetická bezpečnost – online kurz, Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti, Školení kybernetické bezpečnosti, Cybersecurity online courses, Hry kybernetická bezpečnost, Kybernetická bezpečnost simulátory, Kybernetická bezpečnost pomůcky*) do vyhledávacího nástroje Googlu. Došlo k identifikaci 35 z nich nabízejících školení a vzdělávání zaměstnanců a 4 dostupných kurzů s tipy a radami.

Pokud zvážíme, že ČR má 10,5 milionů obyvatel, z čehož v produktivním věku (15-64 let), a tedy mezi „dospělými", se nachází přibližně 6,82 milionu z nich (63,8 % české populace) (ČSÚ [nedat.]), lze konstatovat, že nabídka 39 možností[3], z toho většina není volně dostupných pro veřejnost, nemusí být dostatečným počtem pro pokrytí a zajištění vzdělávání kybernetické bezpečnosti pro dospělé v ČR i s ohledem na fakt, že velké množství z nich se specializuje na firmy, nikoli na veřejnost jako takovou.

Komparativní analýza naplnění 30-ti parametrů[4] (*srozumitelnost, motivace, názornost, logičnost, důslednost, rozvoj a inovace* dle Bruce Schneiera; *postoje, dovednosti a znalosti* dle Kybernetického indexu gramotnosti; *kreativní myšlení, sebe-reflexe, komunikaci, spolupráci, sociální odpovědnost* dle Rámce cambridgeských životních kompetencí; jednotlivých společností *dostupnost, uživatelsky přívětivé, doba licence, bonus, zdarma, cena* dle kategorie uživatelské motivace) jednotlivých organizací přinesla výsledky, z nichž vyplývá, že nejvíce indikátorů (23 ze 30) nabízených školení naplňují *online školení Národního úřadu pro kybernetickou a informační bezpečnost* (dostupná na https://osveta.nukib.cz/local/dashboard/). Následuje neziskový projekt společnosti Avast a influencera Jiřího Krále *Buď safe online* (22 ze 30 parametrů, dostupný na https://www.avast.com/cz/besafeonline/), kurzy neziskové organizace

[3] V průměru by tak na každou připadalo vzdělávání cca 175 000 osob.
[4] Přítomnost jednotlivých parametrů v rámci jednotlivých společností či projektů je značí číslo 1 v tabulce 3.

*Czechitas* (21 ze 30 parametrů), online školení a kurzy společností *CyberSec* a *ITNework* (oboje s hodnotami 20 ze 30 parametrů).

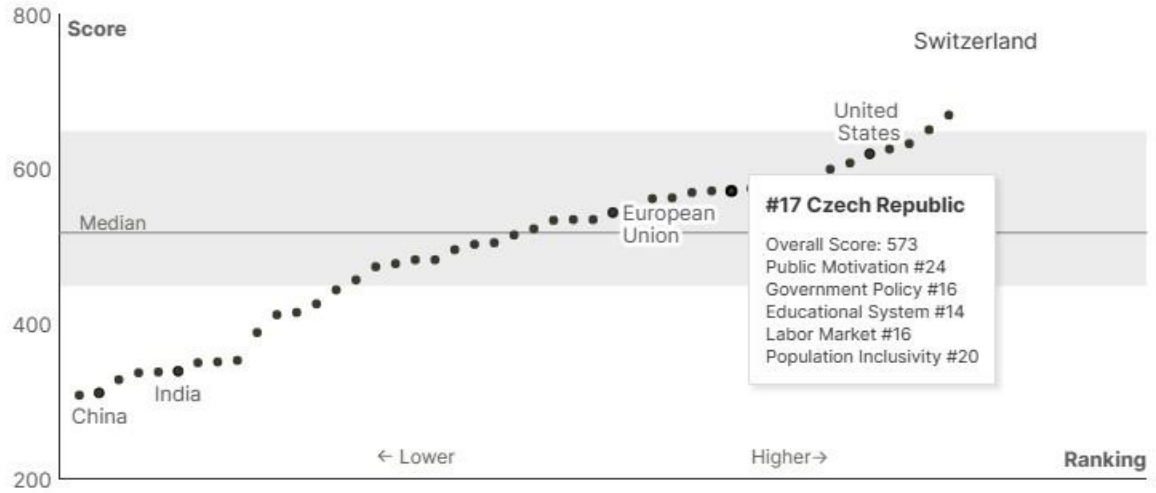
Průměrně pak nabízené varianty vzdělávání jednotlivých společností obsahují cca 18 ze 30 parametrů (průměrná hodnota činí 17,9), tudíž o trochu více, než je polovina, což dokazuje prostor pro zlepšení náplně daných způsobů osvěty.

Žádná z nalezených společností (0) nabízejících vzdělávání a osvětu v kybernetické bezpečnosti na českém trhu nezohledňuje parametr *komunikace, sociální odpovědnosti* a *rozvoje/inovace*. Indikátor *důslednosti* pak zahrnují pouze kurzy společnosti Czechitas (1). Poměrně málo organizací také bere v potaz vliv *zájmu o vzdělávání* (3), *bonusů* (3), *spolupráce* (5), *sebe-reflexe* (5), *důslednosti* (7), *zálohy a obnovení dat* (8) a možnosti nabídky *zdarma* (9). Zde lze identifikovat řadu parametrů, na kterých se dá pracovat a nabízené alternativy vzdělávání zlepšit.

Naopak všechny nabízené vzdělávací a osvětové možnosti jsou *srozumitelné, názorné* a dbající na *silná hesla* (39). 38 ze 39 variant se také zabývá *pojmy, opatřeními, právy a povinnostmi,* stejně jako *hrozbami a riziky* a jejich *rozpoznatelností* v kybernetické bezpečnosti. Jedná se tedy o silné stránky nabízených alternativ.

Jak z představené analýzy vyplývá, v ČR je rozhodně na čem pracovat. Na druhou stranu dle globálního indexu kybernetické gramotnosti a vzdělávání Oliver Wyman Forum (OWF, 2021), který hodnotí v dané oblasti 50 zemí a Evropskou unii na základě pěti hlavních faktorů: *vládní politika a plánování, školní kurikulum a vzdělávání učitelů, univerzitní kurikulum a výzkum, celoživotní učení a společenské povědomí*, má ČR poměrně dobrou úroveň kybernetické gramotnosti a vzdělávání ve srovnání s ostatními zeměmi, což ji řadí mezi středně vyspělé státy v dané oblasti (viz Obrázek 4). V indexu se umístila na 18. a ve stanovených indikátorech nabyla mírně nadprůměrných hodnot. Mezi pěti hlavními faktory OWF indexu dosáhla Česká

republika nejvyššího skóre v oblasti vládní politiky a plánování a nejnižšího skóre v oblasti celoživotního učení.




*Obrázek 4: Index gramotnosti a vzdělávání v oblasti kybernetických rizik OWF (OliverWymanForum, 2021).*

Parametry v této diplomové práci se v některých aspektech překrývají s indexem OWF. Například

- Vzdělávání podle Schneierova přístupu ke KB se částečně překrývá s faktorem školního kurikula a vzdělávání učitelů OWF indexu, který hodnotí kvalitu a dostupnost kybernetického vzdělávání na primárních a sekundárních školách.
- Kybernetický index gramotnosti se pak překrývá s faktorem společenského povědomí OWF indexu, který hodnotí, do jaké míry je veřejnost informována a motivována k zajišťování kybernetické bezpečnosti.
- Rámec cambridgeských životních kompetencí se shoduje s faktorem univerzitního kurikula a výzkumu OWF indexu, který hodnotí kvalitu a dostupnost kybernetického vzdělávání a výzkumu na vysokých školách.
- Uživatelská motivace se částečně překrývá s faktorem celoživotního učení OWF indexu, který hodnotí dostupnost a kvalitu neformálního a profesionálního kybernetického vzdělávání pro dospělé.

Představené parametry v této diplomové práci jsou ale specifičtější a detailnější než faktory OWF indexu, a tak poskytují hlubší analýzu silných a slabých stránek českého kybernetického vzdělávání. Z té vyplývá, že přestože se řadíme mezi top 20 zemí EU v dané oblasti, stále existují mezery, na nichž je třeba v ČR pracovat, ať už se jedná o počet a dostupnost alternativ osvěty v kybernetické bezpečnosti, či jejich obsahu a náplně jednotlivých parametrů.

Dochází tak k potvrzení stanovené hypotézy diplomové práce, která zní: *Aktuální možnosti vzdělávání veřejnosti v oblasti kybernetické bezpečnosti v České republice neodpovídají žádoucímu stavu*

# ARGUMENTACE A DOPORUČENÍ

Dle výsledků představené analýzy je třeba zapracovat na dostupnosti a počtu nabízených alternativ vzdělávání v kybernetické bezpečnosti pro veřejnost a dospělé na českém trhu. Již existující formy by pak měly zvážit začlenění a zohlednění netechnologických parametrů, tedy *komunikace, sociální odpovědnosti* a *rozvoje/inovace*, *důslednosti*, *zájmu o vzdělávání*, *bonusů*, *spolupráce*, *sebe-reflexe*, *důslednosti*, tématu *záloh a obnovení dat* a možnost *přívětivější cenové nabídky*.

Kybernetická bezpečnost je stále důležitějším tématem především v souvislosti s rychlým rozvojem nových technologií, zejména pak umělé inteligence, která absolutně mění „pravidla hry". Přináší mnoho přínosů pro společnost i jednotlivce, ale také z ní vyvstávají nové hrozby a výzvy nejen pro kybernetickou bezpečnost. I s ohledem na tento fakt lze současnou úroveň vzdělávání a osvěty v kybernetické bezpečnosti v kontextu nových technologií, umělé inteligence a progresivního technologického rozvoje považovat za nedostatečnou, nereflexivní a nedynamickou. A to je třeba urychleně změnit.

S ohledem na daný argument i výstupy této práce, lze identifikovat řadu aspektů, na který je nutno v oblasti vzdělávání kybernetické bezpečnosti zapracovat:

- Vzdělávání a osvěta kybernetické bezpečnosti by měly zahrnovat sociální stránku věci. Umělá inteligence ovlivňuje společnost jako celek, stejně jako jednotlivce. Může mít dopad na sociální interakce, komunikaci, kulturu, politiku, ekonomiku nebo právo. Tyto dopady vyžadují sociální povědomí a angažovanost, které nelze naučit pouze technickými dovednostmi. Proto by vzdělávání a osvěta kybernetické bezpečnosti měly zahrnovat sociální vzdělávání a participaci na společenských otázkách souvisejících s umělou inteligencí a kybernetickou bezpečností.
- Vzdělávání a osvěta v kybernetické bezpečnosti by měly pokrývat nejen technickou, ale také etickou stránku věci. Umělá inteligence přináší nové

dilematy a výzvy, které se týkají například ochrany soukromí, transparentnosti, odpovědnosti, spravedlnosti nebo důvěry. Tyto otázky vyžadují kritické myšlení a morální uvážení, které nelze naučit pouze technickými dovednostmi. Proto by vzdělávání a osvěta kybernetické bezpečnosti měly zahrnovat etickou výchovu a diskusi o hodnotách a normách, které by měly řídit používání umělé inteligence a kybernetické bezpečnosti.

- Vzdělávání a osvěta kybernetické bezpečnosti by měly být pokrývat také ekologické aspekty věci. Umělá inteligence má dopad na životní prostředí, neboť spotřebovává velké množství energie a zdrojů, produkuje odpad a emise. Tyto dopady vyžadují ekologickou zodpovědnost a udržitelnost, které nelze naučit pouze technickými dovednostmi. Proto by vzdělávání a osvěta kybernetické bezpečnosti měly zahrnovat ekologické vzdělávání a podporu zelených řešení pro umělou inteligenci a kybernetickou bezpečnost.

Z těchto argumentů vyplývá, že současné vnímání vzdělávání a osvěty kybernetické bezpečnosti je příliš úzké, zaměřené primárně na technickou stránku. To je nedostatečné pro to, aby lidé byli schopni se vyrovnat s komplexností a důsledky technologického vývoje, především v souvislosti s umělou inteligencí, a byli schopní efektivně přijímat kroky pro zajištění kybernetické bezpečnosti na úrovni jednotlivce i společnosti. Potřebujeme změnit toto vnímání a rozšířit vzdělávání a osvětu kybernetické bezpečnosti o etický, sociální a ekologický rozměr. Tím dojde k lepšímu pochopení a ochraně kybernetické bezpečnosti v kontextu nových technologií umělé inteligence a progresivního technologického rozvoje.

Kybernetická bezpečnost představuje zcela zásadní obor přítomnosti i budoucnosti. S ohledem na rostoucí závislost lidstva na technologiích se na ní musí pracovat s komplexním a multioborovým přesahem. Dotýká se technických, sociálních, ekonomických, právních i politických aspektů společnosti. Digitální technologie a internet ovlivňují mezilidské vztahy, komunikaci, ekonomiku, kulturu, ale také identitu, postoje a hodnoty ve společnosti sdílené. Je proto zcela stěžejní

kybernetickou bezpečnost vnímat jako celek a jako nutnost pro efektivní fungování současného systému. Proto by také měla být zařazena do vzdělávacích programů na všech úrovních. Základ pro dosažení tohoto cíle představuje začleňování témat kybernetické bezpečnosti do výuky různých předmětů a oborů, jako například informatiky, mediální výchovy, občanské výchovy, dějepisu, zeměpisu, ekonomie nebo politologie.

Je potřeba také podporovat spolupráci mezi různými disciplínami, sektory a zúčastněnými stranami, státní správy, samosprávy, nadnárodních a národních subjektů, ale i institucí a spolků kteří se věnují vzdělávaní a osvětě, aby se vytvořila společná vize a strategie pro kybernetickou bezpečnost a roli umělé inteligence v ní. Pro podpoření daného argumentu by mělo dojít k:

- Vytvoření multidisciplinárních kurzů a workshopů o etice, sociologii a ekologii kybernetické bezpečnosti a umělé inteligence pro studenty, učitele, pracovníky i veřejnost.
- Vytvoření platforem a sítí pro sdílení znalostí, zkušeností a osvědčených postupů v oblasti kybernetické bezpečnosti a umělé inteligence mezi různými aktéry na místní, národní i mezinárodní úrovni.
- Podpoření výzkumu a inovací v oblasti kybernetické bezpečnosti a umělé inteligence, které budou eticky, sociálně a ekologicky odpovědné a udržitelné.

V neposlední řadě je žádoucí, aby se změnil přístup pedagogů k dané problematice. Je třeba ji nejen zařadit do výuky napříč obory, ale musí být využívány různé zdroje a materiály, které poskytují kvalitní a aktuální informace, inspiraci a podporu pro výuku kybernetické bezpečnosti, například webové stránky, publikace, videa, kurzy nebo konference státních, ale i nestátních institucí. I z toho důvodu bude v následující kapitole představen návrh kurzu zaměřený právě na učitele a pedagogy v ČR.

Vzdělávací systém musí spolupracovat s různými partnery, kteří se zabývají kybernetickou bezpečností z různých úhlů pohledu, a tak mohou nabídnout odbornost, zkušenosti, služby nebo finance pro výuku kybernetické bezpečnosti mezi veřejností.

# NÁVRH VZDĚLÁVACÍHO PROGRAMU / ZÁKLADY KYBERNETICKÉ BEZPEČNOSTI PRO VEŘEJNOST

Vzdělávací program v kybernetické bezpečnosti je nutným programem současnosti. Kybernetická bezpečnost se týká ochrany informací, systémů a služeb před neoprávněným přístupem, zneužitím nebo poškozením. Její zajištění je tedy kruciální nejenom pro jednotlivce, ale i celou společnost. Klíčovou dovedností pro 21. století se tak stává digitální gramotnost. Tu je ovšem nutné předávat jak ve školách novým generacím, tak již dospělým jedincům, kteří taktéž patří mezi aktivní uživatele, jež ovšem neměli přístup ke vzdělávání v dané oblasti z důvodu její neexistence a následnému poměrně rychlému vývoji.

Kybernetická bezpečnost je proces, nikoli produkt. Vzdělávací program v kybernetické bezpečnosti proto musí stát na pevných základech: *prevenci, detekci, reakci, stabilitě, uvědomění a učení*. Tyto kategorie lze použít jako kritéria pro vytváření a hodnocení vzdělávacích programů v kybernetické bezpečnosti.

Následující návrh kurzu zohledňuje parametrické vzdělávací hodnoty, které jsou užívány napříč touto prací:

1. *Vzdělávání podle Schneierova přístupu ke KB*: srozumitelnost, motivace, názornost, logičnost, důslednost, rozvoj a inovace.
2. *Kybernetický index gramotnosti*: postoje, dovednosti a znalosti.
3. *Rámec cambridgeských životních kompetencí*: kreativní myšlení, sebe-reflexe, komunikaci, spolupráci, sociální odpovědnost.
4. *Uživatelská motivace*: dostupnost, uživatelsky přívětivé, doba licence, bonus, zdarma, cena.

Jeho tvorba se pokouší vyplnit obsahovou mezeru na trhu vzdělávání veřejnost v oblasti kybernetické bezpečnosti v České republice. Na druhou stranu neřeší nedostatečné množstevní pokrytí dané záležitosti, kterému by teoreticky mohla napomoci podpora či výzva ze strany státu nebo zájem zainteresovaných aktérů.

**Název kurzu**: Základy kybernetické bezpečnosti pro veřejnost

**Cílová skupina**: Veřejnost, dospělí uživatelé kyberprostoru.

**Cíle kurzu**: Po absolvování tohoto kurzu budou účastníci schopni:

- Chápat a pracovat se základními pojmy a principy kybernetické bezpečnosti.
- Rozpoznat a předcházet běžným kybernetickým hrozbám a útokům.
- Používat technologie bezpečně a efektivně.
- Rozvíjet kritické a kreativní myšlení v oblasti kybernetické bezpečnosti.
- Vytvářet a hodnotit vzdělávací aktivity a materiály v kybernetické bezpečnosti.
- Podporovat pozitivní postoje a motivaci ke kybernetické bezpečnosti u sebe i u ostatních.

**Obsah kurzu**: Kurz se skládá z šesti modulů, které pokrývají různé aspekty kybernetické bezpečnosti. Každý modul obsahuje teoretickou, praktickou a reflexivní část. Teoretická část poskytuje úvod do daného tématu, praktická část umožňuje účastníkům aplikovat a procvičit své znalosti a dovednosti, a reflexivní část podporuje účastníky k zamyšlení nad svým učením a chováním. Kurz zároveň učí základy, jak případně znalosti efektivně a zajímavě předávat dál.

**Délka kurzu**: Časová dotace kurzu je celkem 30 hodin (6 hodin na každý modul). Lze jej absolvovat prezenčně nebo online.

**Cena kurzu**: Kurz je dostupný zdarma, s možným prezenčním odborným výkladem za 6 000,- (tedy přibližně 200 Kč/hodinu pro lektora).

Přehled jednotlivých modulů:

### Modul 1: Co je kybernetická bezpečnost?

Tento modul se zaměřuje na obecný rámec kybernetické bezpečnosti a právní odpovědnosti. Účastníci se seznámí s definicí, cíli, principy a složkami kybernetické bezpečnosti, s hlavními subjekty a zdroji kybernetických hrozeb a útoků, s mezinárodními i národními normami a zákony v oblasti kybernetické bezpečnosti.

### Modul 2: Jak používat technologie bezpečně?

Tento modul se zaměřuje na technické aspekty kybernetické bezpečnosti. Účastníci se naučí, jak chránit svá zařízení, data a komunikaci před neoprávněným přístupem, zneužitím nebo poškozením. Seznámí se s některými běžnými typy kybernetických útoků, jako jsou phishing, malware, ransomware, denial-of-service, man-in-the-middle, brute force, SQL injection a další. Účastníci si také vyzkouší některé nástroje a aplikace pro zvýšení své kybernetické bezpečnosti, jako jsou antivirové programy, firewall, VPN, šifrování, autentizace, digitální podpis a další.

### Modul 3: Jak myslet kriticky a kreativně o kybernetické bezpečnosti?

Tento modul se zaměřuje na rozvoj kritického a kreativního myšlení v oblasti kybernetické bezpečnosti. Účastníci se naučí, jak analyzovat, hodnotit a řešit různé problémy a situace související s kybernetickou bezpečností, jak generovat nové a originální nápady a řešení v oblasti kybernetické bezpečnosti, a jak prezentovat a argumentovat své názory a návrhy v oblasti kybernetické bezpečnosti. Vyzkouší si také některé metody a techniky pro podporu kritického a kreativního myšlení, jako jsou brainstorming, mind mapping, SWOT analýza, PESTEL analýza, SCAMPER metoda, šest klobouků myšlení a další.

### Modul 4: Jak vytvářet a hodnotit vzdělávací aktivity a materiály v kybernetické bezpečnosti?

Tento modul se zaměřuje na vytváření a hodnocení vzdělávacích aktivit a materiálů v kybernetické bezpečnosti pro různé věkové skupiny. Účastníci se naučí, jak stanovit cíle, obsah, metody, prostředky a kritéria pro vzdělávací aktivity a materiály v kybernetické bezpečnosti, jak začlenit téma kybernetické bezpečnosti do oblastí učení, jak zvolit vhodné formy a nástroje pro prezentaci a interakci s případnými studenty. Vyzkouší si také některé příklady vzdělávacích aktivit a materiálů v kybernetické bezpečnosti, jako jsou kvízy, hry, simulace, scénáře, případové studie, projekty a další. Tento modul je klíčový v případě zájmu dále

poznatky o základech kybernetické bezpečnosti dále šířit zajímavou a zábavnou formou. Naskytuje se jim tak příležitost vzdělávat například ostatní dospělé, děti či seniory pohybující se v jejich okolí.

### Modul 5: Jak podporovat motivaci ke kybernetické bezpečnosti?

Tento modul se zaměřuje na podporu pozitivních postojů a motivace ke kybernetické bezpečnosti u sebe i u ostatních. Účastníci se naučí, jak rozvíjet uvědomění si důležitosti kybernetické bezpečnosti pro osobní i profesní život, jak rozvíjet etiku a sociální odpovědnost v kyberprostoru, jak rozvíjet emoční odolnost proti stresu, neúspěchu a změně souvisejícím s kybernetickou bezpečností, a jak rozvíjet zájem a radost z učení se o kybernetické bezpečnosti. Vyzkouší si také některé strategie a techniky pro podporu pozitivních postojů a motivace v kybernetické bezpečnosti, jako jsou nastavování cílů, zpětná vazba, odměny, uznání, povzbuzování, inspirace a další.

### Modul 6: Jak rozvíjet životní kompetence?

Tento modul se zaměřuje na Rámec cambridgeských životních kompetencí. Účastníci se naučí, jak rozvíjet kreativní a kritické myšlení, jak získávat zpětnou vazbu a pracovat s ní. Dále budou představeny základy komunikace a spolupráce v návaznosti na sociální odpovědnost.

# ZÁVĚR

Kybernetická bezpečnost je téma, které by mělo zajímat každého jedince. Dotýká se totiž veškerých aspektů lidských životů. Aby se občané ČR byli schopni v digitálním prostředí bezpečně a eticky orientovat, potřebují proto mít nejen základní technické znalosti a dovednosti, ale také znát širší kontext, ve kterém se kybernetická bezpečnost odehrává. Toto vnímání je důležité pro rozhodování a bezpečné jednání v digitálním prostředí. Vzdělávání v dané oblasti tak představuje stěžejní oblast pro zajištění stávajícího řádu věcí a bezpečnosti české populace.

Cílem této diplomové práce bylo analyzovat možnosti vzdělávání veřejnosti v kybernetické bezpečnosti v České republice a navrhnout případný alternativní vzdělávací program v této oblasti. Výzkum byl řízen za užití hypotézy, že *Aktuální možnosti vzdělávání veřejnosti v oblasti kybernetické bezpečnosti v České republice neodpovídají žádoucímu stavu*. Ten byl definován jako odpovídající *množstevní pokrytí* demografického počtu dospělých vzdělávacími možnostmi v daném oboru, a zároveň *obsahovým zaměřením* kurzů, které by měly obsahovat technické i netechnické aspekty vzdělávání kybernetické bezpečnosti.

Za užití části výzkumu klíčových slov vybraných na základě individuálního brainstormingu (*Kybernetická bezpečnost vzdělávání veřejnosti, Kybernetická bezpečnost – online kurz, Vzdělávání veřejnosti v oblasti kybernetické bezpečnosti, Školení kybernetické bezpečnosti, Cybersecurity online courses, Hry kybernetická bezpečnost, kybernetická bezpečnost simulátory, kybernetická bezpečnost pomůcky*) došlo k identifikaci 39 dostupných vzdělávacích alternativ zaměřených na kybernetickou bezpečnost pro dospělé na českém trhu. Na základě jejich popisu bylo zjištěno, že většina z nich primárně nabízí školení a kurzy pro firmy a zaměstnavatele, nikoli pro veřejnost, přestože i takové možnosti lze najít (např. online kurzy Národního úřadu pro kybernetickou a informační bezpečnost). S ohledem na jejich počet a obsahovou nabídku byla potvrzená hypotéza, z které vyplývá, že by pro český trh bylo s ohledem

na demografickou situaci české populace žádoucí jejich počet, rozsah, dostupnost a působnost rozšířit.

Obsahová nabídka identifikovaných společností byla porovnána dle stanovených parametrů vystávajících z přístupů Mgr. Bruce Schneiera, Ph.D. (*srozumitelnost, motivace, názornost, logičnost, důslednost, rozvoj a inovace*), Kybernetického indexu gramotnosti (*postoje, dovednosti a znalosti*), Rámce cambridgeských životních kompetencí (*kreativní myšlení, sebe-reflexe, komunikaci, spolupráci, sociální odpovědnost*) a autorem nastavených hodnot neboli uživatelské motivace (*dostupnost, uživatelsky přívětivé, doba licence, bonus, zdarma, cena*). Představené parametry reprezentovaly indikátory, které by měly být součástí „ideální" vzdělávací a osvětové aktivity. S nejsilnějším zastoupením vyvstaly parametry *srozumitelnosti, názornosti* a obsah vzdělávacích alternativy u většiny případů představoval problematiku *silných hesel*, *hrozeb a rizik, pojmů, opatření, práva a povinností.* Nejslabším prvkem pak byly indikátory *komunikace, sociální odpovědnosti* a přístup *rozvoje/inovace, důslednosti.* Výsledky potvrdily stanovenou hypotézu a vyzdvihly potřebu zajistit technické, ale i netechnické obsahové zaměření jednotlivých vzdělávacích možností.

Analýza možností vzdělávání veřejnosti v kybernetické bezpečnosti v ČR potvrdila, že přestože se dle mezinárodních indexů tento stát řadí mezi top 20 zemí EU, stále existují obsahové mezery a nedostatečná početní dostupnost alternativ pro pokrytí vzdělávání dospělé populace, na čemž. Na základě výsledků, stanovených parametrů a následné argumentace navrhl autor diplomové práce tvorbu a zavedení 6-ti modulového kurzu *Základů kybernetické bezpečnosti pro veřejnost*, jehož cílovou skupinou má být veřejnost, jakožto stěžejní skupina uživatelů, která potřebuje zajistit vlastní kybernetickou bezpečnost. V rámci navržené osvětové aktivity má dojít k představení nejrůznějších aspektů problematiky na teoretické i praktické bázi.

Diplomová práce ukázala, proč je třeba v kontextu progresivního technologického vývoje změnit vnímání vzdělávání kybernetické bezpečnosti, kdy je třeba zajistit jeho multioborový, technický, etický, sociální, ekologický i další přesah.

# Seznam grafů



# Seznam tabulek

# ZDROJE


ACRESIA. [nedat.]a. „O nás.“ *Acresia.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.acresia.com/index.php/o-nas.

ACRESIA. [nedat.]b. „ELEARNING, WEBINÁŘE A ŠKOLENÍ.“ *Acresia.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.acresia.com/index.php/20-sluzby/106-elearning-webinare-a-skoleni.

AEC. [nedat.]. „Advanced Persistent Threat (APT).“ *AEC.* [online]. [cit. 5.10.2023]. Dostupné z: AEC-Advanced-Persistent-Thread.pdf.

AIRA. [nedat.]. „Co je sniffing.“ *aira.* [online]. [cit. 7.10.2023]. Dostupné z: Co je sniffing? - Správa.sítě.eu (sprava-site.eu).

ALEF. [nedat.]a. „O nás.“ *ALEF Training Center.* [online]. [cit. 14.2.2023]. Dostupné z: https://training.alef.com/cz/o-nas.

ALEF. [nedat.]b. „Our knowledge is your future.“ *ALEF Training Center.* [online]. [cit. 14.2.2023]. Dostupné z: https://training.alef.com/cz/katalog/skoleni.

ALEF. [nedat.]c. „Základy kybernetické bezpečnosti.“ *ALEF Training Center.* [online]. [cit. 14.2.2023]. Dostupné z: https://training.alef.com/cz/zaklady-kyberneticke-bezpecnosti.p2419.html.

ALEF. [nedat.]d. „Kybernetický útok a obrana v praxi.“ *ALEF Training Center.* [online]. [cit. 13.2.2023]. Dostupné z: https://training.alef.com/cz/kyberneticky-utok-a-obrana-v-praxi.p10272.html?variant_id=46621.

ALEF. [nedat.]e. „O nás.“ *ALEF Training Center.* [online]. [cit. 14.2.2023]. Dostupné z: https://training.alef.com/cz/o-nas.

ARMSTRONG, M. *Řízení lidských zdrojů – nejnovější trendy a postupy*, přel. J. Koubek. Praha: GRADA PUBLISHING, 2007. 789 s. ISBN 978-80-247-1407-3.

ASSIST. [nedat.]a. „O nás.“ *ASSIST Intelligence Solutions.* [online]. [cit. 20.2.2023]. Dostupné z: https://www.assist.cz/about.php?lang=cs.

ASSIST. [nedat.]b. „Reference.“ *ASSIST Intelligence Solutions.* [online]. [cit. 20.2.2023]. Dostupné z: https://www.assist.cz/ref.php?lang=cs.

ASSIST. [nedat.]c „Detail školení „Kybernetická bezpečnost pro uživatele.“ *ASSIST Intelligence Solutions.* [online]. [cit. 20.2.2023]. Dostupné z: https://www.assist.cz/edu-ibm.php?lang=cs&id=84.

AVAST. [nedat.]. „Hacker.“ *Avast.* [online]. [cit. 7.10.2023]. Dostupné z: Hacker - kdo to je a jak před ním ochránit vaše PC | Avast.

BARTÁK, Jan. *Jak vzdělávat dospělé*. 1. vyd. Praha: Alfa Nakladatelství, s. r. o., 2008. 200 s. ISBN 978-80-87197-12-7.

Bastl, Martin – Gruberová, Zuzana. 2013. „Kyberprostor jako ‚pátá doména‘?“ *Vojenské rozhledy.* Roč. 22 (54), č. 4, 10-21.

BEDNAŘÍKOVÁ, Iveta. *Kapitoly z andragogiky 2*. Olomouc: Univerzita Palackého v Olomouci, 2006. ISBN 80-244-1193-8.Bruce Schneier. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. Kindle Edition, 2019, ISBN: 978-0393357448.

BENEŠ, M. *Andragogika*. Praha: Eurolex Bohemia, 2003, 216 s. ISBN - 8086432238.

BEPOR.eu. [nedat.]a. „Zpracování a vedení dokumentace BOZP a PO.“ *Bepor.eu.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.bepor.eu/zpracovani-a-vedeni-dokumentace-bozp-a-po.

BEPOR.eu. [nedat.]b. „Školení informační a kybernetické bezpečnosti.“ *Bepor.eu.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.bepor.eu/skoleni-informacni-a-kyberneticke-bezpecnosti.

BIČÍKOVÁ, Zuzana. 2022. „Acronis: Pět nejčastějších technik sociálního inženýrství.“ *ChannelWorld.* 25.7.2022. [online]. [cit. 7.10.2023]. Dostupné z: Acronis: Pět nejčastějších technik sociálního inženýrství - ChannelWorld.

BOZP.cz. [nedat.]a. „BOZP-SYSTEM.cz - komplexní školicí systém. Jak funguje?“ *BOZP.cz.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.skolenibozp.cz/skolici-system/.

BOZP.cz. [nedat.]b. „Ceník.“ *BOZP.cz.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.skolenibozp.cz/cenik/.

BOZP.cz. [nedat.]c. „Školení informační a kybernetické bezpečnosti.“ *BOZP.cz.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.skolenibozp.cz/skoleni-kyberbezpecnosti.

BOZP.cz. [nedat.]d. „Školení BOZP.cz.“ *BOZP.cz.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.skolenibozp.cz/.

BUĎ SAFE ONLINE. [nedat.]. „Online kurz.“ *Avast.com.* [online]. [cit. 24.2.2023]. Dostupné z: https://www.avast.com/cz/besafeonline/online-kurz.

CAMBRIDGE UNIVERSITY, *Cambridge Assessment English a Cambridge University Press, který vedl k vytvoření Cambridge Life Competencies Framework* [online]. [cit. 7.10.2023]. Dostupné z: https://www.cambridge.org/elt/blog/2022/04/07/understanding-developing-digital-literacy/.

CCDCOE. [nedat.]. „Our mission & vision.“ *CCDCOE.* [online]. [cit. 7.10.2023]. Dostupné z: About us (ccdcoe.org).

CENTRUM KYBERNETICKÉ BEZPEČNOSTI. [nedat.]. „KYBERCENTRUM – Centrum kybernetické bezpečnosti.“ *Kybercentrum.cz.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.kybercentrum.cz/.

CERT-EU. [nedat.]. „About Us.“ *CERT-EU.* [online]. [cit. 25.10.2023]. Dostupné z: CERT-EU - About us (europa.eu).

CIESLAV, Jan. 2021. „Karel Řehka: Bezpečnost je třeba řešit od základů.“ *Statisitka & my: Magazín Českého statistického úřadu.* Rozhovor s K. Řehkou. 3.9.2021. [online]. [cit.

25.10.2023]. Dostupné z: Karel Řehka: Bezpečnost je třeba řešit od základů | Statistika&My (statistikaamy.cz).

CLASHING. [nedat.]. „Cyber Security Awareness Training.“ *Clashing.com.* [online]. [cit. 23.2.2023]. Dostupné z: https://www.clashing.com/.

COMPLUS. [nedat.]a. „O společnosti COM PLUS CZ a.s.“ *COMPLUS Security.* [online]. [cit. 11.2.2023]. Dostupné z: https://bezpecneict.cz/o-nas.

COMPLUS. [nedat.]b. „Kurzy a školení.“ *COMPLUS Security.* [online]. [cit. 11.2.2023]. Dostupné z: https://bezpecneict.cz/sluzby/kurzy-a-skoleni.

CYBERSEC. [nedat.]a. „Chraňte svá data proti hackerům!“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/.

CYBERSEC. [nedat.]b. „Ceník licencí.“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/cena/.

CYBERSEC. [nedat.]c. „O nás.“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/garanti/.

CYBERSEC. [nedat.]d. „Chraňte svá data proti hackerům!“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/.

CYBERSEC. [nedat.]e. „Ceník licencí.“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/cena/.

CYBERSEC. [nedat.]f. „Obsah e-learningu.“ *CyberSec.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.cybersec.cz/obsah-skoleni/.

CYBER SECURITY COMPLIANCE. [nedat.]. „Braňte se kybernetickým hrozbám. Systematicky a účinně.“ *Cyber Security Compliance.* [online]. [cit. 21.2.2023]. Dostupné z: https://www.cybersecuritycompliance.cz/.

CYBER SECURITY COMPLIANCE. [nedat.]b. „Školení kybernetické bezpečnosti.“ *Cyber Security Compliance.* [online]. [cit. 24.2.2023]. Dostupné z: https://www.cybersecuritycompliance.cz/skoleni-kyberneticke-bezpecnosti/.

CSIRT.CZ. [nedat.]. „Národní CSIRT České republiky.“ *CSIRT.CZ.* [online]. [cit. 25.10.2023]. Dostupné z: Úvod - CSIRT.

CZECHITAS. [nedat]a. „Jsme největší IT komunitou v Česku. Přidej se.“ *Czechitas.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.czechitas.cz/o-czechitas.

CZECHITAS. [nedat]b. „IT je budoucnost. I tvoje.“ *Czechitas.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.czechitas.cz/.

CZECHITAS. [nedat]c. „Jsme největší IT komunitou v Česku. Přidej se.“ *Czechitas.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.czechitas.cz/o-czechitas.

CZECHITAS. [nedat]d. „Úvod do kybernetické bezpečnosti.“ *Czechitas.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.czechitas.cz/kurzy/uvod-do-kyberneticke-bezpecnosti.

ČESKO.DIGITAL, [nedat.]. „Skrz jedničky a nuly měníme Česko k lepšímu.“ *Česko Digital.* [online]. [cit. 16.2.2023]. Dostupné z: https://cesko.digital/.

ČSÚ. [nedat.]. „Aktuální populační vývoj v kostce.“ [online]. [cit. 6.11.2023]. Dostupné z: https://www.czso.cz/csu/czso/aktualni-populacni-vyvoj-v-kostce.

ČVUT. [nedat.]. „Základy kybernetické bezpečnosti (CZ).“ *Český institut informatiky, robotiky a kybernetiky.* [online]. [cit. 25.10.2023]. Dostupné z: 1_kyberneticka_bezpecnost-zaklady_hsoc.pdf (cesnet.cz).

DATA SYS. 2022. „10 nejčastějších typů kybernetických útoků.“ *DATA SYS*. 8.3.2022. [online]. [cit. 25.10.2023]. Dostupné z: 10 nejčastějších typů kybernetických útoků - DATASYS, s.r.o.

DATA SYS. [nedat.]a. „Inovativní a přesto tradiční.“ *DATA SYS.* [online]. [cit. 21.2.2023]. Dostupné z: https://www.datasys.cz/o-nas/.

DATA SYS. [nedat.]b. „IT pro státní správu a firemní klientelu.“ *DATA SYS.* [online]. [cit. 21.2.2023]. Dostupné z: https://www.datasys.cz/.

DATA SYS. [nedat.]c. „Tvoříme řadu silných partnerství.“ *DATA SYS.* [online]. [cit. 21.2.2023]. Dostupné z: https://www.datasys.cz/partneri/.

DATA SYS. [nedat.]d. „Dodáváme nástroje, řešení i služby.“ *DATA SYS.* [online]. [cit. 21.2.2023]. Dostupné z: https://www.datasys.cz/sluzby/bezpecnost/?gclid=CjwKCAjwzeqVBhAoEiwAOrEmzfOGsJaOhikXuCStAb00_5Y6jeu3NNLPaCp0_D9tpjgRQkDjd8HTTBoCPnQQAvD_BwE.

*Document EU 32018H0604(01), Council Recommendation of 22 May 2018 on key competences for lifelong learning, ST/9009/2018/INIT* [online]. [cit. 7.8.2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2018.189.01.0001.01.ENG&toc=OJ:C:2018:189:TOC.

DOXOLOGIC. [nedat.]a. „Staneme se Vaším partnerem v IT bezpečnosti.“ *DoxoLogic.* [online]. [cit. 17.2.2023]. Dostupné z: https://doxologic.cz/o-nas/.

DOXOLOGIC. [nedat.]b. „Je Vaše firma v bezpečí před kybernetickými útoky?“ *DoxoLogic.* [online]. [cit. 17.2.2023]. Dostupné z: https://doxologic.cz/.

DOXOLOGIC. [nedat.]c. „Chraňte se před hackery: kybernetická bezpečnost polopatě.“ *DoxoLogic.* [online]. [cit. 17.2.2023]. Dostupné z: https://doxologic.cz/kyberneticka-bezpecnost-polopate-early-birds/.

DOXOLOGIC. [nedat.]d. „Cyber Security kurzy a školení.“ *DoxoLogic.* [online]. [cit. 17.2.2023]. Dostupné z: https://doxologic.cz/kurzy-a-skoleni/.

EDJET COURSES. [nedat.]a. „O nás.“ *Edjet.* [online]. [cit. 24.2.2023]. Dostupné z: https://about.edjet.com/cs-cz/o-nas.

EDJET COURSES. [nedat.]b. „Přizpůsobitelné kurzy pro zaměstnance.“ *Edjet.* [online]. [cit. 22.2.2023]. Dostupné z: https://courses.edjet.com/cs-cz.

EDJET COURSES. [nedat.]c. „Kyberbezpečnost.“ *Edjet.* [online]. [cit. 22.2.2023]. Dostupné z: https://courses.edjet.com/cs-cz/online-kurzy/kurz-kyberbezpecnost.

EDJET COURSES. [nedat.]d. „Kurzy pro zaměstnance v cloudu.“ *Edjet.* [online]. [cit. 22.2.2023]. Dostupné z: https://courses.edjet.com/cs-cz/ceny-cloud.

EDUCITY. [nedat.]. „SOVA STUDIO – vaše vzdělávací společnost.“ *Educity.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.educity.cz/firmy/sova-studio-vase-vzdelavaci-spolecnost-id-22928.

E-ESTONIA. 2018. „NATO CCDCOE – Expertise and cooperation make our cyber space safer.“ *e-Estonia.* 16.10.2018. [online]. [cit. 25.10.2023]. Dostupné z: NATO CCDCOE - Expertise and cooperation make our cyber space safer - e-Estonia.

ESET. [nedat.]a. „Co je počítačový virus + druhy virů.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Co je počítačový virus + Druhy virů | ESET.

ESET. [nedat.]b. „Spyware.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Co je Spyware a jak ho spolehlivě odstranit? | ESET.

ESET. [nedat.]c. „Adware.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Co je Adware a jak ho spolehlivě odstranit? | ESET.

ESET. [nedat.]d. „Trojský kůň.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Trojský kůň: Jak odstranit tento vir nejen z mobilu? | ESET.

ESET. [nedat.]e. „Ransomware.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Co je to ransomware a jak se proti němu bránit? | ESET.

ESET. [nedat.]f. „Spam.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Co je to spam? Jak se zbavit spamu? | ESET.

ESET. [nedat.]g. „Vishing: co je to a jak se bránit?“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Vishing: Co je to a jak se bránit? | ESET.

ESET. [nedat.]h. „Botnet.“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Botnet | ESET Glossary | ESET Online nápověda.

ESET. [nedat.]ch. „Phishing.“ *ESET.* [online]. [cit. 5.10.2023]. Dostupné z: Co je phishing? | ESET.¨

ESET. [nedat.]i. „Co je nelegální těžba kryptoměn a jak může ovlivnit vaši firmu?“ *ESET.* [online]. [cit. 25.10.2023]. Dostupné z: Nelegální těžba kryptoměn (cryptojacking a cryptomining) | ESET.

ESET. [nedat.]j. „O nás.“ *ESET.* [online]. [cit. 12.2.2023]. Dostupné z: https://www.eset.com/cz/o-nas/.

ESET. [nedat.]k. „Partneři.“ *ESET.* [online]. [cit. 12.2.2023]. Dostupné z: https://www.eset.com/cz/prodejci/.

ESET. [nedat.]l. „Online školení kybernetické bezpečnosti.“ *ESET.* [online]. [cit. 12.2.2023]. Dostupné z: https://www.eset.com/cz/skoleni-kyberneticke-bezpecnosti-online/#nabidka-skoleni.

EÚŘEDNÍK. [nedat.]a. „Naše e-learningy.“ *eÚředník.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.eurednik.cz/nase-e-learningy.

EÚŘEDNÍK. [nedat.]b. „Jak koupit.“ *eÚředník.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.eurednik.cz/jak-koupit.

EÚŘEDNÍK. [nedat.]c. „Reference.“ *eÚředník.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.eurednik.cz/reference.

EÚŘEDNÍK. [nedat.]. „Kybernetická bezpečnost.“ *eÚředník.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.eurednik.cz/kurzy/12-kyberneticka-bezpecnost.

EVROPSKÁ DATABANKA. [nedat.]. „ACRESIA CONSULTING, S.R.O.“ *Evropská databanka.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.edb.cz/firma-1405074-acresia-consulting-praha-1-stare-mesto.

GAZDÍK, Jan. 2020. „Z lovce islamistů se stal lovec hackerů. Je to pro mě výzva, říká nový šéf kyberúřadu.“ *Aktuálně.cz.* Rozhovor s K. Řehkou. 23. 3. 2020. [online]. [cit.

15.10.2023]. Dostupné z: Z lovce islamistů se stal "lovec" hackerů. Nový šéf NÚKIB - Aktuálně.cz (aktualne.cz).

GORDIC. [nedat.]a. „Profil společnosti.“ *GORDIC.cz.* [online]. [cit. 20.2.2023]. Dostupné z: https://www.gordic.cz/o-spolecnosti/profil-spolecnosti.

GORDIC. [nedat.]b. „Základy kybernetické bezpečnosti.“ *GORDIC.cz.* [online]. [cit. 20.2.2023]. Dostupné z: https://www.gordic.cz/skoleni/detail?nazev=zaklady-kyberneticke-bezpecnosti&termin=22-03-2023.

GRECMANOVÁ, Helena, HOLOUŠOVÁ, Drahomíra, URBANOVSKÁ, Eva. *Obecná pedagogika I*. Olomouc: HANEX, 2002. ISBN 80-85783-20-7.

GOPAS. [nedat.]a. „Co děláme.“ *GOPAS.* [online]. [cit. 17.2.2023]. Dostupné z: https://www.gopas.cz/.

GOPAS. [nedat.]b. „Základy kybernetické bezpečnosti.“ *GOPAS.* [online]. [cit. 17.2.2023]. Dostupné z: https://www.gopas.cz/zaklady-kyberneticke-bezpecnosti_s0.

HIKVISION. [nedat.]a. „Hikvision Company Profile.“ *Hikvision.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.hikvision.com/cz/about-us/company-profile/.

HIKVISION. [nedat.]b. „Kybernetická bezpečnost.“ *Hikvision.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.hikvision.com/cz/support/cybersecurity/.

HIKVISION. [nedat.]c. „Kurz kybernetické bezpečnosti.“ *Hikvision.* [online]. [cit. 15.2.2023]. Dostupné z: https://www.hikvision.com/cz/support/academy/online-courses/cyber-security/.

CHRANIMDATA. [nedat.]a. „Kdo jsme.“ *Chranimdata.com.* [online]. [cit. 22.2.2023]. Dostupné z: https://chranimdata.com/kdo-jsme/.

CHRANIMDATA. [nedat.].b „Vzdělávání informační bezpečnosti na míru.“ *Chranimdata.com.* [online]. [cit. 24.2.2023]. Dostupné z: https://chranimdata.com/kurz-informacni-bezpecnosti-pro-klienty-abra/.

*Index gramotnosti a vzdělávání v oblasti kybernetických rizik (CLE)* [online]. [cit. 26.8.2023]. Dostupné z: https://www.oliverwymanforum.com/content/dam/oliver-wyman/ow-forum/cyber/index/Oliver-Wyman-Forum-CLE-Index-Methodology-Apr-2021.pdf, https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html, https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index/executive-summary.html.

INSTRUCTOR. [nedat.]a. „Česká jednička nejen pro online školení BOZP a PO.“ *Instructor by Prevent.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.instructor.cz/.

INSTRUCTOR. [nedat.]b. „Online kurzy.“ *Instructor by Prevent.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.instructor.cz/online-kurzy.

INSTRUCTOR. [nedat.]c. „Nejlepší řešení za nejlepší cenu.“ *Instructor by Prevent.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.instructor.cz/cenik.

INTEGRA. [nedat.]a. „Strategický partner pro Vaše IT.“ *Integra.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.integra.cz/cs/.

INTEGRA [nedat.]b. „Školení.“ *Integra.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.integra.cz/cs/education/.

INTEGRA. [nedat.]c. „Reference.“ *Integra.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.integra.cz/cs/reference/.

INTEGRA. [nedat.]d. „Vzdělávání uživatelů v oblasti kybernetické bezpečnosti.“ *Integra.cz.* [online]. [cit. 18.2.2023]. Dostupné z: https://www.integra.cz/education/vzdelavani-uzivatelu-v-oblasti-kyberneticke-bezpecnosti/.

ITBIZ.cz. 2009. „Sniffing: Odposlech datové komunikace.“ *ITbiz.cz.* 6.3.2009. [online]. [cit. 25.10.2023]. Dostupné z: Sniffing: Odposlech datové komunikace - ITBiz.cz.

ITNETWORK.cz. [nedat.]a. „O projektu ITnetwork.“ *ITnetwork.cz.* [online]. [cit. 14.2.2023]. Dostupné z: https://www.itnetwork.cz/o-projektu.

ITNETWORK.cz. [nedat.]b. „ITnetwork e-learning – Největší česká IT akademie.“ *ITnetwork.cz.* [online]. [cit. 14.2.2023]. Dostupné z: https://www.itnetwork.cz/it-e-learning.

ITNETWORK.cz. [nedat.]b. „Kybernetická bezpečnost – Online kurz.“ *ITnetwork.cz.* [online]. [cit. 14.2.2023]. Dostupné z: https://www.itnetwork.cz/bezpecnost?gclid=CjwKCAiA9NGfBhBvEiwAq5vSy_kViU-bj6zb73Bf-Xvw2QHMfSCUraA8Akbcb6sx4dPm3iLaHOjb_BoCrA8QAvD_BwE

JAVA T. POINT. [nedat.]. „Types of Cyber Attackers.“ *Java T point.* [online]. [cit. 25.10.2023]. Dostupné z: Types of Cyber Attackers - javatpoint.

JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing.

KEY TRAININGS. [nedat.]a. „Partnerství.“ *KEY Trainings.cz.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.keytrainings.cz/partnerstvi.

KEY TRAININGS. [nedat.]b. „Reference.“ *KEY Trainings.cz.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.keytrainings.cz/reference.

KEY TRAININGS. [nedat.]c. „Kybernetická bezpečnost.“ *KEY Trainings.cz.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.keytrainings.cz/kyberneticka-bezpecnost-c306.

KNOWSPREAD. [nedat.]a. „Vzdělávejte s námi své zaměstnance a klienty jednoduše, hravě, online.“ *Knowspread.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.knowspread.com/.

KNOWSPREAD. [nedat.]b. „Ceník.“ *Knowspread.* [online]. [cit. 14.2.2023]. Dostupné z: https://www.knowspread.com/cenik.

KNOWSPREAD. [nedat.]C. „Kybernetická bezpečnost.“ *Knowspread.* [online]. [cit. 14.2.2023]. Dostupné z: https://www.knowspread.com/kurz/kyberneticka-bezpecnost?utm_id=sme_14548277408_129902153998&gclid=CjwKCAiA9NGfBhBvEi

wAq5vSywRRPEemotazY9GwxBkeWFBv1M-09H-DytGx-PwOaHzI9g7krHjd0RoCsrUQAvD_BwE.

KOLOUCH, Jan – BAŠTA, Pavel – KROPÁČOVÁ, Andrea – KUNC, Martin. 2019. *Cybersecurity*. Praha: Edice CZ.NIC.

*KONCEPT STEM* [online]. NPI [cit. 30.7.2023]. Dostupné z: http://archiv-nuv.npi.cz/p-kap/koncept-stem.html.

KUEHL, Daniel T. 2009. „From Cyberspace to Cyberpower: Defining the Problem." In: *Information Resources Management College/National Defense University Working Paper.* [online]. [cit. 25.10.2023]. Dostupné z: Cyberpower-I-Chap-02.pdf (ndu.edu).

KYBERTEST [nedat.]. „#nePINdej„ *kybertest.cz* [online]. [cit. 13.05.2023]. Dostupné z: https://www.kybertest.cz/.

KYBERŠKOLENÍ.cz. [nedat.]. „Jak systém funguje?". [online]. [cit. 14.2.2023]. Dostupné z: http://www.kyberskoleni.cz/page/co-delame.

KYBEZ. [nedat.]a. „O nás." *kybez.cz.* [online]. [cit. 25.10.2023]. Dostupné z: O nás – KYBEZ.

KYBEZ. [nedat.]b. „Jaké jsou nejčastější typy kybernetických útoků?" *kybez.cz.* [online]. [cit. 25.10.2023]. Dostupné z: Jaké jsou nejčastější typy kybernetických útoků? – KYBEZ.

KYBEZ. [nedat.]c. „Hrozby." *kybez.cz.* [online]. [cit. 25.10.2023]. Dostupné z: Hrozby – KYBEZ.

LORENC, Pavel. [nedat.]a. „Portfolio." *Pavel Lorenc.* [online]. [cit. 21.2.2023]. Dostupné z: https://pavellorenc.cz/portfolio/.

LORENC, Pavel. [nedat.]b. „Kybernetická bezpečnost 2022." *Pavel Lorenc.* [online]. [cit. 21.2.2023]. Dostupné z: https://pavellorenc.cz/portfolio/kyberneticka-bezpecnost/.

MAREŠ, Miroslav. 2002. „Bezpečnost.“ In: Zeman, Petr a kol. 2002. *Česká bezpečnostní terminologie: Výklad základních pojmů.* Ústav strategických studií Vojenské akademie v Brně.

MV. 2014. „Kybernetická bezpečnost – velké téma i pro veřejnou správu.“ *Odbor strukturálních fondů Ministerstva vnitra ČR.* 27. 10. 2014. [online]. [cit. 25.10.2023]. Dostupné z:

MV. [nedat.]. „Kybernetický terorismus, kyberterorismus.“ *Ministerstvo vnitra České republiky.* [online]. [cit. 25.10.2023]. Dostupné z: Kybernetický terorismus, kyberterorismus - Ministerstvo vnitra České republiky (mvcr.cz).

MYCOM SOLUTIONS. [nedat.]a. „Školení kybernetické bezpečnost.“ *MyCom Solutions.* [online]. [cit. 13.2.2023]. Dostupné z: https://mycom.cz/.

MYCOM SOLUTIONS. [nedat.]b. „Školení: Jak na bezpečnost.“ *MyCom Solutions.* [online]. [cit. 13.2.2023]. Dostupné z: https://mycom.cz/wp-content/uploads/2022/03/Skoleni-Jak-na-bezpecnost.pdf.

*Národní strategie kybernetické bezpečnosti České republiky.* [online]. [cit. 7.8.2023]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf.

NBÚ/NCKB. 2015. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* Národní bezpečnostní úřad/ Národní centrum kybernetické bezpečnosti.

NBÚ. 2015. „NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC).“ *Národní bezpečnostní úřad.* 27.8.2015. [online]. [cit. 7.8.2023]. Dostupné z: NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC (nbu.cz).

NGSS. [nedat.]a. „O nás.“ *Next Generation Security Solutions.* [online]. [cit. 17.2.2023]. Dostupné z: https://www.ngss.cz/o-nas.

NGSS. [nedat.]b. „Školení kybernetické bezpečnosti.“ *Next Generation Security Solutions.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.ngss.cz/sluzba/13-skoleni-kyberneticke-bezpecnosti#kontakt.

NOVICOM. [nedat.]a. „Konzultace a školení.“ *Novicom.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.novicom.cz/konzultace_a_skoleni.

NOVICOM. [nedat.]b. „O společnosti.“ *Novicom.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.novicom.cz/o_spolecnosti.

NOVICOM. [nedat.]c. „Naši partneři.“ *Novicom.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.novicom.cz/nasi-partneri.

NOVICOM ACADEMY. [nedat.]. „ACADEMY: Komplexní vzdělávání pro kybernetickou bezpečnost.“ *Novicom Academy.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.novicom.cz/data/374/academy-cz.pdf.

NPI. [nedat.]. „Rozhovor: příklady dobré praxe NÚKIB ve vzdělávání kybernetické bezpečnosti.“ *NPI.* [online]. [cit. 10.2.2023]. Dostupné z: https://www.projektsypo.cz/blog/51-staticke-stranky/blog/1249-rozhovor-priklady-dobre-praxe-nukib-ve-vzdelavani-kyberneticke-bezpecnosti.html.

NÚKIB. 2020. Přednáška NÚKIB: *Role CERT/CSIRT v systému zajišťování národní bezpečnosti.* Masarykova univerzita, 10. 11. 2020. Předmět: Kybernetická bezpečnost. Záštita předmětu: NÚKIB.

NÚKIB. 2021. Přednáška NÚKIB: *Lidský faktor a vzdělávání v kybernetické bezpečnosti.* Masarykova univerzita, 5. 1. 2021. Předmět: Kybernetická bezpečnost. Záštita předmětu: NÚKIB.

NÚKIB. 2022. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021.* Brno: NÚKIB.

NÚKIB. 2023. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022.* Brno: NÚKIB.

NÚKIB. [nedat.]a. „O NÚKIB.“ *nukib.cz.* [online]. [cit. 7.8.2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - O NÚKIB (nukib.cz).

NÚKIB. [nedat.]b. „NCKB.“ *nukib.cz.* [online]. [cit. 7.8.2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Kybernetická bezpečnost (nukib.cz).

NÚKIB. [nedat.]c. „GovCERT.CZ.“ *nukib.cz.* [online]. [cit. 7.8.2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - GovCERT.CZ (nukib.cz).

NÚKIB. [nedat.]d. *Dávej kyber!.* Brno: NÚKIB.

NÚKIB. [nedat.].e „Vzdělávání.“ *Nukib.cz.* [online]. [cit. 10.2.2023]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/

OLYVERWYMANFORUM. 2021. „Executive Summary: Globally, governments fall short relative to their commitments to Cyber Risk Literacy and Education for their citizens.“ *Olyver Wyman Forum.* [online]. [cit. 7.8.2023]. Dostupné z: https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index/executive-summary.html.

OSCE. [nedat.]. „Cyber/ICT Security.“ *OSCE.* [online]. [cit. 7.8.2023]. Dostupné z: Cyber/ICT Security | OSCE.

PALÁN, Zdeněk, 1997. *Výkladový slovník vzdělávání dospělých*. Praha: DAHA. ISBN 80-902232-1-4.

PETERKA, Martin. 2011. „Role a počet bezpečnostních týmů rostou. Co o nich ale víme?“ *Lupa.cz.* 13.5.2011. [online]. [cit. 7.8.2023]. Dostupné z: Role a počet bezpečnostních týmů rostou. Co o nich ale víme? - Lupa.cz.

PIVOŇKA, Michal. 2021. „Karel Řehka: Nejslabší článek kybernetické bezpečnosti je vždycky nepoučený uživatel.“ *CZ Defence: Czech Army and Defence Magazine.* Rozhovor s K. Řehkou. 20.10. 2021. [online]. [cit. 7.8.2023]. Dostupné z: Karel Řehka:

Nejslabší článek kybernetické bezpečnosti je vždycky nepoučený uživatel | CZDEFENCE - czech army and defence magazine.

POLČÁK, Radim – HARAŠTA, Jakub – STUPKA, Václav. 2016. *Právní problémy kybernetické bezpečnosti.* Brno: Masarykova univerzita, Právnická fakulta.

RABUŠICOVÁ, M.; RABUŠIC, L. (editoři) *Učíme se po celý život? O vzdělávání dospělých v České republice.* Brno: Masarykova univerzita Brno, 2008. 337 s. ISBN 978-80-210-4779-2.

RAK, Roman. 2006. „Homo sapiens versus security." *ICT fórum/PERSONALIS 2006.* [přednáška na konferenci 27.9.2006]. Praha.

RENTEL. [nedat.]a. „ReNTEL." *ReNTEL.*[online]. [cit. 22.2.2023]. Dostupné z: https://www.rentel.cz/.

RENTEL. [nedat.]b. „Úvod do kybernetické bezpečnosti." *ReNTEL.*[online]. [cit. 22.2.2023].

SCENARIO. [nedat.]a. „Scenario informační technologie." *Scenario IT.* [online]. [cit. 19.2.2023]. Dostupné z: https://it.scenario.cz/.

SCENARIO. [nedat.]b. „Otázka kybernetické bezpečnosti." *Scenario IT.* [online]. [cit. 19.2.2023]. Dostupné z: https://it.scenario.cz/kyberneticka-bezpecnost/.

SCENARIO. [nedat.]c. „Školení Kybernetické Bezpečnosti." *Scenario IT.* [online]. [cit. 19.2.2023]. Dostupné z: https://it.scenario.cz/skoleni-kyberneticke-bezpecnosti/.

SHEA, Sharon. 2019. „6 different types of hackers, from black hat to red hat." *SearchSecurity.* Říjen 2019. [online]. [cit. 7.8.2023]. Dostupné z: 6 different types of hackers, from black hat to red hat (techtarget.com).

SKOLENI.cz. [nedat.]. „KEY Trainings s.r.o." *Skoleni.cz.* [online]. [cit. 19.2.2023]. Dostupné z: https://www.skoleni.cz/firmy/key-trainings-s-r-o-id-3972413.

SOVA STUDIO. [nedat.]. „Kybernetický bezpečnost." *Sova Studio.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.sovastudio.cz/pravo-a-legislativa/kyberneticka-

bezpecnost?utm_source=educity.cz&utm_medium=pr&utm_campaign=course-info-link.

STARTUPJOBS. [nedat.]. „MyCom Solutions, s.r.o.“ *StartupJobs.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.startupjobs.cz/startup/mycom-solutions-s-r-o-1.

STEIN, Dominik. „S výzkumem klíčových slov k úspěchu SEO: Návod krok za krokem.“ *Raidboxes.io.* 31.5.2022. [online]. [cit. 7.1.2024]. Dostupné z: https://raidboxes.io/cs/blog/online-marketing/keyword-research/#schritt-2-keyword-uebersicht.

SUCHÁNEK, Karol. [nedat.]. „Kybernetická bezpečnost ve vzdělávání.“ *Učímeonline.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.ucimeonline.cz/wp-content/uploads/2020/12/uo-52.pdf.

ŠERÁK, Michal. 2009. *Zájmové vzdělávání dospělých*. Praha : portál, 2009. ISBN 978- 80-7367-551-6.

ŠMEJKAL, Pavel. 2022. „Největší kybernetické hrozby? Rusku je nutné věnovat zvláštní pozornost, říká šéf NÚKIB Karel Řehka.“ *Forum24.* Rozhovor s K. Řehkou. 10.5.2022. [online]. [cit. 7.8.2023]. Dostupné z: Největší kybernetické hrozby? Rusku je nutné věnovat zvláštní pozornost, říká šéf NÚKIB Karel Řehka – Forum24.

TEL-AVIV UNIVERSITY, *Digital Humanities at the Sourasky Central Library, Cyber Literacy Index*. [online]. [cit. 7.8.2023]. Dostupné z: https://en-cenlib.tau.ac.il/digital-humanities, https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html.

THE ECONOMIC TIMES. [nedat.]. „What is ‚Hacking‘?“ *The Economic Times*. [online]. [cit. 13.10.2023]. Dostupné z: What is Hacking? Definition of Hacking, Hacking Meaning - The Economic Times (indiatimes.com).

TOTAL SERVICE. [nedat.]a. „O nás.“ *Total Service.* [online]. [cit. 17.2.2023]. Dostupné z: https://www.totalservice.cz/spolecnost/.

TOTAL SERVICE. [nedat.]b. „Školení.“ *Total Service.* [online]. [cit. 17.2.2023]. Dostupné z: https://www.totalservice.cz/skoleni/.

TRIGAMA.EU. [nedat.]a. „O nás.“ *Trigama.eu.* [online]. [cit. 22.2.2023]. Dostupné z: https://www.trigama.eu/cs/about-us/.

TRIGAMA.EU. [nedat.]b. „Reference.“ *Trigama.eu.* [online]. [cit. 22.2.2023]. Dostupné z: https://www.trigama.eu/cs/references/.

TRIGAMA.EU. [nedat.]c. „Naši zákazníci.“ *Trigama.eu.* [online]. [cit. 22.2.2023]. Dostupné z: https://www.trigama.eu/cs/clients/.

TRIGAMA.EU. [nedat.]d. „Vzdělávací kurzy Trigama.“ *Trigama.eu.* [online]. [cit. 22.2.2023]. Dostupné z: https://www.trigama.eu/cs/educational-courses/.

TUNGGAL, Abi Tyas. 2022. „What is a Cyber Attack? Common Attack Techniques and Targets.“ *UpGuard.* Aktualizováno 26. 6. 2022. [online]. [cit. 13.10.2023]. Dostupné z: What is a Cyber Attack? Common Attack Techniques and Targets | UpGuard.

T-SOFT. [nedat.]a. „T-SOFT a jeho historie.“ *T-SOFT.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.tsoft.cz/o-nas/.

T-SOFT. [nedat.]b. „Partneři T-SOFT.“ *T-SOFT.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.tsoft.cz/o-nas/#partneri.

T-SOFT. [nedat.]c. „Kybernetický workshop.“ *T-SOFT.* [online]. [cit. 13.2.2023]. Dostupné z: https://www.tsoft.cz/bezpecnostni-workshop/.

UČÍME ONLINE. [nedat.]a. „Kybernetická bezpečnost ve vzdělávání.“ *Učímeonline.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.ucimeonline.cz/courses/52-kyberneticka-bezpecnost-ve-vzdelavani/.

UČÍME ONLINE. [nedat.]b. „Naučíme vás, jak učit (nejen) online.“ *Ucimeonline.cz.* [online]. [cit. 16.2.2023]. Dostupné z: https://www.ucimeonline.cz/.

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

# ZDROJE OBRAZOVÝCH PŘÍLOH

KOLOUCH, Jan – BAŠTA, Pavel – KROPÁČOVÁ, Andrea – KUNC, Martin. 2019. *Cybersecurity*. Praha: Edice CZ.NIC.

NÚKIB. 2021. Přednáška NÚKIB: *Lidský faktor a vzdělávání v kybernetické bezpečnosti.* Masarykova univerzita, 5. 1. 2021. Předmět: Kybernetická bezpečnost. Záštita předmětu: NÚKIB.

OLYVERWYMANFORUM. 2021. „Executive Summary: Globally, governments fall short relative to their commitments to Cyber Risk Literacy and Education for their citizens.“ *Olyver Wyman Forum.* [online]. [cit. 7.8.2023]. Dostupné z: https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index/executive-summary.html.

RAK, Roman. 2006. „Homo sapiens versus security.“ *ICT fórum/PERSONALIS 2006.* [přednáška na konferenci 27.9.2006]. Praha.