POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Katedra managementu a informatiky

Metody zvyšování povědomí o kybernetické bezpečnosti ve státní a soukromé sféře

Diplomová práce

Methods of raising awareness of cybersecurity in public and private sector

Master thesis

VEDOUCÍ PRÁCE
PhDr. Mgr. Eliška Jonášová Ph.D.

AUTOR PRÁCE
Bc. Martin Šícha

PRAHA
2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Novém Strašecí, dne 23. 8. 2024

Bc. Martin ŠÍCHA

Poděkování

Rád bych touto cestou poděkoval **PhDr. Mgr. Elišce Jonášové Ph.D.** za odborné vedení při zpracování mé diplomové práce. Dále bych chtěl poděkovat mé přítelkyni a rodině za podporu během celého studia.

ANOTACE

Tato diplomová práce se zabývá problematikou kybernetické bezpečnosti s akcentem na metody zvyšování o jejím povědomí ve státní a soukromé sféře. V úvodu práce jsou definovány základní pojmy a klasifikace kybernetické bezpečnosti, následně jsou představeny aktuální kybernetické hrozby, dostupné metody ochrany a prevence, a také nejnovější trendy v této oblasti. Klíčová kapitola analyzuje a hodnotí současné vzdělávací metody používané k šíření povědomí o kybernetické bezpečnosti a přináší doporučení pro efektivnější vzdělávání veřejnosti. Praktická část je založena na rozhovorech se zástupci státní a soukromé sféry, kteří se aktivně podílejí na vzdělávání a osvětě v oblasti kybernetické bezpečnosti ve svých organizacích.

KLÍČOVÁ SLOVA

kybernetická bezpečnost * informační bezpečnost * ochrana dat * kybernetická kriminalita * kybernetické útoky * zvyšování povědomí * metody vzdělávání

ANNOTATION

This thesis deals with the issue of cyber security with an emphasis on methods of raising awareness of cyber security in the public and private spheres. In the introduction of the thesis, the basic concepts and classifications of cyber security are defined, followed by a presentation of current cyber threats, available methods of protection and prevention, and the latest trends in this area. A key chapter analyzes and evaluates current educational methods used to spread cybersecurity awareness and makes recommendations for more effective public education. The practical part is based on interviews with representatives from the public and private spheres who are actively involved in cybersecurity education and awareness in their organizations.

KEYWORDS

cybersecurity * information security * data protection * cybercrime * cyber attacks * awareness raising * methods of education

Obsah

Úvod

Pro svou diplomovou práci jsem si zvolil téma „Metody zvyšování povědomí o kybernetické bezpečnosti ve státní a soukromé sféře“. Kybernetická bezpečnost se v současnosti stává stále důležitějším tématem jak pro jednotlivce, tak i pro organizace v soukromé a státní sféře. V dnešní době jsou informace a data velmi cenným majetkem, proto jsou často cílem kybernetických útoků. Mnoho organizací a jednotlivců přesto stále nevěnuje dostatečnou pozornost této problematice a často nechápou rizika spojená s kybernetickými hrozbami. Toto téma mě zaujalo především kvůli jeho aktuálnosti a nutnosti neustálého vzdělávání a zdokonalování, aby bylo možné držet krok s novými trendy a hrozbami v této oblasti.

Tato diplomová práce se zaměří na metody zvyšování povědomí o kybernetické bezpečnosti a jejich účinnost ve státní a soukromé sféře. Cílem bude detailně analyzovat současné přístupy a navrhnout doporučení pro zvýšení jejich efektivity při vzdělávání veřejnosti. Práce zhodnotí jednotlivé vzdělávací metody a aktuální stav v České republice, s cílem identifikovat klíčové oblasti pro zlepšení. Závěrem bude soubor doporučení pro implementaci účinných metod, které posílí schopnost široké veřejnosti a zaměstnanců organizací lépe reagovat na současné kybernetické hrozby a chránit své informace.

V úvodní kapitole je nejprve vysvětlen pojem kybernetická bezpečnost, spolu s příbuznými termíny, jako je informační bezpečnost nebo kybernetický incident, včetně stručného exkurzu do historie internetu. Druhá kapitola se věnuje aktuálním kybernetickým hrozbám, se kterými se uživatelé setkávají dnes a denně, mezi které patří malware, ransomware, DDoS, sociální inženýrství a také pojednává o rizicích užívání sociálních sítí. Následující kapitola naopak zahrnuje dostupná ochranná a preventivní opatření, jako jsou například základní zásady bezpečného používání internetu, fyzická bezpečnost či bezpečnost sítí a služeb. S ohledem na neustálý technologický pokrok je pak samostatná kapitola věnována současným trendům, jako je internet věcí, cloud computing, blockchain a stále populárnější umělá inteligence.

Klíčová pátá kapitola se zaměřuje na detailní popis současných metod zvyšování povědomí o kybernetické bezpečnosti. Tyto metody zahrnují širokou škálu přístupů, počínaje osvětovými kampaněmi zaměřenými na veřejnost, až po specializované vzdělávací programy určené pro organizace. Mezi často využívané metody patří školení zaměstnanců, přednášky, testování znalostí a simulované útoky, které pomáhají zaměstnancům lépe pochopit potenciální hrozby a způsoby, jak se proti nim bránit. Kapitola také pojednává o významu konferencí, workshopů a soutěží v oblasti kybernetické bezpečnosti, přičemž zmiňuje i rostoucí roli gamifikace jako efektivního nástroje pro zapojení a motivaci účastníků. Dále se kapitola zaměřuje na výuku kybernetické bezpečnosti v českých školách a vzdělávací programy a iniciativy v zahraničí, kde často probíhá systematičtější a inovativnější vzdělávání v této problematice. Závěrečná kapitola teoretické části práce přináší komplexní zhodnocení aktuální situace v České republice a nabízí konkrétní doporučení pro zlepšení a zefektivnění vzdělávacích aktivit v oblasti kybernetické bezpečnosti, s cílem zvýšit úroveň informovanosti a připravenosti veřejnosti na kybernetické hrozby.

Součástí práce je také praktická část v podobě strukturovaných rozhovorů se zástupci státní a soukromé sféry. Tito odborníci, kteří ve svých pracovních pozicích nesou odpovědnost za kybernetickou bezpečnost svých institucí, hrají zároveň významnou roli při zvyšování povědomí a rozšiřování znalostí zaměstnanců o kybernetických hrozbách a ochranných opatřeních. Rozhovory se zaměřují na jejich zkušenosti, osvědčené postupy a strategie, které využívají k efektivnímu vzdělávání a osvětě. Tato část práce nabízí hlubší pohled na praktické aspekty implementace vzdělávacích metod a osvědčených postupů v reálném prostředí. Výsledky těchto rozhovorů jsou následně analyzovány a vyhodnoceny. Na základě těchto zjištění je vypracován soubor doporučení, který má za cíl přispět k efektivnějšímu a koordinovanějšímu přístupu k osvětě v oblasti kybernetické bezpečnosti, jak ve státním, tak i soukromém sektoru.

1 Kybernetická bezpečnost

Kybernetická bezpečnost se dá bezesporu označit jako jeden z největších fenoménů současnosti. S rozmachem digitalizace a neustále se zvyšující závislostí společnosti na informačních a komunikačních technologiích, které ovlivňují naše životy téměř ve všech aspektech, hraje kybernetická bezpečnost klíčovou roli pro ochranu bezpečnosti a soukromí nejen na úrovni jednotlivců a korporací, ale i světových vlád a mezinárodních organizací.

Vzhledem k tomu, že kybernetická bezpečnost je stále poměrně nový a dynamicky se rozvíjející obor, ve kterém udává tempo technologický pokrok, je nezbytné neustále reagovat na nové výzvy s ním spojené. Klíčovým prvkem v oblasti kybernetické bezpečnosti je prevence a celková informovanost uživatelů, která může předejít vzniku velkých škod a nákladů spojených s kybernetickými útoky. Neméně důležité je také prohlubování vzájemné spolupráce nejen na úrovni národní, ale i té mezinárodní. Kyberprostor totiž není omezen státními hranicemi ani světovými kontinenty. Vzájemné sdílení informací o hrozbách a bezpečnostních opatřeních může pomoci včasné identifikaci a reakci na útoky.

Nové technologie přináší společnosti řadu nesporných výhod, ale zároveň také potenciální hrozby. Inovace v oblasti umělé inteligence, strojového učení, kvantových počítačů, cloud computingu, internetu věcí a dalších technologií mohou poskytnout nové možnosti, ale také zvyšují potenciální rizika. Rozšíření internetu do celého světa a relativní anonymita jeho uživatelů umožňuje páchání kybernetické kriminality zahrnující různé druhy podvodů, šíření dětské pornografie, propagaci terorismu a extremismu či krádeže dat a následné vydírání. V krajním případě pak může dojít i ke kybernetickým útokům na kritickou infrastrukturu, jejíž narušení může mít vážné celospolečenské dopady v podobě ohrožení národní bezpečnosti, ekonomiky a základních životních potřeb obyvatel.[1]

[1] Vláda České republiky. *Kybernetická bezpečnost* [online]. 2021 [cit. 2024-01-24]. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

1.1 Pojem

Vzhledem k tomu, že již samotný nadřazený pojem bezpečnost dosud nemá jednoznačnou a všeobecně přijímanou definici, je tomu stejně tak i u termínu kybernetická bezpečnost. K jednomu z prvních použití tohoto pojmu došlo v roce 1991 ve zprávě Rady pro informatiku a telekomunikace a od té doby byla jeho definice nesčetněkrát modifikována. Jednotný výklad dále komplikuje fakt, že původem jde o pojem převzatý z anglického jazyka, ve kterém jsou zpravidla publikovány i odborné články o kybernetické bezpečnosti. Obecně by se kybernetická bezpečnost dala shrnout jako připravenost systému či služby na potenciální útoky, která jde ruku v ruce s plánováním obnovy funkčnosti při možném narušení.[2]

Jako další z definic kybernetické bezpečnosti dle Výkladového slovníku kybernetické bezpečnosti lze uvést, že se jedná o *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“*.[3]

Pokud vezmeme v úvahu skutečnost, že internet je prostředím relativně nezávislým, které žádná světová vláda ani organizace nemá zcela pod kontrolou, je možné kybernetickou bezpečnost definovat jako ochranu počítačů, jejich sítí a dat před kybernetickými útoky a možným narušením základních atributů bezpečnosti, kterými jsou zejména ohrožení důvěrnosti (z angl. confidentiality), integrity (z angl. integrity) dat uložených v těchto počítačích a jejich sítích a dostupnosti (z angl. availability) počítačů a jejich sítí.[4] Tyto tři kategorie se pak na základě jejich počátečních písmen souhrnně označují jako CIA triáda.[5]

[2] PAČKA, Roman. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Politologická řada. Brno: Centrum pro studium demokracie a kultury, 2019. ISBN 978-80-7325-473-5, s. 11.
[3] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 69.
[4] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 9.
[5] PAČKA, Roman. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Politologická řada. Brno: Centrum pro studium demokracie a kultury, 2019. ISBN 978-80-7325-473-5, s. 11.

1.2 Další související pojmy

Jelikož celá diplomová práce obsahuje řadu pojmů, které jsou specifické pro problematiku informačních a komunikačních technologií a zejména pak pro oblast kybernetické bezpečnosti, je nezbytné některé z nich pro lepší porozumění definovat.

Informační bezpečnost

Nedílnou součástí kybernetické bezpečnosti je problematika bezpečnosti informací. Pojem informační bezpečnost Ministerstvo vnitra České republiky definuje v jedné ze svých studií jako multidisciplinární obor, který usiluje o komplexní přístup k problematice ochrany informací od jejich vzniku, přes zpracování a ukládání, až po přenos a jejich likvidaci. Cílem je pak snižování rizik souvisejících s bezpečností informací a navrhování příslušných opatření z organizačního, řídícího, metodického, technického či právního hlediska.“[6]

Kybernetická kriminalita

S rozvojem informačních a komunikačních technologiích se zvyšuje i kybernetická kriminalita, tedy trestná činnost, při které je určitým způsobem využíván počítač či některé z jeho součástí nebo také větší množství počítačů současně, které mohou být samostatné nebo propojené do počítačové sítě. Počítač může být buď předmětem zájmu této trestné činnosti nebo může sloužit jako prostředí či nástroj pro spáchání trestného činu.[7]

Kybernetický útok

Kybernetickým útokem rozumíme útok na infrastrukturu informačních technologií, jehož účelem je způsobit poškození a získat důvěrná nebo strategicky důležitá data. Kybernetické útoky jsou většinou využívány k prosazování politických či vojenských cílů.[8]

---

[6] Ministerstvo vnitra České republiky. *Základní definice, vztahující se k tématu kybernetické bezpečnosti* [online]. 2009 [cit. 2024-01-26]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

[7] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 69.

[8] Tamtéž, s. 71.

Kybernetický incident

Kybernetický bezpečnostní incident představuje událost, při které dojde k porušení zabezpečení informací v systému. Tato událost může zahrnovat útoky pomocí škodlivého softwaru, jako je například ransomware nebo malware.[9]

Osoby či instituce uvedené v zákoně o kybernetické bezpečnosti jsou povinny neprodleně ohlásit každý kybernetický incident Národnímu úřadu pro kybernetickou a informační bezpečnost.[10]

Internet

Dnešní svět si již pravděpodobně nikdo z nás nedovede představit bez internetu. Umožňuje nám přístup k obrovskému množství informací a možnostem jako je například nakupování, vzdělávání a práce z pohodlí domova či komunikace s přáteli, kteří se v danou chvíli nachází na opačné straně planety.

To vše je možné právě díky internetu, celosvětovému systému propojených počítačových sítí, které jsou založeny na standardních síťových protokolech TCP/IP (Transmission Control Protocol – Internet Protocol). Jedná se v podstatě o síť sítí, která zahrnuje miliony soukromých, veřejných, obchodních, akademických či vládních sítí, které jsou navzájem propojeny pomocí široké škály elektronických, optických a bezdrátových síťových technologií.[11]

Intranet

Interní počítačovou síť, která využívá technologie internetu, označujeme jako síť intranet. Díky ní mohou zaměstnanci uvnitř jednotlivých organizací navzájem komunikovat a sdílet informace.[12]

---

[9] Gov.cz. *Hlášení kybernetických bezpečnostních incidentů* [online]. 2024 [cit. 2024-01-27]. Dostupné z: https://portal.gov.cz/sluzby-vs/hlaseni-kybernetickych-bezpecnostnich-incidentu-S10769

[10] Tamtéž.

[11] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 59.

[12] Tamtéž, s. 61.

1.3 Historie

Problematika kybernetické bezpečnosti začala získávat na významu díky technologickému pokroku v oblasti počítačových systémů, digitalizace a neustále se zvětšující základně uživatelů kyberprostoru. Fenomén kybernetické bezpečnosti by zcela jistě neexistoval bez vzniku sítě internet. Za úplné prvopočátky lze označit polovinu 20. století, kdy začalo ve větší míře docházet k rozmachu digitalizace, tedy postupnému převodu z analogového signálu na digitální.[13]

Poté, co byla v roce 1957 na oběžnou dráhu vyslána historicky první umělá družice Sputnik 1 z dílny Sovětského svazu, si Spojené státy americké uvědomily, že nemohou zaostávat v technologickém pokroku. Hned v roce 1958 proto byla americkým Ministerstvem obrany založena agentura ARPA (Advanced Research Project Agency) s cílem podpory výzkumných iniciativ směřujících k inovativním technologiím. Výsledkem byl vznik předchůdce internetu, projektu zvaného ARPANET, prostřednictvím kterého byla v roce 1969 úspěšně odeslána první zpráva z Los Angeles do Stanfordu. V roce 1973 pak začal ARPANET komunikovat s Evropou. O následné zdokonalení sítě ARPANET se zasloužili Bob Kahn a Vint Cerf.[14]

Počátkem 90. let 20. století byly položeny základní kameny dnešního internetu, tedy transportní vrstvy a síťové protokoly TCP/IP. Tou dobou byl však internet stále ještě užíván pouze v rámci akademické obce. Učiněné legislativní změny umožnily využívat internet ke komerčním účelům v roce 1991, nejprve v USA a následně i v jiných zemích světa. K většímu rozmachu internetu poté došlo díky vzniku služby WWW neboli World Wide Web, za kterou stáli vynálezci Tim Berners-Lee a Robert Cailliau z ženevského Centra jaderného výzkumu CERN. Na území tehdejšího Československa došlo k prvnímu spuštění internetu dne 13. února 1992 na pražské univerzitě ČVUT.[15]

---

[13] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 34.
[14] CZ.NIC. *Jak na internet* [online]. 2012-2014 [cit. 2024-01-29]. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/
[15] Tamtéž.

Na základě uvedených skutečností je zřejmé, že internet byl původně vyvinut jako projekt zaměřený na propojení výzkumných institucí, s prioritou kladenou především na spolehlivost a dostupnost. Bezpečnostní aspekty však byly zpočátku zanedbány, což vedlo k tomu, že s rostoucí celosvětovou adopcí internetu došlo také k prudkému nárůstu kybernetických hrozeb. Tento vývoj přivedl fenomén kybernetické bezpečnosti do centra zájmu odborníků i veřejnosti, přičemž jeho význam neustále narůstá a stává se klíčovým prvkem v ochraně digitálního světa.

2 Kybernetické hrozby

Důležitost kybernetické bezpečnosti vyplývá především z existence řady kybernetických hrozeb. Tyto hrozby představují širokou škálu různorodých nebezpečí a rizik spojených s používáním digitálních technologií a internetu. Jedním z významných aspektů kybernetických hrozeb je jejich neustálý vývoj a adaptace. Útočníci neustále vylepšují své metody a techniky, aby se vyhnuli detekci a odhalení a zvýšili účinnost svých útoků. To vyžaduje neustálou pozornost, obezřetnost, inovace, zdokonalování bezpečnostních opatření a investice do kybernetické bezpečnosti.

Dle Ministerstva vnitra ČR je obecně hrozba definována jako jakýkoli fenomén, který disponuje schopností poškodit státem chráněné hodnoty a zájmy, přičemž míra hrozby je pak dána velikostí potenciální škody a časovým horizontem, ve kterém může dojít k uplatnění takové hrozby.[16]

Ve Výkladovém slovníku kybernetické bezpečnosti je pak bezpečnostní hrozba definována jako *„potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.*[17]

[16] Ministerstvo vnitra České republiky. *Hrozba* [online]. 2003 [cit. 2024-02-02]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

[17] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 25.

Kybernetické hrozby lze rozdělit podle několika kritérií:

- Dle zdroje působení – hrozby vnitřní a vnější.
- Dle úmyslu – hrozby náhodné, nedbalostní a úmyslné.
- Dle původu – hrozby přírodní a hrozby způsobené člověkem.
- Dle směrování na bezpečnostní atributy – hrozby dostupnosti, integrity a důvěrnosti.
- Dle toho, na jaký druh aktiva působí – hrozby pro hardware, síť, operační systém, aplikace, informace a uživatele.
- Dle motivace útočníka – hrozby za účelem finančního zisku, získání konkurenční převahy, dokázání svých schopností, odplaty neplnění povinností.[18]

Jak uvádí Rada Evropské unie ve své nejnovější infografice z roku 2023, mezi nejzávažnější kybernetické hrozby v Evropské unii patří ransomware, phishing, hrozby distribuovaného odmítnutí služby (DDoS), malware, sociální inženýrství, ohrožení dat, útoky s dopadem na dostupnost internetu, hrozby pro dodavatelské řetězce či dezinformace a misinformace. Je odhadováno, že roční náklady spojené s kybernetickou kriminalitou v rámci celosvětové ekonomiky dosáhly ke konci roku 2020 5,5 bilionu eur, což je dvojnásobná hodnota oproti roku 2015. V roce 2022 došlo k výraznému zintenzivnění kybernetických hrozeb, které bylo významně ovlivněno vojenskou agresí Ruska vůči Ukrajině. Tento konflikt vedl k výraznému nárůstu aktivit kybernetických zločinců a státem podporovaných hackerských skupin. Válka nejenže zvýšila frekvenci a závažnost kybernetických útoků, ale také vedla ke zvýšení sofistikovanosti těchto operací. Státem sponzorované skupiny a kybernetičtí útočníci začali cílit na strategickou a kritickou infrastrukturu, což vedlo k závažným narušením a komplikacím v oblastech jako jsou vládní systémy, energetika a komunikace.[19]

[18] KYBEZ. *Hrozby* [online]. 2021 [cit. 2024-02-03]. Dostupné z: https://kybez.cz/hrozby/
[19] Rada Evropské unie. *Infografika – Nejzávažnější kybernetické hrozby v EU* [online]. 2023 [cit. 2024-02-03]. Dostupné z: https://www.consilium.europa.eu/cs/infographics/cyber-threats-eu/

2.1 Malware

Malware je obecným názvem pro veškerý škodlivý software. Mezi škodlivé programy lze zařadit počítačové viry, červy, trojské koně a špionážní software.[20]

Jedná se o zkratku vytvořenou z anglického slovního spojení malicious software. Cíle škodlivého softwaru mohou být různé a na zařízení, které jím bylo napadeno, se může jeho přítomnost projevovat jakýmkoli způsobem. Ve většině případech se malware na napadeném zařízení skrývá a usiluje o to, aby přežil restartování napadeného zařízení. Na koncové zařízení lze malware doručit různými způsoby, těmto způsobům se pak přezdívá vektory útoku a je u nich zpravidla potřeba součinnost oběti, ať už větší či menší.[21]

Mezi vektory útoku lze zařadit například metody drive-by download, kdy ke stažení malware postačí návštěva webové stránky, která je kompromitovaná. Mezi další metody patří také phishing, kdy k doručení malware dochází prostřednictvím přílohy e-mailu. Dalším způsobem je pak stažení trojanizované aplikace, která může být umístěna na některém z online marketů, úložišť či na přenositelném médiu jako je USB flash disk, externí pevný disk, paměťová karta nebo optický disk, tedy CD či DVD.[22]

Podle způsobu, kterým se malware šíří, jej můžeme rozdělit na:

- Virus – kód, který se šíří tím způsobem, že v okamžiku, kdy uživatel spustí jím infikovaný soubor, začne sám sebe kopírovat do ostatních souborů.
- Červ (worm) – program, který sám sebe rozesílá pomocí e-mailů na jiné e-mailové adresy či se šíří tak, že vyhledává jiná zařízení, která nejsou dostatečně zabezpečena nebo nemají aktualizovaný běžící software a na tato se následně kopíruje.

[20] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 115.
[21] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 40.
[22] Tamtéž, s. 40.

- Trojský kůň (Trojan horse) – stejně jako dřevěný kůň z řecké mytologie, tak i tento malware skrývá svůj pravý význam, kdy se vydává za libovolnou mnohdy zdánlivě užitečnou aplikaci, kterou uživatel sám stáhne a nainstaluje do svého zařízení, přičemž malware na pozadí začne provádět odlišnou a převážně škodlivou činnost.[23]

Malware lze dále rozdělit také podle projevů. Zde je možné uvést například špionážní software zvaný spyware, falešný antivirus scareware, reklamní software neboli adware, zadní vrátka známé jako backdoor, logickou bombu, rootkit, bankovní malware či vyděračský software zvaný ransomware, o kterém podrobněji pojednává následující kapitola.[24]

2.2 Ransomware

Ransomwarové útoky jsou v současnosti mezi pachateli kybernetické kriminality velmi populární a jak již bylo zmíněno, jsou také jednou z nejzávažnějších kybernetických hrozeb v Evropské unii. Z tohoto důvodu jim bude věnována samostatná kapitola.

Jak bylo uvedeno v předchozí kapitole, ransomware je jedním z druhů škodlivého programu neboli malware. Pojmem ransomware se konkrétně rozumí vyděračský software, který nejprve zašifruje data a následně nabízí jejich rozšifrování po uhrazení výkupného.[25]

Za jeden z vůbec největších ransomwarových útoků v historii je považován kmen zvaný WannaCry. Tento malware, který byl vypuštěný v roce 2017, ovlivnil tisíce počítačových systémů po celém světě a držel jako rukojmí soubory čtvrt milionu uživatelů operačního systému Microsoft Windows ve 150 zemích. Ransomware WannaCry dokázal infikovat mnoho společností, včetně několika

[23] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 41.
[24] Tamtéž, s. 41-42.
[25] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 97.

systémů NHS v Anglii a Skotsku. To nakonec způsobilo značné narušení zdravotnických služeb, ohrožení mnoha životů a hospodářskou ztrátu ve výši 92 milionů liber.[26]

V České republice se pak nechvalně proslavil ransomware Ryuk, který v roce 2019 zaútočil na benešovskou Nemocnici Rudolfa a Stefanie. Největší ztráty, které nemocnice utrpěla, souvisely s omezením lékařských procedur. Nemocnice také kvůli tomuto kyberútoku neobdržela plnou finanční kompenzaci od zdravotních pojišťoven za původně plánované vyšetření, operace a zákroky. Nemocnice dále musela vynaložit značné finanční prostředky na nový zabezpečovací systém, reinstalaci softwaru a obnovu systémů včetně proškolení personálu. Celková škoda byla vyčíslena na více než 59 milionů korun.[27]

Za zmínku také stojí ransomware Ragnar Locker nazvaný po stejnojmenné organizované skupině. Tento se poprvé objevil v prosinci 2019 a byl zodpovědný za řadu významných útoků na kritickou infrastrukturu po celém světě, například i vůči portugalským národním aerolinkám či izraelské nemocnici. Ransomware využíval strategii tzv. dvojího vydírání, požadoval zaplacení výkupného za odblokování systému a zároveň i za nezveřejnění ukradených dat.

Na operaci TALPA, při které byl tento ransomwarový gang rozprášen, a která proběhla ve dnech 16. až 20. října 2023, se podílely jednotky Francie, Itálie, Japonska, Lotyšska, Nizozemska, Španělska, Švédska, Ukrajiny a USA ve spolupráci s českou Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování Policie České republiky (NCTEKK). Tato operace byla zároveň aktivně podporována Europolem a Interpolem. Vyšetřováním bylo postupně zjištěno, že mozkem celé organizace je Čech, který byl zadržen v Paříži. Další dva hlavní hackeři byli zadrženi ve španělském Alicante a jeden pak v Lotyšsku. Infrastruktura pro provoz ransomwaru byla zabavena v Nizozemsku, Německu a Švédsku.

---

[26] Cyber Magazine. *Top 10 Ransomware Attacks* [online]. 2023 [cit. 2024-02-05]. Dostupné z: https://cybermagazine.com/articles/top-10-ransomware-attacks

[27] ČT24. *Útok na benešovskou nemocnici způsobil šedesátimilionovou škodu. Policie případ odložila* [online]. 2020 [cit. 2024-02-05]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/utok-na-benesovskou-nemocnici-zpusobil-sedesatimilionovou-skodu-policie-pripad-odlozila-45977

Výše uvedená kauza a její úspěšně zakončené vyšetřování je důkazem toho, že spolupráce mezinárodních složek je klíčová pro likvidaci organizovaných zločineckých skupin, které páchají kybernetické útoky vůči kritické informační infrastruktuře nejen prostřednictvím škodlivého programu typu ransomware.[28]

2.3 Sociální inženýrství

Sociálním inženýrstvím se rozumí způsob manipulace lidí, jehož účelem je provedení určité akce či získání určité informace.[29]

Není žádným tajemstvím, že sám člověk je nejslabším článkem, pokud jde o bezpečnost. Elementárním povědomím o základních bezpečnostních pravidlech a principech nedisponují dokonce ani někteří majitelé společností či vedoucí pracovníci, natož například senioři, pro které je velmi obtížné držet krok s rychlostí technologického pokroku.[30]

Útočníci nemusí využívat žádné sofistikované kódy nebo programy, aby způsobili značné škody. Namísto toho, aby hledali slabiny v softwaru nebo síťových zařízeních, útočníci zaměřují svou pozornost na lidi a jejich chování. Dalo by se říct, že sociální inženýrství je spíše uměním než vědou. Útočníci využívají psychologie a techniky spočívající v ovlivňování, přesvědčování a manipulace s lidmi. Osobou, která tyto techniky umí zdatně využívat, je sociotechnik. Cílem sociotechnika je v oslovené osobě vzbudit důvěru a přimět ji, aby poskytla potřebné informace nebo aby provedla, co sociotechnik zrovna potřebuje. Sociotechnici se mnohdy vydávají za zaměstnance renomovaných společností, státní úředníky, bankéře nebo policisty a u oslovených osob uměle vyvolávají dojem časové tísně, kdy je nutí provést akci co nejrychleji. Své aktivity provozují zejména prostřednictvím sociálních sítí, aplikací, telefonních hovorů, SMS zpráv, e-mailů či dokonce osobně.[31]

---

[28] Policie České republiky. *Mezinárodní operace TALPA* [online]. 2023 [cit. 2024-02-06]. Dostupné z: https://www.policie.cz/clanek/mezinarodni-operace-talpa.aspx
[29] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 107.
[30] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 30.
[31] Tamtéž, s. 31.

Útoky s prvky sociálního inženýrství jsou ve většině případů vedeny plošně, nikoli cíleně. Při užívání plošných útoků pak útočníci spoléhají, že naleznou tzv. low hanging fruit, tedy ovoce, které obrazně řečeno visí nízko a lze jednoduše utrhnout, jinými slovy hledají snadnou kořist.[32]

Typickým představitelem sociálního inženýrství je v současnosti velmi populární phishing. Jde o podvodný způsob, jak prostřednictvím internetu získat citlivé informace jako jsou hesla, údaje z platebních karet či přihlašovací údaje k internetovému bankovnictví. Obvykle se jedná o hromadné rozesílání zpráv na sociálních sítích, e-mailů či SMS zpráv, které nabádají adresáta k vyplnění údajů na falešné webové stránce, která se často velmi podobá té oficiální. Uživatel pak v dobré víře do příslušných okének zadá své přihlašovací údaje, čímž tyto údaje poskytne útočníkům, kteří mohou vykrást peníze z jeho účtu.[33]

2.4 DDoS

Distributed Denial of Service neboli distribuované odmítnutí služby je kybernetickým útokem, jehož cílem je dosáhnout odepření služby prostřednictvím zahlcení cíle velkým množstvím požadavků. Oproti zmíněnému phishingu, který je převážně plošným útokem, je DDoS útokem velmi přesně cíleným. Podstata spočívá v tom, že si útočník nebo zájemce o tento typ útoku za poplatek pronajme síť počítačů infikovaných speciálním softwarem, tzv. botnet, který začne navazovat spojení a realizovat dotazy na konkrétní web či server. Enormní množství požadavků následně cílový systém zpomalí či úplně vyřadí z provozu.[34]

Botnety se označují za armády tzv. zombií, což jsou zařízení, které byly infikovány nějakým škodlivým softwarem. Tyto zařízení jsou pod kontrolou útočníka, aniž by to věděli jejich legitimní uživatelé. Součástí botnetu někdy může být i několik milionů kompromitovaných zařízení a nemusí se jednat jen o počítače,

[32] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 32.
[33] Policie České republiky. *Počítačová kriminalita* [online]. 2024 [cit. 2024-02-10]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx
[34] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 52-53.

ale i mobilní telefony či jiné zařízení ze sítě IoT jako jsou IP kamery, routery či chytré televizory.[35]

Pronajmout si základní botnet může být poměrně snadné a cenově dostupné. V analýze služeb nabízejících pronájem botnetů, kterou zveřejnila společnost Kaspersky, se lze dočíst, že výsledná cena pronájmu se odvíjí od počtu zařízení zařazených v botnetu a doby pronájmu, dále dle stupně ochrany cílové sítě, specifických cílů, scénářů útoků či konkrétní země, kde je služba provozována. Kaspersky v této analýze uvádí, že například pronájem botnetu čítajícího tisíc běžných počítačů stojí 7 dolarů za hodinu. Je zřejmé, že náklady za takový pronájem nejsou nijak vysoké a lze tedy očekávat, že popularita DDoS útoků i nadále poroste.[36]

DDoS útoky bývají cíleny na různé vládní organizace, nadnárodní korporace či na konkurenční společnosti. K útokům na e-shopy ze strany konkurence nejčastěji dochází v předvánočním období, kdy vrcholí prodeje zboží a prodejci se snaží nalákat potenciální zákazníky na svůj internetový obchod. Mezi následky způsobené DDoS útoky však nepatří pouze přímá finanční ztráta, která vznikne poškozenému subjektu, ale může dojít také k poškození pověsti dané společnosti, jejíž služba je opakovaně a dlouhodobě nedostupná.[37]

2.5 Rizika sociálních sítí

Sociální sítě se staly nepostradatelnou součástí moderního života, umožňují nám komunikovat, sdílet obsah a udržovat kontakt s přáteli, rodinou či kolegy. Jejich rostoucí popularita však přináší i určité nebezpečí. Rizik spojených s užíváním sociálních sítí je celá řada, ať už se jedná o zveřejnění osobních informací, šíření dezinformací, zneužití identity, kyberšikanu nebo útoky prováděné pomocí již zmíněného sociálního inženýrství.

---

[35] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 46.
[36] Root.cz. *Kolik stojí DDoS? Základní přijde na pár dolarů, pokročilý na stovky* [online]. 2017 [cit. 2024-02-12]. Dostupné z: https://www.root.cz/clanky/kolik-stoji-ddos-zakladni-prijde-na-par-dolaru-pokrocily-na-stovky/
[37] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 53-54.

Kyberšikana

Jedná se o specifický druh šikany, která je realizována prostřednictvím internetu a v současné době k ní většinou dochází na populárních sociálních sítích, jako je Facebook, Instagram či na platformách YouTube nebo TikTok. Nejčastějšími projevy jsou verbální útoky, nadávání, ponižování, vyhrožování, vydírání, krádeže identity a v neposlední řadě také zveřejňování intimních či ponižujících fotografií a videí.[38]

Kybergrooming

Pod tímto pojmem se skrývá jednání uživatelů, kteří se v prostředí internetu snaží získat důvěru dítěte s úmyslem ho zneužít k nelegálním aktivitám, většinou sexuálního rázu.[39] Ke kybergroomingu útočníci nejčastěji používají populární sociální sítě (Facebook, Instagram, Badoo, TikTok, X) nebo internetové komunikační platformy (Facebook Messenger, WhatsApp, Snapchat, Telegram, Skype, Viber, Signal). Obětí kybergroomingu se může stát téměř kdokoli, nicméně nejčastěji se jedná o dívky ve věku 11-17 let, které aktivně používají informační a komunikační technologie a zároveň mnohdy trpí nedostatkem sebedůvěry a pocitem osamění. Pachatelé kybergroomingu se často vydávají za někoho jiného, podle preference oběti. Klíčovou vlastností kybergroomera obvykle bývá trpělivost, jelikož si dokáže s obětí psát někdy i po dobu několika měsíců, aby získal její důvěru a upevnil s ní vztah. O kybergroomingu byl v roce 2020 natočen český dokumentární film V Síti.[40]

Kyberstalking

Jako kyberstalking se označují různé druhy pronásledování a obtěžování prostřednictvím elektronických médií, které mají za cíl vyvolat u oběti pocit strachu, úzkosti nebo ztráty soukromí. Pachatel informace o oběti získává zejména

---

[38] Policie České republiky. *Rizika a nástrahy sociálních sítí* [online]. 2024 [cit. 2024-02-15]. Dostupné z: https://www.policie.cz/soubor/policie-cr-prilohy-kybersikana-doporuceni-pdf.aspx

[39] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 69.

[40] Internetem bezpečně. *Kybergrooming* [online]. 2018 [cit. 2024-02-1]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

z internetu, konkrétně ze sociálních sítí, webových stránek, fór či internetových komunikačních prostředků. Kyberstalking často vede ke spáchání některého z trestných činů spočívajících v omezování osobních práv oběti, fyzickému nebo emocionálnímu zneužívání nebo také donucení oběti ke spáchání trestného činu.[41]

Krádež identity

Krádeží identity rozumíme jednání, kterým se útočník zmocní virtuální identity oběti. Toto zahrnuje například odcizení přihlašovacích údajů k e-mailové schránce, uživatelskému účtu na sociálních sítích či hernímu účtu. Následně se útočník vydává za oběť a využívá její identitu ať už k rozesílání spamu nebo k provádění phishingových útoků na blízké okolí oběti.[42]

Sexting

Tento pojem vznikl spojením slov sex a texting, z čehož je možné odvodit, že se jedná o zasílání textu, fotografií či audio a video nahrávek se sexuálním podtextem. Posílání probíhá podobně jako u kybergroomingu zejména prostřednictvím sociálních sítí nebo internetových komunikačních prostředků.[43]

Dezinformace

S rozmachem internetu a sociálních sítí, kde může svůj názor sdílet každý z nás, získávají na významu dezinformace. Jde o systematické šíření úmyslně nepravdivých informací, jejichž cílem je manipulace a ovlivňování názorů jejich adresátů. Dezinformace mohou mít různé podoby, mezi které patří šíření tzv. fake news, tedy falešných zpráv, nebo například lživé vykládání historických událostí.[44]

---

[41] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 36.

[42] Internetem bezpečně. *Krádež identity* [online]. 2018 [cit. 2024-02-18]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[43] Internetem bezpečně. *Sexting* [online]. 2018 [cit. 2024-02-20]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

[44] Ministerstvo vnitra České republiky. *Definice dezinformací a propagandy* [online]. 2024 [cit. 2024-02-21]. Dostupné z: https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

3 Ochrana a prevence

V dnešní digitální době je v podstatě již nezbytné disponovat efektivní strategií pro zajištění ochrany uživatelů a systémů před širokou škálou kybernetických hrozeb. Tato kapitola se zaměřuje na různé aspekty ochrany a prevence v rámci kybernetické bezpečnosti. Především se jedná o zásady bezpečného používání internetu, fyzickou bezpečnost či bezpečnost sítí a služeb. Tato ochranná opatření jsou velmi důležitá pro minimalizaci rizik a zajištění bezpečnosti dat a systémů. Pro začátek je však nutné si uvědomit, že každé bezpečnostní řešení je pouze tak bezpečné, jak bezpečný je jeho nejslabší článek. Nejslabším článkem nejen každého počítačového systému je obvykle sám jeho uživatel, tedy člověk.[45]

Opatření, jejichž cílem je snížit riziko na přijatelnou úroveň, lze dělit podle několika kritérií. Dle způsobu implementace je možné tato opatření rozdělit na organizační a technická. Organizační opatření zahrnují různé směrnice, standardy a politiky, které určují závazné postupy a pravidla. Dále sem řadíme také školení nebo jiné osvětové akce v oblasti informační bezpečnosti. Mezi technická opatření, která jsou někdy označována také jako fyzická nebo logická, patří například kontrola pohybu osob, které se vyskytují ve střežených prostorách, případně zamezení vstupu neoprávněných osob do těchto prostor. Také sem patří opatření související s kontrolou fyzického a logického přístupu k informačním zdrojům prostřednictvím procesů identifikace, autentizace a autorizace.[46]

Velmi často jsou opatření dělena také na preventivní, detekční a reaktivní. Cílem preventivních opatření je zabránit útočníkům v realizaci jejich úmyslů a předcházet tak různým nežádoucím aktivitám. Detekční jsou užívána k odhalení nežádoucích aktivit, na která přímo navazují opatření reaktivní, která jsou následně aplikována na zjištěné nežádoucí aktivity.[47]

---

[45] itnetwork.cz. *Lekce 1 - Základní pojmy a zásady kybernetické bezpečnosti* [online]. 2024 [cit. 2024-02-23]. Dostupné z: https://www.itnetwork.cz/bezpecnost/zakladni-pojmy-a-zasady-kyberneticke-bezpecnosti

[46] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5, s. 101.

[47] Tamtéž, s. 102.

3.1 Zásady bezpečného používání internetu

V první řadě je třeba vymezit základní zásady, které by měl mít na paměti každý uživatel internetu a moderních technologií. Již jen aplikací těchto zásad je možné zabránit velké části kybernetických hrozeb, které na internetu číhají. Nejdůležitější pravidla jsou přehledně a srozumitelně shrnuta v Základním desateru bezpečnosti na webových stránkách projektu Kybertest, jehož garantem je Česká bankovní asociace. Tento projekt, který je mimo jiné podporován i ze strany Policie České republiky a Národního úřadu pro kybernetickou a informační bezpečnost, se snaží o osvětu veřejnosti v problematice kybernetické bezpečnosti.[48]

Desatero bezpečnosti zahrnuje:

1. Zabezpečení počítače – instalace a pravidelná aktualizace antivirového programu a firewallu na nejnovější verzi
2. Zabezpečení mobilního telefonu – zabezpečení mobilního telefonu obdobným způsobem jako v případě počítače uvedeném v 1. bodě
3. Ověření původu aplikací – stahování programů a aplikací pouze z důvěryhodných a ověřených zdrojů, nejlépe přímo z oficiálních internetových obchodů Google Play či App Store po přečtení uživatelských recenzí a hodnocení u konkrétních aplikací
4. Ochrana přihlašovacích údajů – nikomu nesdělovat přihlašovací údaje a neukládat je na počítačích v rámci veřejných sítí
5. Ochrana PIN kódu – nenechávat jej v blízkosti platební karty a chránit před zneužitím
6. Bezpečné heslo – používání unikátních a silných hesel kombinujících malá a velká písmena, číslice a znaky, nepoužívat stejné heslo pro různé služby, heslo nesdílet a pokud to lze, aktivovat dvoufaktorové ověřování (2FA)
7. Neznámé e-maily, odkazy a přílohy – neotevírat e-maily, odkazy ani přílohy odeslané neznámými nebo podezřelými odesílateli

[48] Kybertest. *Buďte na internetu v bezpečí* [online]. 2024 [cit. 2024-02-24]. Dostupné z: https://www.kybertest.cz/

8. On-line nákupy – nákupy přes internet pouze u důvěryhodných a prověřených prodejců po přečtení uživatelských recenzí a hodnocení
9. Upozornění – věnovat pozornost upozorněním v počítači či upozorněním bankovních institucí
10. Komunikace s bankou – v případě podezřelých aktivit na bankovním účtu ihned informovat bankovní instituci[49]

Na webových stránkách projektu Kybertest nalezneme také seznam aktuálně nejčastějších typů podvodů v České republice, které jsou ze strany útočníků využívány. Patří mezi ně například:

- Podvodné e-maily – phishing
- Podvodné SMS zprávy – smishing
- Podvodné telefonáty údajných policistů, bankéřů či investičních poradců – vishing
- Bazarové podvody
- Podvodné webové stránky a e-shopy
- Podvodné m-platby
- Podvodné mobilní aplikace a udílení oprávnění k aplikacím
- Podvodné veřejné WiFi sítě
- Využívání uživatelů pro legalizaci výnosů z trestné činnosti[50]

Po rozkliknutí jednotlivých druhů podvodů je zde možné si o každém z nich přečíst bližší informace a také rady, jak předejít tomu, aby se uživatel nestal jednou z obětí takových podvodů. Základem úspěšné prevence proti všem typům těchto podvodů je nejen sledování technických aspektů jako je pochybné grafické zpracování, výskyt gramatických či stylistických chyb, nesrozumitelná a často strojově překládaná čeština, ale v každém případě zejména nutnost zapojení kritického myšlení, dostatečná edukace a nejvyšší možná míra obezřetnosti při jakékoli aktivitě, kterou na internetu uživatel provádí. Na první pohled zdánlivě lákavé reklamy a bezkonkurenční nabídky bývají zpravidla podvodné.

[49] Kybertest. *Základní desatero bezpečnosti* [online]. 2024 [cit. 2024-02-24]. Dostupné z: https://www.kybertest.cz/desatero-bezpecnosti-na-internetu
[50] Kybertest. *Nejčastější typy podvodů* [online]. 2024 [cit. 2024-02-24]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu

3.2 Fyzická bezpečnost

Nedílnou součástí kybernetické bezpečnosti je fyzická bezpečnost, která je velmi důležitá a mnohdy opomíjená. Ani drahá technická opatření jako jsou pokročilé antivirové programy a firewally totiž nepomohou, pokud se podaří útočníkovi osobně dostat k zařízení a pomocí USB disku na něj zkopírovat malware či z něj získat důležitá data.[51]

Fyzická bezpečnost zahrnuje širokou škálu opatření jako je zajištění perimetru, kontrola přístupu, vnitřní bezpečnost, ochrana počítačových systémů před rozebráním, úpravou, nebo připojením zařízení k vstupně výstupním portům. Kromě toho lze do fyzické bezpečnosti zahrnout i další prvky jako je ochrana před nepříznivými přírodními vlivy, dodržování elektrotechnických a požárních předpisů, zajištění vhodného prostředí pro provoz techniky či zajištění redundance.[52]

Zajištěním perimetru se v rámci fyzické bezpečnosti rozumí zabezpečení oblasti, která ohraničuje prostor, ve kterém se nachází předmětná chráněná aktiva. Perimetr lze zajistit kupříkladu elektronickými systémy pro detekci pohybu, kamerovými systémy nebo například recepcí, která je schopna identifikovat návštěvu a sledovat její pohyb v rámci chráněného prostoru. Kontrola přístupu zodpovídá za to, aby měli přístup do perimetru pouze k tomu oprávněné osoby. Možností, jak tyto přístupy kontrolovat, je celá řada. Může se jednat o klasické zámky, elektronické systémy, biometrickou identifikaci osob, systém generálního klíče či kontrolu lidskou ostrahou, přičemž vždy je možné tyto kombinovat.[53]

Ochrana prostor, ve kterých jsou umístěna chráněná aktiva, je součástí problematiky vnitřní bezpečnosti. Ta spočívá zejména v řízení přístupů do jednotlivých místností, zabezpečení chráněného prostoru v době, kdy je budova bez personálu a také v zajištění odpovídajících podmínek pro ničím nerušený provoz ICT zařízení. Jedním ze základních pravidel by měla být aplikace tzv. politiky čistého stolu a prázdné obrazovky, kdy by měl každý zaměstnanec

[51] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7, s. 411.
[52] Tamtéž.
[53] Tamtéž, s. 411-412.

při odchodu uzamknout svůj počítačový systém a nenechávat na stole žádné důležité dokumenty. Neméně důležitá pro vnitřní bezpečnost může být též instalace kamerového systému, systém pro detekci pohybu, napojení na pult centrální ochrany, klimatizace, záložní zdroj energie, kouřová čidla či vhodný hasící systém.[54]

3.3 Bezpečnost sítí a služeb

Bezpečnost počítačových sítí je klíčovým prvkem kybernetické bezpečnosti, jelikož bez efektivního zabezpečení počítačových sítí nelze účinně chránit počítačové systémy a data, která obsahují. Zabezpečení sítí zahrnuje různá opatření a technologie, jejichž cílem je minimalizovat rizika spojená s kybernetickými hrozbami a zajišťovat integritu, dostupnost a důvěrnost dat v síti. Tato opatření zahrnují například správu oprávnění a přístupových práv, šifrování dat, monitorování síťového provozu, pravidelné aktualizace softwaru a další.[55]

Autentizace

Zabezpečení sítě začíná procesem ověřování, obvykle pomocí uživatelského jména a hesla. Tento postup, který vyžaduje pouze jediný prvek pro ověření identity uživatele, kterým je uživatelské jméno a heslo/PIN, je často označován jako jednofaktorové ověření pravosti. V současné době dochází stále ve větší míře k adopci dvoufaktorové autentizace (2FA), která je dvoufázovým procesem přihlášení. Tato přidává další vrstvu zabezpečení tím, že k ověření identity vyžaduje, aby měl uživatel nejen znalost uživatelského jména a hesla, ale také například disponoval mobilním telefonem, kam je pomocí SMS zaslán autorizační kód. Třífaktorová autentizace pak ještě více posiluje zabezpečení tak, že navíc ověřuje ještě něco, co je spojeno s člověkem pomocí třetí nezávislé věci, zpravidla biometrických prvků, jako jsou otisky prstů nebo skenování sítnice, jelikož osobní věci, jako je mobilní telefon, mohou být relativně snadno odcizeny.[56]

---

[54] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7, s. 415.
[55] Tamtéž, s. 425.
[56] Peníze.cz. *Autentizační prvky a metody pod drobnohledem* [online]. 2004 [cit. 2024-02-27]. Dostupné z: https://www.penize.cz/investice/16777-autentizacni-prvky-a-metody-pod-drobnohledem

Firewall

Firewall představuje komplexní sadu bezpečnostních opatření, která mají za úkol zabránit neoprávněnému elektronickému přístupu k počítači nebo konkrétním službám v síti. Firewall může být implementován jako hardware, software nebo může kombinovat obě varianty.[57]

Instalace firewallu zvýší celkovou bezpečnost IT infrastruktury ve firmě nebo domácnosti. Pokud je správně nastaven, firewall slouží jako jediné vstupní místo, kterým musí projít veškerá komunikace. Tím chrání všechna zařízení před škodlivými příchozími daty. Firewall však také může blokovat škodlivou nebo nechtěnou odchozí komunikaci.[58]

Antivirový program

V případech, kdy selže firewall a dojde k neoprávněnému přístupu malwaru do počítače, přichází na řadu antivirový program. Jedná se o program, který může plnit jednu či více funkcí, kterými jsou například detekce a odstraňování počítačových virů, léčení infikovaných souborů, obnova a zálohování systémových oblastí na disku, uchovávání kontrolních informací o souborech na disku, poskytování informací o virech a další.[59]

Antivirových programů je na trhu celá řada, některé jsou zcela zdarma a jiné bývají zpoplatněné. Například platforma Forbes Advisor ve svém nejnovějším průzkumu porovnala aktuálně nejlepší antivirový software pro rok 2024 na základě několika faktorů, jako je jednoduchost, funkčnost nebo cena. Na prvních příčkách se umístily programy Bitdefender, Avira, AVG, McAfee, Malwarebytes, Avast, F-Secure, G DATA, Trend Micro či ESET.[60]

---

[57] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 46.

[58] Eset. *Firewall* [online]. 2024 [cit. 2024-02-27]. Dostupné z: https://www.eset.com/cz/firewall/

[59] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 19.

[60] Forbes Advisor. *The Best Antivirus Software (March 2024)* [online]. 2024 [cit. 2024-02-29]. Dostupné z: https://www.forbes.com/advisor/business/software/best-antivirus-software/

4 Aktuální trendy

S dynamickým rozvojem technologií a stále se zvyšujícím počtem kybernetických hrozeb je sledování aktuálních trendů v této oblasti klíčové pro zachování bezpečnosti a integrity dat a systémů. Mezi aktuálními trendy v oblasti kybernetické bezpečnosti v současnosti jednoznačně dominuje rozvoj umělé inteligence a strojového učení, nárůst kybernetických útoků zaměřených na IoT zařízení a cloudové platformy, technologie blockchain, rozvoj ransomware, či rostoucí důraz na ochranu soukromí a dodržování předpisů v oblasti ochrany osobních údajů.[61]

Domnívám se, že je nezbytné věnovat pozornost těmto aktuálním trendům v oblasti kybernetické bezpečnosti, jelikož znalost těchto technologií a jejich efektivní využívání může být velmi účinné v ochraně proti kybernetickým hrozbám. Umožňují uživatelům nejen rychleji a přesněji detekovat potenciální hrozby, ale také zvyšují jejich schopnost pružně reagovat na nové a stále sofistikovanější typy útoků. Zůstat informovaný o těchto trendech je proto klíčové pro efektivní obranu proti kybernetickým rizikům a organizace by je měly zařadit do programů vzdělávání svých zaměstnanců. Taktéž veřejnost by měla na základě dostatku informací pochopit, že není důvod mít z těchto technologií obavy, ale naopak, že mohou v mnoha ohledech usnadnit život.

4.1 Umělá inteligence

Tento fenomén se stal stěžejním bodem diskusí a zájmu ve všech sférách našeho života. Zprávy o umělé inteligenci neboli AI, z anglického artificial intelligence, lze slyšet ve všech médiích a odborníci z různých oblastí neustále zdůrazňují její vliv a význam. Díky AI jsme svědky revoluce v mnoha pracovních odvětvích. Zdravotnictví, finance, výroba a mnohá další již využívají AI k inovacím, automatizaci a řešení složitých problémů. Rostoucí význam AI je neoddiskutovatelný, ovlivňuje každodenní životy lidí po celém světě a přináší nové možnosti a výzvy pro budoucnost. Ačkoli AI existuje již řadu let, pokrok

[61] MasterDC. *Největší kybernetické útoky a trendy pro 2024: AI, zero trust a IoT* [online]. 2024 [cit. 2024-02-28]. Dostupné z: https://www.master.cz/blog/nejvetsi-kyberneticke-utoky-a-trendy-pro-2024-ai-zero-trust-a-iot/

v oblasti výpočetní techniky, přístup k obrovskému množství dat a vývoj nových algoritmů v posledních letech přinesly významný průlom v této oblasti.[62]

Je třeba zmínit, že jednotná definice umělé inteligence neexistuje. Jako jednu z definic lze uvést tu z knižní publikace Kybernetická (ne)bezpečnost, kde je popsána jako *„označení uměle vytvořeného jevu, který dostatečně přesvědčivě připomíná přirozený fenomén lidské inteligence“*. Americký vědec Marvin Lee Minsky, který se zabýval umělou inteligencí, ji definoval jako vědu o vytváření systémů či zařízení, která při řešení konkrétního úkolu používají postupy podobné těm, které by člověk použil, a které by byly obvykle považovány za projev lidské inteligence.[63]

Pro lepší pochopení fungování umělé inteligence je třeba osvětlit problematiku strojového učení. To se zabývá vývojem zařízení, které mají schopnost získávat znalosti z dat a adaptovat se na jejich změny. Hluboké učení, známé také jako deep learning, je disciplínou strojového učení, která umožňuje počítačům samostatně se učit nové koncepty z dostupných dat. Proces hlubokého učení je možný díky vysokému výpočetnímu výkonu a dostatečnému množství výukových dat. Základním principem umělé inteligence je pak snaha simulovat funkce lidského mozku.[64]

S rozvojem umělé inteligence lze bohužel očekávat také nové kybernetické hrozby, stále sofistikovanější útoky a vytváření autentičtějšího podvodného obsahu díky technologii deepfake, která spočívá v generování falešných videí, obrázků, hlasových zpráv nebo napodobování reálných osob. Z tohoto důvodu je možné předpokládat, že dojde k rozmachu spear-phishingu, což jsou cílené útoky na konkrétní osoby.[65]

---

[62] Evropský parlament. *Co je umělá inteligence a jak ji využíváme?* [online]. 2023 [cit. 2024-02-28]. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20200827STO85804/umela-inteligence-definice-a-vyuziti

[63] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 148.

[64] Tamtéž, s. 148-149.

[65] MasterDC. *Největší kybernetické útoky a trendy pro 2024: AI, zero trust a IoT* [online]. 2024 [cit. 2024-02-28]. Dostupné z: https://www.master.cz/blog/nejvetsi-kyberneticke-utoky-a-trendy-pro-2024-ai-zero-trust-a-iot/

Naopak umělá inteligence může hrát důležitou roli též v oblasti kybernetické bezpečnosti. Jako příklady možného využití lze uvést tvorbu pokročilých preventivních opatření, detekci malwaru na základě naučených charakteristik, monitorování síťových anomálií v reálném čase, rychlou identifikaci narušení síťové infrastruktury, aplikaci komplexních analytických metod založených na datech nebo detailní analýzu datových paketů pro odhalení škodlivých obsahů.[66]

Využití umělé inteligence se do širšího povědomí dostalo zejména rozmachem generativní umělé inteligence, která je schopná vytvářet text či obrázky. Mezi nejznámější patří chatbot ChatGPT, Microsoft Copilot nebo generátory umění Midjourney či DALL-E. Možnosti každodenního využití AI jsou ale daleko širší. Umělou inteligenci lze efektivně využít také v rámci zvyšování povědomí o kybernetické bezpečnosti, kdy uživatelům může pomoci včas rozeznat kybernetické hrozby či na míru vytvořit školení, prezentace či znalostní testy.

V současné době často využíváme řadu technologií a aplikací, aniž bychom si uvědomovali, že fungují díky umělé inteligenci. AI je často využívána k poskytování relevantních výsledků vyhledávání či individuálně přizpůsobených doporučení, například na základě našich předchozích vyhledávání nebo online nákupů. Mobilní telefony dnes již disponují virtuálními asistenty, kteří díky AI odpovídají na otázky, dávají doporučení nebo pomáhají s organizací denních úkolů. I když plně autonomní vozidla ještě nejsou běžně využívána, dnešní automobily jsou již vybaveny řadou bezpečnostních funkcí, které využívají umělou inteligenci, stejně tak jako moderní navigační systémy. Velký význam se očekává také v oblasti zdravotnictví. Vědci se snaží nalézt metody využívající umělou inteligenci k analýze rozsáhlých souborů zdravotnických dat a odhalení vzorců, které by mohly vést k novým objevům v oblasti medicíny. Pro příklad lze uvést program pro zpracování tísňových hovorů, který by měl mít schopnost rozpoznat příznaky srdeční zástavy během telefonického hovoru rychleji než pracovník operačního střediska. Nicméně stále jde pouze o špičku ledovce, vzhledem

[66] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2, s. 156.

k objemným investicím do vývoje AI lze do budoucna očekávat ještě mnohem více možností jejího využití.[67]

Dle studie University of Queensland a společnosti KPMG má 61 % lidí k umělé inteligenci rozporuplný vztah nebo jí nechtějí důvěřovat. 85 % dotázaných věří, že umělá inteligence přinese řadu výhod, ale pouze polovina z nich se domnívá, že přínosy AI převáží nad riziky. 73 % lidí je znepokojeno riziky spojenými s umělou inteligencí. Studií bylo také zjištěno, že 82 % respondentů o umělé inteligenci slyšelo, ale přibližně polovina (49 %) neví, jak a kdy se používá. Jedním z nejdůležitějších zjištění je, že 82 % dotázaných se chce o AI dozvědět více.[68]

4.2 Internet věcí

Mezi aktuálními trendy na poli kybernetické bezpečnosti nemůže chybět problematika internetu věcí. Toto velmi diskutované téma je známé zejména pod zkratkou IoT, z anglického Internet of Things. Internet věcí můžeme jednoduše definovat jako prostředí, ve kterém spolu komunikují nebo spolupracují počítače, chytrá zařízení a stroje bez potřeby lidské asistence. Jedná se o běžná zařízení, jako jsou lednice, hodinky, žárovky nebo teploměry, která se díky přidání operačního systému a připojení k internetu proměňují v chytrá zařízení a získávají tak nové možnosti využití a přínos pro každodenní aktivity.[69]

Nositelná elektronika, jako jsou chytré hodinky a fitness náramky, které monitorují zdravotní stav a kvalitu spánku či upozorňují na příchozí hovory, je jen malou ukázkou toho, co IoT přináší. V budoucnosti se chytrá zařízení budou objevovat téměř všude, od chytrého toustovače či lednice, která bude sledovat trvanlivost potravin, až po topení nebo chytrý alarm, které bude možné ovládat vzdáleně pomocí chytrého telefonu. Takovému konceptu se přezdívá chytrá

[67] Evropský parlament. *Co je umělá inteligence a jak ji využíváme?* [online]. 2023 [cit. 2024-02-28]. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20200827STO85804/umela-inteligence-definice-a-vyuziti

[68] The University of Queensland and KPMG Australia. *Trust in Artificial Intelligence: A Global Study* [online]. 2023 [cit. 2024-02-29]. Dostupné z: https://ai.uq.edu.au/project/trust-artificial-intelligence-global-study

[69] Rascasone. *Internet věcí (IoT): definice, příklady, využití, produkty* [online]. 2023 [cit. 2024-03-02]. Dostupné z: https://www.rascasone.com/cs/blog/iot-internet-veci-definice-produkty-historie#co-je-internet-vec-iacute-iot

domácnost (SmartHome) a jeho účelem je spojit jednotlivá zařízení IoT do jednoho centrálního místa, tzv. hubu, kterým bude možné všechna zařízení ovládat prostřednictvím jedné jediné aplikace.[70]

Na chytrou domácnost navazuje koncept chytrých měst, tedy SmartCities. Ten by mohl přinést lepší organizaci dopravy a zajištění bezpečnosti v ulicích měst. Pouliční osvětlení nebo semafory by bylo možné regulováno systematičtěji, stejně jako v případě SmartHome. Kontejnery by pak mohly sledovat svůj stav a informační cedule by se automaticky aktualizovaly podle momentální potřeby.[71]

Kromě výhod je však nutné vnímat i rizika, která IoT přináší. S rostoucím množstvím elektronických zařízení připojených k internetu se zvyšuje riziko phishingových a DDoS útoků.[72]

4.3 Cloud computing

Cloudové služby využívá většina z nás. Bez ohledu na to, zda jde o archivaci fotografií, sdílení dokumentů nebo přístup k datům z libovolného zařízení, cloud je ve všech těchto případech řešením. Uložení dokumentu na počítači a následné zobrazení z mobilního zařízení kdykoli a odkudkoli na světě není díky cloudu nic nemožného. Cloud představuje síť vzájemně propojených vzdálených serverů, sloužící především k ukládání a sdílení dat nebo ke spouštění aplikací a softwaru. Na rozdíl od tradičního pevného disku v počítači, kde jsou data fyzicky uložena, jsou data v cloudu umístěna v úložišti poskytovatele, ke kterému má uživatel přístup z libovolného místa a zařízení. Poskytovatel cloudových služeb je zodpovědný za provoz velkých datových center, která zajišťují bezpečnost, kapacitu a výkon. Uživatelská data tedy nejsou uložena na vlastním fyzickém serveru, ale ve vzdáleném datovém centru.[73]

---

[70] Rascasone. *Internet věcí (IoT): definice, příklady, využití, produkty* [online]. 2023 [cit. 2024-03-02]. Dostupné z: https://www.rascasone.com/cs/blog/iot-internet-veci-definice-produkty-historie#co-je-internet-vec-iacute-iot

[71] Tamtéž.

[72] Tamtéž.

[73] Algotech. *Jak funguje cloud?* [online]. 2024 [cit. 2024-03-04]. Dostupné z: https://www.algotech.cz/novinky/2021-10-27-jak-funguje-cloud

Existují tři typy cloudových služeb:

1. Privátní cloud – vhodný pro velké firmy, které si mohou dovolit vlastní cloudové centrum. Tento typ cloudu je zabezpečený a nedostanou se k němu neoprávněné osoby. Vyšší bezpečnost je však vykoupena vysokými náklady na pořízení a údržbu.
2. Veřejný cloud – poskytuje prostor pro ukládání dat, který je určen široké veřejnosti, jelikož je cenově dostupnější variantou cloudového úložiště. Uživatelé se nemusí starat o provoz a údržbu, platí jen za využitý prostor. Svá data však uživatelé musí svěřit třetí straně, což může ohrozit jejich bezpečnost.
3. Hybridní cloud – kombinuje využití privátního a veřejného cloudu. Firmy mohou mít vlastní datové centrum pro citlivá data a při nedostatku prostoru si mohou pronajmout veřejný cloud, kde platí jen za reálně využitý prostor. Tímto způsobem mohou optimalizovat náklady na využití cloudových služeb.[74]

Pomocí cloudových řešení je dnes možné ale využívat mnohem širší spektrum služeb než jen ukládání dat. Kromě cloudových úložišť je k dispozici celá řada produktů, které spadají pod označení cloud computing. Tento koncept zahrnuje poskytování počítačových technologií ve formě služeb nebo programů na internetových serverech. V této podobě uživatel není vlastníkem, ale pouze uživatelem těchto služeb.[75]

Cloud computing dále zahrnuje:

- Software jako služba (SaaS) – představuje pronájem softwaru na určitou dobu a za poplatek, namísto tradičního zakoupení licence. Tímto způsobem může uživatel využívat cloudové aplikace, jako je například Microsoft Office 365 nebo DropBox.
- Platforma jako služba (PaaS) – produkt, který využívají především vývojáři, neboť podporuje celý životní cyklus webových aplikací

[74] Algotech. *Jak funguje cloud?* [online]. 2024 [cit. 2024-03-04]. Dostupné z: https://www.algotech.cz/novinky/2021-10-27-jak-funguje-cloud
[75] Tamtéž.

od vývoje a testování přes nasazení a správu až po aktualizace. Jednou z nejznámějších forem PaaS je Google App Engine.

- Infrastruktura jako služba (IaaS) – poskytuje kompletní řešení firemního IT, které zahrnuje datové úložiště rozšířené o další hardwarové a softwarové prostředky. Tato služba nabízí veškerou infrastrukturu pro podporu webových aplikací, včetně výpočetních a síťových prostředků. Uživatel platí pouze za reálnou spotřebu dat a služeb.[76]

Mezi nesporné výhody cloud computingu patří jednoduchý upgrade softwaru, snadné klientské stanice a software, garantovaná dostupnost a zejména vcelku levný přístup k obrovskému výpočetnímu výkonu bez nutnosti jakékoli investice do hardwaru. Naopak nevýhody lze spatřovat, že k důvěrným datům, které uživatel umístí na cloud, má přístup zároveň také provozovatel daného cloudu.[77]

4.4 Blockchain

Blockchainová technologie v poslední době získává na významu především v souvislosti s kryptoměnami. Jedná se o decentralizovanou a distribuovanou databázi, která je přístupná všem uživatelům připojeným k internetu. To, že je decentralizovaná a distribuovaná znamená, že není pod kontrolou žádné centrální autority. V blockchainu jsou všichni uživatelé naprosto rovnocenní. Každá změna dat v této databázi, ať už se jedná o jejich úpravu, smazání nebo přidání nových, musí být schválena všemi uzly v síti. Díky tomu jsou všechny transakce na blockchainu považovány za bezpečné a důvěryhodné, jelikož není možné vkládat nepravdivá data nebo je upravovat ve svůj prospěch. Transakce, tedy data, jsou seskupeny do bloků. Tyto bloky jsou poté ověřeny uživateli sítě a pokud jsou v pořádku, dojde k propojení

[76] Algotech. *Jak funguje cloud?* [online]. 2024 [cit. 2024-03-04]. Dostupné z: https://www.algotech.cz/novinky/2021-10-27-jak-funguje-cloud

[77] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6, s. 33.

s předchozími bloky databáze, čímž vznikají řetězce bloků. Úspěšné připojení nového bloku k již existujícímu řetězci je poté odměněno tokeny (kryptoměnou).[78]

Největší výhoda této technologie spočívá v tom, že je zcela nezávislá na autoritách, kterými jsou v současné době například banky a které garantují důvěryhodnost transakce. Nevýhodou současného modelu je, že tato autorita může libovolně rozhodnout o omezení poskytovaných služeb v určitém regionu nebo pro určité uživatele. Dalším problémem je, že kupříkladu výpadek na straně banky může bránit uživatelům v provádění plateb. Naopak blockchain umožňuje spolehlivé transakce i mezi neznámými jednotlivci bez závislosti na autoritě, navíc bez výpadků. Dalším problémem internetu je porušování autorských práv a riziko zneužití osobních údajů. Základní principy důvěryhodnosti a konsensu, na kterých blockchain funguje, dokáží tyto problémy a rizika eliminovat, jelikož celá komunita má kontrolu nad každou transakcí a identita uživatele je chráněna privátním klíčem. Blockchain může být využit nejen k vytvoření bezpečnější digitální identity, ale také jako prostředek k boji proti korupci. Například volební hlasování by nemohlo být ovlivněno žádnou stranou, protože všechny transakce by byly zcela transparentní.[79]

5 Metody zvyšování povědomí o kybernetické bezpečnosti

Zvyšování digitální gramotnosti a povědomí o kybernetické bezpečnosti celé společnosti je klíčem k úspěšnému boji proti útokům v kyberprostoru. Vzhledem k dynamické povaze kybernetických hrozeb a rychlému vývoji technologií je nezbytné neustále aktualizovat a zdokonalovat přístupy ke vzdělávání a osvětě v oblasti kybernetické bezpečnosti. Tato kapitola přináší přehled efektivních metod, které slouží k informování a edukaci zaměstnanců a veřejnosti o nejnovějších hrozbách a úspěšné prevenci proti nim.

Význam nutnosti vzdělání v problematice kybernetické bezpečnosti podtrhuje statistika Policie České republiky, která uvádí, že kybernetická kriminalita za rok 2023 tvořila 10,8 % celkové registrované kriminality s tím,

[78] Rascasone. *Co je blockchain, jak funguje a kde najde využití?* [online]. 2023 [cit. 2024-03-08]. Dostupné z: https://www.rascasone.com/cs/blog/zmeni-technologie-blockchain-cely-svet
[79] Tamtéž.

že ačkoli počet skutků páchaných v kyberprostoru již neroste takovým tempem jako v minulých letech, tak neustále klesá objasněnost kybernetické kriminality. Bohužel na webových stránkách PČR je možné se dočíst pouze informaci, že objasněnost v této oblasti kriminality poklesla meziročně o 1,3 %.[80] Je nutné si proto dohledat stav objasněnosti za rok 2022, který činil 15,1 %. To znamená, že objasněnost kybernetických trestných činů za rok 2023 byla pouhých 13,8 %.[81] Z toho vyplývá, že je každým rokem stále obtížnější držet krok s pachateli kybernetické kriminality. Je důležité také zmínit, že u mnoha kybernetických trestných činů vůbec nedojde k oznámení skutku, ať už z důvodu výše škody, pocitu studu poškozených či právě nízké pravděpodobnosti objasnění ze strany PČR. Práce policie je bezpochyby důležitá, avšak tato řeší až důsledky dokonaného protiprávního jednání. Ještě důležitější je proto těmto hrozbám předcházet, aby k nim vůbec nedošlo. A tou nejúčinnější prevencí proti kybernetické kriminalitě je právě edukace všech uživatelů digitálních technologií.

5.1 Osvětové kampaně pro širokou veřejnost

Osvětové aktivity pro širokou veřejnost mají zásadní význam v rámci prevence proti kybernetickým hrozbám a jsou základním předpokladem pro vytváření odolnější a bezpečnější digitální společnosti. Tyto aktivity pomáhají zvyšovat povědomí a informovanost občanů o nejrůznějších hrozbách a rizicích v kyberprostoru. Díky nim jsou lidé lépe vybaveni k identifikaci možných nebezpečí. Osvětové kampaně by měly upozorňovat na konkrétní příklady kybernetických hrozeb a zároveň adresáty informovat o možnostech, jak se proti nim chránit.

Osobně si myslím, že důležitými aspekty pro úspěšnost takových osvětových aktivit je styl jejich prezentace a propagace. Užití chytlavých sloganů a kampaní se zajímavou grafikou a hudbou může pomoci získat pozornost veřejnosti a přispět tak ke zvýšení tolik důležitého povědomí o kybernetické

[80] Policie České republiky. *Vývoj registrované kriminality v roce 2023* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx
[81] STATISTIKA&MY. *Jak se vyvíjí objasněnost trestných činů v kyberprostoru?* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://www.statistikaamy.cz/2023/05/16/jak-se-vyviji-objasnenost-trestnych-cinu-v-kyberprostoru

bezpečnosti. Nezbytné je také využití propagace prostřednictvím všech dostupných médií, kterými v dnešní době mohou být zejména internet, sociální sítě, podcasty, televizní vysílání, intranet, e-maily, plakáty, billboardy, noviny nebo časopisy.

V České republice působí široké spektrum subjektů, které se aktivně podílejí na pořádání osvětových kampaní zaměřených na kybernetickou bezpečnost. Státní instituce, soukromé firmy, neziskové organizace i vzdělávací instituce, všechny tyto instituce přispívají ke zvyšování povědomí o rizicích, která přináší moderní technologie.

Policie České republiky ve svém zhodnocení roku 2023 uvádí, že svoji preventivní činnost cílila především právě na oblast kyberprostoru. V rámci 14 krajských ředitelství policie a Policejního prezidia ČR bylo uskutečněno celkem 4305 aktivit, včetně různých besed a přednášek na téma prevence kyberkriminality, během kterých bylo osloveno 198267 osob.[82]

Mezi další preventivní aktivity PČR ve spolupráci s Českou bankovní asociací a Národním úřadem pro kybernetickou a informační bezpečnost patřil III. ročník rozsáhlé celonárodní vzdělávací kampaně nazvané „#nePINdej“, která se zaměřovala na schopnost uživatelů rozpoznat phishingové stránky a pokusy o podvodné získání přístupových údajů k bankovním účtům. Tento projekt na svých webových stránkách https://www.kybertest.cz/ umožňuje široké veřejnosti vyzkoušet test zaměřený na kybernetickou bezpečnost, kde je možné si otestovat znalosti a svou obezřetnost před podvodnými SMS zprávami, e-maily a telefonáty. PČR dále pokračovala ve spolupráci se společností ČSOB na projektu „Volač a klikač“ a aktivitě s názvem „Tvoje cesta onlinem“, která byla upravena na aktuální podvodné praktiky, jako je například útok na bankovní účty, krádeže profilů na sociálních sítích či podvodné inzeráty. To vše je důkazem, že zvyšování povědomí o kybernetické bezpečnosti je prioritou jak pro Policii České republiky a Ministerstvo vnitra České republiky, tak i další státní instituce.[83]

[82] Policie České republiky. *Vývoj registrované kriminality v roce 2023* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx
[83] Tamtéž.

Jedním z nejaktivnějších subjektů v České republice, které se věnují vzdělávání v problematice kybernetické bezpečnosti, je jednoznačně výše zmíněný NÚKIB, který je zároveň gestorem kybernetické bezpečnosti v ČR. Tento má na svých webových stránkách spuštěný vzdělávací portál, který obsahuje bezplatné kurzy různého zaměření od pohádek pro nejmenší přes kurzy pro středoškoláky, úředníky, pedagogy, zdravotníky až po seniory a širokou veřejnost.[84]

NÚKIB je každoročně také pořadatelem Festivalu bezpečného internetu, což je osvětová akce plná konferencí a webinářů, kde se nejen běžní uživatelé mohou naučit, jak se správně chránit v kyberprostoru. Probíhají zde také vzdělávací aktivity pro IT experty nebo lektory. Záznamy z minulých ročníků je možné přehrát taktéž na webu NÚKIB.[85]

Osvětových projektů je v ČR celá řada. Za zmínku určitě stojí projekt sdružení CZ.NIC, které několik let vysílalo v hlavní relaci České televize dvouminutové spoty s názvem „Jak na internet“, jejichž cílem bylo zábavnou formou přiblížit televizním divákům možnosti i úskalí internetu.[86]

Osobně si myslím, že u osvětových kampaní je zásadní výběr vhodného sdělovacího prostředku dle konkrétních adresátů. Například u kampaně zaměřené na seniory bude vhodné využít televizní a rozhlasové vysílání, noviny či e-mailovou komunikaci. Naopak u mladších generací je třeba veškeré kampaně směřovat do prostředí internetu a zejména pak na nejnavštěvovanější sociální sítě, které u této cílové skupiny mají jednoznačně největší dosah. Tématu kybernetické bezpečnosti se v minulosti věnovalo hned několik českých influencerů, jako například Kovy nebo Jirka Král, který spolu s technologickou společností Avast natočil sérii videí v rámci projektu Buď safe online.[87]

---

[84] Národní úřad pro kybernetickou a informační bezpečnost. *Vzdělávací portál NÚKIB* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://osveta.nukib.cz/local/dashboard/

[85] Národní úřad pro kybernetickou a informační bezpečnost. *Festival bezpečného internetu* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=111

[86] CZ.NIC. *Jak na Internet* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://www.jaknainternet.cz/

[87] KYBEZ. *Jak vzdělávat v oblasti kyberbezpečnosti na základních a středních školách?* [online]. 2021 [cit. 2024-03-12]. Dostupné z: https://kybez.cz/jak-vzdelavat-v-oblasti-kyberbezpecnosti-na-zakladnich-a-strednich-skolach/

5.2 Vzdělávání zaměstnanců

Lidská chyba je stále nejčastější příčinou kybernetického útoku a kyberzločinci rychle využívají nedostatečného povědomí o kybernetické bezpečnosti k cíleným útokům. Pokud zaměstnanec společnosti umožní útočníkovi přístup k interním systémům firmy, mohou být veškerá technická zabezpečení k ničemu. Na zaměstnance cílí hned několik typů kybernetických útoků, včetně phishingových útoků, útoků za užití sociálního inženýrství nebo útoků typu ransomware a malware. Tyto útoky mohou probíhat různými kanály od e-mailu přes telefonáty až po platformy sociálních médií. Jejich cíl je jediný, přimět zaměstnance k vyzrazení citlivých informací nebo k instalaci škodlivého softwaru.[88]

Pochybení zaměstnance než 90 % všech úspěšných kybernetických útoků je výsledkem informací, které zaměstnanci nevědomky útočníkům poskytli. Vzhledem k tomu, že je stále obtížnější prolomit bezpečnost sítí, kyberzločinci se proto stále častěji zaměřují na zaměstnance, jelikož představují nejjednodušší způsob, jak se do sítě dostat a odcizit citlivé údaje. Zaměstnanci mají zásadní význam pro schopnost organizace fungovat bezpečně a spolehlivě, proto je nezbytné, aby zaměstnanci měli veškeré informace a znalosti, které potřebují k podpoře bezpečnosti firemní sítě a informačních systémů.[89]

5.2.1 Školení a přednášky

Existuje mnoho různých přístupů ke vzdělávání a zaučování zaměstnanců. Lidé mohou být školeni a trénováni různými způsoby, přičemž neexistuje jedno univerzální řešení. Nelze určit, která metoda je nejlepší nebo nejúčinnější, protože to, co funguje pro jeden tým nebo společnost, může být pro jinou zcela nevhodné. Stejně tak se liší i potřeby různých profesí. Výběr správné kombinace metod vzdělávání a školení by měl vždy vycházet z konkrétního povolání,

[88] MetaCompliance. *How to Promote Cyber Security Awareness and Improve Cyber Security at the Workplace* [online]. 2024 [cit. 2024-03-12]. Dostupné z: https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation

[89] Tamtéž.

podmínek, firemní kultury a dalších faktorů. Pro každý druh tréninku nebo předávané zkušenosti se hodí jiná metoda a přístup.[90]

Jedním ze způsobů, jak kybernetickou bezpečnost u zaměstnanců efektivně zařadit mezi priority, je učinit ji již součástí procesu nástupu do zaměstnání. Je také důležité zajistit, aby školení kybernetické bezpečnosti nebylo jednorázovou praxí, ale aby bylo prováděno pravidelně. Tím se posiluje význam kybernetické bezpečnosti a buduje se mezi zaměstnanci bezpečnostní kultura. Vzhledem k tomu, že zaměstnanci jsou první linií obrany, pokud jde o kybernetické útoky, jejich dobré proškolení může výrazně posílit obranyschopnost organizace. Když to shrneme, ideální je kombinovat školení vstupní, periodická a ad hoc, tedy ve výjimečných případech, kdy je to z nějakého důvodu bezodkladně nutné, například pokud dojde ke kybernetickému útoku na danou společnost.[91]

Školení a přednášky mohou probíhat formálně či prostřednictvím e-learningu. Formální školení pak mohou být vedené buď kompetentními zaměstnanci dané firmy nebo také externími instruktory. Instruktorem vedená výuka je jednou z nejtradičnějších a nejčastěji používaných metod školení zaměstnanců, při které instruktor osobně vede školení. Tento přístup obvykle zahrnuje přednášku za užití prezentace doplněné vizuálními prvky.[92]

Ideálně by se školení mělo zaměřovat na reálné situace a scénáře, se kterými se zaměstnanci mohou setkat při každodenní práci. Základem by mělo být informování o základních bezpečnostních zásadách, jako je kupříkladu pravidelná aktualizace software, zvolení dostatečně silných hesel, používání multifaktorové autentizace nebo zásady práce na dálku. Školení by také měla být pravidelně aktualizována, aby reflektovaly nejnovější trendy, technologie a hrozby v oblasti kybernetické bezpečnosti. Důležité je také zapojení zaměstnanců do praktických cvičení a simulací, které jim umožní lépe pochopit vážnost

[90] Aptien. *Způsoby školení a rozvoje zaměstnanců* [online]. 2024 [cit. 2024-07-12]. Dostupné z: https://aptien.com/cs/kb/articles/kinds-of-employee-training-and-development
[91] StickmanCyber. *How to Improve Cyber Security Awareness* [online]. 2022 [cit. 2024-07-12]. Dostupné z: https://www.stickmancyber.com/cybersecurity-blog/how-to-improve-cyber-security-awareness
[92] Aptien. *Způsoby školení a rozvoje zaměstnanců* [online]. 2024 [cit. 2024-07-13]. Dostupné z: https://aptien.com/cs/kb/articles/kinds-of-employee-training-and-development

kybernetických hrozeb a přijmout vhodná opatření. Pro pracovníky IT a bezpečnostní pracovníky jsou pak nutná pokročilá školení zaměřená na specifickou oblast, které se konkrétní zaměstnanec věnuje.[93]

Obecně by školení zaměstnanců na téma kybernetické bezpečnosti mělo být interaktivní, poutavé a informativní, aby zaměstnanci jednoznačně pochopili, co se od nich vyžaduje, a také aby zjistili význam své role při ochraně citlivých údajů organizace.

5.2.2 Testování znalostí

Základním kamenem při vzdělávání zaměstnanců často bývají již zmíněná školení v kombinaci s testováním znalostí. Cílem těchto testování je zjistit úroveň povědomí zaměstnanců o klíčových bezpečnostních tématech, což umožňuje identifikovat mezery v jejich vzdělání. Podobně jako u školení můžeme rozlišit vstupní, periodické či ad hoc testování znalostí zaměstnanců. Testování v dnešní době již bývá velmi často prováděno elektronicky prostřednictvím e-learningových portálů, kdy zaměstnanec může postupovat svým vlastním tempem a tyto testy může absolvovat i z pohodlí domova.

Výběr vhodného řešení pro testování povědomí o kybernetické bezpečnosti zaměstnanců se u každé společnosti bude lišit. Vždy je však důležité, aby uživatelé neustále dostávali přímou zpětnou vazbu. Právě tímto způsobem se učí ze svých vlastních chyb. Dalším neméně důležitým aspektem je funkce reportování, která umožňuje detailně sledovat, jak si jednotliví zaměstnanci v testech vedou a kde mají prostor pro zlepšení. Testy by také měly být stručné a výstižné, čím méně času testování zabere, tím pravděpodobněji se zaměstnanci zapojí a udrží pozornost. Důraz je dále potřeba klást na pravidelnost testování, podobně jako u školení. Obsah testů je pak třeba přizpůsobit aktuálním

[93] MetaCompliance. *How to Promote Cyber Security Awareness and Improve Cyber Security at the Workplace* [online]. 2024 [cit. 2024-07-15]. Dostupné z: https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation

potenciálním hrozbám, kterými mohou být phishing, smishing, sociální inženýrství, ransomware a podobně.[94]

5.2.3 Penetrační testování

Mnoho organizací pro zvýšení povědomí o kybernetické bezpečnosti aplikuje různé druhy školení a testování zaměstnanců, avšak ani tato kombinace nemusí být dostatečná. Často se totiž tato školení a testování zaměřují pouze na teorii a nedokáží tak vybudovat dostatečné povědomí o kybernetické bezpečnosti a proces reakce na incidenty. Kromě školení a testování je proto důležité, aby zaměstnanci zažili kybernetické incidenty v praxi prostřednictvím penetračního testování.

Penetrační testy, které lze přirovnat k mystery shoppingu, simulují skutečné scénáře. Mohou například prověřit fyzickou bezpečnost společnosti tím, že se předem domluvený figurant pokusí pronést USB disky do firmy nebo se dostat k nějakému počítači či jinému zařízení. Velmi často se pak prostřednictvím simulovaných útoků prověřuje, jak jsou zaměstnanci připraveni na techniky sociálního inženýrství nebo spear phishing, což je cílený typ phishingu. O samotném penetračním testování předem obvykle ví jen několik vybraných interních osob a předchází mu detailní smlouva a analýza.[95]

Na základě toho, kolik zaměstnanců podlehlo kupříkladu simulovanému phishingovému útoku, může organizace určit, zda je třeba věnovat větší pozornost phishingu během příštího školení o kybernetické bezpečnosti, nebo zda své zdroje bude věnovat posílení povědomí o jiných aspektech kybernetické bezpečnosti. Penetrační testování je skvělým způsobem, jak otestovat obranyschopnost organizace, a to nejen po technické stránce, ale i po té organizační. Simulované kybernetické útoky může provádět jak interní, tak i externí tým.[96]

---

[94] Guardey. *The 8 best cyber security awareness tests for employees* [online]. 2024 [cit. 2024-07-20]. Dostupné z: https://www.guardey.com/security-awareness-test/

[95] Eset. *7 způsobů jak posílit znalosti zaměstnanců o kybernetické bezpečnosti* [online]. 2020 [cit. 2024-07-20]. Dostupné z: https://www.eset.com/cz/blog/prevence/7-zpusobu-jak-posilit-znalosti-zamestnancu-o-kyberneticke-bezpecnosti/

[96] StickmanCyber. *How to Improve Cyber Security Awareness* [online]. 2022 [cit. 2024-07-20]. Dostupné z: https://www.stickmancyber.com/cybersecurity-blog/how-to-improve-cyber-security-awareness

Jak bylo zjištěno v rámci rozhovorů se zástupci různých subjektů, kteří se věnují tématu kybernetické bezpečnosti, tyto simulované útoky jsou velmi účinným prvkem zvyšování povědomí o kybernetické bezpečnosti napříč všemi organizacemi. Velmi důležité pak také je poskytnutí okamžité zpětné vazby těm zaměstnancům, kteří simulovanému útoku podlehli. Tímto způsobem si zaměstnanci nejlépe zapamatují svá pochybení a sníží se tak i pravděpodobnost, že podobnou chybu v budoucnu zopakují.

5.2.4 Kanály pro dotazy a hlášení incidentů

Jedním z dalších užitečných aspektů pro zlepšení celkové obranyschopnosti organizace proti kybernetickým útokům může být zřízení kanálu pro dotazy či hlášení kybernetických incidentů. Může se například jednat o e-mailovou adresu či portál v rámci intranetu, kam zaměstnanci mohou posílat své dotazy nebo přeposílat podezřelé zprávy. Tento speciálně určený e-mail či portál povzbudí zaměstnance, aby se nebáli ptát na otázky, na které by se jinak nezeptali. Je důležité, aby tento e-mail spravovali výhradně IT experti, kteří mu budou věnovat pravidelnou pozornost. Tito odborníci pak mohou prověřovat obdržené podezřelé zprávy a pomáhat tak uživatelům rozpoznat škodlivý obsah. Trpělivost při odpovídání na dotazy je klíčová, jelikož pečlivě zpracované odpovědi lze využít při následných školeních či přednáškách v rámci celé organizace. Nadstavbou pak mohou být kanály s FAQ, které zaměstnancům umožní rychlé zodpovězení často kladených otázek.[97]

5.2.5 Programy motivace a odměňování

Velmi důležitým prvkem pro zvýšení edukace zaměstnanců v oblasti kybernetické bezpečnosti jsou programy odměňování a motivace zaměstnanců. Správně nastavené motivační programy mohou významně přispět k vyšší angažovanosti zaměstnanců. Tyto programy by měly být strukturované tak, aby zaměstnanci byli motivováni k dodržování bezpečnostních postupů, neustálému vzdělávání v oblasti nových kybernetických hrozeb a proaktivnímu

[97] Eset. *7 způsobů jak posílit znalosti zaměstnanců o kybernetické bezpečnosti* [online]. 2020 [cit. 2024-07-25]. Dostupné z: https://www.eset.com/cz/blog/prevence/7-zpusobu-jak-posilit-znalosti-zamestnancu-o-kyberneticke-bezpecnosti/

hlášení jakýchkoliv bezpečnostních rizik. Odměny pak mohou zahrnovat finanční i nefinanční benefity, které posilují jejich ochotu podílet se na ochraně firemních dat a systémů. Jednotlivci či pracovní týmy mohou být oceněny například za příkladné plnění bezpečnostních postupů, včasné ohlašování bezpečnostních incidentů či samostudium problematiky.[98]

5.2.6 Audit kybernetické bezpečnosti

Audit kybernetické bezpečnosti nabízí komplexní analýzu stavu kybernetické ochrany dané organizace. Jeho cílem je poskytnout přehledné a srozumitelné hodnocení interních procesů a zabezpečení informačních technologií, a zároveň navrhnout komplexní strategii pro zajištění souladu společnosti s příslušnými směrnicemi, aktuálně zejména s evropskou směrnicí NIS2, která bude platit od 1. ledna 2025 a bude přímo vyžadovat pravidelné provádění auditů kybernetické bezpečnosti u více než 6 tisíc subjektů v České republice. Výsledkem bezpečnostního auditu je zpráva zahrnující zjištěné informace, doporučení a návrhy akčních plánů.[99]

5.3 Další metody vzdělávání

Tato kapitola se zaměřuje na vzdělávací metody a aktivity, které přesahují tradiční formy školení a osvěty. Zahrnuje konference, workshopy, soutěže a také aktuálně velmi populární gamifikaci, jejichž účelem je, aby účastníky nejen informovaly, ale také aktivně zapojily do procesu učení. Vzhledem k tomu, že všechny tyto interaktivní aktivity lze efektivně využít jak pro edukaci široké veřejnosti, tak i pro vzdělávání zaměstnanců firem různého zaměření, rozhodl jsem se jim věnovat samostatnou kapitolu, aby se tyto metody neopakovaly v rámci obou předchozích kapitol.

[98] Jenpráce. *Efektivní a dlouhodobá motivace zaměstnanců* [online]. 2024 [cit. 2024-07-27]. Dostupné z: https://www.jenprace.cz/magazin/efektivni-a-dlouhodoba-motivace-zamestnancu#anchorId0

[99] CETIN. *Audit kybernetické bezpečnosti* [online]. 2024 [cit. 2024-07-27]. Dostupné z: https://www.cetin.cz/nis2/nase-sluzby/audit-kyberneticke-bezpecnosti

5.3.1 Konference

Konferencí rozumíme formální setkání, kterého se zpravidla zúčastní větší množství lidí. Účastníci zde, někdy i po dobu více dní, diskutují o různých nápadech nebo problémech týkajících se konkrétního tématu, v tomto případě kybernetické bezpečnosti.[100]

V České republice se každoročně pořádá hned několik konferencí, které jsou zaměřeny na téma kybernetické bezpečnosti. Tyto konference přináší pro účastníky několik benefitů, ať už se jedná o získání kontaktů, networking nebo výměnu zkušeností a praktických rad.

Za zmínku stojí například konference Security, organizovaná společností Aricoma, jejíž historie sahá až do roku 1992, a která je největší nezávislou událostí svého druhu v České republice. Každý rok se konference účastní kolem 600 účastníků včetně odborníků z veřejného i soukromého sektoru, kteří se zaměřují na aktuální otázky v oblasti bezpečnosti informačních a komunikačních technologií.[101]

Jako další lze uvést konferenci s názvem Kybernetická bezpečnost, která letos nese označení KB12, jelikož se koná již 12. ročník. Za touto konferencí stojí česká pobočka asociace AFCEA ve spolupráci s Policejní akademií České republiky v Praze a Národním úřadem pro kybernetickou a informační bezpečnost. Konference je zaměřená na aktuální trendy a hrozby v oblasti kybernetické bezpečnosti.[102]

Do třetice bych zmínil konferenci Future Forces Forum, která není primárně zaměřená na kybernetickou bezpečnost, nýbrž na oblast obrany a bezpečnosti jako celku. Konference zahrnuje výstavy, workshopy či panelové diskuze, kterých se účastní představitelé ozbrojených a bezpečnostních sborů, členové Parlamentu ČR, vládních institucí, státní správy, samosprávy,

---

[100] Britannica. *Conference* [online]. 2024 [cit. 2024-08-02]. Dostupné z: https://www.britannica.com/dictionary/conference

[101] Security. *O konferenci* [online]. 2024 [cit. 2024-08-02]. Dostupné z: https://konferencesecurity.cz/o-konferenci

[102] AFCEA. *Konference Kybernetická bezpečnost KB12* [online]. 2024 [cit. 2024-08-04]. Dostupné z: https://afcea.cz/akce/kb12/

vědeckovýzkumných center i univerzit. Letošní ročník se bude mimo jiné zabývat aktuálními tématy, jako je kybernetická obrana a bezpečnost, disruptivní technologie nebo umělá inteligence.[103]

5.3.2 Workshopy

Tento čím dál populárnější pojem pochází z angličtiny, kdy se zpravidla jedná o seminář nebo jiný typ vzdělávací aktivity ve formě tvůrčího pracovního setkání. Obvykle má předem stanovený program, během kterého lektor předává své znalosti nebo jiným způsobem školí účastníky. Workshopy jsou často zaměřeny na prohloubení dovedností v určité specializované oblasti. Workshopy mohou být přizpůsobeny různým úrovním znalostí, od začátečníků po pokročilé odborníky. Obzvláště užitečné jsou pro organizace, jelikož umožňují zaměstnancům prohloubit své dovednosti a tím zvýšit obranyschopnost celé firmy. Workshopy bývají organizovány odborníky z oblasti IT bezpečnosti nebo specializovanými vzdělávacími institucemi, které nabízejí praktické a přizpůsobené tréninky pro různé skupiny uživatelů. Mohou probíhat jak offline, tak i online ve formě webinářů.[104]

5.3.3 Soutěže

Jak se říká, člověk je tvor od přírody soutěživý, proto jsou soutěže v oblasti kybernetické bezpečnosti ideální formou vzdělávání. Tím, že využívají přirozenou touhu po vítězství, zvyšují motivaci účastníků a zároveň podporují hlubší zapojení do učení. Ať už se jedná o zařazení soutěží do vzdělávacích programů v rámci firem nebo o celorepublikové soutěže týkající se kybernetické bezpečnosti, v obou případech mohou soutěže sehrát významnou roli při edukaci. V České republice je každoročně pořádáno několik soutěží pro širokou veřejnost.

Jednou z nejznámějších je národní soutěž Kyber cena roku pořádaná Centrem kybernetické bezpečnosti. Mezi hlavní cíle této soutěže patří snaha o propojení různých organizací z komerčního, státního i akademického sektoru

[103] Future Forces Forum. *Koncept* [online]. 2024 [cit. 2024-08-04]. Dostupné z: https://future-forces-forum.org/homepage/concept?lang=cs
[104] IT slovník. *Co je to workshop?* [online]. 2024 [cit. 2024-08-05]. Dostupné z: https://it-slovnik.cz/pojem/workshop

s cílem posílit celkovou odolnost české společnosti v oblasti kybernetické bezpečnosti a obrany, inspirace dalších organizací, manažerů a zaměstnanců, aby kybernetické bezpečnosti věnovali zvýšenou pozornost a úsilí, zvyšování povědomí o důležitosti kybernetické bezpečnosti a dále také podpora a motivace mladých talentů, kteří se zajímají o oblast kybernetické bezpečnosti. Soutěží se v několika kategoriích, konkrétně Kyber organizace roku, Kyber manažer roku, Kyber projekt roku, Kyber talent roku, Kyber učitel roku.[105]

Dalším velmi zajímavým projektem je Soutěž v kybernetické bezpečnosti, za kterou opět stojí Centrum kybernetické bezpečnost spolu s NÚKIB. Tato soutěž je součástí iniciativy evropské komise European Cyber Security Challenge, kterou realizuje Evropská agentura pro bezpečnost sítí a informací (ENISA). Soutěž je určena pro všechny studenty základních, středních a vysokých škol v České republice ve věkové kategorii 9 až 24 let, bez ohledu na zaměření školy. V rámci soutěže vznikají materiály, které mohou sloužit nejen středoškolským pedagogům jako cenné metodické pomůcky při výuce studentů v oblastech kybernetické bezpečnosti, informačních a komunikačních technologií či programování.[106]

Soutěže pro zaměstnance pořádané ve firmách představují zábavný způsob, jak obohatit tradiční metody vzdělávání. Interní materiály z přednášek a školení mohou být například využity k vytvoření kvízů, kde účastníci soutěží o drobné ceny. Tyto soutěže nejenže zpestří proces vzdělávání, ale také umožní firmě zjistit, jak dobře zaměstnanci ovládají potřebné znalosti. Jako příklad lze uvést společnost Eset, která každoročně vyhlašuje znalostní soutěž, ve které se obvykle soutěží o unikátní designová trika, která vyhrají tři nejlepší zaměstnanci, Soutěž je rozdělena na dvě obtížnosti, jednu pro IT specialisty a druhou pro ostatní zaměstnance.[107]

---

[105] Kyber cena roku. *O projektu* [online]. 2024 [cit. 2024-08-08]. Dostupné z: https://www.kybercena.cz/o-projektu/

[106] Soutěž v kybernetické bezpečnosti. *Soutěž v kybernetické bezpečnosti* [online]. 2024 [cit. 2024-08-08]. Dostupné z: https://www.kybersoutez.cz/ks_soutez.html

[107] Eset. *7 způsobů jak posílit znalosti zaměstnanců o kybernetické bezpečnosti* [online]. 2020 [cit. 2024-08-09]. Dostupné z: https://www.eset.com/cz/blog/prevence/7-zpusobu-jak-posilit-znalosti-zamestnancu-o-kyberneticke-bezpecnosti/

5.3.4 Gamifikace

Gamifikace je novým fenoménem ve vzdělávání, který zahrnuje integraci herních prvků do procesu učení. Tyto prvky zahrnují systémy odměn, soutěže, stanovení cílů a motivaci k dosažení vzdělávacích výsledků. Koncept gamifikace vychází z poznatku, že aplikace herních mechanismů může zvýšit motivaci a zapojení studentů a tím zlepšit jejich učební výsledky.[108]

V oblasti vzdělávání existují dva hlavní přístupy spojené s hraním her, kterými jsou gamifikace a výuka založená na hře. Gamifikace se zaměřuje na vkládání herních prvků do již existujících vzdělávacích procesů, kdy je využíváno systémů odměn, soutěžení a dalších herních mechanismů ke zvýšení motivace adresátů. Na druhé straně výuka založená na hře se soustředí na vytváření specifických her, které cílí na výuku určitých teorií nebo konceptů. Tyto hry jsou navržené tak, aby studenty zaujaly a umožnily jim interaktivní učení prostřednictvím samotného hraní.[109]

Přínosů gamifikace ve vzdělávání je hned několik:

- Zvýšení motivace studentů
- Dynamické učení prostřednictvím interaktivních úkolů
- Podpora spolupráce a týmové práce
- Personalizace učebního procesu
- Rozvoj schopností kritického myšlení a řešení problémů
- Zlepšení sociálních a komunikačních dovedností
- Vyšší zapojení studentů do procesu učení a dosažení cílů[110]

Gamifikace má značný potenciál pro zlepšení vzdělávání, podporu učení a rozvoj důležitých dovedností. Při správném plánování a řízení může být gamifikace efektivní a atraktivní metodou, jak dosáhnout vzdělávacích cílů a motivovat k aktivnímu a angažovanému učení.[111]

---

[108] EPALE – Elektronická platforma pro vzdělávání dospělých v Evropě. *Země zázraků ve vzdělávání – hry a gamifikace* [online]. 2023 [cit. 2024-08-10]. Dostupné z: https://epale.ec.europa.eu/cs/blog/zeme-zazraku-ve-vzdelavani-hry-gamifikace
[109] Tamtéž.
[110] Tamtéž.
[111] Tamtéž.

5.4 Výuka ve školách

S ohledem na to, že děti a mladí lidé začínají užívat moderní technologie již od útlého věku, vzdělávání v oblasti kybernetické bezpečnosti se stává stále důležitější součástí moderního vzdělávacího procesu. Školy mají klíčovou roli při edukaci studentů spočívající v porozumění základním principům kybernetické bezpečnosti, rozpoznávání hrozeb či osvojování si správných postupů pro ochranu sebe a svých dat.

Bohužel samotné Ministerstvo školství, mládeže a tělovýchovy (MŠMT) se tématu vzdělávání v problematice kybernetické bezpečnosti v posledních letech nevěnuje a ani nevydává žádné materiály ke vzdělávání dětí a mládeže. Naposledy vydalo článek v březnu 2021, kdy pandemie koronaviru přesunula výuku ze školních lavic do distanční formy v online prostředí. Tuto oblast má tak za státní správu na starosti zejména Národní úřad pro kybernetickou a informační bezpečnost.[112]

NÚKIB, gestor kybernetické bezpečnosti v ČR, na svých webových stránkách k tématu vzdělávání v oblasti kybernetické bezpečnosti ve školách uvádí, že na úrovni mateřských, základních a středních škol se zaměřuje zejména na prevenci, která pomáhá žákům vytvářet základní návyky pro bezpečné používání internetu a digitálních technologií. V oblasti vysokého školství se pak soustředí na správu seznamu vysokoškolských oborů zaměřených na kybernetickou bezpečnost a na výuku předmětů, které sami garantují nebo kde působí jako hostující přednášející. Aktivně se také zapojují do odborných panelů v oblasti vzdělávání a přispívají k rozvoji Rámcových vzdělávacích programů. NÚKIB rovněž koordinuje činnost metodiků prevence, prostřednictvím kterých pak poskytuje kontaktní výuku jak pro školy, tak i další organizace, které o to projeví zájem. Podrobněji o kontaktní výuce pojednává kapitola 5.4.5.[113]

[112] Ministerstvo školství, mládeže a tělovýchovy. *MŠMT a NÚKIB k digitalizaci vzdělávání a kyberbezpečnosti* [online]. 2021 [cit. 2024-08-11]. Dostupné z: https://msmt.gov.cz/msmt-a-nukib-k-digitalizaci-vzdelavani-a-kyberneticke

[113] Národní úřad pro kybernetickou a informační bezpečnost. *Školy* [online]. 2024 [cit. 2024-08-12]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/

K samotnému začlenění tématu bezpečného internetu do výuky NÚKIB využívá nástroje nazvaného rozcestník pro učitele, který odkazuje na svůj vzdělávací portál s různými materiály podporujícími výuku kybernetické bezpečnosti, který byl již zmíněn v rámci kapitoly 5.1. Na tomto portálu je možné vyfiltrovat čtyři možnosti, kterými jsou kurzy určené pro veřejnost, pro školy, pro zdravotnictví a pro úřady. V tomto případě nás zajímá záložka pro školy, kde se nachází několik kurzů s různým zaměřením. Jednotlivé kurzy budou popsány v následujících podkapitolách.[114]

5.4.1 Mateřské školy

V dnešní době jsme ze všech stran obklopeni digitálními technologiemi, které jsou již tak běžné, že i malé děti s nimi denně přicházejí do styku. Proto je důležité začít s výukou bezpečného používání těchto technologií už u dětí v předškolním věku, tedy v mateřských školách. NÚKIB pro pedagogy v mateřských školách připravil několik aktivit pro začlenění kybernetické bezpečnosti do výuky, včetně sady her, které hravou formou přibližují dětem téma kybernetické bezpečnosti. Pro předškoláky jsou pak na vzdělávacím portálu NÚKIB připraveny Kyber pohádky.[115]

5.4.2 Základní školy

Základní školy hrají zásadní roli při začleňování témat kybernetické bezpečnosti do výuky. Žáci by zde měli získat základní dovednosti, jak správně pracovat s technologiemi, bezpečně využívat sociální sítě a také jak se vyhnout závislosti na nich. Pro pedagogy základních škol pak NÚKIB připravil rozcestník vzdělávacích materiálů, který nabízí přehled různých výukových zdrojů, jež mohou ve své výuce využít. Stejně jako u předškoláků je k dispozici sada her a interaktivních aktivit, které pomáhají žákům lépe pochopit zásady bezpečného používání digitálních technologií a sociálních sítí, jako je například edukativní komiksový Instagram, který za užití komiksů představuje různé nástrahy internetu.

[114] Národní úřad pro kybernetickou a informační bezpečnost. *Nabízené kurzy pro školy* [online]. 2024 [cit. 2024-08-14]. Dostupné z: https://osveta.nukib.gov.cz/local/dashboard/?tag_id=21

[115] Národní úřad pro kybernetickou a informační bezpečnost. *Mateřské školy* [online]. 2024 [cit. 2024-08-15]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/materske-skoly/

Ve vzdělávacím portálu NÚKIB jsou pro žáky 1. i 2. stupně základních škol k dispozici rovnou čtyři kurzy, rozdělené podle ročníků.[116]

5.4.3 Střední školy

Střední školy poskytují ještě širší možnosti pro začlenění kybernetické výuky, jelikož lze předpokládat, že studenti již ovládají základní technologické dovednosti. Z tohoto důvodu se zde mohou věnovat i náročnějším tématům, jako je sexting nebo závislosti. Mnozí se také začínají více zaměřovat na informační technologie či specificky na kybernetickou bezpečnost. NÚKIB zde opět nabízí rozcestník pro učitele středních škol, který obsahuje přehled vzdělávacích materiálů z oblasti kybernetické bezpečnosti, které jsou vhodné jak pro studenty se všeobecným zaměřením, tak i pro ty specializující se na IT. V České republice totiž řada středních škol umožňuje kromě obecného IT zaměření studovat přímo obor Kybernetická bezpečnost. Pro příklad lze uvést Smíchovskou střední průmyslovou školu a gymnázium v Praze nebo Střední školu informatiky, poštovnictví a finančnictví v Brně.[117]

5.4.4 Vysoké školy

Na vysokých školách se otevírá prostor pro hlubší a komplexnější studium, kdy se navazuje na nabyté znalosti ze základních a zejména pak středních škol. Studenti zde mohou dále prohloubit své znalosti a začít se specializovat na konkrétní oblasti kybernetické bezpečnosti. V rámci vysokých škol je důležité, aby byly vyučovány aktuální a relevantní informace. Studenti by měli mít příležitost pracovat na projektech, účastnit se stáží nebo se zapojit do simulací bezpečnostních incidentů. Tím se podporuje nejen jejich odborný růst, ale také připravenost na profesionální kariéru v oblasti kybernetické bezpečnosti. Studium oboru, který se specializuje na kybernetickou bezpečnost, dnes umožňuje řada veřejných i soukromých českých vysokých škol, například Masarykova univerzita v Brně v rámci bakalářského studijního programu

[116] Národní úřad pro kybernetickou a informační bezpečnost. *Základní školy* [online]. 2024 [cit. 2024-08-15]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/zakladni-skoly/

[117] Národní úřad pro kybernetickou a informační bezpečnost. *Střední školy* [online]. 2024 [cit. 2024-08-15]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/stredni-skoly/

nebo České vysoké učení technické v Praze v rámci magisterského navazujícího studijního programu.

5.4.5 Kontaktní vzdělávání a činnost preventistů

Pod pojmem kontaktní vzdělávání se neskrývá nic jiného než tradiční forma výuky pomocí přednášek a seminářů, která staví na osobním setkání studentů a lektorů. Kontaktní výuku lze využít nejen při vzdělávání žáků, ale i pedagogů a rodičů. Podle studie organizace Kraje pro bezpečný internet žáci preferují, aby témata kyberkriminality a bezpečného chování na internetu přednášeli především pedagogové (40 % žáků) a policisté (32,7 % žáků). Kontaktní vzdělávání v oblasti kybernetické bezpečnosti v ČR umožňuje řada organizací a subjektů, které jsou schopny kontaktní výuku témat, jako je kybergrooming, kyberšikana nebo netolismus, zajistit. Jednotlivé osoby, které působí v oblasti prevence a jejichž pracovní náplní je zvyšování povědomí o kybernetické bezpečnosti nejen mezi žáky a pedagogy, se označují jako metodici prevence nebo preventisté. Těmito preventisty mohou být například příslušníci odborů tisku a prevence Policie České republiky, manažeři prevence kriminality, školní koordinátoři prevence, zaměstnanci Probační a mediační služby, metodici preventivních aktivit nebo zaměstnanci zařízení pro preventivně výchovnou péči. NÚKIB vytvořil pomocí služby Moje mapy společnosti Google přehled organizací a subjektů v ČR, které pro veřejnost poskytují kontaktní vzdělávání. Zájemci o přednášku metodiků prevence si tak mohou odpovídající subjekt najít v této mapě, zkontaktovat jej a domluvit se na zorganizování vzdělávací akce.[118]

5.5 Inspirace v zahraničí

Koncepty zvyšování povědomí o kybernetické bezpečnosti, které jsou aplikovány v ostatních zemích světa, mohou sloužit jako cenný zdroj inspirace. Tyto modely lze přizpůsobit podmínkám v České republice a tím zvýšit efektivitu edukace české veřejnosti v oblasti digitální gramotnosti.

[118] Národní úřad pro kybernetickou a informační bezpečnost. *Kontaktní vzdělávání* [online]. 2024 [cit. 2024-08-16]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/kontaktni-vzdelavani/

Abychom měli představu o tom, které země jsou nejúspěšnější v boji proti kybernetickým hrozbám, můžeme využít například nedávnou studii společnosti mixmode.ai. Za účelem zhodnocení globální situace na poli kybernetické bezpečnosti tato společnost navzájem porovnala 70 zemí světa, kdy použila kombinaci dat a výsledků několika indexů, jako je National Cyber Security Index (NCSI), Global Cybersecurity Index (GCI) či Cybersecurity Exposure Index (CEI). Na základě těchto zdrojů pak bylo vypočítáno měřitelné skóre pro každou zemi. Žebříčku vévodí severské země Finsko, Norsko a Dánsko, které jsou dále následovány Austrálií, Velkou Británií, Švédskem, Rakouskem, Japonskem, Spojenými státy americkými a Kanadou. Tyto země mají vybudovanou robustní infrastrukturu zaměřenou na kybernetickou bezpečnost. Na chvostu tabulky se pro zajímavost umístila Bolívie, Honduras a Venezuela.[119]

Kybernetické hrozby jsou rostoucím problémem po celém světě, včetně severských zemích, jako je Dánsko, Norsko a Švédsko. Tyto země proto přijímají proaktivní opatření k zajištění kybernetické bezpečnosti. Například v Dánsku vláda zahájila Národní strategii pro kybernetickou a informační bezpečnost, která zahrnuje iniciativy na zvýšení povědomí o kybernetických hrozbách, zlepšení IT bezpečnosti ve firmách a organizacích a také posílení spolupráce mezi vládními agenturami a soukromým sektorem. Norsko také zavedlo několik opatření na zlepšení online bezpečnosti, včetně zřízení Národního centra kybernetické bezpečnosti (NCSC) a zvyšování povědomí veřejnosti prostřednictvím vzdělávacích kampaní. Švédsko spustilo program kybernetické bezpečnosti, který je součástí širší strategie na vybudování bezpečné a odolné digitální infrastruktury.[120]

Švédský Stockholm je také každoročně dějištěm konference Nordic IT Security, která již 17 let propojuje odborníky v oblasti kybernetické bezpečnosti z celé Skandinávie. Partnery konference jsou přední světové společnosti

[119] ETCIO. *Cybersecurity Ranking 2024: Which countries are most at risk?* [online]. 2024 [cit. 2024-08-17]. Dostupné z: https://ciosea.economictimes.indiatimes.com/news/security/cybersecurity-ranking-2024-which-countries-are-most-at-risk/110730038

[120] Lyca Mobile. *Staying safe online in the Nordic Countries: A comprehensive guide* [online]. 2024 [cit. 2024-08-17]. Dostupné z: https://www.lycamobile.se/blog/en/staying-safe-online-in-the-nordic-countries-a-comprehensive-guide/

zabývající se kybernetickou bezpečností, jako například Crowdstrike, Zscaler, SentinelOne nebo Cloudflare.[121]

V rámci kybernetických velmocí nelze vynechat Spojené státy americké, kde od roku 2004 vyhlašuje prezident Spojených států a Kongres měsíc říjen jako Cybersecurity Awareness Month, kdy se veřejný a soukromý sektor společně zaměřují na zvyšování povědomí o důležitosti kybernetické bezpečnosti. Tento nápad následně převzaly země po celém světě, z tohoto důvodu se v říjnu v mnoha zemích konají konference a další aktivity různého druhu věnující se vzdělávání v oblasti ochrany proti kybernetickým hrozbám.[122]

Navzdory své rozloze lze digitální supervelmocí označit také Estonsko. Estonští občané vyřídí téměř veškerou agendu online a například i volby zde probíhají elektronicky. V současné době je výuka kybernetické bezpečnosti na estonských základních a středních školách bohužel součástí výhradně volitelných předmětů, jako je informatika nebo tzv. národní obrana. Různé prvky kybernetické bezpečnosti byly však začleněny i do jiných povinných předmětů, jako například matematika nebo společenské vědy. Učební plán kurzu národní obrany dokonce koordinuje ministerstvo obrany a žáci si zde osvojují znalosti v oblastech, jako jsou aktualizace, firewally, zálohování, šifrování, VPN či zabezpečení chytrých zařízení. V Estonsku se také pořádá mnoho soutěží v kybernetické bezpečnosti, kdy tyto iniciativy zahájilo zejména estonské ministerstvo obrany prostřednictvím programu „Cyber Olympic“ zaměřeného na mladé talenty. Estonsko také pořádá jedno z největších cvičení kybernetické bezpečnosti s názvem „Locked Shields“.[123]

Jedním ze společných znaků všech kybernetických velmocí jsou masivní investice do kybernetické bezpečnosti a digitalizace. V České republice průzkum NÚKIB odhalil významné rozdíly v úrovni připravenosti a investic do kybernetické bezpečnosti napříč různými sektory, kdy nejvyšší úroveň investic

[121] Nordic IT Security. *Nordic IT Security* [online]. 2024 [cit. 2024-08-18]. Dostupné z: https://nordicitsecurity.com/

[122] Cybersecurity and Infrastructure Security Agency. *Cybersecurity Awareness Month* [online]. 2024 [cit. 2024-08-18]. Dostupné z: https://www.cisa.gov/cybersecurity-awareness-month

[123] Medium. *Výuka kybernetické bezpečnosti v Estonsku a České republice* [online]. 2021 [cit. 2024-08-19]. Dostupné z: https://medium.com/edtech-kisk/v%C3%BDuka-kybernetick%C3%A9-bezpe%C4%8Dnosti-v-estonsku-a-%C4%8Desk%C3%A9-republice-bfb1fa9c9015

byla zaznamenána v energetice a průmyslu, kde 63 % dotázaných vyjádřilo spokojenost s přidělenými prostředky. Zdravotnictví vykázalo určitá zlepšení, avšak 61 % respondentů stále považuje finanční prostředky za nedostatečné. Bohužel studie také zjistila, že veřejný sektor stále čelí nedostatku finančních zdrojů a odborných kapacit. Investice do kybernetické bezpečnosti jsou klíčovým faktorem nejen pro úspěšnou obranu proti kybernetickým hrozbám, ale také efektivní vzdělávání veřejnosti v této problematice.[124]

6 Analýza současného stavu a návrhy na zlepšení

Na základě zjištěných informací lze konstatovat, že ačkoli se povědomí o kybernetické bezpečnosti v České republice postupně zlepšuje, stále čelíme několika významným výzvám a je zde prostor pro další rozvoj. Je pravdou, že se zvyšuje počet osvětových iniciativ, do kterých se zapojují jak státní instituce, tak i soukromé společnosti nebo neziskové organizace, avšak jedním z hlavních problémů zůstává nedostatečná koordinace těchto aktivit. Když jednotlivé kampaně probíhají nezávisle na sobě, často se stává, že se zaměřují na podobné problémy, zatímco jiné, stejně důležité oblasti, jsou opomíjeny. Tento nedostatek koordinace vede k nerovnoměrnému pokrytí důležitých témat a oslabuje celkovou efektivitu snah o zvyšování kybernetického povědomí. Navíc, pokud je veřejnost vystavena příliš mnoha podobným kampaním od různých subjektů, může dojít k dezorientaci a snížení pozornosti věnované těmto iniciativám. Dalším problémem je také dlouhodobá udržitelnost. Mnoho kampaní zaměřených na osvětu v oblasti kybernetické bezpečnosti má bohužel jednorázový charakter, kdy jim chybí dlouhodobý plán. To často vede k tomu, že jakmile kampaň skončí, její dopad na veřejnost rychle zmizí nebo se o ní veřejnost dokonce ani vůbec nedozví.

Řešením těchto problémů by mohla být existence centrálního subjektu, který by všechny iniciativy efektivně koordinoval. NÚKIB, který se o tuto roli od svého vzniku v roce 2017 snaží, dle mého názoru odvádí dobrou práci ve všech oblastech kybernetické bezpečnosti, včetně vzdělávání.

[124] CZ Defence. *Kybernetická bezpečnost České republiky v roce 2023: Výzvy a trendy* [online]. 2021 [cit. 2024-08-19]. Dostupné z: https://www.czdefence.cz/clanek/kyberneticka-bezpecnost-ceske-republiky-v-roce-2023-vyzvy-a-trendy

Přesto však zůstávají oblasti, kde je prostor pro zlepšení. Je nutné sjednotit všechny osvětové aktivity pod jednotnou strategii, která by zajistila zaměření na prioritní oblasti a jasné rozdělení rolí mezi jednotlivými subjekty. Tento koordinovaný přístup by vedl k efektivnějšímu využití finančních, lidských a technologických zdrojů a zároveň by zlepšil spolupráci a komunikaci mezi všemi zúčastněnými stranami.

Také si myslím, že NÚKIB by měl zlepšit svou prezentaci a výrazněji zviditelnit svou činnost. Dle mého názoru poměrně velká část české populace stále není obeznámena s existencí tohoto úřadu. Modernizace webových stránek, aktivnější působení na sociálních sítích, spolupráce se známými osobnostmi a investice do propagace a marketingových kampaní by mohly zvýšit povědomí o činnosti tohoto subjektu a jeho významu pro kybernetickou bezpečnost v ČR. Dále by bylo přínosné, kdyby se NÚKIB stal centrálním styčným bodem nejen pro organizace, ale i pro jednotlivce, kteří hledají spolehlivé informace a podporu v oblasti kybernetické bezpečnosti. Zvýšení povědomí o NÚKIB a jeho činnosti by mohlo přispět k celkově lepší informovanosti obyvatelstva v oblasti kybernetické bezpečnosti.

Webové stránky a sociální sítě NÚKIB by mohly hrát klíčovou roli v poskytování snadno dostupných a srozumitelných informací o kybernetických hrozbách, preventivních opatřeních, základních bezpečnostních zásadách a nejnovějších trendech v oblasti kybernetické bezpečnosti. Pro maximální efektivitu by bylo užitečné, kdyby se obsah těchto platforem průběžně aktualizoval a rozšiřoval o nové materiály, které by byly přizpůsobeny různým cílovým skupinám, včetně jednotlivců, škol, malých podniků i velkých organizací. Kromě základních informací by webové stránky mohly nabízet i širší škálu vzdělávacích materiálů. To by mohlo zahrnovat interaktivní kurzy, které by poskytovaly praktické dovednosti v oblasti kybernetické bezpečnosti, stejně jako prezentace a podklady určené pro učitele a lektory, kteří chtějí integrovat tuto problematiku do výuky. Postupné rozšiřování databáze vzdělávacích materiálů by mohlo zahrnovat i tematicky zaměřené moduly, které by byly navrženy pro různé úrovně znalostí, od základní orientace až po pokročilé strategie kybernetické ochrany.

Pro zvýšení interaktivity a přístupnosti by mohla být rovněž přínosná implementace chatbotu na bázi umělé inteligence, který by byl schopen nepřetržitě poskytovat uživatelům rady, tipy a odpovědi na běžné otázky. Tento chatbot by mohl nabídnout praktickou pomoc v reálném čase, například v situacích, kdy se uživatelé setkají s potenciálním kybernetickým útokem, stanou se obětí podvodu nebo potřebují informace o aktuálních bezpečnostních hrozbách. Tímto způsobem by NÚKIB mohl vytvořit komplexní a uživatelsky přívětivou platformu, která by efektivně sloužila jako hlavní zdroj informací a podpory v oblasti kybernetické bezpečnosti pro širokou veřejnost.

Mezi další užitečné prvky by například mohly patřit:

- Aktuální zprávy a varování – sekce s pravidelně aktualizovanými zprávami o aktuálních kybernetických hrozbách, útocích a varováních
- Portál pro hlášení incidentů – uživatelé by mohli přímo na stránkách hlásit podezřelé aktivity, kybernetické útoky nebo bezpečnostní incidenty
- Návody a tutoriály – detailní návody a tutoriály, jak krok za krokem nastavit bezpečnostní opatření, jako jsou firewally, antivirové programy, šifrování dat, nebo jak správně používat VPN
- Sekce pro rodiče a pedagogy – speciální sekce zaměřená na kybernetickou bezpečnost pro děti a mladistvé, která by obsahovala materiály pro rodiče a učitele, jak chránit děti online, včetně přehledů o nebezpečných hrách, aplikacích nebo trendech
- Komunitní fórum a FAQ – prostor, kde by mohli uživatelé sdílet své zkušenosti, diskutovat o aktuálních tématech a hledat rady od ostatních. Součástí by mohla být i rozsáhlá sekce často kladených otázek s podrobnými odpověďmi
- Pravidelné webináře a online školení – uživatelé by se mohli přihlásit na pravidelné online kurzy, webináře a školení vedené odborníky z NÚKIB, kde by se probíraly aktuální otázky kybernetické bezpečnosti

7 Strukturované rozhovory

Pro praktickou část této diplomové práce byly zvoleny strukturované rozhovory, tedy jedna z kvalitativních výzkumných metod. Po důkladném uvážení se tato metoda jeví jako nejvhodnější vzhledem k tématu celé diplomové práce, které spočívá v analýze metod zvyšování povědomí o kybernetické bezpečnosti. Rozhovory mají oproti dotazníkovému šetření řadu výhod, které v tomto případě mohou poskytnout přidanou hodnotu v podobě většího množství podrobnějších informací získaných od respondentů, případně možnost upřesnění jejich odpovědí na předem položené otázky.

Byla provedena série celkem šesti rozhovorů, konkrétně se třemi zaměstnanci státní sféry a třemi zástupci soukromého sektoru. Účelem je vzájemné porovnání postojů jednotlivých organizací ve vztahu ke kybernetické bezpečnosti. Důležité je zmínit, že náplní práce všech šesti respondentů je mimo jiné právě osvěta v oblasti kybernetické bezpečnosti. Mají tak možnost se přímo podílet na zvyšování míry edukace ostatních zaměstnanců v této problematice. Tyto rozhovory poskytly cenný pohled na aktuální stav povědomí a postupy používané k zajištění kybernetické bezpečnosti v jejich organizacích.

V rámci státní sféry jsem oslovil příslušníka Policie České republiky, zaměstnance Okresního soudu v Kladně a také zástupce územní samosprávy. Ze soukromé sféry jsem se pak zaměřil na zaměstnance dvou největších mobilních operátorů působících na území České republiky a dále zaměstnance jedné z největších pojišťoven u nás.

Tato rozmanitost respondentů umožnila získat komplexní pohled na to, jak se organizace v obou sférách vypořádávají s rostoucím množstvím kybernetických hrozeb, a jaké strategie a opatření používají k ochraně svých digitálních aktiv. Všem šesti respondentům bylo položeno osm totožných předem definovaných otázek ve stejném pořadí. Použití stejných otázek pro všechny respondenty umožňuje přímé porovnání jejich odpovědí, kde lépe vyniknou podobnosti nebo naopak rozdíly v jejich názorech, zkušenostech či preferencích. Položení totožných otázek všem zúčastněným také umožňuje lépe zajistit rovné podmínky a usnadňuje analytický proces.

Respondentům byly položeny následující otázky:

1. Můžete popsat instituci, kde jste v současné době zaměstnán/a? Na jaké pozici zde působíte?
2. Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?
3. Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?
4. Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?
5. Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?
6. Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?
7. Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro státní/soukromou správu obecně?
8. Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

7.1 Státní sféra

Kapitola věnovaná respondentům ze státní sféry obsahuje tři rozhovory se zaměstnanci, kteří se věnují problematice kybernetické bezpečnosti a metodám jejího zvyšování v prostředí veřejné správy. Ve státní sféře se setkáváme s unikátními výzvami a požadavky na kybernetickou bezpečnost, jelikož veřejné instituce zajišťují důležité služby pro společnost a disponují též citlivými daty svých občanů či neveřejnými nebo dokonce utajovanými informacemi, jejichž vyzrazení by v krajním případě mohlo poškodit zájmy České republiky.

7.1.1 Respondent 1 – Okresní soud v Kladně

Můžete popsat instituci, kde jste v současné době zaměstnán? Na jaké pozici zde působíte?

„Okresní soud v Kladně je s bezmála 120 soudci a zaměstnanci největším okresním soudem ve Středočeském kraji. Rozhoduje jako soud prvního stupně ve věcech trestních a civilních s výjimkou specializované agendy, kterou vykonává odvolací Krajský soud v Praze. Já zde působím jako správce informačních a komunikačních technologií."

Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?

„Na pozici správce informačních a komunikačních technologií působím již 16 let. Mám na starosti správu serverů, stanic, tiskáren, IP telefonů, síťových prvků a ostatních prostředků výpočetní techniky ve vlastnictví zaměstnavatele, dále také zodpovídám za podporu koncových uživatelů a údržbu dokumentace."

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Kybernetická bezpečnost je důležitou součástí každodenního provozu. Podílím se na implementaci nařízení vyplývajících ze zákona a také vyhlášek a nařízení Ministerstva spravedlnosti České republiky a dalších organizací, jako je například Národní úřad pro kybernetickou a informační bezpečnost."

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„V rámci ochranných opatření je u nás aplikována blokace používání neznámých přenosných úložišť, jako jsou USB flash disky nebo externí datové disky a dále také používání antivirové a antispamové ochrany. Kontrola a řízení provozu je pak prováděna prostřednictvím lokálního a centrálního firewallu."

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„Po přijetí musí každý nový zaměstnanec úspěšně absolvovat vstupní test, který zkoumá jeho povědomí o kybernetické bezpečnosti a schopnosti reagovat na potenciální hrozby. Vždy jednou ročně u nás také probíhá plošný test kybernetické bezpečnosti a při akutních hrozbách jsou všichni zaměstnanci seznámeni prostřednictvím nahodilých upozornění pomocí e-mailu či intranetu, případně ad hoc školení."

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Dle mého názoru je současný systém školení a upozornění na kybernetické hrozby, včetně seznámení s konkrétními příklady hrozeb, dostačující. Nikdy však nelze zcela zabránit možné kybernetické hrozbě, vždy to závisí do jisté míry na individuální odpovědnosti uživatele."

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro státní správu obecně?

„Periodicky opakující se školení a osvěta je velmi důležitá. Stále je však nutné, aby i jednotliví uživatelé při své práci přemýšleli a sami vyhodnocovali možná rizika a chovali se zodpovědně. Při školeních nikdy nejde postihnout všechny možnosti, navíc se neustále objevují nové a důmyslnější kybernetické hrozby."

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„Současný stav vzdělávání v problematice kybernetické bezpečnosti je dle mého názoru zcela nedostatečný. Otázku kybernetické bezpečnosti bych rozhodně navrhoval zapracovat již do učiva pro základní školy. Mezi dospělými mladších generací si myslím, že je osvěta na poměrně dobré úrovni. Naopak v rámci starších generací je osvěta zcela nedostatečná, snadno se stávají obětí různých phishingových nebo jiných útoků."

7.1.2 Respondent 2 – Policie České republiky

Můžete popsat instituci, kde jste v současné době zaměstnán? Na jaké pozici zde působíte?

„Jsem příslušníkem Policie České republiky, konkrétně na odboru obecné kriminality pod Úřadem služby kriminální policie a vyšetřování, kde působím v týmu pro boj se zneužíváním dětí online. Dále také působím jako externí vyučující na dvou vysokých školách."

Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?

„Na této konkrétní pozici působím jeden rok, avšak předtím jsem pracoval jako vyšetřovatel mravnostní kriminality páchané v kyberprostoru. Náplň mojí práce je především metodická činnost na tomto úseku a prvotní šetření k obětem této kriminality. Co se týče působení na vysokých školách, jsem lektorem předmětů počítačová kriminalita a informační bezpečnost."

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Kybernetická bezpečnost je velmi důležitý aspekt de facto u každé pracovní role, kde se setkáváme s počítačovými systémy. Co se týče mé pozice, každý den se setkávám s důležitými interními daty, takže bezpečnost a ochrana těchto dat je velmi důležitá."

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„Ta škála ochranných opatření je široká, zabezpečení počítačových systémů a celkově dat v organizaci je velmi důležité. Avšak jaká konkrétní ochranná opatření využíváme, to není tak úplně otázka na mou osobu a musel by na ni odpovědět některý z kolegů, který má na starosti problematiku kybernetické bezpečnosti, kde se přímo zaměřuje na organizační a technická opatření v rámci naší organizace."

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„Naše organizace poměrně nedávno zavedla e-learning v oblasti kybernetické bezpečnosti v rámci našeho služebního intranetu, který však funguje na bázi dobrovolnosti. Taktéž jsou pořádány kurzy celoživotního vzdělání pro všechny příslušníky organizace."

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Rozhodně by bylo zapotřebí více školení, avšak vzhledem k časovým možnostem se domnívám, že dosavadní úroveň je i tak na velmi dobré úrovni. Samozřejmě je třeba neusnout na vavřínech a věnovat se kybernetické bezpečnosti nadále, nicméně si myslím, že je třeba taktéž nezapomínat na bezpečnost fyzickou, která přímo souvisí s tou kybernetickou."

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro státní správu obecně?

„Školení a osvěta v tomto poměrně novém tématu je nesmírně důležitá. Dle mého prevence v rámci kybernetické bezpečnosti zastává de facto nejdůležitější oblast vůbec. V dnešní době, kdy se kybernetické hrozby stávají stále sofistikovanějšími, je potřeba, aby s nimi byl každý zaměstnanec obeznámen a věděl, jak se proti nim bránit."

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„Dle mého názoru stav vzdělávání v České republice, co se týče kybernetické bezpečnosti, není ideální a je rozhodně co zlepšovat. Stále se setkávám s lidmi, kteří například vůbec nevědí, co je dvoufázové ověření účtu a podobné důležité prvky. Je třeba osvětu cílit i na laickou veřejnost, což poté přímo souvisí s kybernetickými útoky typu phishing a dalších."

7.1.3 Respondent 3 – Statutární město Kladno

Můžete popsat instituci, kde jste v současné době zaměstnán? Na jaké pozici zde působíte?

„Statutární město Kladno je městem s rozšířenou působností. Zastávám zde funkci vedoucího Odboru bezpečnostních rizik a IT outsourcingu a zároveň působím v roli manažera kybernetické bezpečnosti a pověřence pro ochranu osobních údajů."

Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?

„Na této pozici působím již 5 let. Náplní mé práce je zajišťování a aplikování kybernetické, informační a fyzické bezpečnost v celé šíři, což znamená řízení kybernetické bezpečnosti a ochrany osobních údajů v působnosti města a organizací městem řízených nebo založených. Dále spolupracuji s Městskou policií Kladno ohledně řízení změn MKDS, tedy Městského kamerového dohlížecího systému a CCTV včetně návrhu klíčových aspektů nových technologií."

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Téma kybernetické bezpečnosti je v dnešní digitální době velmi důležité, obzvlášť pro manažery kybernetické bezpečnosti odpovědné za řízení bezpečnosti dané organizace. Zaměřuji se primárně na ochranu informací a dat organizace před hrozbami, které na nás v současné době dopadají. Povinnosti zahrnují vedení bezpečnostních opatření, sledování hrozeb a zranitelnosti, vypracování bezpečnostních politik a školení. Hlavním úkolem je flexibilita reakce na incidenty, spolupráce s dalšími subjekty a následné zvyšování bezpečnosti organizace. Má role vyžaduje technickou zdatnost, ale také schopnost komunikace s netechnickými zaměstnanci, a hlavně vedením města. Sleduji bezpečnostní události, snažím se minimalizovat rizika a hledám další způsoby, jak neustále zlepšovat kybernetickou bezpečnost naší organizace. Myslím si, že pro trvalé zlepšování je klíčová metoda PDCA. Je možné konstatovat, že jsem součástí boje proti stále se vyvíjejícím hrozbám v digitálním světě.

V současné geopolitické situaci, kdy nárůst kybernetických útoků na infrastrukturu je skutečně enormní a legislativní rámec nás v říjnu 2024 ustanoví skrze směrnici NIS2 povinnou osobou, je ochrana dat skutečně důležitým posláním.“

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„Naše organizace disponuje jak technickými, tak organizačními opatřeními. Mezi základní a nejúčinnější technické aspekty mohu zařadit zálohování, pravidelné aktualizace software, ochranu sítě a pokročilou ochranu proti hrozbám. Popsat to můžeme jako několikavrstvé zabezpečení organizace. Pokud budeme směřovat na koncového uživatele, můžeme mluvit o perimetru, kde je NGFW neboli Next Generation Firewall, který je sám o sobě základním aspektem ochrany. Následně není jiné možnosti než při vzdáleném připojení využívat VPN v kombinaci s 2FA. Dalším technickým opatřením je zavedení monitoringu a zde je rozdíl v postavení privilegovaný user a user, kdy u privilegovaného uživatele je vždy zaznamenávána obrazovka a monitoruje se, co vykonává v prostředí, kdežto user je jen logován. Veškerá koncová zařízení, koncové stanice a servery jsou osazeny takovým řekněme antivirovým systémem, jde o systém včetně sandboxu a platformy EDR, tedy ochrany koncových bodů. Je také zaveden systém ochrany před únikem informací v síti (DLP) a systém PAM pro zabezpečení identit. Všechna naše koncová zařízení jsou navíc šifrována. Co se týče organizačních opatření v rámci naší organizace, pořádáme pravidelná školení na téma kybernetické bezpečnosti a pravidelně informujeme zaměstnance o aktuálních hrozbách. Dále je důležitá také pravidelná obměna uživatelských hesel. Provádíme také phishing kampaně, testování zranitelnosti a penetrační testování. V rámci všech ochranných opatření postupujeme v souladu s doporučeními NÚKIB a zákonem o kybernetické bezpečnosti.“

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„Dochází k pravidelnému vzdělávání stanovenému bezpečnostní politikou. Jedná se zpravidla o roční cykly, které jsou, v případě zjištění nějakého

pochybení, doplněné dodatečným proškolením všech zaměstnanců. V oblasti kybernetické bezpečnosti je v naší organizaci prováděno vstupní a pak opakované školení, které je vždy zakončeno testem. V rámci vzdělávání vždy kladu důraz na to, že bezpečnost začíná u každého doma a že je třeba být ke všemu dostatečně kritický.“

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Ze strany vedení je třeba podpora a zároveň tlak na uživatele, protože bez zájmu uživatele a s myšlenkou, že všechno vím, se špatně vzdělává. Ze své osobní zkušenosti mohu říct, že pravidelné schůzky skrze platformu Teams považuji již za přežité, lidé často pouze předstírají, že poslouchají a přínos je proto nulový. Co se týče e-learningu, je to obdobné, opět zde sleduji nezájem lidí, odmítání a stížnosti na komplikovanost. Zde je však pro splnění povinnosti skvělá dokumentace o průchodu uživatele školením. Dle mého je však stále ze všeho nejužitečnější osobní školení.“

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro státní správu obecně?

„Kybernetická bezpečnost začíná u každého jednotlivce doma. Bez vzdělávání to prostě nejde a je úplně jedno, zda se jedná o státní nebo soukromou sféru.“

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„V rámci ČR existuje hodně komunit a také vzdělávacích zařízení v oblasti kybernetické bezpečnosti. Myslím, že se stav obecně zlepšuje. NÚKIB nebo CZ.NIC nabízejí možnost vzdělávání i pro širokou veřejnost a platí reklamy v TV, kde ukazují nejčastější hrozby na internetu. Otázkou zůstává, zda má veřejnost chuť se vzdělávat. Všichni dle mého fungují, až když se někomu něco stane a pak se ptají a diví se. Je to stejné jako, když mi někdo řekne, že on není zajímavý, tak proč by ho někdo měl sledoval a podobně, jenže všichni máme nějakou cenu. Je důležité mluvit a sdělovat široké veřejnosti, co se děje,

jaká jsou rizika a jaká jsou možná opatření. Je to stejné jako, když nám říkali v dětství, abychom se rozhlíželi u přechodu, zkrátka od dětství se po nás všech chtělo, abychom vyhodnocovali možná rizika. Teď je potřeba mluvit i o těch kybernetických, co nejsou na první pohled vidět. Nejčastějším příkladem je, když za mnou lidé chodí s tím, že jim někdo odcizil během pár minut e-mailovou schránku nebo účet na Facebooku, LinkedIn nebo jiné službě a pláčou, že nic nemají. Ale proč? Protože mají všude stejné heslo a nikde nemají zapnuté 2FA. Jenže tohle přesně může v krajním případě přerůst až k průniku do informačního systému zaměstnavatele.“

7.1.4 Zhodnocení rozhovorů

Prostřednictvím tří rozhovorů se zástupci státní sféry bylo možné zjistit, že ačkoli každý působí v naprosto odlišné organizaci zabývající se úplně jinou agendou, existuje v rámci kybernetické bezpečnosti několik přístupů, ochranných opatření a výukových metod, které aplikují všechny organizace bez rozdílu. Jedná se především o zákaz používání externích datových úložišť, zajištění ochrany proti kybernetickým útokům pomocí firewallu a antivirových programů a zvyšování povědomí o kybernetické bezpečnosti prostřednictvím různých druhů školení.

Co se týče rozdílů, je patrné, že pouze u Policie České republiky neexistují žádná vstupní ani jiná povinná školení pro zaměstnance v problematice kybernetické bezpečnosti, což mohu potvrdit, jelikož sám působím na základním článku PČR.

7.2 Soukromá sféra

Tato kapitola přináší pohled z opačné perspektivy. Skrze rozhovory se třemi zaměstnanci soukromé sféry zjistíme, jakým způsobem se v rámci jejich organizací aktivně podílejí na ochraně před kybernetickými útoky, a jaké metody zvyšování povědomí v praxi užívají pro lepší vzdělanost zaměstnanců v oblasti kybernetické bezpečnosti. Díky těmto rozhovorům získáme ucelený pohled na strategie jednotlivých soukromých společností v boji proti současným kybernetickým hrozbám.

7.2.1 Respondent 1 – T-Mobile Czech Republic a.s.

Můžete popsat instituci, kde jste v současné době zaměstnán? Na jaké pozici zde působíte?

„T-Mobile Czech Republic a.s. je největší telekomunikační společnost v České republice, která poskytuje nejen základní služby v podobě mobilního či fixního volání, ale i služby pro firemní zákazníky, jako je housing datových center, bezpečnostní služby a podobně. Já konkrétně působím na pozici senior specialista informační bezpečnosti se zaměřením na řízení kontinuity podnikání, krizové řízení a plnění role manažera kybernetické bezpečnosti.“

Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?

„Na této pozici působím od roku 2021. Hlavní náplní mé práce je především tvorba krizového plánování, provádění analýz dopadů, včetně plánů kontinuity a jejich testování. Všechny tyto dokumentace pak reálně využíváme v praxi při krizových situacích. Další náplní je zajištění souladu se zákonem o kybernetické bezpečnosti a vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti.“

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Jelikož naplňuji roli manažera kybernetické bezpečnosti, která vyplývá ze zákona, tak kybernetická bezpečnost je každodenní součástí mého pracovního dne. Aktuálně v naší společnosti probíhá i příprava na přijetí nového zákona o kybernetické bezpečnosti, který musí vycházet ze směrnice Evropské unie, tzv. NIS2.“

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„Naše společnost musí naplňovat veškerá bezpečnostní opatření, která vyplývají ze zákona a vyhlášky o kybernetické bezpečnosti. Tato opatření stanovuje Národní úřad pro kybernetickou a informační bezpečnost, který také provádí hloubkové kontroly pro ověření, zda postupujeme dle pokynů v zákoně

a vyhlášce. Mezi opatření, které implementujeme, abychom zajistili odolnost vůči kybernetickým hrozbám, patří především detekční systémy, antimalware systémy, procesy zvládání kybernetických incidentů, řízení rizik, řízení kontinuity, penetrační testování a samozřejmě vzdělávání našich zaměstnanců v oblasti kybernetické bezpečnosti.“

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„Každý zaměstnanec musí na pravidelné bázi projít bezpečnostním školením. V našem prostředí využíváme formu e-learningu na naší interní vzdělávací platformě. Kurz je online formou se závěrečným testem a vydáním certifikátu. Dále se snažíme reagovat na aktuální hrozby a trendy v oblasti kybernetické bezpečnosti prostřednictvím tzv. interní sociální sítě, kde zveřejňujeme aktuality, upozornění a novinky z oblasti kybernetické bezpečnosti. Neméně důležitým aspektem je i reálné testování, jako jsou phishingové kampaně nebo simulace spoofingu na naše zaměstnance za účelem získat přístupové údaje. Jednou ročně také pořádáme „Security Days“ – jedná se o třídenní akci, kde provádíme školení zábavnou formou a pořádáme odborné diskuze (např. Security days - Jak se cítit bezpečněji v kybernetickém prostoru? - YouTube) a mnoho dalšího.“

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Oblast vzdělávání musí proaktivně reagovat na nové hrozby, proto je důležité, aby byl v organizacích určen vždy jeden zaměstnanec, který se bude naplno věnovat oblasti vzdělávání ostatních zaměstnanců. Můj osobní pohled je takový, že ne každá organizace takového zaměstnance má určeného. Každý zaměstnanec by se měl podílet na zachování kybernetické bezpečnosti dané organizace a myslím si, že investice do vzdělávání je jedním z nejefektivnějších způsobů, jak tohoto cíle dosáhnout. To je za mě určitě krok, který by v boji proti kybernetickým hrozbám obecně velmi pomohl.“

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro soukromou správu obecně?

„Jak jsem již uvedl v předchozí otázce, vzdělávání je ten nejúčinnější nástroj, jak předcházet kybernetickým útokům. Pokud bude každý znát charakteristiku jednotlivých útoků a dokáže je rozpoznat, bude zároveň schopen se mu zcela vyhnout. Pomocí školení v každém vzbudíte ostražitost a potřebu ověřovat si informace, které se zaměstnancům dostanou pod ruce. Celá organizace je vždy silná tak, jak je silný její nejslabší článek, což většinou bývá právě zaměstnanec. Základní postupy, jakými jsou uzamykání počítače nebo telefonu při odchodu z pracovního místa, ověřování odesílatele e-mailů, zdržení se rozkliknutí podezřelého odkazu nebo odolnost vůči možnému vydírání ze strany útočníků, jsou základní aspekty, které by měl každý znát a dodržovat.“

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„Společnost bych, co se týče oblasti kybernetické bezpečnosti, rozdělil do tří skupin – děti, dospělí a senioři. Pokud se podíváme na seniory, jde o nejvíce ohroženou skupinu, které je třeba se věnovat. I z tohoto důvodu jsme v rámci naší společnosti implementovali do aplikace Můj T-Mobile sekci „bezpečnost“, která obsahuje základní informace včetně zábavného kvízu pro osvětu a vzdělávání nejen seniorů. V rámci svého zaměstnaní také provádím školení problematiky kybernetické bezpečnosti pro základní školy a zde musím říct, že jsem často velmi překvapen, kolik toho dětí znají a jak rychle a efektivně dokážou rozpoznat rizika. U dospělých jedinců ve věku cca 30-50 let to bývá rozporuplné, zhruba půl na půl. Je to ale generace, která se nebojí zeptat, pokud si není jistá, což je za mě velmi správný přístup.“

7.2.2 Respondent 2 – O2 Czech Republic a.s.

Můžete popsat instituci, kde jste v současné době zaměstnána? Na jaké pozici zde působíte?

„Pracuji v telekomunikačním odvětví u společnosti O2 Czech Republic a.s., která je druhou největší telekomunikační společností v České republice a je poskytovatelem kompletního spektra informačních a komunikačních služeb. Působím zde na pozici Business Continuity Manager v rámci oddělení s názvem Informační bezpečnost & BCM.“

Jak dlouho jste již zaměstnána na této pozici a jaká je náplň Vaší práce?

„Na této pozici jsem zaměstnána necelý rok a půl, od září 2022. Mám za úkol implementovat, udržovat a rozvíjet systém Business Continuity Management. Všechny činnosti vyplývají z normy ISO 22301, přičemž mezi hlavní činnosti patří například analýza dopadů BIA, tvorba Business Continuity plánů a Disaster Recovery plánů, jejich aktualizace a testování. Kromě toho spolupracuji s útvarem Customer Network Operation Centre, který provádí dohled nad službami, a tím pádem řídí krizový management.“

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Kyberbezpečnost je součástí mého zaměstnání. Mít zavedený systém BCM vyplývá přímo ze zákona o kybernetické bezpečnosti.“

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„Využíváme všechna organizační a technická opatření, která jsou uvedena v zákoně o kybernetické bezpečnosti, potažmo ve vyhlášce o kybernetické bezpečnosti. V rámci nového zákona o kybernetické bezpečnosti se chystá rozdělení subjektů na subjekty s režimem vyšších nebo nižších povinností. Jakožto subjekt kritické infrastruktury bude společnost O2 Czech Republic a.s. spadat do režimu vyšších povinností, a bude tak muset plnit přísnější požadavky.“

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„V rámci naší společnosti funguje tzv. Virtuální univerzita, ve které jsou vytvořena školení pro interní zaměstnance. Většinou je to buď ve formě prezentace nebo interaktivního kurzu. Pro ukončení školení je potřeba splnit test. Zároveň vydáváme články na intranetu, které se týkají aktuálních kybernetických událostí a obecně kybernetické bezpečnosti. V minulém roce proběhlo i gamifikované školení, což v praxi znamená, že zaměstnanec se učí tím, že hraje hru. Je to kombinace tradičního výukového obsahu v kombinaci s prvky hry."

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Obecně si myslím, že aktivity týkající se povědomí o kybernetické bezpečnosti jsou častější a klade se na ně větší důraz, tím pádem je awareness v O2 na vysoké úrovni. Nicméně, podle mého názoru, chybí v naší firmě i školení zaměřené na kyberbezpečnost formou workshopu nebo přednášky, kterých by se zaměstnanci účastnili osobně a obecně by školení byla více interaktivní."

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro soukromou správu obecně?

„Za mě je vzdělávání v této oblasti jednou z nejdůležitějších aktivit. Lidé/zaměstnanci musí vědět, co za incidenty jim potenciálně hrozí, jak se proti nim bránit a hlavně, jak jim předcházet. Co se týká důležitosti školení, tak záleží, o jaké úrovni se bavíme, ale obecně by se, podle mého názoru, mělo začínat u široké veřejnosti a největší důraz pak dávat na školení zaměstnanců subjektů kritické infrastruktury."

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„Podle mě se o kyberbezpečnosti začíná více mluvit a začíná se to brát více v potaz. S tím, že se rozvíjí kybersvět a s ním přichází i sofistikovanější útoky, je důležité, aby byli všichni, veřejná správa, soukromý sektor i široká veřejnost, připraveni."

7.2.3 Respondent 3 - Allianz pojišťovna, a.s.

Můžete popsat instituci, kde jste v současné době zaměstnán? Na jaké pozici zde působíte?

„Pracuji v soukromé společnosti Allianz pojišťovna, a.s., která je součástí největšího světového pojišťovacího koncernu Allianz Group. V současné době zastávám pozici Protection & Resilience Specialist.“

Jak dlouho jste již zaměstnán na této pozici a jaká je náplň Vaší práce?

„Na této pozici působím téměř 2 roky. Mám na starosti oblast Business Continuity Management, fyzickou bezpečnost, řízení incidentů a další aktivity z oblasti informační bezpečnosti.“

Jaký je Váš vztah k tématu kybernetické bezpečnosti ve Vaší pracovní roli? Je kybernetická bezpečnost a ochrana dat důležitou součástí Vašeho zaměstnání?

„Tématu kybernetické bezpečnosti se v rámci své pracovní role intenzivně věnuji, neboť kybernetické incidenty, jako jsou útoky ransomware, úniky dat a narušení IT představují největší obavy nejen pro naši, ale také ostatní společnosti. S tímto také úzce souvisí nebezpečí přerušení činností, kterému se plně věnuji.“

Jaká ochranná opatření proti kybernetickým hrozbám využívá Vaše organizace?

„Mezi opatření, která naše společnost využívá, patří aktivní brány firewallu, vulnerability management, monitoring síťového provozu a detekce anomálií, školení zaměstnanců a incident management.“

Můžete popsat některé konkrétní příklady školení nebo jiných osvětových akcí, které Vaše organizace poskytuje zaměstnancům v oblasti kybernetické bezpečnosti?

„Ano, v rámci zvyšování povědomí o kybernetické bezpečnosti děláme pravidelné phishingové kampaně, a to plošné nebo cílené. Poté bych zmínil CySAM (Cyber Security Awareness Month), kdy v rámci tohoto měsíce pořádáme

soutěže a také setkání s naším týmem tak, abychom naši práci přiblížili všem zaměstnancům společnosti.“

Jak by podle Vás mohla organizace ještě více zlepšit a zdokonalit své aktivity v oblasti zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci?

„Z mého hlediska je klíčové, aby pracovníci v oblasti bezpečnosti byli viditelní. To platí jak na pracovišti, tak i během akcí pořádaných společností. V případě, že dojde k nějakému incidentu, je důležité, aby lidé věděli, na koho se obrátit. A poté jsou samozřejmě důležité rozsáhlé phishingové kampaně, které je třeba dělat nejen plošně, ale také cíleně na vybrané zaměstnance.“

Jaký je Váš osobní názor na důležitost školení a osvěty v oblasti kybernetické bezpečnosti pro Vaši organizaci a pro soukromou správu obecně?

„Toto vnímám jako velmi důležitou součást vzdělávání v rámci organizace u všech zaměstnanců, a to nejen v rámci naší organizace, ale obecně u všech organizací, jak soukromých, tak také státních, neboť informační systémy jsou čím dál více využívané a je třeba, aby uživatelé tyto informační systémy využívali správně a hlavně bezpečně, protože tím chrání sebe i organizaci, v níž pracují.“

Jaký je Váš osobní názor na současný stav vzdělávání v oblasti kybernetické bezpečnosti mezi širokou veřejností?

„V této oblasti dle mého názoru dochází k pokroku a lidé si začínají uvědomovat důležitost kybernetické bezpečnosti. K tomu přispívá jednak medializace kybernetické bezpečnosti a také čím dál větší množství osvětových článků či online testů/her na toto téma. Nicméně stále ta úroveň není tak vysoko, jak by měla, a je třeba toto téma nadále propagovat a vzdělávat nejen své zaměstnance, ale také širokou veřejnost.“

7.2.4 Zhodnocení rozhovorů

Rozhovory se zaměstnanci soukromé sféry ukázaly, že standardy kybernetické bezpečnosti jsou v rámci všech tří společností na srovnatelné úrovni. Všechny tři organizace disponují zaměstnanci, kteří se plně věnují prevenci nebezpečí přerušení činností neboli business continuity managementu, jejichž pracovní náplní je též kybernetická bezpečnost. U všech tří společností pravidelně probíhají různá interaktivní školení, akce či kampaně zaměřené na kybernetickou bezpečnost.

7.3 Shrnutí rozhovorů a doporučení

Jak uvedl zaměstnanec Okresního soudu v Kladně, mezi kybernetická bezpečnostní opatření používaná v jejich organizaci patří blokace externích datových úložišť, používání aktualizovaných firewallů a antivirových programů. Co se týče metod zvyšování povědomí o kybernetické bezpečnosti mezi zaměstnanci, mají zavedené povinné vstupní a periodické testování, a v případě potřeby také ad hoc kybernetická školení. Dle mého pohledu se jedná o dostatečný přístup k ochraně proti kybernetickým hrozbám.

V rámci Policie České republiky mohu tento rozhovor doplnit vlastními zkušenostmi ohledně bezpečnostních opatření. Plošně je u PČR využívána ochrana pomocí firewallů a antivirových programů. Jelikož působím pátým rokem na obvodním oddělení, mohu uvést, že se během výkonu služby používají soukromá přenosná paměťová zařízení zcela běžně. Vzhledem k nedostatku služebních USB flash disků by bylo jinak v podstatě nemožné vykonávat standardní služební úkony, jako je například zajištění kamerových záznamů. Ke vzdělávání v problematice kybernetické bezpečnosti u PČR lze uvést, že v rámci intranetu je možnost sebevzdělávání prostřednictvím e-learningu, avšak toto je nepovinné. Žádná povinná vstupní či pravidelná školení u PČR neprobíhají, což si myslím, že je velmi špatně. Zejména pokud vezmeme v úvahu, že právě policisté na základních článcích přijímají prvotní oznámení týkající se kybernetické kriminality a ve většině případů také provádějí šetření. Zde by mělo jednoznačně dojít k zefektivnění edukace příslušníků.

Velmi profesionální pohled na téma kybernetické bezpečnosti poskytl zástupce územní samosprávy, konkrétně zaměstnanec Statutárního města Kladna. Zálohování, pravidelné aktualizace software, ochrana sítě, monitoring uživatelů a pokročilá ochrana proti hrozbám včetně Next Generation Firewallu či šifrování všech koncových zařízení, to je výčet některých technických opatření implementovaných u této organizace. Co se týče organizačních opatření, pořádají pravidelná školení na téma kybernetické bezpečnosti a pravidelně informují zaměstnance o aktuálních hrozbách. Pořádají také phishing kampaně, testování zranitelnosti nebo penetrační testování.

Mezi bezpečnostní opatření společnosti T-Mobile Czech Republic a.s. patří především detekční systémy, antimalware systémy, procesy zvládání kybernetických incidentů, řízení rizik, řízení kontinuity, penetrační testování a také důkladné vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti. Každý zaměstnanec musí pravidelně absolvovat bezpečnostní školení formou e-learningu na interní vzdělávací platformě. Kurz je online formou se závěrečným testem a vydáním certifikátu. Dále informují zaměstnance o aktuálních hrozbách a trendech v oblasti kybernetické bezpečnosti prostřednictvím tzv. interní sociální sítě. Důležitým aspektem je provádění reálného testování pomocí phishingových kampaní či simulací spoofingu na zaměstnance. Jednou ročně také pořádají třídenní akci „Security Days“, během které se provádí školení zábavnou formou a pořádají odborné diskuse na téma kybernetické a fyzické bezpečnosti.

Společnost O2 Czech Republic a.s., podobně jako její konkurent, používá veškerá ochranná opatření v souladu se zákonem o kybernetické bezpečnosti. Velmi zajímavé jsou pak metody, které tato organizace užívá ke zlepšení informovanosti zaměstnanců v problematice kybernetické bezpečnosti. Například se jedná o tzv. Virtuální univerzitu, ve které jsou vytvořena školení pro zaměstnance buď ve formě prezentace nebo interaktivního kurzu, kdy pro ukončení školení je potřeba splnit test. Zároveň organizace vydává články na intranetu, které se týkají aktuálních kybernetických událostí. V minulém roce také společnost pořádala gamifikované školení spočívající ve vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti pomocí hraní her.

Posledním zástupcem soukromé sféry byl zaměstnanec společnosti Allianz pojišťovna, a.s. Mezi bezpečnostní opatření, která společnost využívá, patří aktivní brány firewallu, vulnerability management, monitoring síťového provozu, detekce anomálií či incident management. Co se týče zvyšování povědomí o kybernetické bezpečnosti, tato organizace pořádá pravidelné phishingové kampaně, a to plošné nebo cílené. Jednou ročně v rámci Cyber Security Awareness Month pak společnost pořádá různé soutěže a setkání zaměstnanců celé společnosti s týmem Business Continuity Management za účelem přiblížení jejich práce všem zaměstnancům organizace a také jejich dalšího vzdělávání v oblasti kybernetické bezpečnosti.

Na základě rozhovorů se zástupci soukromé sféry lze konstatovat, že kybernetická bezpečnost je v této oblasti na velmi vysoké úrovni. Firmy si uvědomují rostoucí rizika spojená s digitálním prostředím a kladou velký důraz na osvětu a vzdělávání svých zaměstnanců. Investice do moderních bezpečnostních technologií a pravidelná školení a testování jsou zde standardem, což pomáhá udržovat vysokou úroveň ochrany před kybernetickými hrozbami. Na osvětu se zde klade opravdu velký důraz, a navíc zajímavým a originálním způsobem. Na druhé straně, ve státní sféře, zejména v případě Policie České republiky, je situace méně optimistická. Zde chybí dostatečná finanční podpora, koordinace a moderní přístup ke kybernetické bezpečnosti, což vede k nižší úrovni zabezpečení. Osvěta a školení v této oblasti jsou méně důrazné a nejsou implementovány s takovou důsledností jako v soukromém sektoru. To vytváří mezery, které mohou být zneužity k útokům, a zároveň snižuje celkovou připravenost státní sféry čelit moderním kybernetickým hrozbám.

Rozdíly mezi soukromou a státní sférou v přístupu ke kybernetické bezpečnosti tak poukazují na potřebu posílení kapacit a investic do bezpečnostních opatření ve veřejném sektoru, aby byla zajištěna lepší ochrana nejen pro státní instituce, ale také pro občany, které tyto instituce obsluhují. Bylo by vhodné se inspirovat u soukromých organizací a implementovat některý z druhů osvětových kampaní, čímž by se zvýšily nejen znalosti zaměstnanců, ale také celková kybernetická bezpečnost v rámci státních organizací a v případě PČR také efektivita v rámci objasňování kybernetické kriminality.

Závěr

V dnešní době, kdy informace a data představují cenná aktiva, je kybernetická bezpečnost stále důležitějším tématem pro jednotlivce i organizace. Přestože jsou dnes kybernetické útoky již běžnou realitou, mnoho uživatelů stále nedostatečně chápe rizika spojená s těmito hrozbami a zanedbává jejich prevenci. Pandemie koronaviru a probíhající válka na Ukrajině význam kybernetické bezpečnosti ještě prohloubila, jelikož došlo k rapidnímu nárůstu kybernetické kriminality. Základním kamenem ochrany proti kybernetickým hrozbám je důkladná informovanost a vysoká úroveň vzdělanosti široké veřejnosti v oblasti kybernetické bezpečnosti. Pouze prostřednictvím systematického vzdělávání a šíření důležitých informací mohou jednotlivci i organizace včas rozpoznat potenciální rizika a přijmout adekvátní opatření na ochranu svých digitálních aktiv.

Cílem práce bylo analyzovat současné metody zvyšování povědomí o kybernetické bezpečnosti a formulovat doporučení pro zvýšení jejich efektivity při vzdělávání veřejnosti. Současně se práce zaměřila na evaluaci aktuální úrovně informovanosti české populace v oblasti kybernetické bezpečnosti, přičemž cílem bylo identifikovat klíčové oblasti, kde je zapotřebí dalšího zlepšení. Stanovených cílů bylo dosaženo, kdy hlavním přínosem práce je nejen ucelený souhrn jednotlivých vzdělávacích metod, ale zejména soubor konkrétních návrhů a doporučení, které mohou přispět k efektivnějšímu vzdělávání a informování veřejnosti v problematice kybernetické bezpečnosti.

Teoretická část práce nejprve definovala samotný pojem kybernetická bezpečnost, související terminologii a historii. Dále rozebrala aktuální kybernetické hrozby, ochranná opatření a současné trendy. Stěžejní pátá kapitola se věnovala konkrétním metodám zvyšování povědomí o kybernetické bezpečnosti a jejich efektivitě, které jsou v současnosti využívány, ať už při vzdělávání veřejnosti, zaměstnanců organizací či studentů škol. Poslední kapitola teoretické části práce pak shrnula aktuální situaci v České republice a poskytla vlastní návrhy a doporučení, jak by se současný stav vzdělanosti české veřejnosti dal vylepšit.

Praktická část práce zahrnovala strukturované rozhovory se zástupci státní a soukromé sféry, kteří mají odpovědnost za kybernetickou bezpečnost svých institucí a podílejí se na zvyšování povědomí a znalostí zaměstnanců. Tyto rozhovory poskytly důležité praktické poznatky o využívaných metodách a postupech, které využívají k efektivnímu vzdělávání a osvětě zaměstnanců v oblasti kybernetické bezpečnosti. Rozhovory byly následně analyzovány a vzájemně porovnány. Výsledkem je soubor doporučení, jakým způsobem by se přístupy jednotlivých organizací v rámci státního a soukromého sektoru daly zlepšit.

Ačkoli by se dle názvu této diplomové práce mohlo zdát, že existují specifické metody zvyšování povědomí o kybernetické bezpečnosti, které jsou využívány výhradně ve státní nebo soukromé sféře, na základě zjištěných poznatků jsem dospěl k závěru, že takové striktní oddělování jednotlivých metod není vhodné a prakticky ani není možné. Naopak se domnívám, že nejefektivnější je vždy kombinace různých metod v rámci obou sfér, přičemž rozdíly by měly vycházet spíše z obsahu vzdělávání a specifických potřeb dané organizace. Tyto rozdíly se mohou odrážet například v zaměření na konkrétní kybernetické hrozby, kterým organizace čelí, nebo v požadavcích vyplývajících z jejího zaměření a činnosti. Dle zaměstnanců, s nimiž byly vedeny rozhovory, pak vyplývá, že základem by vždy mělo být pravidelné provádění simulovaných útoků, tedy například phishingové testování zaměstnanců.

Závěrem lze konstatovat, že přestože povědomí o kybernetické bezpečnosti v České republice roste, stále existují výzvy a prostor pro zlepšení. Jedním z klíčových problémů je nedostatečná koordinace mezi různými osvětovými iniciativami, mnohé z kampaní navíc postrádají dlouhodobý plán. Řešením by mohl být veřejně známý subjekt, jakýsi centrální styčný bod, který by koordinoval veškeré aktivity a spolupráci jak na mezinárodní úrovni, tak i mezi státní, soukromou a akademickou sférou, o což v posledních letech usiluje NÚKIB. Je však nutné, aby úřad zvýšil povědomí veřejnosti o své činnosti například prostřednictvím modernizace svých webových stránek, aktivnějšího působení na sociálních sítích a širší propagace v médiích. To vše by mohlo přispět k lepší informovanosti a zvýšení kybernetické bezpečnosti v České republice.

Seznam použité literatury

Monografie

1. PAČKA, Roman. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Politologická řada. Brno: Centrum pro studium demokracie a kultury, 2019. ISBN 978-80-7325-473-5.

2. JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

3. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

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

5. RAMEŠOVÁ, Kristina. *Právní regulace kybernetické bezpečnosti a její meze*. Beckova edice právní instituty. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-931-0.

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

7. VANĚK, Jiří; NOVÁK, Jiří a KALIKA, David. *Jak na Internet bezpečně*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2018. ISBN 978-80-88168-29-4.

Webové stránky a elektronické zdroje

8. Vláda České republiky. *Kybernetická bezpečnost* [online]. 2021. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/#

9. Ministerstvo vnitra České republiky. *Základní definice, vztahující se k tématu kybernetické bezpečnosti* [online]. 2009. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

10. Gov.cz. *Hlášení kybernetických bezpečnostních incidentů* [online]. 2024. Dostupné z: https://portal.gov.cz/sluzby-vs/hlaseni-kybernetickych-bezpecnostnich-incidentu-S10769

11. CZ.NIC. *Jak na internet* [online]. 2012-2014. Dostupné z: https://www.jaknainternet.cz/page/1205/historie-internetu/

12. Ministerstvo vnitra České republiky. *Hrozba* [online]. 2003. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

13. KYBEZ. *Hrozby* [online]. 2021. Dostupné z: https://kybez.cz/hrozby/

14. Rada Evropské unie. *Infografika – Nejzávažnější kybernetické hrozby v EU* [online]. 2023. Dostupné z: https://www.consilium.europa.eu/cs/infographics/cyber-threats-eu/

15. Cyber Magazine. *Top 10 Ransomware Attacks* [online]. 2023. Dostupné z: https://cybermagazine.com/articles/top-10-ransomware-attacks

16. ČT24. *Útok na benešovskou nemocnici způsobil šedesátimilionovou škodu. Policie případ odložila* [online]. 2020. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/utok-na-benesovskou-nemocnici-zpusobil-sedesatimilionovou-skodu-policie-pripad-odlozila-45977

17. Policie České republiky. *Mezinárodní operace TALPA* [online]. 2023. Dostupné z: https://www.policie.cz/clanek/mezinarodni-operace-talpa.aspx

18. Policie České republiky. *Počítačová kriminalita* [online]. 2024. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

19. Root.cz. *Kolik stojí DDoS? Základní přijde na pár dolarů, pokročilý na stovky* [online]. 2017. Dostupné z: https://www.root.cz/clanky/kolik-stoji-ddos-zakladni-prijde-na-par-dolaru-pokrocily-na-stovky/

20. Policie České republiky. *Rizika a nástrahy sociálních sítí* [online]. 2024. Dostupné z: https://www.policie.cz/soubor/policie-cr-prilohy-kybersikana-doporuceni-pdf.aspx

21. Internetem bezpečně. *Krádež identity* [online]. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

22. Internetem bezpečně. *Sexting* [online]. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

23. Ministerstvo vnitra České republiky. *Definice dezinformací a propagandy* [online]. 2024. Dostupné z: https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

24. Internetem bezpečně. Kybergrooming [online]. 2018. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

25. itnetwork.cz. *Lekce 1 - Základní pojmy a zásady kybernetické bezpečnosti* [online]. 2024. Dostupné z: https://www.itnetwork.cz/bezpecnost/zakladni-pojmy-a-zasady-kyberneticke-bezpecnosti

26. Kybertest. *Buďte na internetu v bezpečí* [online]. 2024. Dostupné z: https://www.kybertest.cz/

27. Kybertest. *Základní desatero bezpečnosti* [online]. 2024. Dostupné z: https://www.kybertest.cz/desatero-bezpecnosti-na-internetu

28. Kybertest. *Nejčastější typy podvodů* [online]. 2024. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu

29. Peníze.cz. *Autentizační prvky a metody pod drobnohledem* [online]. 2004. Dostupné z: https://www.penize.cz/investice/16777-autentizacni-prvky-a-metody-pod-drobnohledem

30. Eset. *Firewall* [online]. 2024. Dostupné z: https://www.eset.com/cz/firewall/

31. Forbes Advisor. *The Best Antivirus Software (March 2024)* [online]. 2024. Dostupné z: https://www.forbes.com/advisor/business/software/best-antivirus-software/

32. MasterDC. *Největší kybernetické útoky a trendy pro 2024: AI, zero trust a IoT* [online]. 2024. Dostupné z: https://www.master.cz/blog/nejvetsi-kyberneticke-utoky-a-trendy-pro-2024-ai-zero-trust-a-iot/

33. Evropský parlament. *Co je umělá inteligence a jak ji využíváme?* [online]. 2023. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20200827STO85804/umela-inteligence-definice-a-vyuziti

34. The University of Queensland and KPMG Australia. *Trust in Artificial Intelligence: A Global Study* [online]. 2023. Dostupné z: https://ai.uq.edu.au/project/trust-artificial-intelligence-global-study

35. Rascasone. *Internet věcí (IoT): definice, příklady, využití, produkty* [online]. 2023. Dostupné z: https://www.rascasone.com/cs/blog/iot-internet-veci-definice-produkty-historie#co-je-internet-vec-iacute-iot

36. Algotech. *Jak funguje cloud?* [online]. 2024. Dostupné z: https://www.algotech.cz/novinky/2021-10-27-jak-funguje-cloud

37. Rascasone. *Co je blockchain, jak funguje a kde najde využití?* [online]. 2023. Dostupné z: https://www.rascasone.com/cs/blog/zmeni-technologie-blockchain-cely-svet

38. Prevence kriminality. *Kyberkriminalita* [online]. 2024. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

39. Policie České republiky. *Vývoj registrované kriminality v roce 2023* [online]. 2024. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx

40. STATISTIKA&MY. *Jak se vyvíjí objasněnost trestných činů v kyberprostoru?* [online]. 2024. Dostupné z: https://www.statistikaamy.cz/2023/05/16/jak-se-vyviji-objasnenost-trestnych-cinu-v-kyberprostoru

41. Národní úřad pro kybernetickou a informační bezpečnost. *Vzdělávací portál NÚKIB* [online]. 2024. Dostupné z: https://osveta.nukib.cz/local/dashboard/

42. Národní úřad pro kybernetickou a informační bezpečnost. *Festival bezpečného internetu* [online]. 2024. Dostupné z: https://osveta.nukib.cz/course/view.php?id=111

43. CZ.NIC. *Jak na Internet* [online]. 2024. Dostupné z: https://www.jaknainternet.cz/

44. KYBEZ. *Jak vzdělávat v oblasti kyberbezpečnosti na základních a středních školách?* [online]. 2021. Dostupné z: https://kybez.cz/jak-vzdelavat-v-oblasti-kyberbezpecnosti-na-zakladnich-a-strednich-skolach/

45. MetaCompliance. *How to Promote Cyber Security Awareness and Improve Cyber Security at the Workplace* [online]. 2024. Dostupné z: https://www.metacompliance.com/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation

46. Aptien. *Způsoby školení a rozvoje zaměstnanců* [online]. 2024. Dostupné z: https://aptien.com/cs/kb/articles/kinds-of-employee-training-and-development

47. StickmanCyber. *How to Improve Cyber Security Awareness* [online]. 2022. Dostupné z: https://www.stickmancyber.com/cybersecurity-blog/how-to-improve-cyber-security-awareness

48. Guardey. *The 8 best cyber security awareness tests for employees* [online]. 2024. Dostupné z: https://www.guardey.com/security-awareness-test/

49. Eset. *7 způsobů, jak posílit znalosti zaměstnanců o kybernetické bezpečnosti* [online]. 2020. Dostupné z: https://www.eset.com/cz/blog/prevence/7-zpusobu-jak-posilit-znalosti-zamestnancu-o-kyberneticke-bezpecnosti/

50. Jenpráce. *Efektivní a dlouhodobá motivace zaměstnanců* [online]. 2024. Dostupné z: https://www.jenprace.cz/magazin/efektivni-a-dlouhodoba-motivace-zamestnancu#anchorId0

51. CETIN. *Audit kybernetické bezpečnosti* [online]. 2024. Dostupné z: https://www.cetin.cz/nis2/nase-sluzby/audit-kyberneticke-bezpecnosti

52. Britannica. *Conference* [online]. 2024. Dostupné z: https://www.britannica.com/dictionary/conference

53. Security. *O konferenci* [online]. 2024. Dostupné z: https://konferencesecurity.cz/o-konferenci

54. AFCEA. *Konference Kybernetická bezpečnost KB12* [online]. 2024. Dostupné z: https://afcea.cz/akce/kb12/

55. Future Forces Forum. *Koncept* [online]. 2024. Dostupné z: https://future-forces-forum.org/homepage/concept?lang=cs

56. IT slovník. *Co je to workshop?* [online]. 2024. Dostupné z: https://it-slovnik.cz/pojem/workshop

57. Kyber cena roku. *O projektu* [online]. 2024. Dostupné z: https://www.kybercena.cz/o-projektu/

58. Soutěž v kybernetické bezpečnosti. *Soutěž v kybernetické bezpečnosti* [online]. 2024. Dostupné z: https://www.kybersoutez.cz/ks_soutez.html

59. EPALE – Elektronická platforma pro vzdělávání dospělých v Evropě. *Země zázraků ve vzdělávání – hry a gamifikace* [online]. 2023. Dostupné z: https://epale.ec.europa.eu/cs/blog/zeme-zazraku-ve-vzdelavani-hry-gamifikace

60. Ministerstvo školství, mládeže a tělovýchovy. *MŠMT a NÚKIB k digitalizaci vzdělávání a kyberbezpečnosti* [online]. 2021. Dostupné z: https://msmt.gov.cz/msmt-a-nukib-k-digitalizaci-vzdelavani-a-kybernetice

61. Národní úřad pro kybernetickou a informační bezpečnost. *Školy* [online]. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/

62. Národní úřad pro kybernetickou a informační bezpečnost. *Nabízené kurzy pro školy* [online]. 2024. Dostupné z: https://osveta.nukib.gov.cz/local/dashboard/?tag_id=21

63. Národní úřad pro kybernetickou a informační bezpečnost. *Mateřské školy* [online]. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/materske-skoly/

64. Národní úřad pro kybernetickou a informační bezpečnost. *Základní školy* [online]. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/zakladni-skoly/

65. Národní úřad pro kybernetickou a informační bezpečnost. *Střední školy* [online]. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/skoly/stredni-skoly/

66. Národní úřad pro kybernetickou a informační bezpečnost. *Kontaktní vzdělávání* [online]. 2024. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/kontaktni-vzdelavani/

67. ETCIO. *Cybersecurity Ranking 2024: Which countries are most at risk?* [online]. 2024. Dostupné z: https://ciosea.economictimes.indiatimes.com/news/security/cybersecurity-ranking-2024-which-countries-are-most-at-risk/110730038

68. Lyca Mobile. *Staying safe online in the Nordic Countries: A comprehensive guide* [online]. 2024. Dostupné z: https://www.lycamobile.se/blog/en/staying-safe-online-in-the-nordic-countries-a-comprehensive-guide/

69. Nordic IT Security. *Nordic IT Security* [online]. 2024. Dostupné z: https://nordicitsecurity.com/

70. Cybersecurity and Infrastructure Security Agency. *Cybersecurity Awareness Month* [online]. 2024. Dostupné z: https://www.cisa.gov/cybersecurity-awareness-month

71. Medium. *Výuka kybernetické bezpečnosti v Estonsku a České republice* [online]. 2021. Dostupné z: https://medium.com/edtech-kisk/v%C3%BDuka-kybernetick%C3%A9-bezpe%C4%8Dnosti-v-estonsku-a-%C4%8Desk%C3%A9-republice-bfb1fa9c9015

72. CZ Defence. *Kybernetická bezpečnost České republiky v roce 2023: Výzvy a trendy* [online]. 2021. Dostupné z: https://www.czdefence.cz/clanek/kyberneticka-bezpecnost-ceske-republiky-v-roce-2023-vyzvy-a-trendy

Seznam zkratek

AI – Artificial intelligence

ARPA – Advanced Research Project Agency

BCM – Business Continuity Management

BIA – Business Impact Analysis

CCTV – Closed Circuit Television

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

CySAM – Cyber Security Awareness Month

DDoS – Distributed Denial of Service

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

EU – Evropská unie

GDPR – General Data Protection Regulation

ICT – Information and Communication Technologies

IoT – Internet of Things

MKDS – Městský kamerový dohlížecí systém

NCKB – Národní centrum kybernetické bezpečnosti

NCTEKK – Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PAM – Privileged Access Management

VPN – Virtual Private Network

2FA – Two-Factor Authentication