Kyberbezpečnost jak součást digitální gramotnosti: Jak mohou školy vytvářet podpůrné a bezpečné prostředí z hlediska kybernetické bezpečnosti

Cybersecurity as a part of digital literace: How schools can create a supportive and secure environment from the perspective od cybersecurity

Martin Beneš

Abstrakt: Článek se zaměřuje na strategie, které mohou školy využít k posílení kyberbezpečnosti a podpory digitální gramotnosti. V současném rychle se vyvíjejícím digitálním světě je nezbytné, aby vzdělávací instituce učinily kroky k zajištění bezpečného prostředí pro své studenty, zároveň jim poskytly dovednosti potřebné k navigaci v digitálním světě. Tento článek prozkoumává klíčové aspekty potřebné pro úspěšnou integraci kyberbezpečnosti do školního prostředí. Jedním z hlavních bodů je vývoj a implementace bezpečnostních politik. Článek zkoumá, jak mohou školy vytvářet a uplatňovat politiky, které sníží riziko, že se studenti setkají s online hrozbami, zatímco podporují bezpečné využívání technologií pro vzdělávací účely. Zahrnuje to nejen technické aspekty, jako jsou firewally a antivirové programy, ale také administrativní a organizační opatření, jako jsou pravidla pro používání internetu a sociálních médií. Zvláštní důraz je kladen na multidisciplinární přístup. Tento přístup uznává, že kyberbezpečnost není jen technickou záležitostí, ale zahrnuje i behaviorální a psychologické aspekty. Článek zkoumá, jak mohou různé disciplíny, od informatiky přes sociologii po psychologii, přispět k lepšímu pochopení a řešení kyberbezpečnostních výzev. Zahrnuje také diskusi o významu osvěty a vzdělávání učitelů v oblasti kyberbezpečnosti, což je zásadní pro vytváření bezpečného a podpůrného vzdělávacího prostředí.

Klíčová slova: školní bezpečnostní politiky, pedagogické metody, behaviorální aspekty kyberbezpečnosti, vzdělávací programy, digitální gramotnost

DOI:

Abstract: The article focuses on strategies that schools can utilize to enhance cybersecurity and support digital literacy. In today's rapidly evolving digital world, it is essential for educational institutions to take steps to ensure a safe environment for their students, while also providing them with the skills necessary to navigate the digital world. This article examines the key aspects required for successful integration of cybersecurity into the school environment. One of the main points is the development and implementation of security policies. The article explores how schools can create and apply policies that mitigate the risk of students encountering online threats while supporting the safe use of technology for educational purposes. This includes not only technical aspects, such as firewalls and antivirus programs, but also administrative and organizational measures, such as rules for internet and social media use. Special emphasis is placed on a multidisciplinary approach. This approach recognizes that cybersecurity is not just a technical matter, but also includes behavioral and psychological aspects. The article investigates how various disciplines, from computer science to sociology and psychology, can contribute to a better understanding and resolution of cybersecurity challenges. It also includes a discussion on the importance of awareness and education of teachers in the field of cybersecurity, which is crucial for creating a safe and supportive educational environment.

Key words: school security policies, pedagogical methods, behavioral aspects of cybersecurity, educational programs, digital literacy

Úvod

Kybernetická bezpečnost se v posledních letech stala klíčovým aspektem vzdělávacího procesu. S rostoucí integrací digitálních technologií do výuky čelí vzdělávací instituce naléhavé potřebě přijmout komplexní opatření, která zajistí nejen bezpečné prostředí pro žáky, ale také rozvoj kompetencí nezbytných pro orientaci v digitálním světě. Tento článek se zabývá analýzou různých strategií, jež mohou školy implementovat s cílem posílit kybernetickou bezpečnost a podpořit digitální gramotnost (Williams & Krueger, 2005).

Je nezbytné, aby vzdělávací instituce vyvinuly a zavedly robustní bezpečnostní politiky a programy, které sníží rizika spojená s online hrozbami a zároveň podpoří bezpečné a efektivní využívání technologií pro vzdělávací účely. V současné době přesahuje kybernetická bezpečnost pouhou ochranu před externími útoky a stává se fundamentálním prvkem ve výchově informovaných a zodpovědných digitálních občanů.

V kontextu těchto výzev je klíčové zaměřit se na rozvoj kompetencí žáků v oblasti kybernetické bezpečnosti. S narůstající integrací technologických zařízení do výukových plánů je podstatné, aby žáci porozuměli potenciálním rizikům a osvojili si dovednosti nezbyt-

né pro ochranu sebe samých i svých dat v online prostředí. Toto porozumění je klíčové pro vytvoření zdravého digitálního ekosystému, v němž se žáci mohou efektivně učit a rozvíjet (Pangrazio & Cardozo-Gaibisso, 2020).

Neméně důležitou roli v tomto procesu hrají pedagogičtí pracovníci, kteří potřebují adekvátní podporu a vzdělávání. Významným aspektem pro vytvoření bezpečného a podpůrného vzdělávacího prostředí je také důraz na osvětu a vzdělávání pedagogických pracovníků v oblasti kybernetické bezpečnosti. Učitelé zastávají klíčovou roli při formování povědomí žáků o kybernetické bezpečnosti, a proto je nezbytné zvyšovat jejich kompetence v této oblasti (Maqsood & Chiasson, 2021).

Tento článek prozkoumá klíčové aspekty potřebné pro úspěšnou integraci kyberbezpečnosti do školního prostředí. Zaměříme se na vývoj a implementaci bezpečnostních politik, multidisciplinární přístup zahrnující technické, pedagogické a psychologické aspekty a analýzu vybraných vzdělávacích programů v oblasti kybernetické bezpečnosti v českém prostředí. Závěrem budou diskutovány limity současného výzkumu a navrženy směry pro budoucí studie v této oblasti.

Kybernetická bezpečnost

Kybernetická bezpečnost představuje komplexní soubor technik, procesů a postupů, jejichž cílem je ochrana digitálních zařízení, sítí a informací před neoprávněným přístupem, krádeží nebo modifikací dat. Tato oblast zahrnuje širokou škálu strategií a nástrojů, které slouží k zajištění bezpečnosti dat a infrastruktury v digitálním prostředí (BOZP, 2022).

Pro pochopení základních principů kybernetické bezpečnosti je klíčovým konceptem tzv. CIA triáda. CIA triáda představuje tři fundamentální pilíře ochrany informací v digitálním světě: důvěrnost (Confidentiality), integritu (Integrity) a dostupnost (Availability). Důvěrnost se zaměřuje na ochranu osobních údajů a omezení přístupu k informacím pouze pro autorizované osoby. V kontextu školního prostředí to znamená zajistit, aby citlivé informace o žácích, učitelích a chodu školy byly přístupné pouze oprávněným osobám (Gashi, Luma, & Aliu, 2022). Integrita zajišťuje přesnost a úplnost dat, přičemž změny mohou být prováděny pouze oprávněnými subjekty a musí být řádně zaznamenány (Sherman et al., 2018). Pro školy je to zásadní při správě akademických záznamů, hodnocení a dalších důležitých dokumentů. Dostupnost garantuje, že informace jsou přístupné a využitelné oprávněnými stranami v okamžiku potřeby, a to i navzdory potenciálním hrozbám, jako jsou hardwarová selhání nebo kybernetické útoky. To je obzvláště důležité pro zajištění kontinuity vzdělávacího procesu, zejména v době rostoucího významu online výuky (Cabric, 2015).

Ve školním prostředí se principy CIA

triády promítají do různých aspektů kybernetické bezpečnosti. Důvěrnost se zaměřuje na ochranu osobních údajů žáků a učitelů, zajišťuje, že citlivé informace o studijních výsledcích nebo osobních záležitostech jsou přístupné pouze oprávněným osobám. Integrita dat je klíčová pro zachování přesnosti a spolehlivosti školních záznamů, například známek nebo docházky. Dostupnost zajišťuje, že vzdělávací materiály a systémy jsou přístupné žákům a učitelům, když je potřebují, což je v současné době rovněž (Sherman et al., 2018; Cabric, 2015).

Pro implementaci těchto principů musí školy vytvářet a realizovat komplexní bezpečnostní politiky (Peltier, 2016). Technická opatření, jako jsou firewally, antivirové programy a systémy pro detekci průniku, pomáhají chránit školní sítě a systémy. Neméně důležité je vzdělávání a osvěta v oblasti kybernetické bezpečnosti pro žáky a učitele, aby pochopili svou roli v udržování bezpečného digitálního prostředí (Livingstone et al., 2011). Řízení přístupu prostřednictvím systémů pro správu identit zajišťuje, že k citlivým informacím mají přístup pouze oprávnění uživatelé. Pravidelné zálohování a plány obnovy dat pak pomáhají zajistit dostupnost informací i v případě kybernetických útoků nebo technických problémů.

Pochopení a aplikace principů CIA triády v kontextu vzdělávacích institucí je zásadní pro vytvoření komplexní strategie kybernetické bezpečnosti. V následujících kapitolách se zaměříme na konkrétní aspekty implementace těchto principů v prostředí škol, včetně vývoje bezpečnostních politik, integrace technologií a vzdělávání v oblasti kybernetické bezpečnosti.

Vývoj a implementace bezpečnostních politik

Bezpečnostní politika

Bezpečnostní politika představuje fundamentální součást úspěšného programu kybernetické bezpečnosti ve školách. Jejím primárním cílem je nalézt rovnováhu mezi bezpečnostními potřebami organizace a jejími vzdělávacími prioritami. Efektivní bezpečnostní politika by měla být srozumitelná, dobře strukturovaná a pravidelně aktualizovaná (Donaldson, Siegel, Williams, & Aslam, 2015). Je důležité si uvědomit, že význam a rozsah bezpečnostní politiky se může lišit v závislosti na typu organizace, charakteru informací, které spravuje, a specifických bezpečnostních požadavcích (Mishra, Alzoubi, Gill, & Anwar, 2022).

Při tvorbě bezpečnostních politik pro vzdělávací instituce je klíčové zohlednit několik zásadních aspektů. Především by měly být formulovány jasně a stručně, aby byly snadno pochopitelné pro všechny uživatele, včetně žáků a učitelů. Zároveň musí být dostatečně detailní, aby pokrývaly všechny relevantní aspek-

ty kybernetické bezpečnosti. Komplexní pokrytí bezpečnostních politik by mělo zahrnovat témata jako správa hesel, používání osobních zařízení, přístup k citlivým datům, používání sociálních médií a reakce na bezpečnostní incidenty.

Vzhledem k rychle se vyvíjejícímu charakteru kybernetických hrozeb je nezbytné pravidelně revidovat a aktualizovat bezpečnostní politiky, aby zůstaly relevantní a efektivní. Tato dynamická povaha kybernetické bezpečnosti vyžaduje, aby školy byly připraveny pružně reagovat na nově vznikající hrozby a upravovat své politiky podle aktuálních potřeb.

Další důležitou dimenzí při tvorbě bezpečnostních politik je zajištění souladu s příslušnými zákony a předpisy týkajícími se ochrany osobních údajů a kybernetické bezpečnosti, jako je například GDPR. Tento právní aspekt je zásadní pro zajištění, že školy nejen chrání své systémy a data, ale také dodržují zákonné povinnosti a respektují práva jednotlivců na ochranu osobních údajů.

Při tvorbě a implementaci politik je důležité zapojit všechny relevantní skupiny, včetně vedení školy, IT oddělení, učitelů, žáků a rodičů. Tento inkluzivní přístup zajišťuje, že politiky budou komplexní, prakticky proveditelné a budou reflektovat potřeby a obavy všech zúčastněných stran. Zapojení různých skupin také pomáhá budovat podporu a porozumění pro bezpečnostní opatření napříč celou školní komunitou.

Implementace bezpečnostních politik

Implementace bezpečnostních politik vyžaduje aktivní zapojení všech členů školní komunity. Žáci a učitelé musí být průběžně vzděláváni v principech kybernetické bezpečnosti a ve svých rolích a povinnostech v rámci bezpečnostních politik. Pravidelná školení a osvětové kampaně pomohou vybudovat kulturu kybernetické bezpečnosti a zvýšit povědomí o potenciálních hrozbách (Flowerday & Tuyikeze, 2016).

Efektivní bezpečnostní politiky jsou základním předpokladem pro vytvoření bezpečného a podpůrného digitálního prostředí ve školách. Jejich vývoj a implementace vyžaduje multidisciplinární přístup, který zohledňuje technické, pedagogické, psychologické a sociální aspekty. Pouze prostřednictvím komplexní a dobře promyšlené bezpečnostní politiky mohou školy snížit rizika spojená s kybernetickými hrozbami a zajistit, že technologie budou využívány bezpečným a odpovědným způsobem. Tento holistický přístup k bezpečnostním politikám je klíčový pro vytvoření robustního a adaptabilního rámce kybernetické bezpečnosti, který může efektivně reagovat na měnící se digitální prostředí a nové výzvy v oblasti bezpečnosti.

Integrace technologií pro zvýšení zabezpečení ve školách

Implementace efektivních technických nástrojů představuje zásadní krok k vytvoření bezpečnějšího a informovanějšího digitálního prostředí ve školách. Tyto nástroje hrají klíčovou roli při ochraně citlivých dat škol a při vytváření bezpečného prostředí pro učitele a žáky. Bez adekvátních technických opatření jsou školní sítě a systémy vystaveny značnému riziku narušení, které může vést k úniku citlivých dat, ztrátě integrity informací nebo narušení dostupnosti kritických vzdělávacích zdrojů (Waghere et al., 2023).

Při výběru vhodných technologických řešení je nezbytné pečlivě zvážit několik faktorů včetně jejich efektivity, uživatelské přívětivosti a kompatibility s existující infrastrukturou školy. Komplexní strategie kybernetické bezpečnosti by měla zahrnovat robustní antivirové programy pro detekci a eliminaci škodlivého softwaru, firewally pro řízení síťového provozu a filtrování potenciálně nebezpečných spojení a také pokročilé nástroje pro detekci a prevenci neoprávněného přístupu (narušení), které monitorují síťovou aktivitu a identifikují anomálie a potenciální hrozby v reálném čase (Waghere et al., 2023).

Implementace těchto technologií vytváří vícevrstevnou ochranu, která významně snižuje riziko úspěšných kybernetických útoků a zajišťuje důvěrnost, integritu a dostupnost citlivých informací a systémů. Nicméně samotná instalace technických nástrojů není dostačující pro zajištění dlouhodobé efektivity kybernetické obrany. Kybernetické hrozby jsou vysoce dynamické a neustále se vyvíjejí, což vyžaduje pravidelnou aktualizaci a údržbu bezpečnostních technologií.

Je nezbytné, aby školy měly zavedené procesy pro průběžné monitorování a vyhodnocování nových typů útoků a zranitelností a aby byly schopny rychle reagovat prostřednictvím aktualizací softwarů, bezpečnostních záplat a úprav konfigurace. Tento úkol vyžaduje nejen technickou odbornost, ale také trvalou vzdělávací podporu ze strany školních administrátorů a IT profesionálů (Pencheva et al., 2020). Pravidelná školení a certifikace zajistí, že odpovědní pracovníci budou mít aktuální znalosti a dovednosti potřebné pro efektivní správu bezpečnostních technologií.

Příklady úspěšné integrace technologických nástrojů ve školním prostředí ukazují, jak mohou být tyto nástroje využity nejen pro zvýšení celkové úrovně kybernetické bezpečnosti, ale také pro kultivaci povědomí a dovedností v oblasti digitální bezpečnosti mezi žáky a zaměstnanci. Zapojení žáků a učitelů do procesu implementace a správy bezpečnostních technologií, například prostřednictvím praktických workshopů nebo interaktivních cvičení, může významně přispět k budování kultury kybernetické bezpečnosti a odpovědnosti. Tato angažovanost

posiluje porozumění významu technických opatření a jejich roli v celkové strategii kybernetické obrany.

Integrace efektivních technických nástrojů představuje zásadní krok k vytvoření bezpečnějšího a informovanějšího digitálního prostředí, ve kterém se žáci mohou učit a rozvíjet své dovednosti bez obav z kybernetických hrozeb. Nicméně je důležité zdůraznit, že technologická řešení jsou pouze jednou stránkou komplexního přístupu ke kybernetické bezpečnosti ve vzdělávání. Stejně důležité je rozvíjet lidský faktor prostřednictvím osvěty, vzdělávání a budování odpovědného chování v digitálním světě. Pouze kombinací technických, vzdělávacích a procesních opatření mohou školy vytvořit skutečně odolné a adaptabilní prostředí, které dokáže čelit neustále se měnícím výzvám kybernetické bezpečnosti (Dawson & Thomson, 2018).

Behaviorální a psychologické aspekty kybernetické bezpečnosti ve školách

Efektivní strategie kybernetické bezpečnosti ve školách musí vycházet nejen z technických řešení, ale také z porozumění behaviorálním a psychologickým aspektům, které ovlivňují chování uživatelů v digitálním prostředí. Chování jako rutiny, návyky a sociální normy hrají významnou roli v tom, jak lidé reagují na kybernetické hrozby. Například způsob, jakým žáci sdílejí informace na sociálních médiích nebo jak učitelé zabezpečují svá digitální zařízení, má přímý dopad na bezpečnost celé školy. Porozumění těmto behaviorálním aspektům je klíčové pro vytvoření efektivních strategií kyberbezpečnosti (Lahcen et al., 2020).

Tradiční přístupy, které se zaměřují především na technologická řešení a striktní bezpečnostní politiky, často selhávají v důsledku chyby lidského faktoru (Schneier, 2000). Uživatelé mohou vnímat bezpečnostní opatření jako překážku, která jim komplikuje práci nebo narušuje jejich soukromí, což může vést k obcházení těchto opatření nebo ignorování bezpečnostních postupů (Sasse, Brostoff & Weirich, 2001). Proto je nezbytné při implementaci bezpečnostních opatření zohlednit psychologické faktory, jako je vnímání rizika, důvěra v technologie a instituce, individuální zkušenosti a znalosti, sociální vlivy a normy a také kognitivní a emocionální procesy, které řídí lidské chování (Reason, 1990; Adams & Sasse, 1999).

Výzkum v této oblasti se zaměřuje na identifikaci klíčových faktorů, které formují postoje a rozhodování uživatelů ve vztahu ke kybernetickým hrozbám. Pochopení toho, jak žáci a učitelé vnímají a reagují na bezpečnostní opatření, může pomoci při navrhování efektivnějších a uživatelsky přívětivějších řešení. Například studie ukazují, že existuje významný vztah mezi povědomím žáků o kyberbezpečnosti a jejich rizikovým chováním online. Žáci s vyšším pově-

domím o kyberbezpečnosti jsou méně náchylní k rizikovým aktivitám, jako je sdílení osobních informací na internetu a vystavení se kyberútokům (Sarathchandra et al., 2016).

Úloha učitelů

Učitelé jsou klíčovými aktéry v procesu vzdělávání o kybernetické bezpečnosti. Jejich role zahrnuje nejen předávání technických znalostí, ale také porozumění behaviorálním a psychologickým faktorům, které ovlivňují chování žáků v online prostředí. Aby mohli efektivně plnit tuto úlohu, je nezbytné, aby byli vybaveni odpovídajícími znalostmi a zdroji. Pencheva zdůrazňuje, že školení a profesní rozvoj v těchto oblastech jsou zásadní pro vytváření bezpečného a informovaného školního prostředí (2020).

Komplexní příprava učitelů je základním předpokladem pro budování kultury kybernetické bezpečnosti ve školách. Pouze dobře informovaní a vyškolení profesionálové mohou účinně vést žáky k bezpečnému a odpovědnému chování v digitálním prostředí a reagovat na neustále se vyvíjející hrozby (Sherman et al., 2018). S rostoucími kybernetickými hrozbami, zejména v online vzdělávání, je nutné, aby učitelé měli přístup k vhodným nástrojům, zdrojům a vzdělávacím praktikám, které zajišťují nejen kontinuitu, ale také kvalitu a efektivitu vzdělávání.

Nový přístup ke vzdělání v oblasti kybernetické bezpečnosti, kde klíčovou roli hraje školení středoškolských učitelů, může být velmi přínosný. Tito učitelé mohou nejen učit kyberbezpečnost, ale také integrovat kyberbezpečnostní koncepty do svých učebních plánů a propagovat IT bezpečnost jako atraktivní kariérní cestu (Javidi & Sheybani, 2018). Využití zážitkové pedagogiky a her v kyberbezpečnostním vzdělávání může být účinné pro zvýšení povědomí žáků a zároveň pro výuku učitelů.

Aby mohli učitelé efektivně začlenit vzdělávání o kybernetické bezpečnosti do školních vzdělávacích programů, je nezbytné poskytnout jim odpovídající podporu, zdroje a možnosti profesního rozvoje. Školy by měly investovat do školení učitelů v oblasti kyberbezpečnosti, podporovat inovativní výukové metody a spolupracovat s odborníky v této oblasti. Pouze prostřednictvím komplexního přístupu, který zahrnuje jak technické, tak pedagogické aspekty, mohou učitelé efektivně připravit žáky na výzvy digitálního světa a pomoci jim stát se odpovědnými a informovanými uživateli technologií.

Chování žáků v online prostředí

S rostoucím významem online vzdělávání se zvyšuje i potřeba vzdělávání o kyberbezpečnosti a vytváření povědomí mezi žáky. Výzkum zdůrazňuje, že žáci čelí různým hrozbám v online prostředí, jako je kyberšikana, online podvody a cílení předsudků. Vzdělávání o kyberbez-

pečnosti může žákům pomoci chránit se před těmito hrozbami (Amankwa, 2021). Studie také ukázaly, že existuje významný vztah mezi povědomím žáků o kyberbezpečnosti a jejich rizikovým chováním online. Žáci s vyšším povědomím o kyberbezpečnosti jsou méně náchylní k rizikovým aktivitám, jako je sdílení osobních informací na internetu a vystavení se kyberútokům (Sarathchandra et al., 2016).

Jiný výzkum provedený mezi vysokoškolskými studenty odhalil, že vyšší úroveň vědomostí o kyberbezpečnosti má pozitivní dopad na jejich online chování, jako je ochrana osobních údajů a opatrnost při používání sociálních médií (Haque et al., 2023). Důležitost osobní zodpovědnosti a sebereflexe v otázkách kyberbezpečnosti je také zdůrazňována výzkumem. Žáci, kteří jsou si vědomi potenciálních online rizik, mají větší pravděpodobnost, že budou jednat bezpečněji a odpovědněji v kyberprostoru (Tirumala, Sarrafzadeh, & Pang, 2016).

Výuka o kyberbezpečnosti ve školách může hrát klíčovou roli během změn chování žáků v digitálním světě. Vytváření povědomí a pochopení kyberbezpečnostních rizik a hrozeb je zásadní pro ochranu žáků před kyberzločiny (Yuliana, 2022). Začlenění témat kyberbezpečnosti do školních vzdělávacích programů a poskytování praktického vzdělávání může žákům poskytnout dovednosti a znalosti potřebné k bezpečné navigaci v online prostředí a k přijímání informovaných rozhodnutí při používání digitálních technologií. Je důležité poznamenat, že efektivní vzdělávání v oblasti kyberbezpečnosti by mělo být přizpůsobeno věku a úrovni znalostí žáků (Livingstone et al., 2011). Pro mladší žáky může být vhodné používat interaktivní a hravé metody výuky, zatímco pro starší žáky mohou být přínosnější praktické workshopy a simulace reálných scénářů kybernetických hrozeb. Tímto způsobem lze zajistit, že vzdělávací obsah bude pro žáky relevantní a snadno pochopitelný. Kromě toho je důležité zdůraznit roli rodičů a celé školní komunity v podpoře bezpečného online chování žáků. Školy by měly aktivně zapojovat rodiče do vzdělávacího procesu o kyberbezpečnosti, poskytovat jim informace a nástroje pro podporu bezpečného používání internetu doma. Tato spolupráce mezi školou a rodinou může významně přispět k vytvoření konzistentního a komplexního přístupu k bezpečnému chování v online prostředí.

Tímto komplexním přístupem, který zahrnuje vzdělávání žáků, podporu učitelů a zapojení rodičů, mohou školy vytvořit kulturu kyberbezpečnosti, která bude žáky připravovat na bezpečné a odpovědné fungování v digitálním světě.

Technické aspekty kybernetické bezpečnosti ve škole

Při implementaci technických aspektů kybernetické bezpečnosti ve školním

prostředí je klíčové zvolit vhodný operační systém na počítačích. Systémy jako Chrome OS nabízejí ve srovnání s Windows větší míru zabezpečení, protože mají již v základu zablokované mnohé nežádoucí funkce (Fernanda, n.d.). Volba operačního systému však také závisí na konkrétních potřebách školy, například zda žáci pracují převážně v cloudovém prostředí, nebo vyžadují specifické aplikace dostupné pouze pro Windows. Zvolená politika zásad zabezpečení a způsob, jakým je prezentována žákům, může významně ovlivnit jejich vnímání a postoj ke kybernetické bezpečnosti (Kovacevic et al., 2017).

Fyzické zabezpečení hardwaru je dalším klíčovým aspektem kybernetické bezpečnosti ve školním prostředí. Obzvláště důležité je zabezpečení školního serveru, na kterém jsou uložena citlivá data. Server by měl být umístěn v uzamykatelné místnosti s omezeným přístupem a chráněn proti neoprávněné manipulaci (Alkahtani, 2018).

Pozornost je třeba věnovat také zabezpečení běžných počítačů, které žáci a učitelé denně používají. Jednou z hrozeb, o které je dobré vědět, jsou USB keyloggery. Tato zařízení se připojují mezi klávesnici a počítač a zaznamenávají všechny stisknuté klávesy, což může vést k odcizení citlivých informací, jako jsou přihlašovací údaje nebo osobní data (Tetmeyer & Saiedian, 2010). Keyloggery existují jak v hardwarové, tak v softwarové podobě. Na softwarové úrovni je důležité správné nastavení firewallu, který řídí síťový provoz a může blokovat přístup na nevhodné nebo potenciálně škodlivé webové stránky.

Školy mohou zvážit také omezení přístupu k sociálním sítím, které mohou být zdrojem rozptýlení a potenciálních bezpečnostních rizik (Willard, 2007). Efektivní správa uživatelských účtů je dalším klíčovým prvkem. Každý žák by měl mít vlastní přihlašovací údaje, ideálně vázané na školní e-mailový účet. Toto opatření zajišťuje odpovědnost a umožňuje sledovat aktivitu jednotlivých uživatelů. Je třeba se vyvarovat používání sdílených účtů, které představují značné bezpečnostní riziko. Pokud se žák zapomene odhlásit, jeho účet může být snadno zneužit. Nastavení maximální doby platnosti cookies a automatické odhlašování po určité době nečinnosti může toto riziko dále snížit.

V rámci omezení potenciálních hrozeb je vhodné zvážit také omezení spustitelných aplikací na nezbytné minimum. Tím se sníží riziko spuštění škodlivého softwaru a zjednoduší se správa a údržba systémů. Implementace těchto technických opatření vyžaduje pečlivé plánování, pravidelnou údržbu a průběžné přizpůsobování měnícím se hrozbám.

Je důležité zdůraznit, že technická opatření sama o sobě nestačí. Musí být doprovázena odpovídajícím vzděláváním a budováním povědomí o kybernetické bezpečnosti mezi žáky i učiteli. Pouze kombinací technologií a lidského faktoru lze vytvořit skutečně odolné a bezpeč-

né digitální prostředí ve školách. Tento holistický přístup zahrnující technické, vzdělávací a procesní aspekty je klíčový pro vytvoření komplexní strategie kybernetické bezpečnosti v moderním vzdělávacím prostředí.

Charakteristika analyzovaných vzdělávacích programů v oblasti kybernetické bezpečnosti

V této části se zaměříme na analýzu vybraných vzdělávacích programů a iniciativ v oblasti kybernetické bezpečnosti, které jsou realizovány v České republice. Tyto programy byly vybrány na základě jejich relevance, dopadu a inovativního přístupu k vzdělávání v oblasti kybernetické bezpečnosti. Cílem této analýzy je poskytnout přehled o současných trendech a přístupech k budování povědomí o kybernetické bezpečnosti mezi žáky, učiteli a širší veřejností.

Metodologie analýzy

Analýza se soustředí na identifikaci klíčových charakteristik vzdělávacích programů, jejich cílů, metod výuky a potenciálních dopadů na zvyšování povědomí o kybernetické bezpečnosti mezi žáky. Výzkum se zaměřuje na tři hlavní oblasti: 1) identifikaci programů a iniciativ v oblasti kybernetické bezpečnosti ve školním prostředí v České republice, 2) analýzu charakteristik těchto programů, jejich cílů a metod výuky a 3) zhodnocení přínosu těchto programů ke zvýšení digitální gramotnosti a kybernetické bezpečnosti žáků. Pro účely této analýzy byla využita kvalitativní obsahová analýza veřejně dostupných zdrojů. Tento postup zahrnoval rešerši odborné literatury týkající se kybernetické bezpečnosti ve vzdělávání, analýzu oficiálních webových stránek relevantních programů a projektů a využití databází grantových projektů a vzdělávacích iniciativ v České republice. Kritéria pro zařazení programů do analýzy zahrnovala zaměření na kybernetickou bezpečnost, cílovou skupinu žáků základních a středních škol v České republice, dostupnost podrobných informací o programu a jeho multidisciplinární přístup zahrnující oblasti jako informační technologie, pedagogika a psychologie.

Vybrané programy byly podrobeny detailní kvalitativní analýze, která se zaměřila na identifikaci deklarovaných cílů, analýzu obsahu a použitých vzdělávacích metod, hodnocení dostupných informací o výsledcích a efektivitě programu a identifikaci zapojených stakeholderů. Je třeba poznamenat, že tato analýza má své limity, zejména v oblasti dostupnosti dat o některých programech a časovém rámci výzkumu, který nemusí zachytit nejnovější iniciativy. Přes snahu o maximální objektivitu je také nutné brát v úvahu možnost subjektivity v interpretaci dat.

Projekt E-Bezpečí

Projekt E-Bezpečí, působící na území České republiky, představuje respektovaný program zaměřený na široké spektrum aktivit souvisejících s internetovým prostředím. Primárním cílem projektu je prevence, osvěta, výzkum a intervence v oblastech spojených s rizikovým chováním v online prostoru a s fenomény, které s tímto chováním úzce souvisí. V poslední době došlo k rozšíření projektu o podporu pozitivního využívání informačních technologií ve vzdělávacím procesu i v každodenním životě.

Klíčovými oblastmi, na které se projekt E-Bezpečí zaměřuje, jsou různé formy kybernetických hrozeb, mezi které patří kyberšikana, sexting, kybergrooming, kyberstalking a rizika spojená se sociálními sítěmi. Projekt se dále věnuje problematice šíření hoaxů, spamu, fake news, online závislostí, fenoménu youtuberingu a zneužívání osobních údajů v elektronických médiích (E-bezpečí, n.d.).

Projekt E-Bezpečí se zaměřuje na detailní zkoumání jednotlivých forem rizikového chování. Například kyberšikana je definována jako „úmyslné a opakované působení újmy prostřednictvím počítačů, mobilních telefonů a jiných elektronických zařízení". Sexting, definovaný jako „sdílení sexuálně explicitních materiálů prostřednictvím mobilních telefonů či internetu" (Döring, 2014), představuje další významnou hrozbu zejména pro mladé uživatele. Kybergrooming, tedy „navazování kontaktu s dítětem prostřednictvím informačních a komunikačních technologií za účelem jeho sexuálního zneužití" (Kopecký, 2012), je další oblastí, které projekt věnuje pozornost.

Hlavním pilířem projektu je terénní práce s různými cílovými skupinami, mezi které patří žáci, pedagogičtí pracovníci, odborníci v oblasti prevence sociálně patologických jevů, policisté a další profesionálové, zároveň však i rodiče. Projekt klade důraz na přednáškovou činnost a preventivní vzdělávací akce, které jsou interaktivní a zahrnují multimediální prezentace a video ukázky zaměřující se jak na konkrétní případy nebezpečí, tak na metody prevence a ochrany.

Z psychologického a sociálně-pedagogického hlediska je důležité zdůraznit, že projekt E-Bezpečí usiluje o komplexní přístup k problematice bezpečnosti na internetu. Pravidelné výzkumy ohledně rizikové komunikace v online prostředí, provoz online poradny, vydávání tiskovin pro žáky a učitele a šíření osvěty o bezpečném chování na internetu jsou klíčovými aktivitami, které projekt realizuje. Tento multidisciplinární přístup umožňuje efektivně oslovit různé cílové skupiny a poskytovat jim relevantní informace a podporu. Projekt E-Bezpečí tak hraje významnou roli v prevenci a řešení problémů spojených s rizikovým chováním v online prostředí. Jeho aktivity přispívají k vytváření bezpečnějšího internetového prostředí a rozvoji digitální gramotnosti uživatelů v České republice.

Využití peer programů

Peer programy se ukazují jako účinný nástroj pro prevenci kyberšikany a podporu bezpečného užívání internetu na základních školách v České republice. Dokument metodiky „Žij online bezpečně!“ od Centra inkluze, o.p.s. z roku 2016 popisuje projekt zaměřený na zavádění peer programů v opavském regionu s cílem předcházet rizikovému chování spojenému s užíváním internetu a online komunikací.

Hlavním principem peer programů je zapojení předem proškolených peerů (vrstevníků) do aktivit, které mají podpořit jejich vrstevníky v oblasti primární prevence rizikového chování. Tito vrstevníci jsou obvykle žáci stejného nebo podobného věku jako cílová skupina, což jim umožňuje lépe navázat vztah a důvěru se svými vrstevníky. Peeři mohou působit jako pozitivní vzory, sdílet své zkušenosti a poskytovat rady a podporu v oblasti bezpečného používání internetu a prevence kyberšikany.

Projekt „Žij online bezpečně!“ se zaměřil nejen na samotnou realizaci peer programů, ale také na vytvoření a ověření metodiky práce s peery. Tato metodika poskytuje školám a pedagogům praktické nástroje a postupy, jak efektivně připravit a vést peer programy v oblasti kyberbezpečnosti. Součástí metodiky mohou být například školení pro peery, tematické workshopy, diskusní skupiny nebo online zdroje (Centrum inkluze o. p. s., 2016).

Výzkumy ukazují, že peer programy mohou mít pozitivní vliv na názory a postoje mladých lidí. Žáci jsou často více otevřeni radám a zkušenostem svých vrstevníků než formálním přednáškám od dospělých. Peer programy tak mohou přispět k vytvoření kultury bezpečného a zodpovědného používání internetu mezi žáky a podpořit otevřenou diskusi o tématech kyberšikany a online bezpečnosti (Kopecký & Szotkowski, 2015). Projekt „Žij online bezpečně!“ a využití peer programů představují slibný přístup k prevenci kyberšikany a podpoře bezpečného užívání internetu na základních školách v České republice. Je důležité, aby školy měly přístup k ověřeným metodikám a nástrojům, které jim pomohou efektivně implementovat peer programy a přizpůsobit je specifickým potřebám jejich žáků. Zároveň je nezbytné zajistit dlouhodobou udržitelnost a kontinuitu těchto programů, aby měly trvalý dopad na postoje a chování mladých lidí v online prostředí.

WebRangers jako příklad úspěšného peer programu

Jednou z úspěšných iniciativ, která se zaměřuje na zvyšování povědomí o kyberbezpečnosti mezi mladými lidmi v České republice, je projekt WebRangers společnosti Google. Tento projekt se soustředí na děti a mládež ve věku 13 až 16 let a jeho cílem je podpořit smysluplné a kreativní využívání současných technologií, informačních a komunikač-

ních možností a zároveň minimalizovat vystavení nežádoucím rizikům (Projekt E-bezpečí, 2015; Vybíral, 2015).

WebRangers si klade za cíl vzdělávat mladé lidi v oblasti kyberbezpečnosti interaktivním a angažovaným způsobem. Projekt využívá různé formáty, jako jsou workshopy, soutěže a online zdroje, aby žáky zaujal a motivoval k aktivnímu zapojení do procesu učení. Důraz je kladen na rozvoj kritického myšlení, mediální gramotnosti a odpovědného chování v online prostředí.

Úspěch projektu WebRangers v České republice ukazuje, že existuje rostoucí poptávka po vzdělání v oblasti kybernetické bezpečnosti a že mladí lidé jsou ochotni se aktivně zapojit do iniciativ, které jim pomáhají chránit se před online hrozbami. Projekty jako WebRangers jsou důležitým doplňkem formálního vzdělávání v oblasti kyberbezpečnosti ve školách. Spolupráce mezi soukromým sektorem, vzdělávacími institucemi a vládními orgány může pomoci vytvořit komplexní ekosystém peer vzdělávání v oblastech kyberbezpečnosti, který bude reagovat na potřeby a výzvy digitální éry.

O2 Chytrá škola

O2 Chytrá škola je vzdělávací projekt, který vznikl z iniciativy společnosti O2 Czech Republic s cílem podpořit využívání digitálních technologií ve výuce na základních a středních školách v České republice. Tento projekt si klade za cíl pomoci školám, učitelům i žákům lépe se orientovat v moderních technologiích a naučit se je efektivně využívat při výuce i samotném procesu učení.

Projekt nabízí školám a pedagogům širokou škálu vzdělávacích materiálů a metodik, které ukazují, jak smysluplně zapojit digitální technologie do výuky různých předmětů. Součástí projektu jsou také semináře, workshopy a konference, kde se učitelé mohou seznámit s nejnovějšími trendy a možnostmi využití tabletů, interaktivních tabulí, online nástrojů a dalších technologií ve vzdělávání (O2 Chytrá škola, n.d.).

O2 Chytrá škola také vyhlašuje soutěže a granty, které mají za cíl podpořit inovativní vzdělávací projekty na školách, jež efektivně využívají moderní technologie. Projekt spolupracuje s řadou odborníků a institucí v oblasti školství a vzdělávání, aby zajistil vysokou kvalitu a odbornost všech svých aktivit. Nedílnou součástí O2 Chytré školy je online platforma, která učitelům poskytuje inspiraci, zdroje a nástroje pro jejich práci.

Smyslem celého projektu je přispět k modernizaci českého školství, zvýšit digitální kompetence učitelů i žáků a zatraktivnit výuku pomocí smysluplného využití technologií. O2 Chytrá škola tak reaguje na rostoucí důležitost digitálních dovedností, které jsou nezbytné pro uplatnění v 21. století. Tento projekt je významným příspěvkem k rozvoji digitální gramotnosti a bezpečnosti v českém vzdělávacím systému.

Křečci v síti (Seznam se bezpečně)

Křečci v síti je projekt, který vznikl ve spolupráci společnosti Seznam.cz a Divadla v Dlouhé. Jedná se o sérii krátkých hraných videí, která upozorňují na různá rizika spojená s používáním internetu a sociálních sítí, jako je sexting, kybergrooming, kyberšikana a další. Projekt navazuje na úspěšné dokumentárně vzdělávací filmy „Seznam se bezpečně", které byly určeny dětem ve věku 10–16 let, jejich rodičům a pedagogům. První i druhý díl získal záštitu MŠMT ČR a byl distribuován do všech základních škol v České republice (Safer Internet Center, n.d.; Projekt E-bezpečí, n.d.).

Série videí Křečci v síti je natočena formou krátkých příběhů, které ukazují, jak snadno se mohou děti a dospívající na internetu dostat do nebezpečných situací. Každý díl se věnuje jinému tématu a je doplněn o informace a rady, jak se v podobných situacích chovat a na koho se obrátit pro pomoc. V jednotlivých příbězích jsou ukázána rizika anonymního seznamování, poskytování intimních fotografií, vydírání a další hrozby.

Cílem projektu je zvýšit povědomí o online rizicích mezi dětmi, rodiči i pedagogy a poskytnout jim nástroje, jak těmto rizikům předcházet a jak se před nimi chránit. V rámci projektu byly vytvořeny pracovní a metodické příručky pro pedagogy, které navrhují, jak s videi hraných scének zacházet v rámci vzdělávání dětí. Videa jsou volně dostupná na webu služby Stream.cz a jsou určena pro použití ve školách, v rodinách i pro individuální zhlédnutí. Tento projekt představuje inovativní přístup k vzdělávání v oblasti kybernetické bezpečnosti, který využívá sílu storytellingu a vizuálního média k efektivnímu předávání důležitých informací a varování před online riziky.

Be Internet Awesome (Interland)

Projekt „Be Internet Awesome" společnosti Google představuje komplexní vzdělávací program zaměřený na rozvoj digitální gramotnosti a online bezpečnosti u dětí. Tento bezplatný program si klade za cíl poskytnout mladým uživatelům internetu nezbytné znalosti a dovednosti, které jim pomohou orientovat se v digitálním prostředí zodpovědně a bezpečně.

Program se skládá z pěti klíčových modulů, které pokrývají oblasti jako chytré vyhledávání a ověřování informací, ochrana soukromí, prevence kyberšikany, zabezpečení účtů a odpovědné sdílení na sociálních sítích. Každý modul obsahuje interaktivní materiály, včetně her, videí a praktických aktivit, které jsou přizpůsobeny různým věkovým kategoriím. Tento multimediální přístup umožňuje dětem osvojit si důležité koncepty zábavnou formou (Google, n.d.).

Jedním z hlavních prvků projektu je

hra Interland, která slouží jako platforma pro procvičování získaných dovedností. Prostřednictvím herních mechanismů jsou děti vedeny k aplikaci naučených principů v simulovaném online prostředí. Tento praktický nácvik pomáhá upevnit znalosti a podporuje rozvoj žádoucích návyků (Cortesi et al., 2020).

Materiály programu „Be Internet Awesome" jsou volně dostupné a snadno implementovatelné ve školním prostředí. Učitelé mají k dispozici ucelený soubor zdrojů, který mohou začlenit do výuky informatiky, mediální výchovy či průřezových témat. Program tak poskytuje pedagogům nástroje k systematickému rozvoji digitálních kompetencí žáků (Walters et al., 2019).

Je však důležité poznamenat, že program „Be Internet Awesome" má i své limity. Studie autorů Seale a Schoenberger (2018) přináší cenný kritický pohled na tento program a poukazuje na některé jeho potenciální nedostatky. Jejich analýza obsahu programu odhaluje, že ačkoli program pokrývá klíčová témata online bezpečnosti, jeho přístup může být poněkud povrchní a neposkytuje dětem dostatečně hluboké a komplexní porozumění. Autoři upozorňují na to, že program se zaměřuje především na základní informace a doporučení, ale nevěnuje dostatek pozornosti složitějším aspektům používání internetu a bezpečnosti.

Dalším problematickým aspektem, na který studie poukazuje, je malá pozornost věnovaná řešení externích hrozeb a výzev, které jsou mimo kontrolu uživatele. Pochopení těchto vnějších rizik je přitom zásadní pro komplexní vzdělávání v oblasti online bezpečnosti. Tento poznatek zdůrazňuje potřebu, aby vzdělávací programy překročily hranice pouhého předávání základních pravidel bezpečnosti na internetu.

Navzdory těmto omezením projekt „Be Internet Awesome" svým systematickým přístupem k výuce digitální gramotnosti a online bezpečnosti přispívá k přípravě mladé generace na nové výzvy kyberprostoru. Tato snaha je v souladu s obecnou potřebou posílit kompetence žáků v oblasti informačních a komunikačních technologií a podporovat jejich odpovědné a bezpečné užívání (Livingstone et al., 2014).

V kontextu českého vzdělávacího prostředí může být „Be Internet Awesome" cenným doplňkem k již existujícím lokálním iniciativám. Jeho globální dosah a rozsáhlé zdroje mohou poskytnout inspiraci a nástroje pro další rozvoj vzdělávacích programů v oblasti kybernetické bezpečnosti v České republice.

Kybertest.cz

Kybertest.cz je interaktivní vzdělávací platforma, která si klade za cíl poskytnout uživatelům praktické znalosti a dovednosti, jak rozpoznat a čelit různým typům kybernetických hrozeb (Česká bankovní asociace, n.d.). Tato iniciativa představuje inovativní přístup k vzdělávání v oblasti kybernetické bezpečnosti, který využívá princi-

py gamifikace a interaktivního učení. Jedním z klíčových aspektů platformy Kybertest.cz je využití herních principů pro zvýšení motivace a angažovanosti uživatelů. Gamifikace vzdělávacího obsahu má potenciál zvýšit zájem a zapojení žáků, což vede k lepším výsledkům učení (Kapp, 2012). Kybertest.cz staví účastníky do role správce virtuálních financí, který má za úkol ochránit svěřené prostředky před různými typy kybernetických podvodů. Tento přístup umožňuje uživatelům aktivně aplikovat získané znalosti v realistickém kontextu.

Efektivní zpětná vazba je klíčovým prvkem procesu učení (Hattie & Timperley, 2007). Kybertest.cz poskytuje uživatelům okamžitou a informativní zpětnou vazbu po každé testové otázce. Toto podrobné vysvětlení správného řešení umožňuje účastníkům poučit se ze svých chyb a zlepšovat své výsledky v dalších kolech. Začlenění zpětné vazby do vzdělávacího procesu je v souladu s principy formativního hodnocení, které se zaměřuje na podporu učení a rozvoj dovedností (Black & Wiliam, 2009).

Vývoj platformy Kybertest.cz probíhal ve spolupráci s týmem renomovaných odborníků z předních českých firem specializujících se na kyberbezpečnost (Česká bankovní asociace, n.d.). Tato spolupráce zajišťuje, že obsah platformy je přesný, aktuální a relevantní pro reálné situace, kterým uživatelé čelí v online prostředí. Zapojení odborníků z praxe do procesu tvorby vzdělávacích materiálů je v souladu s principy autentického učení, které zdůrazňuje význam propojení akademických znalostí s reálným světem (Herrington & Oliver, 2000).

Interaktivní vzdělávací platforma Kybertest.cz představuje inovativní přístup ke zvyšování povědomí o kyberbezpečnosti. Využití herních principů, poskytování efektivní zpětné vazby a spolupráce s odborníky z praxe jsou klíčovými faktory, které přispívají k účinnosti této platformy. Kybertest.cz má potenciál oslovit široké spektrum uživatelů a významně přispět k rozvoji digitální gramotnosti a odolnosti vůči kybernetickým hrozbám v současné společnosti.

Je však třeba poznamenat, že pro plné zhodnocení efektivity platformy Kybertest.cz by bylo vhodné provést další výzkum. Tento výzkum by se mohl zaměřit na vyhodnocení dopadu platformy na znalosti a chování uživatelů v oblasti kybernetické bezpečnosti, a to pomocí kvantitativních a kvalitativních metod. Zároveň by bylo přínosné zkoumat možnosti implementace této platformy v různých vzdělávacích kontextech, od základních škol až po vzdělávání dospělých.

Iniciativy jako Kybertest.cz představují důležitý krok směrem k vytvoření komplexního ekosystému vzdělávání v oblasti kybernetické bezpečnosti v České republice. Kombinací inovativních přístupů, spolupráce s odborníky a využití moderních technologií mohou tyto projekty významně přispět k zvýšení digitální gramotnosti a bezpečnosti v online prostředí.

Limity výzkumu

Výzkum v oblasti kybernetické bezpečnosti ve školním prostředí čelí několika významným limitům a výzvám. Rychlý vývoj technologií a neustále se měnící povaha kybernetických hrozeb představují pro výzkumníky náročný úkol. Aby udrželi krok s rychlým tempem změn, musí neustále sledovat nejnovější trendy a přizpůsobovat své metody a přístupy (Kenneally & Claffy, 2010). Tento dynamický charakter kybernetických hrozeb ztěžuje provádění dlouhodobých studií a zobecňování výsledků.

Dalším limitem je omezená zobecnitelnost výzkumů, které jsou často prováděny na specifických vzorcích populace, například na určité věkové skupině nebo v konkrétním regionu. Tato specifičnost může omezit platnost výsledků pro širší populaci nebo odlišné kontexty (Pusey & Sadera, 2011). Výzkumníci by měli pečlivě zvažovat charakteristiky svých vzorků a být opatrní při zobecňování zjištění na jiné skupiny nebo prostředí.

Měření a kvantifikace dopadů intervencí v oblasti kybernetické bezpečnosti představuje další metodologickou výzvu. Výzkumníci čelí obtížím při navrhování robustních experimentálních designů, kontrole nežádoucích proměnných a sběru validních a spolehlivých dat (Bada, Sasse, & Nurse, 2019). Etické a praktické překážky mohou omezovat možnosti provádění kontrolovaných experimentů v reálném školním prostředí, což vyžaduje inovativní metodologické přístupy.

Výzkum v oblasti kybernetické bezpečnosti často pracuje s citlivými daty a informacemi o účastnících, což vede k etickým a právním otázkám. Výzkumníci musí pečlivě zvážit etické a právní aspekty sběru, uchovávání a analýzy dat, aby ochránili soukromí a bezpečnost účastníků (Kenneally & Claffy, 2010). Dodržování etických standardů a právních předpisů může být náročné, zejména při práci s nezletilými účastníky ve školním prostředí.

Kybernetická bezpečnost je komplexní a multidisciplinární oblast, která vyžaduje spolupráci odborníků z různých oborů, jako jsou informační technologie, psychologie, pedagogika a další (Kessler & Ramsay, 2013). Koordinace a integrace poznatků z různých disciplín může být náročná, což vyžaduje efektivní komunikaci a spolupráci mezi výzkumníky s různým zázemím a odbornými znalostmi.

Dynamika školního prostředí je dalším faktorem, který může ovlivnit implementaci a účinnost bezpečnostních opatření. Výzkumníci musí zohlednit organizační, kulturní a sociální faktory, které se mezi školami liší (Pusey & Sadera, 2011). Tyto faktory mohou zahrnovat technologickou infrastrukturu školy, postoje a znalosti učitelů, školní politiky a další kontextuální proměnné, které mohou ovlivnit výsledky výzkumu.

V neposlední řadě je třeba zmínit, že mnohé dopady intervencí v oblasti kybernetické bezpečnosti se mohou projevit až v delším časovém horizontu. Longitudinální studie, které sledují účastníky po

delší dobu, jsou nezbytné pro pochopení dlouhodobých účinků a udržitelnosti intervencí (Bada et al., 2019). Tyto studie jsou však náročné na realizaci, vyžadují dlouhodobé zdroje a závazek ze strany výzkumníků i účastníků.

I přes tyto limity a výzvy je výzkum v oblasti kybernetické bezpečnosti ve školním prostředí naprosto nezbytný. Pouze prostřednictvím systematického zkoumání a důkladného porozumění problematice lze vytvořit efektivní strategie a intervence, které pomohou chránit žáky a zajistit, že technologie budou využívány bezpečným a odpovědným způsobem.

Závěr

Kybernetická bezpečnost je v moderním vzdělávání stejně důležitá jako tradiční předměty. S narůstající integrací technologií do výuky čelí školy naléhavé potřebě přijmout komplexní opatření, která sníží rizika spojená s online hrozbami a zároveň podpoří rozvoj digitálních kompetencí žáků. Tento článek analyzoval různé strategie, jež mohou vzdělávací instituce implementovat s cílem posílit kybernetickou bezpečnost a digitální gramotnost.

Z provedené analýzy vyplývá, že efektivní přístup ke kybernetické bezpečnosti ve školách vyžaduje multidisciplinární perspektivu, která zahrnuje technologické, pedagogické a psychologické aspekty. Implementace robustních bezpečnostních politik, integrace moderních technologií a důraz na vzdělávání a osvětu jsou klíčovými pilíři komplexní strategie kybernetické bezpečnosti (Williams & Krueger, 2005; Pangrazio & Cardozo-Gaibisso, 2020; Maqsood & Chiasson, 2021).

Vývoj a implementace bezpečnostních politik představuje zásadní krok v budování odolného digitálního prostředí. Tyto politiky musí být srozumitelné, dobře strukturované a pravidelně aktualizované, aby reflektovaly dynamickou povahu kybernetických hrozeb (Donaldson et al., 2015; Mishra et al., 2022). Zapojení všech členů školní komunity do procesu tvorby a realizace bezpečnostních politik je nezbytné pro vytvoření kultury kybernetické bezpečnosti (Flowerday & Tuyikeze, 2016).

Integrace efektivních technických nástrojů, jako jsou firewally, antivirové programy a monitorovací systémy, poskytuje základní úroveň ochrany před kybernetickými útoky (Waghere et al., 2023). Nicméně samotná technologická řešení nestačí. Je nezbytné zohlednit lidský faktor a behaviorální aspekty prostřednictvím kontinuálního vzdělávání, osvěty a rozvoje digitálních kompetencí žáků i učitelů (Lahcen et al., 2020; Pencheva et al., 2020).

Analýza také poukázala na význam peer programů a iniciativ, jako je projekt E-Bezpečí (Kopecký, 2012; Döring, 2014), WebRangers (Projekt E-bezpečí, 2015; Vybíral, 2015) nebo „Žij online bezpečně!“ (Centrum inkluze o. p. s., 2016), které přispívají k prevenci rizikového

chování a podporují bezpečné užívání internetu mezi mladými lidmi v České republice. Tyto programy zdůrazňují důležitost aktivního zapojení žáků do procesu učení a rozvoje digitálních kompetencí.

Inovativní přístupy, jako je gamifikace vzdělávacího obsahu v případě platformy Kybertest.cz, ukazují potenciál interaktivních a zábavných metod výuky kybernetické bezpečnosti. Tyto přístupy mohou významně zvýšit angažovanost žáků a efektivitu vzdělávacího procesu (Česká bankovní asociace, n.d.; Kapp, 2012).

Závěrem lze konstatovat, že vytvoření bezpečného a podpůrného digitálního prostředí ve školách vyžaduje komplexní a koordinovaný přístup, který kombinuje technologická řešení, robustní bezpečnostní politiky, vzdělávání a osvětu. Pouze prostřednictvím úzké spolupráce mezi IT odborníky, pedagogy, psychology a dalšími zainteresovanými stranami lze účinně čelit výzvám kybernetické bezpečnosti a připravit žáky na zodpovědný život v digitálním věku (Pencheva et al., 2020).

Investice do kybernetické bezpečnosti a digitální gramotnosti jsou nezbytné pro budoucnost vzdělávání a pro snížení rizik, jimž je mladá generace vystavena v online světě. Přestože výzkum v této oblasti čelí mnoha výzvám a omezením, jeho význam pro vytváření efektivních strategií a intervencí je nezpochybnitelný. Budoucí výzkum by se měl zaměřit na překonání identifikovaných limitů zejména prostřednictvím longitudinálních studií a robustnějších metodologických přístupů, které umožní lépe pochopit dlouhodobé dopady a účinnost různých intervencí v oblasti kybernetické bezpečnosti ve školním prostředí.

Literatura

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, *42*(12), 40–46.

Alkahtani, K. D. (2018). Cyber security challenges and solutions for V2X communications: A survey. Computer Networks, 151, 144–156. https://doi.org/10.1016/j.comnet.2018.12.018

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security. https://doi.org/10.4236/jis.2021.124013.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Black, P., & Wiliam, D. (2009). Developing the theory of formative assessment. Edu-

cational Assessment, Evaluation and Accountability, *21*(1), 5–31. https://doi.org/10.1007/s11092-008-9068-5

Cabric, M. (2015). Confidentiality, Integrity, and Availability, 185–200. https://doi.org/10.1016/B978-0-12-802934-3.00011-1.

Centrum inkluze o. p. s. (2016). Využití peer programů na základních školách v oblasti prevence kyberšikany: Metodická příručka pro pedagogy.

Česká bankovní asociace. (n.d.) Kybertest.cz

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9, 744. https://doi.org/10.3389/fpsyg.2018.00744

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). Sample Cybersecurity Policy. 335–351. https://doi.org/10.1007/978-1-4302-6083-7_19.

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? Cyberpsychology: Journal of Psychosocial Research on Cyberspace, *8*(1), Article 9. https://doi.org/10.5817/CP2014-1-9

Fernanda. (2024, March 15). Best practices for chromebook security in K-12 schools. GAT for Education. https://gatlabs.com/education/blog/best-practices-for-chromebook-security-in-k-12-schools/

Flowerday, S., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. Comput. Secur., 61, 169–183. https://doi.org/10.1016/j.cose.2016.06.002.

Gashi, L., Luma, A., & Aliu, A. (2022). A comprehensive review of cybersecurity perspective for Wireless Sensor Networks. 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 392–395. https://doi.org/10.1109/ISMSIT56059.2022.9932788.

Google. (n.d.). Be internet awesome. https://beinternetawesome.withgoogle.com/en_us

Haque, M., Ahmad, S., Haque, S., Kumar, K., Mishra, K., & Mishra, B. (2023). Analyzing University Students' Awareness of Cybersecurity. 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 250–257. https://doi.org/10.1109/ETNCC59188.2023.10284971.

Hattie, J., & Timperley, H. (2007). The Power of Feedback. Review of Educational Research, *77*(1), 81–112. https://doi.org/10.3102/003465430298487

Herrington, J., & Oliver, R. (2000). An instructional design framework for authentic learning environments. Educational Technology Research and Development, *48*(3), 23–48. https://doi.org/10.1007/BF02319856

Javidi, G., & Sheybani, E. (2018). K-12 Cybersecurity Education, Research, and

Outreach. 2018 IEEE Frontiers in Education Conference (FIE), 1–5. https://doi.org/10.1109/FIE.2018.8659021.

Kapp, K. M. (2012). The gamification of learning and instruction: Game-based methods and strategies for training and education. Pfeiffer, A Wiley Imprint.

Kenneally, E. E., & Claffy, K. (2010). Dialing privacy and utility: a proposed data-sharing framework to advance Internet research. IEEE Security & Privacy, *8*(4), 31–39.

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. Journal of Homeland Security Education, 2, 35–44.

Kopecký, K. (2012). Sexting among Czech preadolescents and adolescents. New Educational Review, *28*(2), 39–48

Kopecký, K., & Szotkowski, R. (2015). Kyberšikana a další formy rizikového chování českých dětí v prostředí internetu. Adiktologie, *15*(3), 166–173.

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors related to cyber security behavior. IEEE Access, 6, 26–27. DOI:10.1109/ACCESS.2020.3007867

Lahcen, R., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3, 1–18. https://doi.org/10.1186/s42400-020-00050-w.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. EU Kids Online, London School of Economics and Political Science, London.

Magazín BezpečnostPráce.info, z.s. (2022, September 1). Kybernetická a informační bezpečnost. Legislativa, Povinnosti, útoky. BezpečnostPráce.info. https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/

Maqsood, S., & Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. ACM Transactions on Privacy and Security (TOPS), 24, 1–37. https://doi.org/10.1145/3469821.

Mishra, A., Alzoubi, Y., Gill, A., & Anwar, M. (2022). Cybersecurity Enterprises Policies: A Comparative Study. Sensors (Basel, Switzerland), 22. https://doi.org/10.3390/s22020538.

O2 chytrá škola. (n.d.). O nás. https://o2chytraskola.cz/

Pangrazio, L., & Cardozo-Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. Digital Education Review, 37, 49–63. https://doi.org/10.1344/der.2020.37.49-63.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management (3rd ed.). CRC Press.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating

Cybersecurity Into Secondary School Education. IEEE Security & Privacy, 18, 68–74. https://doi.org/10.1109/MSEC.2020.2969409.

Portál E-bezpečí. (2015). WebRangers – leták A4. https://www.e-bezpeci.cz

Portál E-bezpečí. (n.d.). https://www.e-bezpeci.cz

Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. Journal of Digital Learning in Teacher Education, *28*(2), 82–88.

Reason, J. (1990). Human error. Cambridge University Press.

Safer Internet Center. (n.d.) O nás. https://www.bezpecnyinternet.cz/cs/o-nas/

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. 2016 Cybersecurity Symposium (CYBERSEC), 68–73. https://doi.org/10.1109/CYBERSEC.2016.018.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‚weakest link'—a human/computer interaction approach to usable and effective security. BT Technology Journal, *19*(3), 122–131.

Seale, Jim & Schoenberger, Nicole. (2018). Be Internet Awesome. Emerging Library & Information Perspectives. 1. 10.5206/elip.v1i1.366.

Schneier, B. (2000). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

Sherman, A., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., Herman, G., & Thompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. Cryptologia, 42, 337–377. https://doi.org/10.1080/01611194.2017.1362063.

Tetmeyer, A., & Saiedian, H. (2010). Security threats and mitigating risk for USB devices. IEEE Technology and Society Magazine, *29*(4), 44–49. https://doi.org/10.1109/MTS.2010.939228

Tirumala, S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. 2016 14th Annual Conference on Privacy, Security and Trust (PST), 223–228. https://doi.org/10.1109/PST.2016.7906931.

Vybíral, O. (2015). Google projekt – Web Rangers potřetí. Portál o školství v Jihomoravském kraji. https://www.jmskoly.cz

Waghere, S., Pardeshi, H., Patil, S., Kurhe, K., & Karad, P. (2023). CyberSecureHub: Integrating Cyber Security Tools. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-13144.

Walters, M.G., Gee, D., & Mohammed, S. (2019). A literature review: Digital citizenship and the elementary educator. International Journal of Technology in Education (IJTE), *2*(1), 1–21.

Willard, N. E. (2007). The authority and responsibility of school officials in responding to cyberbullying. Journal of Adolescent Health, *41*(6), 64–S65. https://doi.org/10.1016/j.jadohealth.2007.08.013

Williams, C., & Krueger, K. (2005). Is Your Network Safe? Why Educators Should Care about Cybersecurity-And What They Should Do about It. T.H.E. Journal Technological Horizons in Education, 33, 36.

PhDr. Martin Beneš
Pedagogická fakulta, Katedra informačních technologií a technické výchovy
Karlova univerzita
martin.benes@pedf.cuni.cz