1/2025, Volume 17, Issue 1
ISSN 1803-537X

CURRENT STATE AND FUTURE DIRECTIONS OF CYBERSECURITY EDUCATION IN CZECHIA

Willi LAZAROV*, Vysoké učení technické v Brně, Česká republika

Přijato: 3. 3. 2025 / Akceptováno: 14. 09. 2025
Typ článku: Teoretická studie
DOI: 10.5507/jtie.2025.009

Abstract: The need to educate users in cybersecurity to some extent is critical given the ever-increasing number of cyber threats. However, the approach to education cannot be easily generalized due to the different environments, technical expertise, and age groups of users. Cybersecurity, as a distinct domain within the ICT field, involves challenging disciplines that are largely technical, and therefore it is important to include hands-on learning in the education process. The field has evolved considerably over the last 10 years, including different approaches and options for its study at higher and secondary levels of education. This article focuses on this domain in the context of the Czech environment. First, the historical development and current state of cybersecurity education is presented, highlighting the increase in the number of study programs in the countries of the European Union. Subsequently, the conducted analysis is presented, focusing more closely on the Czech education system from the higher to the primary level of education. It shows that 6 universities offer accredited study programs with a primary focus on cybersecurity. The analysis also examined the coverage of cybersecurity education at the secondary level, where 41 secondary schools (31.3%) offer at least one separate course in cybersecurity, and 18 of these schools also offer a study subfield or specialization. Considering the need for hands-on learning, the article also presents tools and methods that can be integrated to create a controlled, safe, and interactive learning environment. In this aspect, the article discusses in detail the use of local virtualization, the concept of sandboxing, cyber range platforms, and gamification techniques to increase student engagement. These methods and tools were subsequently applied and tested in the lessons by university, high school, and grammar school students. From the feedback received from the test groups, the combination of interactive and gamified methods appears to be suitable for supporting cybersecurity education.

Key words: cybersecurity, hands-on learning, educational platforms, interactivity, gamification, virtualization.

*Autor pro korespondenci: lazarov@vut.cz

1/2025, Volume 17, Issue 1
ISSN 1803-537X

SOUČASNÝ STAV A BUDOUCÍ SMĚRY VZDĚLÁVÁNÍ KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Abstrakt: Potřeba do určité míry vzdělávat uživatele v oblasti kybernetické bezpečnosti je vzhledem k stále se zvyšujícímu počtu kybernetických hrozeb kritická. Přístup k výuce však nelze jednoduše zobecnit z důvodu odlišných prostředí, technických znalostí a věkových skupin uživatelů. Kybernetická bezpečnost, jakožto samostatná doména v oblasti informačních a komunikačních technologií, zahrnuje náročné disciplíny, které jsou ve velké míře technického charakteru, a proto je důležité do vzdělávání zahrnout i praktickou výuku. Toto odvětví se za posledních 10 let výrazně posunulo, včetně různých přístupů a možností jeho studia na vysokém a středním stupni vzdělání. Tento článek se na uvedenou problematiku zaměřuje v kontextu českého prostředí. Nejprve je představen historický vývoj a současný stav vzdělávání v oblasti kybernetické bezpečnosti, který poukazuje na nárůst počtu studijních programů v zemích Evropské unie. Následně je prezentována provedená analýza, která se již blíže věnuje českému vzdělávacímu systému od vysokého po základní stupeň vzdělání. Z té plyne, že 6 vysokých škol nabízí akreditované studijní programy s primárním zaměřením na kybernetickou bezpečnost. Analýza dále zkoumala míru pokrytí výuky na středním stupni, kde 41 středních škol (31,3 %) vyučuje alespoň jeden samostatný předmět kybernetické bezpečnosti, a z toho 18 škol nabízí i oborové zaměření nebo specializaci. S ohledem na potřebu praktického vzdělávání článek dále představuje nástroje a metody, které lze integrovat za účelem vytvoření kontrolovaného, bezpečného a interaktivního výukového prostředí. V tomto ohledu článek diskutuje použití lokální virtualizace, koncept sandboxingu, platformy cyber range a formy gamifikace pro zvýšení zapojení studentů. Tyto metody a nástroje byly následně aplikovány a ve výuce testovány studenty vysoké školy, žáky střední průmyslové školy a gymnázia. Ze získané zpětné vazby od testovacích skupin se kombinace interaktivních a gamifikovaných metod jeví jako vhodná pro podporu výuky kybernetické bezpečnosti.

Klíčová slova: kybernetická bezpečnost, praktická výuka, vzdělávací platformy, interaktivita, gamifikace, virtualizace.

1 Úvod

Potřeba vzdělávání a osvěty v oblasti kybernetické bezpečnosti se s rostoucím počtem uživatelů internetu v moderní společnosti dotýká všech bez ohledu na věk, pohlaví a stupeň vzdělání. Tato skutečnost vyvstává zejména z pokračujícího nárůstu počtu kybernetických hrozeb, které cílí jak na soukromé společnosti, státní

organizace, tak i jednotlivce. Dopad úspěšně provedeného kybernetického útoku může být vysoký od ztráty citlivých údajů až po značné finanční škody způsobené nedostupností napadených služeb, poškozených aktiv nebo trestněprávní odpovědnosti (Tzavara & Vassiliadis, 2024). Z toho důvodu je žádoucí do určité míry vzdělávat všechny skupiny laické i odborné veřejnosti včetně žáků základních a středních škol nebo vysokoškolských studentů (De Bruijn & Janssen, 2017).

Naplnit uvedenou potřebu však není jednoduché. Doména kybernetická bezpečnosti se s ohledem na intenzivní technologický vývoj výrazně rozšířila na samostatné disciplíny, jejichž studium může být časově i technicky náročné. Právě technické profese vyžadují praktický trénink, jehož realizace zahrnuje mj. virtualizované prostředí (např. VMware, Virtual Box aj.), specializovaná zařízení (směrovače, přepínače, serverové stanice apod.) a softwarové licence. To společně s nutností takové prostředí průběžně aktualizovat a dále spravovat vede k vyšším finančním nákladům. Z toho důvodu může být vzdělávání personalizováno na specifické oblasti, a to ať už v rámci škol ve formě samostatných oborů a předmětů, tak i odborných kurzů, které nabízí soukromé společnosti.

2 Historický vývoj a současný stav

Historicky se i přes dlouhodobou potřebu vzdělávat všechny uživatelské skupiny touto problematikou zabývali převážně odborníci pracující v oblasti ICT (Information and Communication Technologies), jako jsou například správci sítě, systémový integrátoři atd. S dalším rozvojem studia aplikované informatiky na technických univerzitách postupně docházelo k integraci výuky kybernetické bezpečnosti do existujících studijních programů. Tuto integraci lze spatřit ve formě samostatných předmětů, oborového zaměření a později i nových studijních programů (Catota et al., 2019). V dnešní době je na kybernetickou bezpečnost kladen důraz i na středních průmyslových školách, které ji integrují do svých studijních plánů. Setkat se s touto oblastí lze i na základním stupni, ale je třeba zdůraznit, že se v této oblasti jedná převážně o osvětové programy (Mouheb et al., 2019). Mimo školství je další oblastí školení zaměstnanců státních i soukromých organizací ve formě certifikovaných kurzů, školení nebo profesního vzdělávání.

Na vysokém stupni vzdělání jsou již dnes běžné samostatné bakalářské nebo navazující magisterské studijní programy. Pro příklad v zemích spadajících do Evropské unie a Evropského sdružení volného obchodu nabízí studium kybernetické bezpečnosti 30 zemí v počtu 38 bakalářských (22,5 %), 122 magisterských

(72,2 %) a 9 postgraduálních (5,3 %) studijních oborů (ENISA, 2025). Podobná je i situace v USA, kde studium kybernetické bezpečnost nabízí 170 univerzit (Harris, 2024). Z pohledu náplně a plánu studia se přístup jednotlivých univerzit liší. Obecně však hlavní náplň studia těchto studijních programů tvoří samostatné odborné předměty, ve kterých se studenti seznamují s pokročilými tématy, jako je například kryptografie, etický hacking nebo digitální forenzní analýza. Kromě toho může být obsah související s kybernetickou bezpečností začleněn i do jiných ICT předmětů, jako je vývoj softwarových aplikací nebo počítačové sítě. Mimo výše uvedené programy mohou vysoké školy nabízet také samostatná školení a kurzy zaměřené na osvětu kybernetické bezpečnosti určené i pro studenty s netechnickým vzděláním.

Na středním stupni se výuka kybernetické bezpečnosti liší v závislosti na studijním oboru. V netechnických oborech se žáci mohou setkat převážně se základy kybernetické bezpečnosti, zejména ve formě osvěty. Naproti tomu ve studijních oborech zaměřených na ICT může být kybernetická bezpečnost vyučována jako samostatný předmět nebo i celý studijní obor. V takovém případě se studenti podobně jako na vysokých školách seznamují kromě základů a teorie také s praktickými aspekty kybernetické bezpečnosti. Tyto předměty jsou však méně technicky náročné a mají poskytnout hlubší pohled a všeobecné vzdělání v této oblasti (Mountrouidou et al., 2019). Vzdělávání v oblasti kybernetické bezpečnosti však nelze na této úrovni vzdělávání příliš zobecňovat, protože se učební plány mohou v jednotlivých zemích a přístupu samotných škol lišit.

Ve srovnání s vysokým a středním stupněm je podíl výuky kybernetické bezpečnosti na základních školách minoritní. Důvodem je příliš obecné zaměření studia s pouze základními nebo chybějícími technickými předměty. V pedagogické literatuře je však prezentováno více přístupů, jak u dětí zvýšit povědomí o kybernetické bezpečnosti. Z pasivních přístupů se jako pozitivní osvědčila videa, interaktivní vyprávění příběhů a digitální komiksy (Quayyum et al., 2021). Kromě toho byly mezi dětmi zkoumány i gamifikované přístupy a méně technická témata, jako je například výzkum zaměřující se na povědomí o digitálním soukromí (Bioglio et al., 2019; Kumar et al., 2018; Vanderhoven et al., 2015), který u dětí prokázal zvýšení jejich povědomí. Vzhledem k tomu, že v dnešní době jsou i malé děti uživateli internetu, kde jsou vystaveny poměrně velkému množství kybernetických hrozeb, je potřeba do určité míry integrovat vzdělávání v této oblasti i na základní školy a víceletá gymnázia. To však s ohledem na značné věkové rozdíly mezi žáky otevírá další výzvy k zajištění efektivního vzdělávání.

1/2025, Volume 17, Issue 1
ISSN 1803-537X

3 Analýza pokrytí vzdělávání v České republice

Stejně jako v mezinárodní rovině, tak i na národní úrovni je důležité posuzovat zkoumanou problematiku s ohledem na stupeň vzdělání. Za účelem analýzy dostupnosti vzdělávání v oblasti kybernetické bezpečnosti byly shromážděny dostupné informace o studijních programech českých škol, které byly dále analyzovány s cílem zmapovat pokrytí nabízeného studia v této specifické oblasti. V rámci této kapitoly jsou postupně prezentovány výstupy provedené analýzy na vysokém, středním a základním stupni vzdělání (pořadí stupňů vzdělání je dáno historickém vývojem).

Dle Ministerstva školství, mládeže a tělovýchovy je v České republice zřízeno celkem 26 veřejných a 2 státní vysoké školy (MŠMT, 2025). Historicky první integrace kybernetické bezpečnosti do výuky byla realizována v roce 2008 na Fakultě informatiky Masarykovy Univerzity ve formě oborové specializace navazujícího magisterského studijního programu Informatika (MUNI, 2015). Vývoj v této oblasti významně pokročil v roce 2015, kdy došlo k historicky prvního akreditaci bakalářského studijního programu Informační bezpečnost na Fakultě elektrotechniky a komunikačních technologií Vysokého učení technického v Brně (VUT, 2015). Tomu následovala v pokračujících letech akreditace obdobných programů na dalších českých vysokých školách. Přehled akreditovaných programů kybernetické bezpečnosti na tomto stupni vzdělání je podrobněji uveden v tabulce 1 (seřazeno dle roku první akreditace). Veškeré uvedené programy jsou vyučovány prezenční formou a zatím doposud na žádné z českých vysokých škol nebyla akreditována kombinovaná forma studia. Existují však programy profesního vzdělávání, jako je například proCyber od VUT v Brně (FEKT, 2025) nebo studium MBA od Asociace škol kritické infrastruktury (ASKI, 2025).

Vysoká škola	Program	Akreditace
Vysoké učení technické v Brně	Informační bezpečnost	*B* (2015), *MN* (2019)
České vysoké učení technické	Kybernetická bezpečnost	*B* (2019), *MN* (2016)
VŠB – Technická univerzita Ostrava	Informační a komunikační bezpečnost	*MN* (2016)
Univerzita obrany	Kybernetická bezpečnost	*M* (2019)
Masarykova univerzita	Kyberbezpečnost	*B* (2020), *MN* (2019)
Univerzita Hradec Králové	Informační a síťová bezpečnost	*B* (2024)

Tabulka č. 1: Akreditované studijní programy na vysokém stupni vzdělání.
Pozn: B (bakalářské studium), M (magisterské studium), MN (magisterské navazující studium).

Mimo výše uvedené akreditované studijní programy nabízí některé vysoké školy a jejich fakulty specializaci, která je součástí jiného programu. Pro ak. rok 2024/2025 se jedná o program Informační technologie a umělá inteligence na Fakultě informatiky VUT v Brně (VUT, 2024) a Informační technologie[1] na Univerzitě Tomáše Bati ve Zlíně (UTB, 2024).

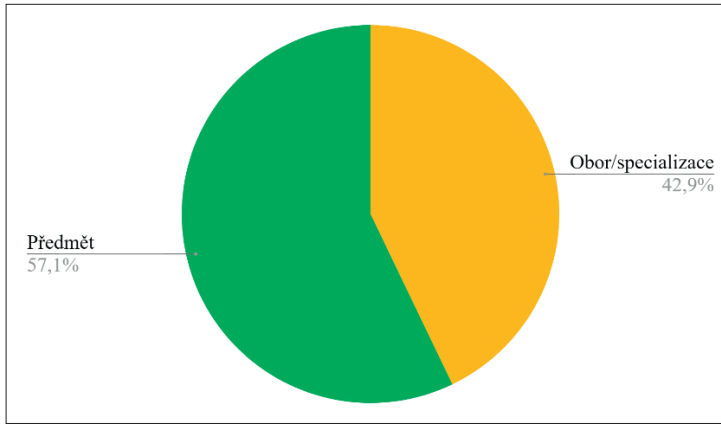
V případě středního stupně vzdělání došlo k první integraci v roce 2018, kdy byl na Střední škole informatiky, poštovnictví a finančnictví v Brně otevřen první maturitní obor Kybernetická bezpečnost, a ve stejném roce pak obdobný obor i na Smíchovské střední průmyslové škole a gymnáziu v Praze (Chvalkovská, 2018). Od té doby tento trend pokračoval i na dalších školách integrací kybernetické bezpečnosti do samostatných předmětů. Pro analýzu pokrytí výuky na tomto stupni vzdělání byl vzhledem k vysokému počtu škol postup zúžen na akreditovaný maturitní obor Informační technologie (18-20-M/01), přičemž analýza byla provedena v následujících krocích:

1. Z rejstříku MŠMT (2025) byl vytěžen seznam škol nabízející obor 18-20-M/01.
2. Na webových stránkách škol byl dohledán ŠVP (školní vzdělávací program).
3. Pokud nebyl ŠVP dané školy veřejně dostupný, byl analyzován učební plán.
4. V získaných materiálech byly vyhledány předměty kybernetické bezpečnosti.
5. Dle dostupnosti a formy studia byla provedena kategorizace.

Z analyzovaných 131 učebních plánů 41 středních škol (31,3 %) kybernetickou bezpečnost jako samostatnou jednotku integrovalo do svého školního vzdělávacího programu. Z této množiny pak 18 škol nabízí obor nebo volitelnou specializaci studia, zatímco ostatní výuku pouze ve formě předmětu. Je důležité podotknout, že samostatné studijní obory zaměřené na kybernetickou bezpečnosti stále vystupují pod akreditovaným oborem 18-20-M/01. To stejné platí pro specializaci studia, kterou si studenti mohou sami zvolit. Z toho důvodu byly tyto dva případy v rámci srovnání sloučeny do jedné skupiny. Procentuální rozložení nabízené formy vzdělávání na středním stupni vzdělání lze vidět na Obr. č. 1. Přestože převažuje integrace ve formě předmětu, tak 42,9% zastoupení oborů a specializací ukazuje zájem těchto škol o vyšší míru výuky kybernetické bezpečnosti než pouze v rámci jednoho nebo integrace do již existujícího předmětu. S ohledem na historický vývoj od roku 2018 v této oblasti lze očekávat nárůst integrace v obou sledovaných skupinách.

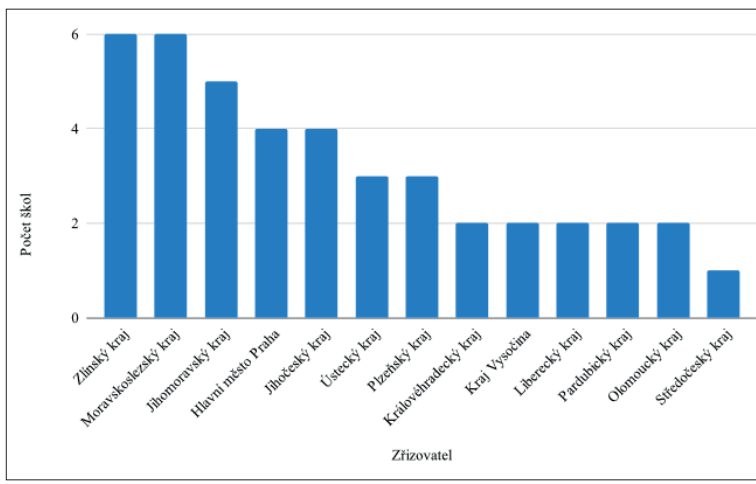
[1] Pro tento obor nabízí Univerzita Tomáše Bati ve Zlíně prezenční i kombinovanou formu studia.

1/2025, Volume 17, Issue 1
ISSN 1803-537X



Obr. č. 1: Rozdělení nabízené výuky kybernetické bezpečnosti.

Dále byla množina škol kategorizována dle zřizovatele. Z rozdělení plyne, že kromě Karlovarského kraje pokrývají výuku kybernetické bezpečnosti všechny, přičemž největší zastoupení mají střední školy ve Zlínském a Moravskoslezském kraji (6), nejméně pak ve Středočeském kraji (1). Celkový přehled všech zřizovatelů je znázorněn na Obr. č. 2.



Obr. č. 2: Počet škol pokrývajících výuku kybernetické bezpečnosti dle zřizovatele.

Měřitelnost míry integrace kybernetické bezpečnosti do výuky na základním stupni vzdělání je problematická. Základní školy se až na výjimky oborově nespecializují, a proto je nelze kategorizovat jako u středních a vysokých škol. V rámci všeobecného vzdělávání lze do určité míry snahy o vzdělávání v této oblasti sledovat ve formě osvěty. Aktivní je v tomto ohledu zejména Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB, 2024) nebo Pedagogická fakulta Univerzity Palackého v Olomouci s projektem E-Bezpečí (2024). Přímá integrace na tomto stupni zůstává převážně sporadická a lze očekávat, že budoucí vývoj se bude opírat o nově vznikající populárně-naučné programy a zvyšování povědomí o kybernetické bezpečnosti ze strany třetích stran. Tento směr je však pochopitelný a lze ho přirovnat ke snahám prevence, jako je tomu například v oblasti konzumace drog a alkoholu. Žáky na základních školách jsou děti, a je proto žádoucí vzdělávání v této oblasti koncipovat za účelem prevence nežli praktickému tréninku v odborných předmětech, které mnohdy stanovují náročné prerekvizity z odvětví ICT.

4 Nástroje a metody pro výuku kybernetické bezpečnosti

Pro hlubší náhled do problematiky se tato kapitola věnuje metodám a nástrojům, pomocí kterých lze realizovat nebo podpořit výuku kybernetické bezpečnosti. Jak již bylo uvedeno v úvodu článku, tak toto odvětví klade vysoké technické požadavky na praktické vzdělávání. K jeho realizaci lze využít tradiční postupy již ověřené z jiných ICT předmětů (např. virtualizace) nebo nové metody uzpůsobené pro oblast kybernetické bezpečnosti.

Základem pro praktickou výuku je vytvoření bezpečného prostředí. Za tímto účelem lze klientské a serverové stanice virtualizovat pomocí platforem, jako je například Oracle VirtualBox, VMware, KVM nebo Hyper-V. Hlavní výhodou tohoto přístupu je izolování virtuálních strojů od hostitelského zařízení s možností provádět ofenzivní operace, které jsou běžnou součástí tréninku etického hackingu nebo analýzy škodlivého kódu. Virtuální stanice lze navíc dle potřeby uvést do původního stavu, což je vhodné zejména v případě blokové výuky různých skupin studentů. Naopak nevýhodou jsou hardwarové požadavky kladené na hostitelské stanice, nutnost stanice konfigurovat a problémy s kompatibilitou obrazů virtuálních strojů napříč různými verzemi virtualizačních platforem.

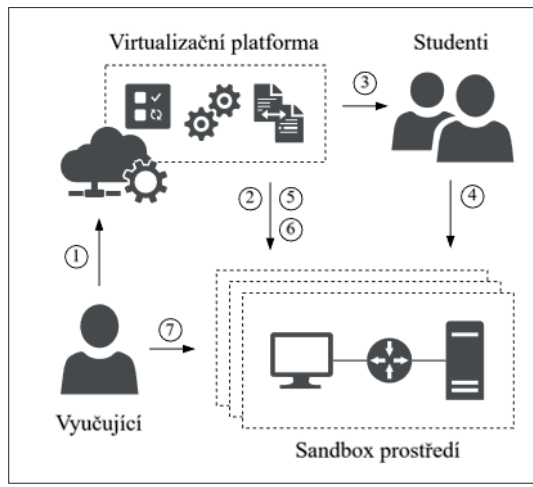
Opačným přístupem k lokální virtualizaci je využití veřejného nebo privátního cloudu, ve kterém lze provést celý výše popsaný proces nasazení virtuálního vý-

1/2025, Volume 17, Issue 1
ISSN 1803-537X

ukového prostředí. Za tímto účelem lze využít koncept tzv. sandboxingu. Sandbox představuje bezpečné izolované prostředí, který se skládá z jednoho a více virtuálních strojů. Tvorbu a správu sandbox prostředí lze rozdělit do následujících fází:

1. Vyučující před výukou zahájí proces nasazení.
2. Virtualizační platforma nasadí sandbox prostředí.
3. Studentům je postupně přidělen vlastní sandbox.
4. Studenti individuálně interagují se sandbox prostředím.
5. Prostředí je dle potřeby uvedeno do původního stavu.
6. Sandbox prostředí je zničeno (proces uvolnění).

Uvedené body výše jsou pro sandboxing kritické a mohou být virtualizační platformou zcela automatizovány (orchestrace). K tomu se využívají různé vlastní, komerčních (např. Azure, AWS, OVH aj.), nebo open source řešení (např. Open Stack a Ansible AWX), popřípadě jejich kombinace (Katsantonis et al., 2023). Jednotlivé fáze od nasazení sandboxu po jeho úplné zničení jsou znázorněny na Obr. č. 3.



Obr. č. 3: Životní cyklus sandbox prostředí.

Hlavní výhodou použití sandboxingu pro výuku kybernetické bezpečnosti je plná kontrola nad nasazeným prostředím. Sandbox je navíc izolovaný od hostitelského zařízení, čímž je uživateli k dispozici bezpečné prostředí (např. pro ana-

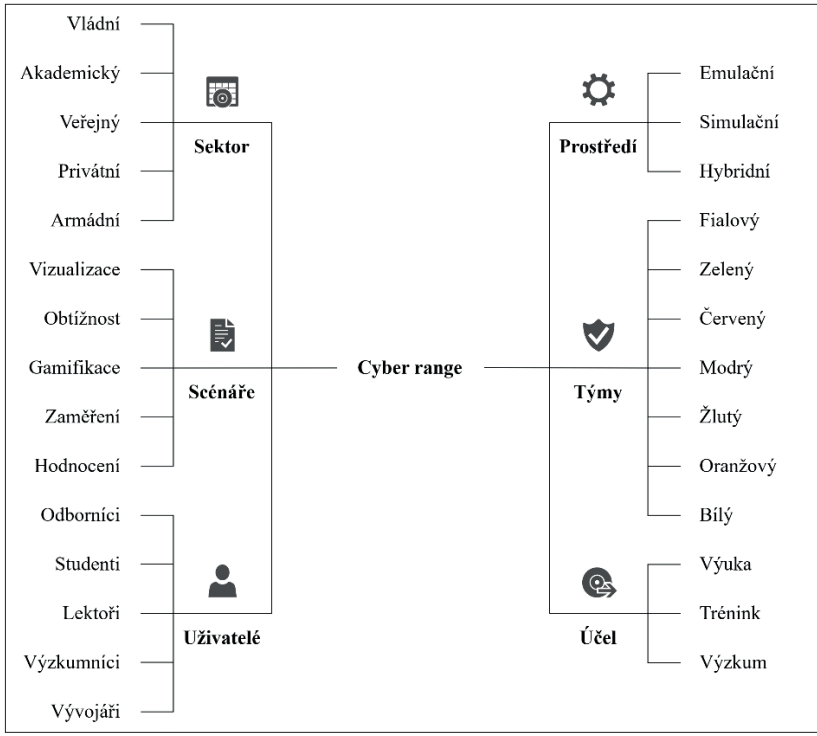
1/2025, Volume 17, Issue 1
ISSN 1803-537X

lýzu škodlivého kódu) a zároveň je omezen o možnost provedení destruktivních operací v produkčním prostředí. Naopak nevýhodou je složitost nasazení a provozu těchto prostředí, a proto je žádoucí automatizace tohoto procesu ze strany cloudových platforem (Stodůlka & Fujdiak, 2022). V oblasti kybernetické bezpečnosti se s aplikací sandboxingu pro praktické vzdělávání lze nejčastěji setkat v doméně cyber range.

Cyber range platformy představují komplexní prostředí pro výuku, trénink, testování nebo výzkum v oblasti kybernetické bezpečnosti. Jejich počet od vzniku tohoto odvětví výrazně narostl, přičemž mezi ty nejznámější patří platformy Hack The Box (2025) a TryHackMe (2025). Cyber range řešení lze dále kategorizovat podle jejich účelu, typu prostředí, charakteristiky scénářů, cíleného sektoru nebo uživatelů, jako je znázorněno na Obr. č. 4. Hlavní výhodou těchto platforem je možnost automaticky nasadit kontrolované a izolované sandbox prostředí uzpůsobené pro praktické vzdělávání kybernetické bezpečnosti. S cyber range platformami se však pojí i několik nevýhod omezující jejich použití, jako je zejména technická složitost a náklady spojené s nasazením, provozem a údržbou. K tomu je potřeba zajistit vlastní infrastrukturu s dostatečným výpočetním výkonem, nebo využít prostředky veřejného cloudu.

Ať už prostřednictvím cyber range platforem, samostatnou aplikací nebo lokální virtualizací se lze v této oblasti setkat také s použitím konceptu hry o vlajku, tzv. CTF (Capture the Flag). Jedná se o gamifikovaný způsob pro praktické ověřování znalostí v kybernetické bezpečnosti. Jak už z názvu plyne, tak cílem CTF je získat vlajku, která představuje správné řešení pro daný úkol. Vlajkou může být cokoliv v kontextu daného scénáře, např. dešifrovaný text, IP adresa, uživatelské heslo aj. (McDaniel et al., 2016). Řešení úkolu v podobě vlajky zadávají jednotlivci nebo týmy do hodnotícího systému dané platformy, přičemž některé CTF hry poskytují během řešení také nápovědy, jejichž použití může být penalizováno ztrátou určitého počtu bodů.

1/2025, Volume 17, Issue 1
ISSN 1803-537X



Obr. č. 4: Vlastnosti cyber range platforem.

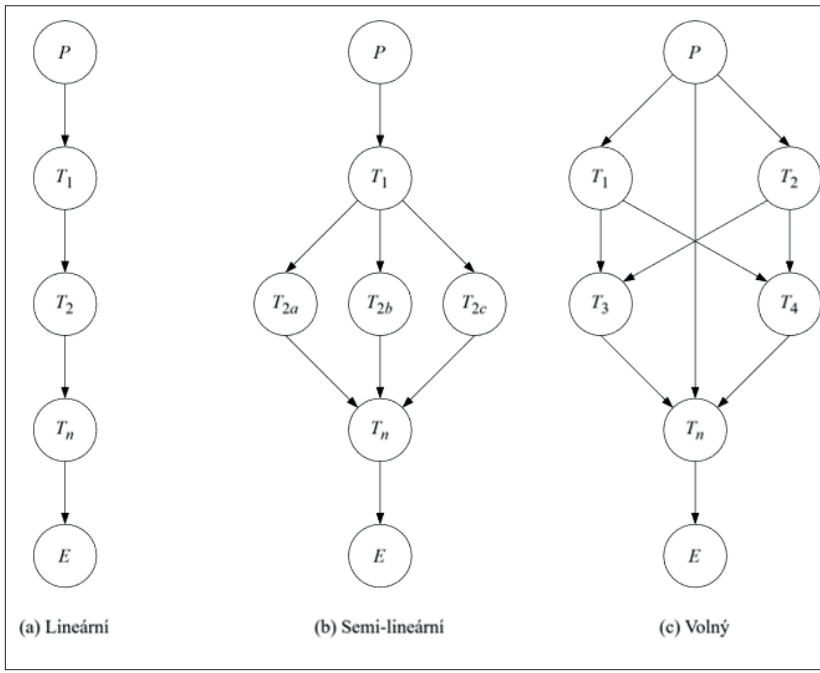
Mezi hlavní výhody CTF patří zejména vyšší uživatelský zážitek, podpora praktické výuky a tréninku, systém automatického bodování a poměrně efektivní způsob, jak pomocí gamifikace podpořit vzdělávání v oblasti kybernetické bezpečnosti (Vykopal et al., 2020). Podle koncepce se CTF scénáře dále dělí na následující typy (Kucek et al., 2022):

- **Jeopardy** – postupné řešení různorodých praktických výzev.
- **Attack-Defense** – formát, kde na sebe týmy útočí a brání své virtuální prostředí.
- **King of the Hill** – cílem je zmocnit se systému a ubránit ho před ostatními hráči.
- **Mixed (smíšené)** – kombinace nebo vlastní uzpůsobení ostatních formátů CTF.

1/2025, Volume 17, Issue 1
ISSN 1803-537X

Průchod CTF scénářem se může lišit v závislosti na konkrétním typu, zaměření a struktuře daného scénáře. Je-li CTF scénář založen na řešení předem stanovených úloh, lze průchod scénářem rozdělit na (viz Obr. č. 5):

- **lineární** – uživatel postupně řeší předdefinovanou sekvenci úkolů,
- **semi-lineární** – průchod scénářem se může větvit,
- **volný** – postup není předem určen a závisí na uživateli.

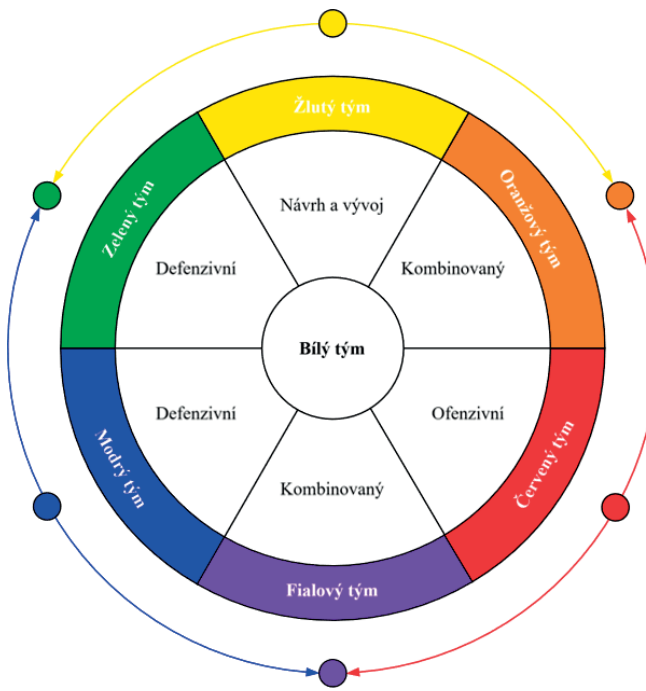


Obr. č. 5: Typy průchodu CTF scénářem.

Princip hry o vlajku bývá využíván v cyber range a jiných online platformách, které cílí na interaktivní výuku a trénink kybernetické bezpečnosti. Z těch největších lze jmenovat např. Hack The Box (2025), TryHackMe (2025), CTFd (2024) nebo RingZer0 (2024). Koncept CTF se využívá také v národních a mezinárodních soutěžích, jako jsou např. DEF CON, PicoCTF, MITCTF, MITRE CTF, FBCTF, CSAW, CyberSEED, CPTC, ISTS a další (Balon et al., 2023).

1/2025, Volume 17, Issue 1
ISSN 1803-537X

Pro další dělení lze kybernetickou bezpečnost kategorizovat také dle primárních barev, jejichž kombinací lze vytvořit barvy sekundární (Wright, A. C., 2017), kde jednotlivé barvy slouží k odlišení kybernetické bezpečnosti na ofenzivní (červená), defenzivní (modrá a zelená), vývojová (žlutá), kombinovaná (fialová a oranžová) nebo neutrální (bílá). V případě větších cvičení mohou být uživatelé rozděleny do barevných týmů, které mezi sebou soutěží, nebo plní předurčenou roli (např. červený tým útočí na modrý tým). Barevné týmy lze také v kontextu CTF použít ke kategorizaci scénářů (např. defenzivní bezpečnost, bezpečné psaní kódu atd.), kde největší zastoupení tvoří ofenzivní scénáře, tj. červená barva (Lazarov et al., 2023). Nemusí se tedy vždy jednat o zapojení více osob, a scénář tak může být zaměřen na jednotlivce, nebo jednu skupinu, přičemž roli jiného týmu lze emulovat (Yamin et al., 2020). Barevné dělení týmů je znázorněno na Obr. č. 6.



Obr. č. 6: Barevné dělení kyberzpečnostních týmů.

1/2025, Volume 17, Issue 1
ISSN 1803-537X

5 Aplikace interaktivních a gamifikovaných metod

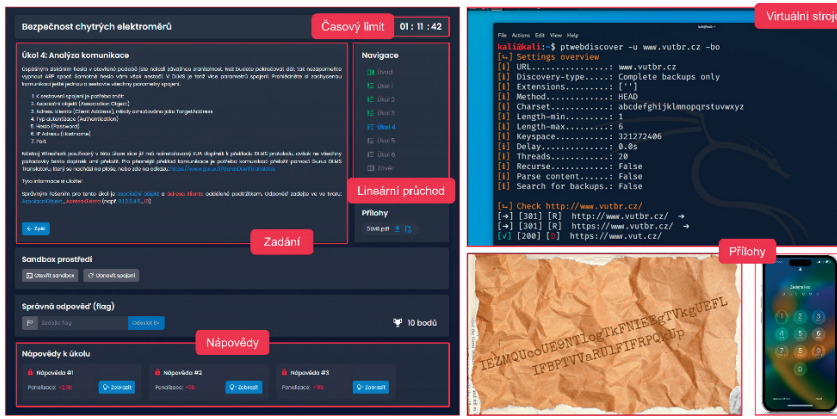
V návaznosti na předchozí teoretický rozbor a provedenou analýzu současného stavu tato kapitola prezentuje aplikaci představených metod a nástrojů pro vzdělávání v oblasti kybernetické bezpečnosti. Prezentována je inovace studijního programu Informační bezpečnost a vzdělávací akce na VUT v Brně (domovské univerzitě autora).

Jak již bylo prezentováno v kapitole 2, tak v akademickém roce 2015/2016 byl na Fakultě elektrotechniky a komunikačních technologií VUT v Brně akreditován první český bakalářský studijní program Informační bezpečnost, který v pilotním roce mimo řadu ICT předmětů nabízel 6 technických předmětů orientovaných na kybernetickou bezpečnost – Základy, kryptografie, Aplikovaná kryptografie, Zabezpečovací systémy, Bezpečnost ICT 1, Bezpečnost ICT a Teorie kryptografických protokolů. K tomu byl ve spolupráci s Právnickou fakultou Masarykovy Univerzity doplněn o tematicky relevantní právní předměty, konkrétně o Úvod do práva ICT 1, Úvod do práva ICT 2, Softwarové právo a Kyberkriminalita. Další akreditace navazujícího magisterského studia v akademickém roce 2018/2019 pokračující studium rozšířila o předměty Kryptografie v informatice, Bezpečnost ICT3 a Seminář informační bezpečnosti.

Od té doby se program dál vyvíjel, zejména ve studijních materiálech a laboratorních úlohách, a v akademickém roce 2024/2025, mimo již uvedené předměty, nabízí navíc předměty Bezpečnost databázových systémů, Vývoj bezpečných aplikací a Network Security od CISCO akademie. V případě navazujícího magisterského studia pak předměty Moderní kryptografie, Odpovědnost v právu ICT a předmět Teorie kryptografických protokolů, který byl přesunut z bakalářského do magisterského studia.

Praktická výuka v uvedených předmětech byla do akademického roku 2023/2024 koncipována převážně formou lokální virtualizace v prostředí VMware a VirtualBox. Studenti si na začátku počítačového cvičení kopírovali předpřipravené obrazy virtuálních strojů do vlastních adresářů, ze kterých je následně dle instrukcí dané laboratorní úlohy naimportovali do virtualizační platformy a provedli potřebné nastavení, tj. přidělení výpočetních zdrojů virtuálním strojům a konfigurace síťování pro vzájemnou konektivitu. Tento přístup se však běžně setkával s technickými problémy diskutovanými v kapitole 2, zejména se jednalo o selhání procesu importování, zdlouhavou přípravu nebo chybu v konfiguraci ze strany studentů (např. chybné nastavení sítě).

V akademickém roce 2024/2025 došlo k výrazné inovaci počítačových cvičeních kybernetické bezpečnosti v předmětech Bezpečnost ICT 2 a Bezpečnost ICT 3, kdy byla do výuky integrována cyber range platforma BUTCA (Brno University of Technology Cyber Arena). Cílem této integrace bylo nahradit lokální virtualizaci a eliminovat tak výše uvedené problémy. Laboratorní úlohy proto byly transformovány z původních statických PDF zadáních do formátu CTF. Ukázka vybraného scénáře je znázorněna na Obr. č. 7.



Obr. č. 7: Výukový scénář v platformě BUTCA.

Výukové scénáře jsou lineární s předem stanoveným časovým limitem. Praktické úkoly obsahují zadání, nápovědy k řešení a v závislosti na scénáři i přílohy ke stažení. Základem je sandbox prostředí, které umožňuje vzdálený přístup k virtuálním strojům, které bylo studentům přiřazeno, díky čemuž není nutné provádět lokální virtualizaci. Studenti tak k veškeré činnosti potřebují pouze webový prohlížeč. Sandbox je studentovi přiřazen v moment spuštění scénáře a po jeho dokončení je obnoven do původního stavu. Po konci výuky se celé sandbox prostředí zničí a rezervované výpočetní zdroje se uvolní.

Před nasazením platformy BUTCA do produkčního provozu byla provedena série experimentálního testování výukových CTF scénářů. V rámci tohoto pilotního testování hodnotila[2] kontrolní skupina 55 studentů (věková skupina 19–25 let) bakalářského studijního programu Informační bezpečnost na VUT tento přístup jako kladný (43,6 %) až velmi kladný (56,4 %). Dále po této první zkušenosti

[2] Hodnotící škála: velmi negativní, negativní, neutrální, kladné, velmi kladné.

pak 98,8 % studentů projevilo zájem o integraci představené formy výuky. Tento přístup jsme také testovali na středním stupni vzdělání, konkrétně se skupinou 51 žáků (věková skupina 12–18 let) 3. ročníku oboru Informační technologie ze Střední průmyslové školy Třebíč a s 10 žáky (věková skupina 12–18 let) 3. ročníku z Gymnázia Brno, třídy Kapitána Jaroše. V případě středoškoláků bylo CTF v platformě BUTCA hodnoceno jako kladné (43,2 %) až velmi kladné (56,8 %), přičemž zájem o integraci projevilo 80,4 % žáků. Zpětná vazba byla podobná i u skupiny gymnazistů, kteří výukový scénář hodnotili jako kladný (40 %) až velmi kladný (60 %) a zájem o integraci v tomto případě projevili všichni zúčastnění.

Co se týká hodnocení ze strany vyučujících, tak to v rámci aplikace představených metod a nástrojů měřeno nebylo. Nicméně vymezit se lze ke změnám, které jsme sledovali v porovnání se způsobem praktické výuky na VUT, jež testování předcházel. Konkrétně byly minimalizovány technické nedostatky spojené s lokální virtualizací, kdy studenti na začátku výuky dostali pokyn k importování, nastavení a spuštění virtuálních strojů. To s sebou však neslo identifikované potíže popsané v kapitole 4, jako je nezdařilý import, chybné nastavení a problémy s virtuální sítí. Díky využití sandboxingu v platformě BUTCA bylo virtuální prostředí automaticky včas nasazeno, a studenti tak bez jakékoliv prodlevy a uvedených technických problémů mohli zahájit praktickou výuku. Z této skutečnosti plyne zásadní výhoda nejen v přípravě stabilního výukového prostředí, ale také ušetření celkového času, který lze využít pro věcnou část výuky. Tyto výhody potvrzuje předchozí výzkum (Lazarov et al., 2025) i další autoři, kteří aplikovali podobné platformy do výuky kybernetické bezpečnosti (Beauchamp et al., 2023).

6 Diskuze

Jak bylo poukázáno v teoretické rovině i z výsledků výzkumu, tak oblast kybernetické bezpečnosti může klást poměrně náročné požadavky na realizaci praktické výuky. Výzkum prezentovaný v tomto článku se kromě analýzy současného stavu zaměřil na možnosti její realizace. Z představených možností byl pro ověření vybrán koncept cyber range a CTF, jakožto moderní přístup k výuce v této oblasti. Na základě analýzy současného stavu, aplikaci interaktivních a gamifikovaných metod a získané zpětné vazby byl tento přístup shledán jako vhodný pro podporu praktické výuky kybernetické bezpečnosti. Výhody lze z výsledků výzkumu shrnout do dvou perspektiv:

1/2025, Volume 17, Issue 1
ISSN 1803-537X

- Studenti mají k dispozici bezpečné a interaktivní prostředí pro praktické zvýšení svých dovedností. Lineární scénáře jim úkoly předkládají postupně s předchozí návazností, přičemž v případě nutnosti mají k dispozici nápovědy. Výuka navíc neprobíhá pasivně a díky interaktivitě a gamifikace scénářů se zvyšuje zapojení studentů. Celé prostředí je od začátku předpřipravené a netřeba ho konfigurovat.
- Učitelé mají přehled nad celým výukovým prostředím. Během aktivního procesu učení mohou sledovat pokrok studentů prostřednictvím analytického modulu. Ten dále zahrnuje indikaci, na kterých úlohách se momentálně studenti nachází, jejich aktuální skóre, použité nápovědy a chybně zadané odpovědi. Po dokončení scénáře mají učitelé přístup k výsledkům jednotlivých studentů.

Mimo výše uvedené výhody lze také opět zdůraznit mitigaci technických problémů, která plyne z funkcí sandboxingu (automatické nasazení virtuálních strojů, konfigurace, obnova prostředí atd.). Dále při použití cyber range ve formě služby jsou požadavky kladené na hardwarové a softwarové vybavení minimalizovány platformou. Možnosti tohoto přístupu jsou však omezeny výpočetní kapacitou cloudového prostředí cyber range platformy, což zároveň představuje i jeho nevýhodu. Pokud by došlo k maximálnímu vytížení, nelze v daný moment výuku pro další skupiny studentů realizovat. Tento problém lze řešit vyšší alokací cloudových zdrojů nebo optimalizaci jejich využití při plánování výuky, kdy se omezí paralelní počet souběžně běžících scénářů do série bloků.

Přes identifikované výhody použitých metod a nástrojů byl prezentovaný výzkum omezen na samotnou aplikaci a nezkoumal tak didaktický pohled na obsah CTF scénářů použitých během testování, z čehož plyne směr pro budoucí výzkum. Dalším aspektem, který by mohl být zohledněn v navazujícím výzkumu je identifikace slabých a silných stránek učených osob s ohledem na stanovené prerekvizity, praktické úkoly a celkovou obtížnost CTF scénářů. Zohlednit lze také hodnotící systém v platformě cyber range, který by mohl být na základě analýzy výukových dat rozšířen o deskriptivní zpětnou vazbu. Za tímto účelem lze zvážit využití generativní umělé inteligence.

7 Závěr

Článek na základě historického vývoje a současného stavu vzdělávání v oblasti kybernetické bezpečnosti zmapoval pokrytí studijních programů a oborů zaměřující se na toto odvětví na vysokém a středním stupni vzdělání. Prezentovány byly dále moderní metody a nástroje pro praktickou výuku kybernetické bezpečnosti, které zahrnují lokální virtualizaci, sandboxing, cyber range platformy a koncept CTF pro gamifikaci výuky. Diskutována byla také kombinace představených metod, včetně jejich výhod a nevýhod. Dále byla prezentována aplikace platformy BUTCA a CTF scénářů, které byly otestovány skupinou studentů vysoké školy a žáků střední průmyslové školy a gymnázia. Na základě provedeného testování a získané zpětné vazby lze konstatovat, že kombinace cyber range, sandoxingu a CTF představuje interaktivní a bezpečné prostředí pro praktickou výuku kybernetické bezpečnosti podporující jak učené osoby, tak i vyučující, kteří mají nad výukovým prostředím přehled a k dispozici cenná data pro další hodnocení. Na základě analýzy dosavadního vývoje lze v této oblasti očekávat jak akreditaci nových studijních programů a předmětů, tak i pokračující integraci kybernetické bezpečnosti na středním stupni vzdělání či rozvoj nástrojů pro podporu samotného vzdělávání.

8 Literatura

ASKI (2024). *MBA v oblasti kybernetické bezpečnosti v České republice a Slovensku*. Asociace škol kritické infrastruktury. Dostupné z: https://mba.aski.cz/mba-studium-manazer-kyberneticke-bezpecnosti/

Balon, T., & Baggili, I. (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Education and Information Technologies*, 28(9), 11759–11791. https://doi.org/10.1007/s10639-022-11451-4

Beauchamp, C., Beach, V., & Matuscovich, V. H. (2023). Educational cyber ranges: A mixed-method study of significant learning experiences using cyber ranges for cybersecurity education. *Cybersecurity Pedagogy & Practice Journal*, 2(1), 4–11.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., Pensa, R.G. (2019). A Social Network Simulation Game to Raise Awareness of Privacy Among School Children. *IEEE Transactions on Learning Technologies*, 12(4), 456–469. https://doi.org/10.1109/TLT.2018.2881193

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

Chvalkovská, P. *V ČR startuje středoškolské studium kybernetické bezpečnosti.* KYBEZ. Dostupné z: https://kybez.cz/v-cr-startuje-stredoskolske-studium-kyberneticke-bezpecnosti/

CTFd (2024). *The Easiest Capture the Flag Platform*. CTFd. Dostupné z: https://ctfd.io/
De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007
E-Bezpečí (2024). *Vzdělávejte se s E-Bezpečím*. E-Bezpečí. Dostupné z: https://vzdelavani.e-bezpeci.cz/
ENISA (2025). *CYBERHEAD - Cybersecurity Higher Education Database*. European Union Agency for Cybersecurity. Dostupné z: https://tools.enisa.europa.eu/topics/education/cyberhead/
FEKT (2024). *Master of Science in Cybersecurity proCyber*. FEKT VUT. Dostupné z: https://www.utko.fekt.vut.cz/master-science-cybersecurity-procyber
Hack The Box (2025). *The #1 Cybersecurity Performance Center*. HTB. Dostupné z: https://www.hackthebox.com/
Harris, G. (2024). How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States. *Journal of Cybersecurity Education, Research and Practice*, 2024(1), 27. https://doi.org/10.62915/2472-2707.1194
Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, 22(4), 1005–1027. https://doi.org/10.1007/s10207-023-00680-4
Kucek, S., & Leitner, M. (2020). An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. *Journal of Network and Computer Applications*, 151, 102470. https://doi.org/10.1016/j.jnca.2019.102470
Kumar, P., Vitak, J., Chetty, M., Clegg, T.L., Yang, J., McNally, B., Bonsignore, E. (2018). *Co-designing online privacy-related games and stories with children*. Proceedings of the 17th ACM Conference on Interaction Design and Children (s. 67–79). Trondheim Norway: ACM. https://doi.org/10.1145/3202185.3202735
Lazarov, W., Stodulka, T., Schafeitel-Tähtinen, T., Helenius, M., & Martinasek, Z. (2023). *Interactive Environment for Effective Cybersecurity Teaching and Learning*. Proceedings of the 18th International Conference on Availability, Reliability and Security (s. 1–9). https://doi.org/10.1145/3600160.3605007
Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P. & Fujdiak, R. (2025). Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. *Technology, Knowledge and Learning*, 1–36. https://doi.org/10.1007/s10758-025-09840-ys
McDaniel, L., Talvi, E., & Hay, B. (2016). *Capture the Flag as Cyber Security Introduction*. 2016 49th Hawaii International Conference on System Sciences (HICSS) (s. 5479–5486). https://doi.org/10.1109/HICSS.2016.677
Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. *Transactions on Edutainment XV*, 93–107. https://doi.org/10.1007/978-3-662-59351-6_9
Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., Yuen, T. T. (2019). *Securing the human: A review of literature on broadening diversity in cybersecurity education*. Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education (s. 157–176). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3344429.3372507
MŠMT (2022). *Registr vysokých škol a uskutečňovaných studijních programů*. Ministerstvo školství, mládeže a tělovýchovy. Dostupné z: https://regvssp.msmt.cz/
MŠMT (2025). *Rejstřík škol a školských zařízení*. eEdu portál. Dostupné z: https://regvssp.msmt.cz/

MUNI (2001). *Studijní katalog Fakulty informatiky v akademickém roce 2001/2002*. FI MU. Dostupné z: https://www.fi.muni.cz/docs/sez01-02.pdf

NÚKIB (2024). *Vzdělávací portál NÚKIB*. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://osveta.nukib.gov.cz/

Quayyum, F., Cruzes, D. S., Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

RingZer0 (2024). *RingZer0 Team Online CTF*. RingZer0 Team Online CTF. Dostupné z: https://ringzer0ctf.com/

Stodůlka, T., & Fujdiak, R. (2022). Budování Cyber Range platformy s technologií cloud computingu. Vysoké učení technické v Brně.

TryHackMe (2025). *Learn Cyber Security*. THM. Dostupné z: https://tryhackme.com/hacktivities

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, 23(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

UTB (2024). *Kybernetická bezpečnost*. Univerzita Tomáše Bati ve Zlíně. Dostupné z: https://www.utb.cz/vyhledavac-oboru/informacni-technologie-mgr/kyberneticka-bezpecnost-mgr/

Vanderhoven, E., Willems, B., Hove, S. V., All, A. (2015). *Wait and see? Studying the Teacher's Role During In-Class Educational Gaming*. Proceedings of the European Conference on Games-Based Learning (s. 540–547).

VUT (2015). *Informační bezpečnost*. Vysoké učení technické v Brně. Dostupné z: https://www.vut.cz/studenti/programy/obor/10687

VUT (2024). *Informační technologie a umělá inteligence*. Vysoké učení technické v Brně. Dostupné z: https://www.vut.cz/studenti/programy/program/8967

Vykopal, J., Švábenský, V., & Chang, E. C. (2020). *Benefits and Pitfalls of Using Capture the Flag Games in University Courses*. Proceedings of the 51st ACM Technical Symposium on Computer Science Education (s. 752–758). https://doi.org/10.1145/3328778.3366893

Wright, A. C. (2017). *Orange is the new purple*. USA: BlackHat. Dostupné z: https://www.blackhat.com/docs/us-17/wednesday/us-17-Wright-Orange-Is-The-New-Purple-wp.pdf

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88, 101636. https://doi.org/10.1016/j.cose.2019.101636