**POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE**

Fakulta bezpečnostně právní

Katedra managementu a informatiky

# Kybernetické útoky v prostředí vzdělávacích institucí

*Diplomová práce*

**Cyber attacks in the environment of educational institutions**
**Master thesis**

VEDOUCÍ PRÁCE
**RNDr. Václav HNÍK, CSc.**

AUTOR PRÁCE
**Bc. Martin PÁTECKÝ**

PRAHA
2022

## Čestné prohlášení

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

V Praze, dne 14. 3. 2022

Bc. Martin PÁTECKÝ

**ANOTACE**
Práce se zabývá problematikou kybernetických útoků v prostředí vzdělávacích institucí. V počáteční části práce je vymezena problematika obecné kybernetické bezpečnosti, a také kybernetické bezpečnosti vzdělávacích institucí. Dále jsou charakterizovány základní druhy útoků, se kterými se lze v prostředí vzdělávacích institucí setkat nejběžněji. Následující část je věnována analýze a experimentálnímu testování kybernetické bezpečnosti konkrétní vzdělávací instituce. V této části je popsána příprava, cíle a provedení čtyř druhů kybernetických útoků, vzniklé škody a možné způsoby obrany proti nim.

**KLÍČOVÁ SLOVA**
vzdělávací instituce * kybernetická bezpečnost * kyberprostor * škola * kybernetický útok * škodlivý kód * počítačová síť

**ANNOTATION**
This thesis deals with the issue of cyber attacks in the environment of educational institutions. The initial part of the thesis defines the issue of cyber security in general as well as cyber security of educational institutions. In addition, the basic types of attacks that can be most commonly encountered in the environment of educational institutions are being characterized. The following part is devoted to the analysis and experimental testing of cyber security of a particular educational institution. This part describes the preparation, objectives and execution of four types of cyber attacks, the damage caused and possible ways of defending against them.

**KEYWORDS**
educational institutions * cyber security * cyberspace * school * cyber attack * malicious code * computer network *

# Obsah

# Úvod

Nedávná doba ukázala, že vzdělávací proces se dnes již neobejde bez informačních a komunikačních technologií. S příchodem pandemie onemocnění COVID-19 se na určitou dobu prakticky celá část vzdělávání přesunula do prostředí kyberprostoru. Pedagogové, žáci, studenti, ale i pracovníci spravující informační a komunikační technologie čelili novým výzvám spojeným se zajišťováním co možná nejplnohodnotnějšího vzdělávání. Jednalo se především o zřízení a přechod na platformy umožňující vzdálenou komunikaci, organizaci a spolupráci při vzdělávacím procesu. Po znovuotevření vzdělávacích institucí však prvek kyberprostoru nadále zůstává součástí vzdělávacího procesu a je více než pravděpodobné, že míra využívání kyberprostoru a jeho výhod plynoucích z „*on-line*“ vzdělávání bude mít vzrůstající tendence.

S výhodami však přichází i možná rizika, a to jak pro poskytovatele vzdělávání, tak pro osoby vzdělávané. Množství dat, která jsou rozličnými komunikačními kanály kyberprostoru přesouvána, dosahují mnohonásobně větší míry, než tomu bylo v minulosti. Tato data však mohou být v ohrožení, ať už se jedná o jejich zničení, únik, krádež či podvodné zašifrování, a měl by být kladen důraz obzvláště na zajištění jejich bezpečnosti. Ačkoliv vzdělávací instituce nejsou primárním cílem kyberzločinců, lze předpokládat, že se útoky cílící právě na vzdělávací instituce budou objevovat stále častěji. V praxi se lze setkat s mnoha případy, kdy se školy a univerzity staly cílem kybernetického útoku, ať už cíleného přímo na konkrétní instituci, nebo v podobě nekontrolovaného šíření hrozby.

Problematika kybernetické bezpečnosti vzdělávacích institucí je tématem, které zůstává často upozaděno. Právě vzdělávací instituce mohou mít pozitivní vliv na vnímání kybernetické bezpečnosti a vzděláváním uživatelů, nejen studentů, mohou přispět k bezpečnějšímu virtuálnímu prostředí. Kyberprostor se stal součástí běžného života každého z nás. Jeho prostředky využíváme nejen ke vzdělávání, ale také ke komunikaci s vrstevníky a kolegy, ke sdílení informací o našem životě, k práci i zábavě. Vzdělávací instituce zahrnují prakticky všechny tyto body a hrají významnou roli ve formování přístupu uživatelů ke kybernetické bezpečnosti.

Cílem práce je podat ucelený pohled na kybernetickou bezpečnost vzdělávacích institucí. Její znění by mělo být, nejen pro uživatele vzdělávacích institucí, ale také pro odbornou veřejnost, hlubším vhledem do této problematiky. Zjištění, poznání, rešerše aktuálních pramenů a výsledky experimentů mohou sloužit pro vzdělávací účely, ale také pro další analýzy a rozbory.

Práce se zabývá problematikou kybernetické bezpečnosti ve vzdělávacích institucích. Poznatky, informace a závěry v této práci vychází nejen z rešerše aktuálních pramenů a témat souvisejících s kybernetickou bezpečností, ale také z profesních a praktických zkušeností autora. Ten působí jako pedagog se zaměřením na výuku informatiky a mimo pedagogickou činnost vykonává také činnost poradní ve vztahu ke kybernetické bezpečnosti vzdělávací instituce.

V teoretické části práce je vymezena problematika kybernetické bezpečnosti, která je následně specificky zasazena do prostředí vzdělávacích institucí. Další část práce je věnována představení konkrétních kybernetických útoků, se kterými se lze v prostředí vzdělávacích institucí setkat. Popsány jsou jejich charakteristiky, dopady na vzdělávací instituci, běžné způsoby provedení, možné způsoby ochrany a prevence kybernetických útoků. Teoretickou část uzavírá problematika spojená se vznikem vedlejších škod v důsledku kybernetických útoků.

Praktická část práce se věnuje kybernetickým útokům v prostředí konkrétní vzdělávací instituce. Z počátku je popsáno prostředí a infrastruktura vzdělávací instituce, včetně analýzy jejich jednotlivých částí. Analýza se zaměřuje na identifikaci slabých míst, ve kterých lze spatřovat rizika vzhledem ke kybernetické bezpečnosti instituce. Pozornost je také věnována doporučením, která lze učinit s cílem předcházet vzniku bezpečnostních incidentů a s nimi spojeným škodám. Závěr praktické části je věnován experimentálnímu nedestruktivnímu testování kybernetické bezpečnosti čtyřmi reálnými útoky, které cílí na stěžejní části a kritické prvky vzdělávací instituce. Ve vyhodnocení experimentů je popsána příprava, průběh, hrozby, škody a následky konkrétních útoků včetně doporučení vhodných pro předcházení jejich vzniku.

# 1. Vzdělávací instituce

Definici pojmu vzdělávací instituce v českém právním systému nenalezneme. Její výklad lze učinit na základě zákona č. 561/2004 Sb., Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání. Pro účely práce pak z § 7 tohoto zákona vyplývá, že školy a školská zařízení poskytují vzdělání na základě vzdělávacích programů uvedených v totožném zákoně. Jako druhy škol vymezuje školy mateřské, základní, střední, ale také konzervatoře, umělecké školy a jazykové školy s právem vykonávat státní jazykové zkoušky. Pracuje taktéž se zmíněným pojmem školská zařízení. Tato zařízení pak poskytují doplňující a podpůrné vzdělání, které doplňuje vzdělávání ve školách, popřípadě se vzděláváním přímo souvisí.[1]

Tato definice klade důraz především na obecné vymezení vzdělávací instituce, avšak vzhledem k povaze této diplomové práce ji autor doplnil o některé pojmové znaky.

Za vzdělávací instituci je v této práci považována každá instituce, bez ohledu na zřizovatele, která poskytuje a organizuje vzdělávání osob všech věkových kategorií, k čemuž poskytuje všem zúčastněným osobám zázemí.

Organizace procesu vzdělávání spočívá zejména v plánovaném předávání poznatků, vědomostí a zkušeností mezi zúčastněnými osobami. Zahrnuje také běžnou agendu, jako je například vedení záznamů o studentech a pedagozích, nutnou k zajištění správného fungování a provozování souvisejících databází a systémů.

Pod zázemí pak lze zařadit fyzické komponenty, jako jsou vzdělávací pomůcky nebo místnosti, ale také komponenty abstraktní povahy, především virtuální obsah kyberprostoru ve formě software, databází, systémů, vzdělávacích prostředí či programů využívaných k zajištění vzdělávacího procesu.

[1] Zákon č. 561/2004 Sb., *Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání* ve znění k 18.11.2021

# 2. Kybernetická bezpečnost

Kybernetická bezpečnost je pojmem skloňovaným v aktuální době prakticky nepřetržitě. Dotýká se každého, bez ohledu na věk, sociální skupinu či pracovní pozici. Kyberprostor se stal součástí běžného života většiny obyvatel planety. Stejně jako je třeba chápat bezpečnost ve světě reálném, je nutné vnímat rizika a hrozby kyberprostoru. Definicí pojmu kybernetická bezpečnost je celá řada, každá instituce či subjekt si pojem upravuje dle potřeby a přesvědčení.

Jednu z definic nalézáme ve výkladovém slovníku kybernetické bezpečnosti od Jiráska, Nováka a Požára. Definice je vhodná pro účely této práce vzhledem k faktu, že zmiňuje důležitý aspekt vzdělávání. Kybernetickou bezpečnost vymezují jako: „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*“ Definice je obecného charakteru, přesto dle názoru autora velmi výstižná.[2]

Jako další definici kybernetické bezpečnosti lze zmínit vymezení ministerstva vnitřní bezpečnosti Spojených států amerických. Tato vládní agentura definuje kybernetickou bezpečnost následovně: „*Kybernetická bezpečnost je umění ochrany sítí, zařízení a dat před neoprávněným přístupem nebo kriminálním zneužitím a zajištěním důvěrnosti, integrity a dostupnosti informací.*“ Tato definice je od předchozí značně specifická a vyjma samotné bezpečnosti klade důraz také na dostupnost informací. Chybí v ní však aspekt vzdělávání.[3]

Poslední zde zmíněnou definicí je vymezení dle společnosti Cisco. Ta definuje kybernetickou bezpečnost jako: „*Činnost zajišťující ochranu systémů, sítí a programů před digitálními útoky. Obvykle je jejich cílem přístup k citlivým informacím, jejich změna nebo zničení, vymáhání peněz z uživatelů, nebo narušování běžných podnikových procesů.* “ První část definice je sama o sobě dle názoru autora dostačující. Její upřesnění ve zbylé části je pro obecnou definici příliš specifické. Kybernetickou bezpečnost je třeba chápat v širším smyslu,

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

[3] Security Tip (ST04-001): What is Cybersecurity?. *Cybersecurity and Infrastructure Security Agency* [online]. Rosslyn, Arlington, Virginia: CISA, May 06, 2009 [cit. 28.11.2021]. Dostupné z: https://www.cisa.gov/uscert/ncas/tips/ST04-001

protože zahrnuje mnoho odvětví. Základní definice pro tuto práci by tak měla setrvávat v obecné rovině.[4]

## 2.1 Kybernetická bezpečnost vzdělávacích institucí

Rapidní vývoj informačních a komunikačních technologií s sebou přinesl do prostředí vzdělávacích institucí nové příležitosti, s nimi však také nová rizika. Do povědomí se tak stále častěji dostávají události, při kterých jsou vzdělávací instituce cílem kybernetických útoků. Dopady těchto útoků mohou být devastující, zvláště v recentní době, kdy řada vzdělávacích institucí spoléhá na plnou funkčnost a integritu všech součástí struktury informačních a komunikačních technologií při zajišťování výuky a řízení běžného provozu. Bezpečnostní incidenty pak mohou narušit chod instituce, napáchat nevratné škody a způsobit chaos uvnitř vzdělávací instituce.

V první řadě je třeba konstatovat, že vzdělávací instituce koncentrují na jediném místě značně vysoký počet osob. Každá z těchto osob zastává v rámci celého komplexního systému určitý post, na který se váže zvláštní druh odpovědnosti ve spojitosti se zajišťováním kybernetické bezpečnosti vzdělávací instituce. Všechny osoby – uživatelé, by měli být seznámeni s bezpečnostními standardy, možnými riziky, a měli by být poučeni o možném řešení a hlášení bezpečnostních incidentů. Lze se domnívat, že většina vzdělávacích institucí všechny takto odpovědné osoby vzdělává v oblasti kybernetické bezpečnosti alespoň v základní podobě. Formy, kterými lze docílit dostatečné erudovanosti v tomto tématu je mnoho, avšak lze předpokládat, že instituce často zohledňují především finanční náročnost dané formy. Mezi ty nejběžnější formy lze zařadit rozesílání aktuálních informací o kybernetických nástrahách, školení zaměstnanců a vzdělávání studentů v rámci hodin informatiky.

Ze srovnání soukromého sektoru a veřejných vzdělávacích institucí z hlediska kybernetické bezpečnosti je na první pohled patrné, že zmíněné finanční hledisko hraje rozhodující roli při determinaci připravenosti a aktuálního stavu kybernetické bezpečnosti v prostředí vzdělávacích institucí. Společnosti

[4] What Is Cybersecurity?. *Cisco* [online]. San Jose, CA, USA: Cisco Systems, c2022 [cit. 28.11.2021]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

v soukromém sektoru si často mohou finančně dovolit vzdělávat své zaměstnance v oblasti kybernetické bezpečnosti kvalitně, opakovaně a především pravidelně. Právě pravidelnost a aktuálnost předávaných informací hraje důležitou roli při připravenosti na aktuální hrozby z prostředí kyberprostoru. Vzdělávací instituce si však tento přístup často nemohou dovolit, a to z důvodu absence finančních prostředků či domněnky, že základní poučení zaměstnance při nástupu do pracovního poměru v oblasti kybernetické bezpečnosti je dostatečnou ochranou před možnými škodami.[5]

Důležitou část tvoří nejpočetnější skupina uživatelů, tedy studenti vzdělávací instituce. Ti jsou společně s ostatními uživateli nejzranitelnějším článkem celého komplexního systému. Ti se zároveň podstatně liší od uživatelů velkých institucí v soukromém sektoru, kde dochází ve srovnání se vzdělávacími institucemi k mnohem méně početné pravidelné obměně uživatelů. Absolventi vzdělávací instituce opouštějí a zároveň přicházejí noví studenti. Dalším faktorem ovlivňujícím kybernetickou bezpečnost vzdělávacích institucí je počet a správa zařízení, která přistupují do vnitřních sítí. Soukromý sektor je schopen prakticky všechna zařízení spravovat samostatně a vymezit přesně stanovené podmínky pro užívání zařízení, která nejsou v jejich správě. Oproti tomu vzdělávací instituce často nemají efektivní a finančně dostupný způsob, kterým by bylo možné zařízení v síti monitorovat, spravovat či regulovat. Většina uživatelů vzdělávací instituce disponuje soukromým zařízením v jejich vlastnictví, ať už je to chytrý telefon, tablet či notebook. Tato zařízení pak nelze žádným způsobem spravovat a kontrolovat tak jejich bezpečnost, aktuálnost či míru rizika pro celou síť.[6]

Každé takové zařízení pak teoreticky představuje potenciální bezpečnostní riziko. Lze navrhnout přísné filtrování obsahu, ke kterému je uživatelům povolen přístup, nicméně toto řešení je značně časově náročné a nepříliš přínosné pro efektivitu práce. Nejvíce efektivním způsobem obrany proti kybernetickým útokům tak zůstává především pravidelné vzdělávání studentů, pedagogů a všech dalších

[5] KRESA, Dan. 3 výzvy kybernetické bezpečnosti ve vzdělávacím sektoru. *KYBEZ* [online]. Jihlava: GORDIC, c2021, 16. 5. 2018 [cit. 28.11.2021]. Dostupné z: https://www.kybez.cz/3-vyzvy-kyberneticke-bezpecnosti-ve-vzdelavacim-sektoru/

[6] BREJCHA, Pavel. Útoky na univerzity jsou v kybernetickém prostoru novým standardem. *Fakespace* [online]. Fakescape, c2021, 28. 12. 2021 [cit. 28.11.2021]. Dostupné z: https://www.fakescape.cz/blog/kyberneticke-utoky-univerzity

pracovníků společně s poskytováním aktuálních informací všech uživatelů o možných nástrahách kyberprostoru.[7]

### 2.1.1 Zajišťování kybernetické bezpečnosti

Vzdělávací instituce v České republice se při zajišťování kybernetické bezpečnosti dle průzkumu společnosti ESET, provedeného v listopadu roku 2019, potýkají především s nedostatkem finančních prostředků. Více jak polovina dotázaných institucí uvedla, že na zajištění vysokého standardu kybernetické bezpečnosti postrádá finanční prostředky. Mírně znepokojivým zjištěním průzkumu byly případy, kdy se o kybernetickou bezpečnost vzdělávací instituce stará učitel informatiky působící na dané instituci jako pedagog, celkem se jednalo téměř o pětinu všech dotazovaných institucí. Fundovaní specialisté na kybernetickou bezpečnost dovednosti uplatňují spíše v soukromém sektoru, a to zvláště z důvodu finančního ohodnocení. Vzdělávací instituce si zde nemohou dovolit investovat stejné množství finančních prostředků jako společnosti ze soukromého segmentu.[8]

Mezi nejběžnější způsoby zajišťování kybernetické bezpečnosti na vzdělávacích institucích patří osvěta a výuka. Nejpočetnější skupina uživatelů, studenti, jsou v rámci hodin informační a výpočetní techniky vzděláváni v oblasti kybernetické bezpečnosti. Důraz je kladen nejvíce na zodpovědnost, ostražitost a užívání kritického myšlení. Běžně řešená témata jsou například dostatečně silná hesla, podezřelé odkazy obsažené v e-mailové korespondenci, pravidelná aktualizace všech zařízení, digitální stopy a možnost jejich zneužití, základní seznámení s různými typy kybernetických útoků, bezpečnost sítí nebo antivirová ochrana. Dle názoru autora práce by měla být osvěta a výuka vždy doplněna o konkrétní kazuistiku. Samotný apel na uživatele je zřídkakdy dostatečným argumentem k přesvědčení, že kybernetické hrozby se přímo týkají i jejich osoby. Problematika by měla být předkládána komplexně a s konkrétními příklady

[7] BREJCHA, Pavel. Útoky na univerzity jsou v kybernetickém prostoru novým standardem. *Fakespace* [online]. Fakescape, c2021, 28. 12. 2021 [cit. 28.11.2021]. Dostupné z: https://www.fakescape.cz/blog/kyberneticke-utoky-univerzity

[8] ESET: Kybernetickou bezpečnost na školách v pětině případů řeší učitel informatiky. *ESET* [online]. Bratislava: ESET, c1992 – 2022, 21. 11. 2019 [cit. 28.11.2021]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-kybernetickou-bezpecnost-na-skolach-v-petine-pripadu-resi-ucitel-informatiky/

bezpečnostních hrozeb, jejich dopadů a následků. K výuce a osvětě lze využít celou řadu materiálů, příkladem jsou volně dostupné materiály a kurzy základů kybernetické bezpečnosti poskytované Národním úřadem pro kybernetickou a informační bezpečnost. Uživatelé se mohou chovat zodpovědně v celém kyberprostoru, nebo v žádné z jeho částí. Požadovaného efektu mohou dosáhnout pouze tehdy, pokud budou dodržovat pravidla bezpečného chování v kyberprostoru jak v osobním, tak pracovním prostředí.[9]

Vzdělávání v oblasti kybernetické bezpečnosti je nutné podrobovat také zaměstnance vzdělávací instituce. Důležité je pravidelně vyzdvihovat význam neustálé obezřetnosti a seznamování se s novými riziky. Pro pedagogy, stejně jako studenty, existuje řada volně přístupných kurzů a zpracovaných materiálů. Stanovena by měla být vnitřní pravidla kybernetické ochrany uvnitř vzdělávací instituce, která budou shrnovat základní požadavky na bezpečné využívání všech součástí infrastruktury vzdělávací instituce, včetně všech systémů, služeb a hardware.

### 2.1.2 Bezpečnostní rizika

Vzdělávací instituce ve vztahu k zajištění procesu vzdělávání pracují s řadou databází, systémů, dat, a také financemi. Všechny zmíněné prvky představují potenciální cíl útoků a možnosti vzniku škod. Prvním, a zároveň kritickým, prvkem jsou databáze a systémy shromažďující údaje o studentech a zaměstnancích. Potřeba těchto databází plyne z povahy nutnosti evidence a agendy, kterou instituce ve vztahu ke studentům a zaměstnancům zajišťuje.[10]

V případě studentů se jedná o evidenci jména, příjmení, data narození, rodného čísla, bydliště, státní příslušnosti a případně dalších osobních údajů. Tyto databáze taktéž často obsahují jméno a příjmení zákonných zástupců, včetně jejich telefonních kontaktů a e-mailových adres. Tyto databáze pak mohou být

[9] viz str. 4, HÁJEK, Martin. Kurz základů kybernetické bezpečnosti. *Dávej kyber* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 4.12.2021]. Dostupné z: https://osveta.nukib.cz/mod/resource/view.php?id=1024

[10] ČERNÝ, Michal. *Informační systémy ve vzdělávání: od matrik k sémantickým technologiím a dialogovým systémům pro učení* [online]. Brno: Masarykova univerzita, 2016 [cit. 4.12.2021]. ISBN 978-80-210-9129-0. Dostupné z: https://is.muni.cz/el/1421/jaro2016/VIKMB39/um/kniha_Informacni_systemy_ve_vzdelavani_kor_MG.pdf

vedeny centrálně v síťovém úložišti vzdělávací instituce s podmíněným přístupem autorizovaných osob na základě znalosti přístupových údajů, nebo na konkrétním místě, často pouze v jediném zařízení na celé instituci, ke kterému má přístup pouze vymezený okruh osob. Databáze tohoto typu není vhodné provozovat a přechovávat v prostředí cloudového úložiště třetí strany. V ideálním případě by měly být databáze z vnějšku instituce zcela nepřístupné. Pokud existuje podstatný důvod databázi v cloudovém úložišti provozovat, mělo by se toto úložiště fyzicky nacházet v budově instituce, dostatečně fyzicky a kyberneticky zabezpečené. Především by mělo být spravováno osobou s dostatečnou znalostí problematiky kybernetické bezpečnosti.

Systémy zajišťující běžnou agendu, zejména docházku, zápisy hodin a hodnocení studentů vzhledem k požadavku přístupnosti z internetu, nelze provozovat výše zmíněnými způsoby. Informační systémy vzdělávacích institucí jsou pomyslným komunikačním nástrojem mezi vzdělávací institucí a studentem, který skrze tento systém získává všechny podstatné informace týkající se studia. Datový obsah těchto systému nebývá zdaleka tak citlivý, jako je tomu u databází s osobními údaji. Důvodem je opodstatněná obava z možné kompromitace systému a odcizení dat. Informační systémy vzdělávacích institucí mohou být provozovány samotnou institucí, popřípadě třetí stranou. V případě středních škol je velmi rozšířený systém Bakaláři, který nabízí kromě samotného systému i službu hostování serveru, na kterém je systém zprovozněn. Bezpečnostní rizika spojená s narušením informačního systému lze sledovat hlavně ve vzniku chaosu v důsledku odepření přístupu, například DoS útoky.[11]

Finanční stránku vzdělávací instituce lze rozdělit na dvě části – finance spravované ve formě hotovosti a finance spravované digitálně. V případě hotovosti se jako vhodné jeví sumy vyšší nominální hodnoty uchovávat v trezoru pevně spojeném se základy budovy či v obdobných zabezpečovacích zařízeních. U dispozice s digitálními financemi je třeba zajistit ochranu celého procesu. Primárně je bezpečnost digitálních platebních prostředků na našem území zajišťována na základě zákona č. 370/2017 Sb., O platebním styku. § 223 tohoto

[11] Co všechno umíme?. *BAKALÁŘI* [online]. Příbram: BAKALÁŘI software, c2022 [cit. 4.12.2021]. Dostupné z: https://www.bakalari.cz/Static/WhatWeKnow
Více viz kapitola 2.2.3 DoS

zákona stanoví požadavek „*silného ověření uživatele*“ jehož primárním cílem je snižovat riziko a předcházet podvodům a zneužití platebních prostředků. Jedná se o mechanismus zabezpečení ve formě dvoufaktorové autentizace. To znamená, že přístup k bankovnímu účtu a akce s ním spojené jsou vázány na minimálně dva prvky zabezpečení. Mezi prvky zabezpečení patří prvek znalosti, biometrické údaje nebo majetkový prvek. Cílem silného ověření uživatele je zamezit bezpečnostním hrozbám i v případech, kdy je kompromitován jeden z bezpečnostních prvků ověření. I přes tato opatření je však třeba dbát zvýšené opatrnosti při aktivitách oprávněných osob vzdělávací instituce v internetovém nebo mobilním bankovnictví.[12]

Vzhledem k doznívající pandemii vznikla nová bezpečnostní hrozba plynoucí z on-line výuky. Na internetu je možné se běžně setkat se záznamy vyučování, které mohou být zveřejňovány vzdělávací institucí, ale také samotnými žáky či pedagogy. Problémem je zde ochrana osobních údajů. Zveřejněné záznamy totiž často vyobrazují studenty s jejich jmény a přenášeným obrazem webkamery. Z těchto záznamů je tedy velmi jednoduché ztotožnit konkrétní osoby, často nezletilé. Ze záznamů je možné vidět vyjma výše zmíněného taktéž sociální podmínky daných osob. Instituce by měly usilovat o stažení těchto materiálů, jelikož mohou představovat nejen potenciální problém z hlediska ochrany osobních údajů, ale také bezpečnostní riziko pro samotné studenty. Tyto materiály mohou být využity například k vydírání pedagogů či vzdělávací instituce jako celku, ale také ke kyberšikaně a zesměšňování vyobrazených osob.[13]

Problematiku bezpečnosti vzdělávací instituce je třeba chápat v širších souvislostech. Nelze se zaměřit pouze na konkrétní prvek instituce v domnění, že zabezpečení tohoto konkrétního prvku bude dostatečným opatřením. Komplexní přístup k problému bezpečnosti začíná u analýzy prostředí jakožto celku a stanovení rizikových segmentů. V potaz by měly být vzaty nejen virtuální a fyzické prvky instituce, ale také uživatelé. Právě uživatelé se stávají největším

[12] Zákon č. 370/2017 Sb., *Zákon o platebním styku* ve znění k 11. 12. 2021

Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. EPRAVO.CZ, c1999-2022, 18. 9. 2019 [cit. 8.12.2021]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

[13] NÚKIB. Online výuka a bezpečnost. *YouTube* [online]. 25. 3. 2021 [cit. 5.12.2021]. Dostupné z: https://www.youtube.com/watch?v=8y9Z-f97_3M

potenciálním bezpečnostním rizikem a jejich dostatečné proškolení, pravidelné vzdělávání a seznamování s riziky by nemělo být podceňováno. Provoz, správné fungování a zachování integrity vzdělávací instituce stojí především na základech bezpečného chování uživatelů.

## 2.2 Kybernetické útoky

V této kapitole jsou představeny základní charakteristiky kybernetických útoků, kterými se tato práce zabývá, a se kterými dále pracuje v praktické části. Jednotlivé útoky jsou popsány z pohledu možných napáchaných škod vzdělávacím institucím společně s riziky z nich následně vyplývajícími. Útoky byly vybrány na základě pozorování běžného fungování uživatelů a rozličných prvků struktury informačních a komunikačních technologií konkrétní vzdělávací instituce.

### 2.2.1 Phishing

Název tohoto útoku je odvozen z anglického *fishing* – *rybaření*. Cílem phishingu je získání důvěry oběti, která je následně zneužita k získání citlivých dat, finančních prostředků či přístupových údajů. Formy phishingu jsou různorodé, nejběžněji však mívají povahu e-mailu zaslaného oběti, ve kterém je dále schován odkaz na podvodnou webovou stránku. Tyto podvodné webové stránky pak kopírují, často naprosto přesně, vzhled oficiální webové stránky. Rozpoznat tak podvrh od legitimního e-mailu nebo webové stránky může být pro běžné uživatele často obtížné. Phishingové útoky se často na první pohled tváří jako naprosto legitimní požadavky, například od bankovních institucí, IT oddělení či dalších poskytovatelů služeb, ke kterým je vyžadován přístup pomocí přihlašovacích nebo jiných ověřovacích údajů.[14]

Phishing je v dnešní době jedním z nejběžněji používaných kybernetických útoků. Na území ČR tvořil tento typ útoku celkem 16 % z celkového počtu útoků zaznamenaných ve statistikách Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020 publikované Národním úřadem pro kybernetickou

[14] What Is Phishing?. *Phishing.org* [online]. Clearwater, Florida, USA: KnowBe4 [cit. 18.12.2021]. Dostupné z: https://www.phishing.org/what-is-phishing

a informační bezpečnost. V těchto statistikách je zahrnuto celkem 222 subjektů, z čehož klíčový podíl pro tuto práci tvoří 20 vzdělávacích institucí.[15]

Zamezit situacím, kdy se uživatelé stávají obětí phishingu, lze zejména dostatečnou obezřetností a opatrností. Uživatelé by nikdy neměli otevírat hypertextové odkazy, u kterých neznají původ nebo cíl tohoto odkazu. Odhalit phishingový útok lze často i z pouhého oslovení uvedeného v e-mailové zprávě. Ty často začínají obecnými frázemi, například *„Vážený uživateli“* nebo *„Vážený kliente“*. Problém vyvstává tehdy, kdy je phishingový útok za pomoci sociálního inženýrství upraven přesně pro konkrétní osobu (*tzv. spear-phishin*g). Zde již nelze aplikovat obecné pravidlo oslovení z důvodu útočníkovy možné znalosti jména oběti. Vyjma oslovení správným jménem mohou zprávy obsahovat řadu jiných pravdivých informací, které se útočníkovi podařilo získat, například konkrétní jména pracovníků instituce, pracovní pozice, odkazy na legitimní webové stránky instituce a další podobné údaje, které dokáží v oběti vzbudit důvěru. Uživatelé by nikdy neměli otevírat podezřelé odkazy nebo stahovat a otevírat podezřelé soubory, které se v těchto zprávách nacházejí. Vždy, když si uživatel není jist legitimitou, měl by obsah konzultovat s odesílající osobou prostřednictvím jiného komunikačního kanálu pro ověření, zda daná osoba zprávu opravdu odeslala. Pokud není uživatel schopen žádným dostupným způsobem ověřit legitimitu sdělení, je vhodné jej konzultovat s osobou pověřenou řešením kybernetických hrozeb v dané instituci.[16]

### 2.2.2 Spam

Dalším z řady kybernetických útoků, se kterými se lze v prostředí vzdělávacích institucí setkat, je spam. Toto označení je užíváno pro zprávy, které jsou uživateli zasílány bez jeho souhlasu, obecně se pak označují jako nevyžádaná elektronická pošta. Spam ve své surové podobě nepředstavuje zvýšené bezpečnostní riziko, nebezpečný začíná být ve chvíli, kdy je jeho součástí podezřelá příloha, odkazy vedoucí na neznámé, podvodné a nelegální stránky

[15] viz str. 9, *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020.* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 26. 7. 2021 [cit. 21.12.2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

[16] Phishing. *Avast* [online]. Praha: AVAST, c1988-2022 [cit. 28.12.2021]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

nebo jiný druh škodlivého kódu. Charakteristické pro spam je pak opakované zasílání stejného sdělení.[17]

V praxi jsou dnes již naprosto běžné filtry spamu, které jsou schopné rozpoznat, zda se jedná o hromadné nevyžádané sdělení a přesunout ho následně do příslušné složky, obvykle označované poskytovateli e-mailových schránek jako *nevyžádaná pošta* nebo *spam.* Tyto filtry však nejsou neomylné a existuje tak šance, že filtr zprávu nedokáže rozpoznat a neprovede její filtraci. Zpráva se pak ocitne mezi doručenou poštou, k čemuž rozesílatelé spamu využívají řadu technik. Mezi ty nejběžnější pak patří využití proxy serverů, které spam rozesílají na základě požadavků a skrývají tak reálnou identitu odesílatele. Spam filtry spam odhalují na základě řady kritérií, mezi které mimo jiné patří IP adresa odesílatele a doména. V případě domény vzdělávací instituce poskytovatelé služeb elektronické pošty často filtrují i příchozí zprávy z jiných domén, často však pouze zobrazením upozornění, že odesílatel zprávu odeslal z účtu mimo doménu.[18]

Pro vzdělávací instituce může spam i v čistě surové podobě představovat určitou míru nebezpečí, minimálně je pak nutné zhodnotit časové hledisko, kdy velké množství spamu dokáže pracovníky značně zdržovat a obtěžovat při běžné pracovní činnosti. Největší riziko autor pak spatřuje v momentu, kdy je množství spamu neúměrně vysoké, zejména v situacích, kdy je odesílatel spamu schopen zprávy odesílat se shodným obsahem pole příjemce a odesílatele. Uživateli se zpráva zobrazí, jako kdyby ji zaslal sám sobě, a často je tímto způsobem ošálen filtr spamu. Za neméně nebezpečné lze považovat taková nevyžádaná sdělení, která obsahují neznámé odkazy a přílohy. Obsah sdělení, u kterého uživatel nemá znalost původu, je podezřelý či neobvyklý, by neměl být otevírán a zpráva by měla být oznámena osobě odpovědné za řešení podobných incidentů. Na místě je pak

[17] viz str. 100, *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online* [online]. Praha: CZ.NIC, 2013. [cit. 1.2.2022]. ISBN 978-80-904248-6-9. Dostupné z: https://knihy.nic.cz/files/edice/bud_panem_sveho_prostoru.pdf

[18] viz str. 32-33, SPAMMER-X, POSLUNS, Jeffrey, ed. *Inside the SPAM Cartel: Trade Secrets From The Dark Side*. Rockland, MA: Syngress, c2004. ISBN 1-932266-86-0.

IP Address. *TechTerms* [online]. Minneapolis, MN, United States: Sharpened, c2020 [cit. 8.1.2022]. Dostupné z: https://techterms.com/definition/ip_address

všem zaměstnancům ohlásit možný výskyt podobného sdělení a připomenout správné chování v této situaci.

Pro instituci je spam vysokým rizikem především proto, že e-mailové adresy většiny vzdělávacích institucí jsou veřejně dostupné. Pro útočníka je tak přípravná fáze – získávání adresátů, značně zjednodušena a může útok cílit plošně na řadu e-mailových schránek. Při nesprávném nastavení nebo nefunkčnosti filtru spamu mohou nastat i situace, kdy dojde k zahlcení schránek. V některých případech, zejména u institucí, které mají e-mailové servery s nízkou kapacitou úložiště, lze očekávat zaplnění tohoto úložiště a následné zablokování příjmu dalších zpráv. Dále je možné zaznamenat riziko zahlcení e-mailového serveru, někdy až jeho přehlcení, kdy přestane zprávy přijímat nebo zapříčiní jejich opožděný příjem.

### 2.2.3 DoS

Název DoS je zkratkou anglického Denial of Service. Volně lze toto spojení přeložit jako odepření služby. Cílem DoS útoků je paralyzovat určitý prvek sítě informačních a komunikačních technologií nebo celou síť. Způsob, kterým je stavu odepření služby docíleno, je zahlcení cíle mnoha požadavky. Cíl, kterým může být například konkrétní server, jeho konkrétní služba, síť nebo její prvky, není schopen tento velký počet požadavků zpracovávat. Důsledkem je pak nedostupnost cíle legitimním uživatelům. V praxi se lze setkat se zkratkou DDoS – Distributed Denial of Service, tedy distribuované odepření služby. Běžně je tento útok veden z řady výpočetních strojů, proto je odhalení a potlačení útoku často velmi složité, až nemožné.[19]

Škoda způsobená DoS útoky není spojena se ztrátou nebo narušením integrity uložených dat, jedná se pouze o odepření přístupu k těmto datům z vnější strany sítě. Útok je často cílen na konkrétní server nebo službu dané organizace. V případě vzdělávacích institucí lze za potenciální cíl vzít v potaz webové stránky, informační vzdělávací systémy, počítačové sítě v odborných učebnách nebo WiFi sítě, přesněji aktivní prvky sítí. Nutné je však vzít v potaz i DoS útoky vedené uvnitř

[19] What is a denial of service attack (DoS) ?. *Palo Alto Networks* [online]. Kalifornie, USA: Palo Alto Networks, c2022 [cit. 8.1.2022]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

sítě, kdy infikovaný stroj připojený do lokální sítě infikuje škodlivým kódem ostatní stroje, které následně vedou útok na dostupné služby či servery.

Řada vzdělávacích institucí začíná upouštět od běžné evidence v papírové podobě. Například evidence docházky či zápisy hodin se již nezanášejí do papírových třídních knih, nýbrž do elektronických systémů a databází. Tyto databáze jsou běžně provozovány na serveru a jsou zpřístupněny dle kompetencí daným uživatelům vzdělávací instituce. Kompetence se pak liší v závislosti na tom, zda je uživatelem administrátor, pedagog nebo třídní učitel. Náhradou papírových třídních knih se často celý proces evidence značně zjednodušil, urychlil a zpřehlednil, nicméně vyvstala nová rizika plynoucí z digitální povahy těchto evidencí. Servery hostující služby vzdělávacích informačních systémů jsou pak nedílnou součástí běžného provozu instituce a jejich nedostupnost může způsobit značný chaos a řadu nepříjemností spojených s následným doplňováním evidencí.

S DoS útoky na informační systémy vzdělávacích institucí, především pak vysokých škol, se lze setkat velmi běžně, a také pravidelně. Nutné je zde zmínit, že tyto útoky se odehrávají s určitou pravidelností. Nejedná se o útoky v pravém slova smyslu, avšak zcela naplňují všechny jeho znaky. Onou pravidelnou událostí, která činí informační systémy vzdělávacích institucí nedostupné, je pravidelný zápis předmětů před začátky semestrů. Obrazně řečeno útočníky se zde stávají stovky studentů, kteří ve snaze získat zápisový lístek do některého z předmětů přistupují k informačnímu systému často i z několika zařízení zároveň. Nelze tedy předpokládat, že při vpuštění například 300 uživatelů k zápisu předmětů bude počet požadavků roven stejnému počtu. Často se jedná o několikanásobně větší množství požadavků, právě z důvodu přístupu uživatelů z více než jednoho zařízení. Tyto situace lze řešit několika způsoby. Za vhodné řešení lze považovat postupné otevírání databáze zápisu, po vlnách, pro menší počty studentů, a jejich dostatečné časové oddělení s cílem předcházet stavu, kdy se informační systém zahltí a přestane zpracovávat požadavky.

DoS útoky vedené úmyslně, nejen proti vzdělávacím institucím, může být značně obtížné filtrovat a bezpečně jim předcházet. Řada služeb vzdělávacích institucí je dostupná z internetu nemalému počtu uživatelů, proto je při předcházení DoS útokům prakticky nemožné filtrovat legitimní uživatele od

uživatelů útočících. Servery jsou často koncipovány tak, aby byly schopné odbavovat běžný provoz a z finančního hlediska by bylo značně nehospodárné provozovat takové servery, které by byly schopny odbavovat požadavky v řádech desetinásobků, a díky tomu vydržet nápor požadavků, ať už legitimních či nelegitimních. V praxi lze požadavky filtrovat dvěma způsoby. Prvním způsobem je nasazení filtru přímo do datového toku, kdy jsou všechny požadavky filtrovány před vpuštěním na server. Druhou možností je sledování provozu a ve chvíli, kdy se objeví abnormální počet požadavků, dojde k odklonění provozu na zařízení, které požadavky před vstupem na server filtruje. Nicméně je třeba podotknout, že každý DoS útok je specifický a nelze učinit taková opatření, která by spolehlivě zabránila všem útokům. Nutno také zmínit, že sofistikovaná řešení na ochranu před DoS útoky jsou velmi nákladná a pro vzdělávací instituce finančně často nedostupná.[20]

### 2.2.4 Sociální inženýrství

Informační a komunikační technologie se, i přes jejich neustálý a rapidní rozvoj, neobejdou bez zásahu lidské bytosti. K jejich správnému fungování, zprovoznění a údržbě je stále třeba lidské síly. Lidé, v tomto případě uživatelé, vykazují obecně větší míru rizika chybovosti, protože na rozdíl od strojů vstupují do jejich procesu rozhodování lidské city, emoce, stres a další faktory ovlivňující tento proces. Útočníci jsou si těchto nedostatků lidských bytostí vědomi a patřičně jich k realizaci útoků zneužívají.

Sociální inženýrství je technika využívající lidské chybovosti a důvěřivosti s cílem vylákat z oběti citlivá data, přístupové údaje, přístupy k systémům a další podobné důvěrné informace. Důvěra v obětech je často vzbuzována za pomoci falešné identity útočníků, kteří se vydávají za spolupracovníky, administrátory, či pracovníky technické podpory. Samotné útoky sociálního inženýrství mohou být doprovázeny dalšími podvodnými jevy, například donucení oběti k instalaci nebo rozšíření malware či jiného škodlivého kódu. Technikami manipulace jsou útočníci

[20] KRČMÁŘ, Petr. DDoS útoky: jak se účinně bránit?. *Root.cz* [online]. Praha: Internet Info, c1998 – 2022, 16. 5. 2016 [cit. 15.1.2022]. Dostupné z: https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/

schopni oběti oklamat a zmást takovým způsobem, aby jednali přesně tak, jak útočníci chtějí.[21]

Stěžejním prvkem k realizaci úspěšného útoku pomocí sociálního inženýrství je komunikace mezi útočníkem a obětí. Na rozdíl od ostatních kybernetických útoků je sociální inženýrství možné realizovat v určitých částech, zejména ve fázi získávání důvěry a přístupových či jiných údajů, mimo kyberprostor. Útočníci tak místo komplikovanějších útoků na specifické prvky v kyberprostoru cílí na reálné osoby – uživatele, kteří jsou z hlediska kybernetické bezpečnosti nejzranitelnějším článkem celé soustavy informačních a komunikačních technologií.

V praxi lze dle autora rozlišovat dva druhy cíle útoku sociálního inženýrství. Prvním cílem je narušit integritu dat, systémů, databází či jejich funkčnosti. V těchto případech se útočníci zaměřují na napáchání co možná největšího množství škod právě narušením integrity zmíněných prvků. Druhým cílem je krádež, kdy útočníci získají přístup k datům, přístupovým údajům, systémům nebo databázím, a následně data, která jsou v těchto prvcích obsažena, odcizí. Následovat může fáze vydírání, při které se pod výhružkami zveřejnění, či smazání databází, dat nebo nevratného narušení databáze, snaží útočníci z obětí vylákat finanční prostředky.[22]

V prostředí vzdělávacích institucí je třeba mít na paměti, že sociální inženýrství může zneužít prakticky kdokoliv z vnitřní struktury. Útočníky mohou být pedagogové, ale také studenti. V některých případech se může jednat o hloupé žerty, nicméně i tyto útoky mohou být nebezpečné. Interní informace by měly zůstat interními. Vyzrazování byť i pocitově nepodstatných informací mimo vzdělávací instituci může vést k jejich zneužití či uskutečnění jiného kybernetického útoku. Informace, které jsou pro vzdělávací instituci citlivé a kritické, by neměly být zbytečně šířeny mezi uživatele, kteří jejich znalost k výkonu povolání nepotřebují. Podobně by mělo být zacházeno s kýmkoliv, kdo se bude informace snažit získat. V situaci, kdy osoba žádá informace potenciálně

[21] *SOCIAL ENGINEERING HANDBOOK: How to Take the Right Action* [online]. Bratislava:ESET, c1992 - 2021 [cit. 11.1.2022]. Dostupné z: https://datasecurityguide.eset.com/storage/download-widget-files/ESET_Data%20Security%20Guide_Social%20Engineering%20Handbook_UK.pdf

[22] Tamtéž.

citlivé povahy, je vždy vhodné odkázat na příslušnou osobu oprávněnou informace poskytovat.

Sociální inženýrství cílí na nejslabší článek celého bezpečnostního systému, kterým je uživatel. Pro prevenci a ochranu před tímto druhem útoku je vhodné uživatele seznámit se základní problematikou sociálního inženýrství, aby ve chvíli, kdy je proti nim použito, jej byli schopni rozpoznat. K sociálnímu inženýrství je každý uživatel náchylný odlišnou mírou, roli zde nehraje pouze znalost problematiky, ale taky řada psychologických a osobnostních faktorů. Ty mohou ovlivnit náchylnost uživatele k podlehnutí domnělé důvěře a vyzrazení citlivých informací. V potaz přichází vzdělávání reálnými případy, kdy uživatelé na základě zjištění možných následků získají určitou míru obezřetnosti jen na základě vyděšení.

### 2.2.5 Podvodný přístupový bod

Podvodný přístupový bod (z anglického rogue access point) je aktivní prvek, ve formě přístupového bodu nebo routeru, umístěný do sítě bez vědomí vlastníka či správce sítě. Takto umístěný přístupový bod může být potenciálním rizikem pro uživatele, který se k němu připojí a využívá jej pro komunikaci s internetem a zbytkem sítě. V prostředí vzdělávací instituce se lze běžně setkat s přístupovými body, které do sítě bez vědomí administrátora umístí některý ze zaměstnanců, aniž by měl podvodné úmysly. Často tak řeší například slabý signál bezdrátové sítě legitimního přístupového bodu nebo nedostatek portů pro připojení zařízení pomocí kabelu.[23]

Nebezpečí podvodných přístupových bodů spočívá zejména v možné krádeži dat přenášených skrze tento bod. Útočník, který bod do sítě umístil, je schopen data odcizit, sledovat nebo pozměnit. V praxi tento útok využívá dvě metody zachycování dat, aktivní a pasivní. Při pasivním zachycování dat útočník stojí v komunikaci v jejím středu, odposlouchává ji a přenesená data může shromažďovat. Při aktivním zachycování útočník data od odesílatele přijme, pozmění a pak odešle dále v podvržené podobě. Tomuto typu útoku se lze bránit

[23] Rogue access point. *PCMag* [online]. New York, NY: PCMag, c1996-2022 [cit. 12.1.2022]. Dostupné z: https://www.pcmag.com/encyclopedia/term/rogue-access-point

především šifrovanou komunikací, například protokolem HTTPS nebo využitím VPN.[24]

Protokol HTTPS komunikaci mezi uživatelem a cílovým serverem šifruje pomocí SSL na bázi asymetrické šifry. Pracuje se dvěma klíči, soukromým a veřejným. Strana komunikace, která chce navázat spojení, využije veřejný klíč k zašifrování datového přenosu. Následně je přenesená komunikace na základě soukromého klíče dešifrována. Pokud by došlo k zachycení komunikace útočníkem, nebude její obsah bez soukromého klíče možné číst.[25]

VPN (zkratka pro Virtual Private Network, česky virtuální privátní síť) je druh zabezpečeného spojení označovaného jako tunel v internetu mezi uživatelem a cílovou sítí. Komunikace procházející skrze VPN je šifrována a zajišťuje tak bezpečný přenos všech dat od uživatele přes internet do konkrétního místa. Šifrovaná komunikace je v případě zachycení síťového provozu útočníkem nečitelná. Instituce tuto technologii také běžně využívají ke správě vzdáleného přístupu do vnitřní privátní sítě.[26]

Na první pohled podvodné přístupové body, nazývané *Honeypots*, mohou být v síti umisťovány úmyslně správci za účelem odchytu potenciálních útočníků. Tyto body jsou monitorovány, nezabezpečeny a odpovědná osoba si je jejich přítomností v síti vědoma. Důležité je pak vyrozumět všechny ostatní uživatele sítě o přítomnosti tohoto bodu, popřípadě implementovat metodu, pomocí které bude možné přesně oddělit útočníky od legitimních uživatelů.[27]

---

[24] SHAH, Abhishek. Rogue access points. *Khan Academy* [online]. Kalifornie, USA: Khan Academy, c2022 [cit. 15.1.2022]. Dostupné z: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks

[25] VILLANUEVA, John C. An Introduction To Cipher Suites | SSL/TSL Cipher Suites Explained. *JSCAPE* [online]. Eugene, OR: JSCAPE, c2022, May 16, 2018 [cit. 15.1.2022]. Dostupné z: https://www.jscape.com/blog/cipher-suites

[26] What Is a VPN? - Virtual Private Network. *Cisco* [online]. San Jose, CA, USA: Cisco Systems, c2022 [cit. 18.11.2021]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[27] Understanding Rogue Access Points. *Juniper Networks* [online]. Sunnyvale, California, USA: Juniper Networks, c1999 - 2022, 5-Oct-18 [cit. 26.1.2022]. Dostupné z: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html

### 2.2.6 Krádež identity

Pod krádeží identity si již nelze obecně představovat činy jako například padělání dokladů či listin, tyto techniky jsou sice stále aktuální, nicméně jsou čím dál častěji nahrazovány pro útočníky „*bezpečnějšími*“ technikami užívanými v kyberprostoru. Kyberprostor útočníkům poskytuje značně vyšší míru anonymity, než svět reálný, kde riskují, že bude jejich podvodná či podezřelá činnost zaznamenána jinou osobou. Nelze se však domnívat, že podvodná činnost v kyberprostoru je neviditelná, útočníci po sobě zanechávají stopy, ale některé z těchto stop lze efektivně manipulovat a zastírat takovým způsobem, aby odhalení bylo značně obtížné.

Obecně lze krádež identity vymezit jako podvodné jednání útočníka s cílem získat data osobní povahy a zneužít je ke svému prospěchu. Toto zneužití je pak kryto právě ukradenou identitou, kdy se útočník přímo vydává za poškozeného, který mnohokrát nemá tušení, že se stal obětí útoku. Zjištění oběti pak často přichází až ve chvíli, kdy zjistí, že přišel o finanční prostředky nebo přístup do svého účtu. V případě zneužití identity pro získání citlivých dat je pak prakticky nemožné zjistit, kde se data po odcizení nachází a jak je s nimi dále nakládáno.[28]

Samotná krádež identity může probíhat prostřednictvím specifických útoků, především pak za využití technik sociálního inženýrství, phishingu a malware či ransomware. V souvislosti se vzdělávacími institucemi pak bude tento útok nejčastěji mířen na citlivá data, finanční prostředky instituce, ale také na její pověst a dobré jméno. Útočník získanou identitu může využít nejen k vydírání, ale také k vystupování jménem instituce, což může nepochybně vést k poškození pověsti.[29]

Krádež identity prostřednictvím malware, kterým útočník získá totožný otisk systému oběti, může vést k situaci, kdy oběť ztratí veškerou kontrolu nad vlastním systémem. Tento typ krádeže identity je velice efektivní, zejména pak v tom, že útočník získá plný přístup ke všem odcizeným částem systému a oběť ani vnější svět netuší, že tato identita byla kompromitována. Útočník tak může například

[28] WHAT IS IDENTITY THEFT?. *Terranova Security* [online]. Laval, Quebec, Canada: Terranova Worldwide, c2022 [cit. 2.2.2022]. Dostupné z: https://terranovasecurity.com/what-is-identity-theft/

[29] Identity Theft. *ESET* [online]. Bratislava: ESET, c1992 – 2022 [cit. 18.2.2022]. Dostupné z: https://www.eset.com/uk/types-of-cyber-threats/identity-theft/

zneužít e-mailové korespondence, kompromitovat vnitřní systémy a databáze, odcizit citlivá data.

Obranou proti tomuto druhu útoků je především uživatelská obezřetnost a dostatečně vysoká míra zabezpečení všech zařízení, systémů a databází. V první řadě by uživatel neměl nikdy sdílet své přístupové údaje, a to ani se spolupracovníky, popřípadě ostatními studenty – v tomto případě se může jednat o útok prostřednictvím sociálního inženýrství. Ve chvíli, kdy je tak učiněno, přestává mít uživatel kontrolu nad prozrazenými přístupovými údaji, které mohou být nevědomě, ale i vědomě prozrazeny dalším osobám a zneužity k podvodným aktivitám.

## 2.3 Vedlejší škody

Kybernetické útoky jsou často prováděny a koncipovány tak, aby zasáhly konkrétní cíl, nicméně je třeba vzít v potaz možnost, že útok napáchá i vedlejší škody nebo zamýšlený cíl mine, tedy situace, kdy se škodlivé účinky útoku projeví mimo původně stanovený cíl. Tento pojem je spjat zejména s využitím kybernetických útoků ve spojitosti s dosahováním národních, mezinárodních a válečných cílů, kdy je diskutována obzvláště morální stránka a poměr mezi výhodou plynoucí z dosažení cíle a způsobenými vedlejšími škodami. V dnešní době je naprosto běžné, že jsou pracovní prostředí mnoha odvětví propojena takovým způsobem, aby bylo možné vyvíjet činnost i mimo lokální síť v zaměstnání. To umožňuje pracovní proces v určitých poměrech zjednodušit, zrychlit, ale také učinit méně bezpečným.[30]

Příkladem vedlejších škod může být malware určený pro kompromitaci a zašifrování databáze či systému vzdělávací instituce, šířený prostřednictvím škodlivého kódu umístěného do odkazu či souboru v e-mailu. Ten je následně zaslán na adresu některého ze zaměstnanců instituce. Šiřitel škodlivého kódu se domnívá, popřípadě spoléhá na to, že adresát škodlivý kód otevře uvnitř lokální sítě instituce nebo na zařízení, jehož součástí je i cílený systém nebo databáze. Může však nastat situace, kdy adresát tento kód z e-mailu spustí mimo lokální síť

[30] ROMANOSKY, Sasha a Zachary K. GOLDMAN. What Is Cyber Collateral Damage? And Why Does It Matter?. *Lawfare* [online]. The Lawfare Institute, c2022, November 15, 2016 [cit. 11.2.2022]. Dostupné z: https://www.lawfareblog.com/what-cyber-collateral-damage-and-why-does-it-matter

instituce, například na počítači, který má v místě bydliště a běžně jej mimo osobního využívá také jako pracovní. Škodlivý kód tak může způsobit škody pouze na tomto stroji, který není součástí lokální sítě. Zašifrovaná či kompromitovaná databáze pouze na jediném, v tomto případě osobním stroji je „*zanedbatelná*“ škoda oproti situaci, kdy se malware začne šířit uvnitř celé lokální sítě instituce. Za vedlejší škody lze považovat také situace, kdy se škodlivý kód z lokální sítě začne šířit mimo ni.

Šíření škodlivého kódu mimo lokální síť, ale také z vnějšku do lokální sítě, může být kvůli dnes hojně využívané technologii VPN mnohem jednodušší, než by tomu tak bylo bez této technologie. Principem této technologie je chránit uživatele v reálném čase před sledováním a potenciální krádeží dat při využívání veřejné sítě za pomoci šifrování komunikace a jejího ověření. Vyjma této ochrany skýtá další výhody, například umožňuje uživateli se vzdáleně připojit a pracovat v lokální síti zaměstnání. Zde však narážíme na problém, kdy tato chráněná a šifrovaná komunikace nezabrání přenosu škodlivého kódu. Myšleny jsou takové případy, kdy uživatel mimo lokální síť skrze VPN přenese, vědomě či nevědomě, do lokální sítě infikovaný soubor, který se následně v síti může šířit. Může nastat i situace obrácená, kdy uživatel z lokální sítě přenese škodlivý kód na stroj stojící běžně mimo lokální síť. Obě zmíněné situace lze považovat za vedlejší škody útoku.[31]

Množství způsobené škody je pak přímo závislé na aplikovaných bezpečnostních opatřeních a zabezpečeních lokální sítě, strojů a ostatních přidružených prvků. Jako účinné metody obrany je vhodné zmínit pravidelné zálohování všech částí sítě a systémů, ze které lze všechny zašifrovaná či jinak poškozená data obnovit. Na paměti je třeba mít i fakt, že zálohovací systémy mohou vytvářet zálohy, které jsou poškozené či zašifrované. Měly by proto být nastaveny tak, aby byly přítomné zálohy minimálně několik dní zpět. Kritické systémy a databáze by pak měly být zálohovány takzvaně „*air-gapped“*, tedy takovým způsobem, kdy nejsou přístupné ze sítě.

[31] What Is a VPN? - Virtual Private Network. *Cisco* [online]. San Jose, CA, USA: Cisco Systems, c2022 [cit. 19.2.2022]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

# 3. Kybernetická bezpečnost vzdělávací instituce Alfa

Praktická část diplomové práce se zabývá analýzou a rozborem sítě informačních a komunikačních technologií specifické vzdělávací instituce, realizací konkrétních kybernetických útoků na tuto instituci, analýzou všech jednotlivých komponent těchto útoků a popisem jednotlivých částí útoků.

Hned z počátku je třeba zdůraznit, že všechna probíhající činnost a obsah podléhá schválení ze strany ředitele vzdělávací instituce. Před samotným zahájením byl o plánované činnosti informován ve všech částech, obsahu, náležitostech a vyslovil souhlas s činností v plném dohodnutém rozsahu. Pro potřeby této práce byl vyhotoven informovaný souhlas, jehož plné znění v písemné podobě je k dispozici u ředitele vzdělávací instituce. V informovaném souhlasu bylo mezi autorem a ředitelem vzdělávací instituce dohodnuto, že vzdělávací instituce nebude konkretizována. Z tohoto důvodu je v této části práce odkazováno na konkrétní instituci pouze jako na vzdělávací instituci „*Alfa*“. Vyjma ředitele byly o probíhající činnosti, avšak pouze v základní rovině bez podrobností, informovány další dvě osoby vyučující informační a komunikační technologie.

Obě tyto osoby mají taktéž na starost část infrastruktury Alfy. První zajišťuje správu vzdělávacího informačního systému Bakaláři a webu, druhá se podílí na zajišťování sítě po hardwarové stránce. Jejich obeznámenost s probíhající činností byla nutná pro zachování plnohodnotného provozu vzdělávací instituce. Zmíněné osoby však byly poučeny, aby v důsledku této vědomosti nebyli lhostejní vůči probíhající činnosti a při zaznamenání či oznámení bezpečnostního rizika z jakéhokoliv zdroje podnikly opatření dle standardních postupů.

Metody a postupy využité pro realizaci praktické části této diplomové práce jsou nedestruktivní povahy – útoky nepáchají žádnou reálnou újmu uživatelům, systémům, síťovým prvkům a infrastruktuře informačních a komunikačních technologií. Žádný z útoků taktéž úmyslně neshromažďuje data vedoucí ke ztotožnění konkrétního uživatele.

Každý útok je doplněn o teoreticky možné způsobené škody a jejich vliv na vzdělávací instituci, a dále o doporučení k předcházení těmto útokům a možným škodám. Některá doporučení jsou obecnějšího charakteru a lze je tak bezprostředně aplikovat na vzdělávací instituci odlišnou od zde analyzované Alfy,

avšak mohou vyžadovat pro správné plnění funkce drobné korekce dle specificity konkrétní vzdělávací instituce.

Zjištění a doporučení obsažená v této kapitole lze aplikovat nejen na konkrétní vzdělávací instituci, ale taktéž na vzdělávací instituce obecně – dle názoru autora práce se lze důvodně obávat, že útoky cílící na vzdělávací instituci Alfa nejsou v reálném, tedy nesimulovaném a kontrolovaném prostředí, cíleny pouze na jednu vzdělávací instituci, ale jedná se o útoky plošné. Takto cílené specifické druhy útoků, někdy taktéž nazývány jako „*kobercové nálety*“, jsou totiž značně efektivnější, než kdyby byly cíleny pouze na jedinou vzdělávací instituci. S důrazem na tento fakt lze pak stanovená bezpečnostní opatření obecně aplikovat na jakoukoliv vzdělávací instituci a mohou sloužit jako nástroj určený ke vzdělávání uživatelů a metodiků kybernetické bezpečnosti vzdělávacích institucí.

V neposlední řádě bude tato práce použita ke vzdělávání a osvětě všech uživatelů, studentů, pedagogů a dalších pracovníků vzdělávací instituce Alfa s cílem zvýšit povědomí a vzdělanost o bezpečnosti ve spojitosti s kybernetickou bezpečností. Cílem je všechny jednotlivé prvky zabezpečit, zejména vzdělat uživatele takovým způsobem, aby bylo riziko možnosti vzniku škody vinou hrozby sníženo na co nejnižší úroveň.

## 3.1 Prostředí a infrastruktura vzdělávací instituce Alfa

V této kapitole je popsáno prostředí vzdělávací instituce Alfa ve smyslu fyzické koncepce a jsou analyzována potenciální slabá místa infrastruktury. Popsána je síťová infrastruktura bez koncových zařízení, kterým je věnována pozornost v následujících kapitolách.

Před analýzou jednotlivých částí je nutné podotknout, že vstup do budovy je monitorován kamerovým systémem, který však dle vyjádření vzdělávací instituce nemá z důvodů ochrany osobních údajů záznamové zařízení – jedná se pouze přímý přenos, který lze sledovat na monitoru ve vrátnici.

Samotný vstup do Alfy je možný pouze přes vstupní halu, která je opatřena zámky. Klíče k vstupním dveřím mají všichni zaměstnanci vzdělávací instituce. Studenti v ranních hodinách vchází do budovy skrze stejnou halu, ve které je přítomen dozorující pedagog. Hala je odpovědnou osobou uzavřena se začátkem vyučování, tedy v 8:00, a vstup osob bez klíče po této hodině je podmíněn

vpuštěním stále přítomnou osobou ve vrátnici. Odchod z budovy je možný díky klice na vstupních dveřích. Studenti jsou v rámci bezpečnosti poučování o možnosti vniknutí cizí osoby na pozemek vzdělávací instituce Alfa. Pokud zjistí, že se na pozemku školy vyskytuje neznámá osoba, jsou povinni tuto skutečnost neprodleně oznámit zaměstnancům vzdělávací instituce.

## 3.2 Síť vzdělávací instituce Alfa

Vnitřní síť vzdělávací instituce Alfa se skládá z několika navazujících částí. První část zprostředkovává veškerou komunikaci instituce s internetem, skládá se z bezdrátové antény s parabolou umístěnou na střeše instituce, a dále z router switche MikroTik RB2011UiAS-2HnD-IN. Tento aktivní prvek je spravován poskytovatelem internetové konektivity a jeho konfigurace ze strany vzdělávací instituce je tak značně omezena. Dle vyjádření poskytovatele je tak činěno s cílem „*vyloučit bezpečnostní rizika vzniklá vlivem špatné konfigurace ze strany klienta na minimum*“. Přístupný je na základě znalosti MAC adresy zařízení, přihlašovacího jména a hesla.

Druhou a zároveň páteřní částí celé sítě je switch D-Link DGS-1210. Zde již konfigurace podléhá čistě dikci instituce. Páteřní switch propojuje všechny části síťové infrastruktury, které prostřednictvím logických nezávislých síti vzájemně odděluje a zajišťuje jejich správné fungování. Instituci rozděluje na síť pro administrativu, učebny, kabinety a VOIP telefony na základě VLAN.

Třetí část tvoří infrastruktura pro WiFi síť. Páteřním prvkem této sítě je switch Ubiquiti US-24-250W sloužící ke správě přístupových bodů a napájení některých z nich. Dále slouží tento aktivní prvek ke konfiguraci a správě celého rozhraní WiFi sítě.

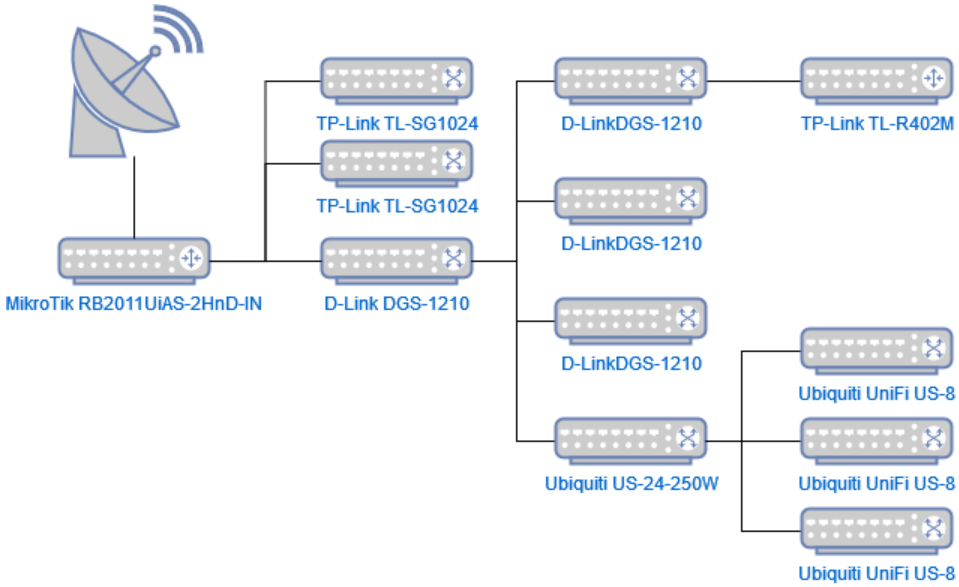
Všechny dosud zmíněné prvky sítě, vyjma antény na střeše budovy, jsou umístěny v serverové rozvodné skříni, která se nachází v technické místnosti. Dveře technické místnosti jsou osazeny zámkem s cylindrickou vložkou, rozvodná skříň pak cylindrickým zámkem. Do místnosti mají přístup pouze vybraní zaměstnanci.

Z páteřního switche se síť dále větví na tři podružné rozvaděče umístěné na chodbách u stropu. Tyto rozvaděče místně seskupují velké množství připojených místností se zařízeními v různých částech budovy instituce. Rozvaděče jsou

osazeny aktivními prvky D-Link DGS-1210, a taktéž Ubiquiti UniFi US-8, které zajišťují propojení a napájení přístupových bodů WiFi sítě. Všechny rozvaděče jsou osazeny cylindrickým zámkem a jsou dostupné pouze ze skládacího žebříku.

Další část sítě tvoří dvě odborné učebny informační a výpočetní techniky (dále jen IVT). V každé z učeben je rozvaděč umístěn, stejně jako v předchozích případech, u stropu učebny a je opatřen cylindrickým zámkem. V jedné z učeben je však cylindrický zámek poškozen a nelze jej uzamknout. Oba rozvaděče jsou osazeny aktivním prvkem TP-Link TL-SG1024. Aktivní prvky nejsou napojeny na páteřní switch, ale přímo do router switche MikroTik. Důvodem, proč nejsou učebny vedeny přes zmiňovaný páteřní switch D-Link je historické hledisko, kdy na provoz sítě vzdělávací instituce stačil pouze router switch MikroTik.

Vzdělávací instituce Alfa provozuje jídelnu, které taktéž poskytuje síťovou infrastrukturu. Vzhledem k nutnosti zajištění funkcionality systému pro správu jídelny je kancelář jídelny vybavena aktivním prvkem v podobě switche D-Link DGS-1210, který je umístěn v kanceláři hospodářky jídelny. Instalaci celého systému jídelny prováděla společnost BARDA SW, HW s.r.o., která oddělení podsítě řešila na základě vytvoření VLAN pomocí routeru TP-Link TL-R402M. Vzhledem k nutnosti oddělení, ale zároveň provázání se zbytkem sítě, zůstal při modernizaci tento aktivní prvek v síťové infrastruktuře a propojuje pouze části nutné k provozu systému jídelny. Obrázek 1 níže znázorňuje schéma sítě Alfy.




*Obrázek 1: Schéma sítě Alfy*

### 3.2.1 Učebny

Vzdělávací instituce Alfa rozděluje učebny na kmenové, odborné a multimediální. Každá z učeben je vybavena datovou zásuvkou, která je zakončena v příslušném rozvaděči. V odborných a multimediálních učebnách se vyjma datových zásuvek nachází také stolní počítač nebo notebook, který pedagogům slouží k propojení se zbylým technickým vybavením třídy. Toto technické vybavení tvoří především projektory, reproduktory a adaptéry bezdrátového monitoru.

Datové zásuvky v kmenových učebnách nejsou momentálně osazeny žádným zařízením. Důvod jejich přítomnosti je dán historickým hlediskem, kdy instituce nebyla pokryta bezdrátovou sítí a jednotlivá zařízení byla připojena právě do těchto zásuvek. Dnes nejsou datové zásuvky prakticky využívány, přesto zůstávají funkční a do určité míry představují bezpečnostní riziko. Lze mít důvodné obavy o možné připojení útočníka právě prostřednictvím těchto zásuvek z vnitřku. Pro předcházení těmto útokům je důležitý zejména dohled nad zmíněnými prostory. Přestože je tato část sítě, tedy kmenové učebny, na základě logické sítě oddělena od ostatních logických sítí, může docházet k šíření škodlivého kódu mezi ostatní uživatele na stejné logické síti. Vzhledem k téměř neustálému dohledu, přítomnosti pracovníků instituce ve zmíněných místech, výslovnému zákazu studentů využívat datové zásuvky a nevyužívání této části sítě zaměstnanci lze považovat toto riziko za méně významné.

Odborné a multimediální učebny představují vyšší míru bezpečnostního rizika, právě z důvodu přítomnosti stále připojeného počítače. Tyto počítače navíc nejsou v drtivé většině žádným způsobem zabezpečeny, tedy k přístupu do nich není třeba žádného přihlašovacího jména nebo hesla. Učiněno je tak z důvodu přístupnosti daného stroje všem vyučujícím bez nutnosti znalosti a zapamatování přístupových údajů.

Jediným, dle zkušeností a informací poskytnutých vzdělávací institucí Alfa dostačujícím, způsobem zabezpečení zmíněných zařízení je fyzické zabezpečení v podobě dveří osazených zámkem s cylindrickou vložkou. Klíči k odborným učebnám disponují osoby, které v daných místnostech vyučují, a ze strany vzdělávací instituce Alfa byli důrazně poučeni, že v místnosti musí být

s jinými osobami vždy přítomni. Přístup do místností mají dále školník a zaměstnanci úklidu.

Zmíněné počítače jsou však využívány i studenty, zejména v situacích, kdy vystupují v rámci výuky před třídou, například prezentují projekty či seminární práce. Zde je nutné počítat s možností, že student při duplikaci obrazovky na projektor, může na obrazovce počítače dělat prakticky cokoliv bez vědomí přítomného pedagoga sledující výstup z druhé strany učebny. Nejpravděpodobnějším útočníkem a pachatelem kybernetické trestné činnosti se na základě těchto dostupných informací stává student vzdělávací instituce Alfa, ale v potaz je třeba vzít taktéž pedagogy, kteří mohou teoreticky tato zařízení a jejich obsah zneužít k vydírání nebo kyberšikaně ostatních pedagogů.

Při pravidelných ročních kontrolách všech zařízení, která se na vzdělávací instituci Alfa nacházejí, byl na minimálně jednom z nich vždy nalezen soubor obsahující data citlivé povahy. Jednalo se o soubory, které obsahovaly data ztotožňující konkrétní osoby, například výsledkové listiny soutěží obsahující jména a data narození. Potenciálně nejnebezpečnějším nalezeným souborem byla tabulka, která obsahovala jména, telefonní čísla, rodná čísla a místa bydliště studentů společně s e-mailovým a telefonním kontaktem na zákonné zástupce.

Výše zmíněné nálezy představují velmi závažné bezpečnostní riziko. Vzhledem k nezabezpečení počítačů se k daným souborům může dostat prakticky kdokoliv, kdo je zrovna přítomen u daného zařízení. Soubory tohoto druhu by pak potenciální útočník mohl využít k vydírání vzdělávací instituce, pronásledování a vydírání osob na základě v souboru uvedených údajů nebo všechna data zveřejnit a poškodit tak soukromí všech osob ze seznamu.

Další problematickou částí učeben zůstává možnost šíření škodlivého kódu po síti, přesněji zevnitř sítě. K datovým zásuvkám v kmenových učebnách se v průběhu přestávek může kterýkoliv student s potřebným hardware vybavením, tedy UTP kabelem, připojit a šířit tak v síti škodlivý kód. Vzhledem k povaze osob, které se v daných místech vyskytují a mohou disponovat znalostmi umožňujícími tento druh útoku provést, se nelze spoléhat na jejich čestnost. Jen pouhá zvědavost či snaha předvést svoje dovednosti před vrstevníky může způsobit vzdělávací instituci nežádoucí problémy či škody.

### 3.2.2 Kabinety

Kabinety slouží pedagogům jako kanceláře pro přípravu výuky, odkládání osobních věcí, vyučovacích pomůcek a další. Důležité je zmínit, že kabinety jsou sdíleným prostorem, každý z kabinetů shromažďuje pedagogy dle jejich zaměření.

Podobně jako v případě odborných učeben jsou kabinety zabezpečeny cylindrickým zámkem a klíči disponují pouze osoby, kterým je kabinet určen, dále školník a pracovníci úklidu. V každém kabinetu je osazena datová zásuvka a umístěn počítač, který mohou pedagogové využívat pro pracovní účely. Nutno podotknout, že počítače jsou využívány i pro účely osobní, jak bylo zjištěno při pravidelných ročních kontrolách.

Počítače v kabinetech se uplatní při řadě nezbytných činností, zmínit lze zejména přípravu materiálů k výuce, správu e-mailové pošty a v době pandemie také k realizaci distanční výuky. Pedagogové Alfy je dále využívají pro přístup ke studijnímu informačnímu systému ve webovém rozhraní, třídní pedagogové pak také k přístupu prostřednictvím RDP protokolu ke vzdálené ploše stejného systému hostovaného na serveru mimo vzdělávací instituci Alfa.[32]

Zmiňovaný přístup ke vzdálené ploše představuje potenciální nebezpečí pro cílový server, v potaz lze vzít zejména útoky, kdy útočník stojí v cestě komunikace mezi uživatelem a cílovým serverem. Tato komunikace v drtivé většině případů využívá port 3389, pro útočníky je tak realizace útoku díky znalosti portu zjednodušena. Dalším způsobem útoku je odcizení přístupových údajů, případně jejich prolomení hrubou silou – zkoušením všech možných kombinací přístupových údajů (tzv. brute force attack).[33]

V případě vzdělávací instituce Alfa je přístup ke vzdálené ploše studijního informačního přístupu zabezpečen uspokojivým způsobem. Komunikační port pro RDP je odlišný od výchozího portu 3389. K autentizaci uživatele při přístupu do vzdálené plochy je vyžadována znalost přihlašovacích údajů a přístup je nakonfigurován pouze pro třídní pedagogy. Samotný přístup do informačního

[32] Zkrácená cesta protokolu RDP služby Azure Virtual Desktop pro spravované sítě. *Microsoft* [online]. Washington, USA: Microsoft, c2022 [cit. 19.2.2022]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/virtual-desktop/shortpath

[33] What are the security risks of RDP? | RDP vulnerabilities. *Cloudflare* [online]. Kalifornie, USA: Cloudflare, c2022 [cit. 19.2.2022]. Dostupné z: https://www.cloudflare.com/learning/access-management/rdp-security-risks/

systému v prostředí vzdálené plochy pak podléhá ověření dalšímu, prostřednictvím odlišných přihlašovacích údajů. Možné riziko zneužití RDP vzniká při uložení přihlašovacích údajů. Alarmující je však zjištění, že některé z počítačů využívající funkce vzdálené plochy v kabinetech Alfy nejsou zabezpečena přístupovým heslem k uživatelskému profilu. Při kompromitaci daného počítače tak vzniká značné riziko navazující kompromitace RDP na základě uložených přihlašovacích údajů.

V kabinetech se dále mohou vyskytovat zařízení připojitelná k síti, která si pedagogové přinesli například z domova. Zejména se jedná o tiskárny, které se na první pohled mohou zdát jako nezajímavý cíl nebo prostředek pro realizaci útoku. Tiskárny, stejně jako řada dalších zařízení, mají vlastní firmware, který zajišťuje správné fungování tiskárny. Firmware v tiskárnách však může být zastaralý a u starších modelů bez podpory ze strany výrobce. Stejně jako například operační systémy může firmware tiskáren obsahovat zranitelnosti, kterých útočníci využívají pro realizaci útoků.[34]

Pro bezpečné pracovní prostředí pedagogů je nutné dbát na bezpečnostní pokyny ze strany vzdělávací instituce. Na sdílených zařízeních by neměly být dlouhodobě přechovávány soubory obsahující citlivá data. Ve vnitřní síti by neměla být užívána zařízení, která představují bezpečností riziko. Jedná se především o osobní zařízení, která nejsou majetkem instituce a mohou úmyslně či neúmyslně obsahovat škodlivý kód, nebezpečné aplikace a zranitelnosti na základě chybějících bezpečnostních záplat. Všechna užívaná zařízení, včetně software, by měla být pravidelně aktualizována, aby byla zajištěna přítomnost bezpečnostních záplat známých zranitelností. V případech, kdy zaměstnanci mají požadavek o umístění vlastního zařízení do prostor kabinetů, je nutné tuto skutečnost konzultovat s osobami odpovědnými za kybernetickou bezpečnost, zejména z důvodu potenciální nebezpečnosti daného zařízení.

[34] WINDER, Davey. Critical HP Printer Security Warning: 150 Models Exposed To Hack Attack. *Forbes* [online]. Jersey City, NJ: Forbes Media, c2022, Dec 4, 2021 [cit. 10.2.2022]. Dostupné z: https://www.forbes.com/sites/daveywinder/2021/12/04/critical-hp-printer-update-warning-150-models-open-to-hack-attack/

### 3.2.3 Zálohovací systém

Vzdělávací instituce má implementovaný systém záloh, který se dělí na dvě hlavní části. Jedná se o offline část a o síťové úložiště. Zálohována jsou však pouze kritická koncová zařízení, která se přímo podílejí na chodu vzdělávací instituce. Přesněji se jedná o celkem pět počítačů z řad administrativy, které jsou využívány pro práci s databázemi a systémy nezbytnými k provozu vzdělávací instituce Alfa.

Offline zálohy se skládají z kopie kořenového adresáře včetně jeho obsahu a bitové kopie. Přítomnost bitové kopie v záloze je kritická pro možnost bezprostředního obnovení zmíněných kritických koncových zařízení a zachování bezproblémového chodu instituce. Offline je prováděna každý měsíc, a to na dva externí disky o kapacitě 1 TB. Díky realizaci zálohy na dva disky zároveň je splněna podmínka redundance – při poškození či nefunkčnosti jednoho z disků lze ze zálohy zmíněná zařízení stále obnovit. Disky jsou uloženy na dostatečně zabezpečeném místě, přesněji se jedná o trezor umístěný v kanceláři administrativy, ke kterému má přístup a klíč pouze hospodářka vzdělávací instituce Alfa. Kompromitace tohoto druhu zálohy by tak vyžadovala extenzivní hrubou sílu v podobě překonání celkem dvou uzamčených prostor a narušení integrity trezoru, což je značně nepravděpodobné. Pro maximalizaci zabezpečení záloh by však bylo vhodné disky šifrovat.[35]

Záloha prostřednictvím síťového úložiště probíhá v oddělené logické síti administrativy. Zařízení, na kterém dochází k ukládání záloh je NAS QNAP TS-231K. Osazeno je dvěma plotnovými disky o kapacitě 2 TB v konfiguraci RAID1 – tedy zrcadlení disků, díky které je stejně jako v případě offline záloh zachována podmínka redundance. Oba disky jsou šifrované, a pokud by došlo k jejich fyzickému odcizení, nebyla by v nich obsažená data čitelná. Síťové úložiště je přístupné pouze z vnitřku sítě, cloudový přístup není povolen, což je pro takto kritickou část IT infrastruktury vzdělávací instituce Alfa velmi podstatné. Přístup koncových zařízení k cílovému adresáři zálohy je možný pouze na základě znalosti ověřovacích údajů z konkrétních zálohovaných zařízení. Po opakovaném

[35] Back up and restore your PC. *Microsoft* [online]. Washington, USA: c2022 [cit. 10.2.2022]. Dostupné z: https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c

neúspěšném použití přihlašovacího hesla se správným uživatelským jménem dojde k zablokování daného profilu, tímto způsobem je síťové úložiště chráněno před útoky hrubou silou. Dalším prvkem zabezpečení je povolené připojování k síťovému úložišti pouze z konkrétních IP adres koncových zařízení. Zabezpečení tohoto systému se jeví jako uspokojivé, avšak vhodné by bylo implementovat metodu ověřování pomocí SSL certifikátů. Tyto certifikáty zajišťují ověřování a šifrovanou komunikaci mezi zařízeními, v případě tohoto systému zálohování mezi síťovým úložištěm a počítačem. Fyzickému odcizení je předcházeno umístěním v uzamčené technické místnosti.[36]

### 3.2.4 Jídelna

Infrastruktura jídelny tvoří důležitou část vzdělávací instituce. Zajišťuje stravování pro více jak 600 osob a využívána je i sousední vzdělávací institucí. Její funkcionalita je závislá na provozování výdejního systému, který se skládá z několika částí. První částí je server, na kterém je provozován výdejní systém. Server je spouštěn pouze před zahájením výdeje stravování, a po ukončení stravování je opět vypnut. S výdejním systémem je také vázána webová aplikace, ve které si mohou uživatelé volit obědy. Tuto aplikaci poskytuje BARDA SW, HW s.r.o., která taktéž instalovala celý systém.

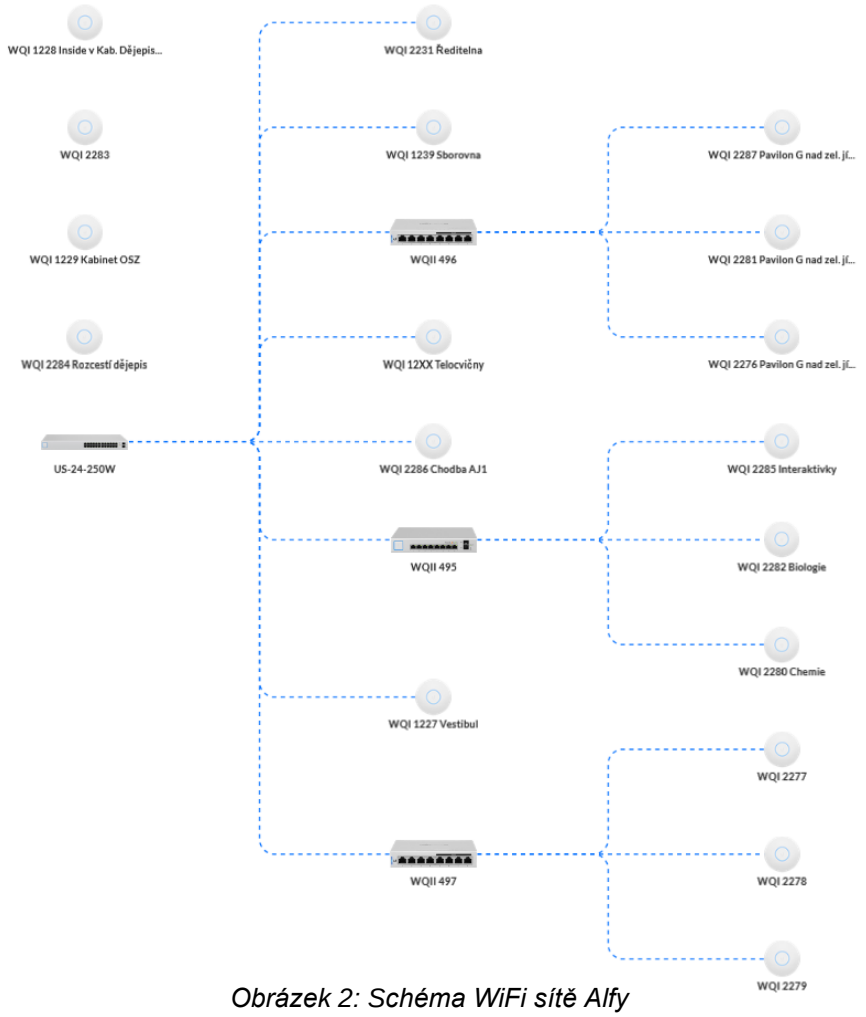
Tento systém se skládá z celkem pěti zařízení – dvou výdejních terminálů v podobě AIO počítačů, serveru s výdejním systémem zároveň sloužící pro práci s výdejním systémem, počítače kanceláře kuchyně a objednávkového počítače. Všechny zmíněné prvky jsou v oddělené logické síti, která je využívána pouze těmito zařízeními.

Server s výdejním systémem a počítač kanceláře kuchyně jsou fyzicky zabezpečeny v místnostech, kam mají přístup pouze oprávněné osoby a přihlášení k jejich uživatelským účtům je možné pouze na základě znalosti přístupových údajů.

[36] What is an SSL Certificate ?. *DigiCert* [online]. Lehi, Utah: DigiCert, c2022 [cit. 10.2.2022]. Dostupné z: https://www.digicert.com/what-is-an-ssl-certificate

### 3.2.5 WiFi

WiFi síť je ve vzdělávací instituci tvořena celkem dvaadvaceti aktivními prvky, z čehož je osmnáct přístupových bodů, tři podružné a jeden páteřní switch. Jejím účelem je poskytovat studentům a pracovníkům vzdělávací instituce přístup na internet ze všech částí budovy. Přístupové body vysílají SSID sítě, ke které se mohu připojovat jak studenti, tak pedagogové. Zabezpečena je pomocí WPA2 a v blízké budoucnosti je plánován přechod na bezpečnější verzi WPA3. Vyjma zabezpečení přístupu do sítě a komunikace umožňuje tato technologie volný pohyb uživatelů mezi přístupovými body bez nutnosti opětovného ověřování. Přístupové heslo je studentům sdělováno pedagogy s apelem na nesdílení hesla s uživateli mimo vzdělávací instituci. Schéma WiFi sítě Alfy je znázorněno na obrázku 2 níže.[37]




*Obrázek 2: Schéma WiFi sítě Alfy*

[37] Jaký je rozdíl mezi WPA2, WPA3, WPA, WEP, AES a TKIP?. *AIRWAYNET* [online]. Praha: AIRWAYNET, c2022 [cit. 12.2.2022]. Dostupné z: https://www.airwaynet.cz/jaky-je-rozdil-mezi-wpa2-wpa3-wpa-wep-aes-a-tkip/

V prostředí sítě jsou na základě příznaků rozlišována zařízení spadající pod správu vzdělávací instituce od ostatních zařízení. Tento postup umožňuje na základě logické sítě oddělit zařízení instituce od zbylých, kterým je vyhrazena separátní logická síť. Příznaky jsou přiřazovány správcem na konfigurovatelném aktivním prvku Ubiquiti US-24-250W. Využity mohou být nejen pro rozlišení příslušnosti uživatelů ke správné logické síti, ale také ke stanovení uživatelských profilů uvnitř sítě. Pomocí profilů pak lze dále stanovit práva zařízení, omezení rychlosti či omezení přístupu. Každé zařízení je možné samostatně monitorovat, mezi hlavní sbírané metriky patří UP a DOWN link, datový tok za posledních 24 hodin a aktuální připojení ke konkrétnímu přístupovému bodu.

Koncová zařízení, tedy přístupové body, jsou umístěny viditelně ve stropním podhledu. Pokrytí bylo na vzdělávací instituci rozšiřováno postupně. Při prvním zřízení WiFi infrastruktury byly pořízeny celkem čtyři přístupové body Ubiquiti UniFi UAP, a čtyři přístupové body Ubiquiti UniFi UAP-LR. Těchto osm přístupových bodů bylo rozmístěno do jednotlivých koridorů vzdělávací instituce, nicméně pokrytí a síla signálu byla v mnoha místech vzdělávací instituce nedostačující či neexistující. V další vlně rozšiřování infrastruktury WiFi sítě byla pořízena aktualizovaná verze přístupových bodů Ubiquiti UniFi UAP-AC-LR v počtu 10 kusů. Aktuálně je provozováno celkem 18 přístupových bodů, které zajišťují více jak 90% pokrytí území vzdělávací instituce WiFi sítí.

Zmíněné přístupové body již nejsou ze strany výrobce od 1. března 2021 podporovány. Nedostávají tak aktualizace firmware, bezpečnostní záplaty, opravy kritických chyb a nelze je z nového konfiguračního software konfigurovat. Absence možnosti konfigurace je překážkou při nutnosti aplikace změn v prostředí WiFi sítě instituce. Z bezpečnostního hlediska představují riziko chybějící bezpečnostní záplaty a opravy chyb. Výrobce po dobu životnosti produktu poskytuje všem uživatelům produktů pravidelné záplaty zajišťující bezpečnost zařízení. Tyto přístupové body by bylo vhodné vyměnit za novější, které budou ze strany výrobce podporovány a budou dostávat aktualizace včetně bezpečnostních záplat.[38]

[38] Select UniFi Access Point (AP) Models Obsoletion Date: March 1, 2021. *Ubiquiti* [online]. New York: Ubiquiti, c2022, March 1, 2019 [cit. 13.2.2022]. Dostupné z: https://community.ui.com/questions/Select-UniFi-Access-Point-AP-Models-Obsoletion-Date-March-1-2021/65487283-ce9d-49f4-85b9-b6aa54659ef7

Infrastruktura WiFi sítě Alfy je značně komplexní, což lze považovat za určité riziko. Z hlediska správy lze systém hodnotit pozitivně, samotná zařízení by však mohla být více sjednocena. Myšlena je tím hromadná aktualizace všech dosavadních, již zastaralých, zařízení za nová. Narážíme zde však na problém z hlediska financí a tvorby rozpočtu, kterému se musí správci při výběru jednotlivých komponent infrastruktury podřídit. Komplexnost celé sítě také poskytuje vyšší prostor pro chybovost ze strany uživatele. Konfigurační systém je však uživatelsky velmi přívětivý, umožňuje totiž nastavit jedno koncové zařízení dle požadavku správce a všechna další připojená zařízení pak konfiguraci automaticky nahrají z prvního nastaveného. Problém přichází v situaci, kdy je součástí infrastruktury nepodporované koncové zařízení, ta jsou konfigurovatelná pouze pomocí starších verzí konfiguračního systému. Pozitivně lze hodnotit přístup ke konfiguračnímu systému. Ten je umožněn pouze autorizovaným zařízením a uživatelům při přímém hardwarovém spojení. Cloudový přístup ke konfiguračnímu systému je možný, ale opět pouze na základě znalosti přihlašovacích údajů, předchozí autorizace v systému při fyzické přítomnosti zařízení ve stejné síti.

## 3.3 Doména vzdělávací instituce Alfa

Vzdělávací instituce Alfa, jako dnes prakticky každá, má vlastní doménu. Tato doména slouží jak pro potřeby zaměstnanců, tak pro potřeby studentů. Z dostupných informací o DNS záznamech domény je pak možné dále zjistit, že obsahuje položku odkazující na e-mailový server stable.cz *(který mění v blízké době název na Webglobe),* a dále položku odkazující na e-mailový server google.com. Z dalších dostupných informací, zejména návodu a informací zveřejněných na webových stránkách instituce lze uvést, že k práci a spojení mezi pedagogickým sborem, a zároveň studenty, je užíváno vzdělávací prostředí G Suite vytvořené společností Google.

Tato samotná informace uvedená na webových stránkách může být potenciálně nebezpečná, vezmeme-li v potaz, že útočník je díky znalosti prostředí užívaného vzdělávací institucí schopen zkonstruovat věrohodný phishingový útok a přesně jej cílit. Samotnému přesnému zacílení pak dopomáhají veřejně dostupná e-mailová spojení na téměř všechny zaměstnance instituce Alfa. Ta jsou

zveřejněna včetně jmen, příjmení a titulů, útočník si tak může vybrat prakticky jakoukoliv identitu a tu využít k útoku.

Dle názoru autora by bylo vhodné zveřejňovat na webových stránkách Alfy pouze nutné informace na základě zákona. Zveřejněné kontakty na prakticky všechny zaměstnance instituce jsou, zejména pro rodiče studentů, jistým zjednodušením ve vztahu k e-mailové korespondenci, nicméně se stávají prostředkem k realizaci výše zmíněného scénáře útoku.[39]

Vhodným a nutno podotknout i mnohem bezpečnějším způsobem je zpřístupňování databáze či adresáře kontaktních údajů pouze osobám, které mají oprávněný zájem na získání kontaktu na konkrétní zaměstnance, kteří nejsou součástí vedení nebo kontaktní osobou vzdělávací instituce. Adresář kontaktních údajů je v rámci instituce zřízen na doménové úrovni v prostředí Google. Každý ze studentů a zaměstnanců má v tomto prostředí k dispozici adresář s kontakty. Ten je tak možné zobrazit pouze po přihlášení k doméně pomocí správcem vydaných přihlašovacích údajů k zřízenému uživatelskému účtu. Nedochází tak ke zveřejnění kontaktních údajů na místech přístupných všem osobám, zejména pak těm, které mohou mít nekalé úmysly s těmito údaji.

Dalším možným řešením je korespondence prostřednictvím informačního vzdělávacího systému Bakaláři, který je hojně využíván vzdělávacími institucemi na úrovni základních a středních škol. Dle zveřejněných dat využívá tento informační systém přes 60 % všech škol na území ČR. Tento systém slouží především pro koordinaci výuky a poskytování informací studentům, zákonným zástupcům a zaměstnancům instituce. Mezi tyto informace patří rozvrhy žáků a pedagogů, suplování, plánované akce, docházka a klasifikace. Uživatelské účty v tomto informačním systému jsou zřizovány pouze osobám, které jsou oficiálně součástí vzdělávací instituce a ve chvíli, kdy tento stav pomine, jsou uživatelské účty zrušeny. V prostředí informačního systému Bakaláři je možnost využití funkce Komens, která umožňuje zasílat zprávy mezi uživateli systému. Přijaté a odeslané zprávy jsou díky uživatelskému účtu vydanému správcem systému dostatečně věrohodné a lze předpokládat, že nedošlo k přijetí zprávy podvodné.[40]

[39] Zákon č. 106/1999 Sb., *Zákon o svobodném přístupu k informacím* ve znění k 15.2.2022

[40] Bakaláři. [Online]. Příbram: BAKALÁŘI software, c2022 [cit. 15.2.2022]. Dostupné z: https://bakalari.cz/

## 3.4 Segmenty vzdělávací instituce Alfa

Vzdělávací instituce Alfa byla rozdělena na segmenty, které se od sebe liší zejména tím, že kromě odlišné vnitřní funkce se každý z nich typicky dostává do kontaktu s jiným druhem kybernetické hrozby. Lze se pak důvodně domnívat, že každý ze segmentů bude pro řešení a předcházení hrozbám aplikovat různé přístupy a opatření s cílem zamezit vzniku škod v důsledku kybernetické hrozby.

Obecně lze aplikovat řadu pravidel pro všechny segmenty hromadně, nicméně v dílčích částech se od sebe budou lišit. Tyto odlišnosti je třeba dostatečně zdůraznit jednotlivým segmentům, kterých se nejvíce dotýkají. Přesto by měly všechny segmenty mít znalost ve všech částech, nejen těch důležitých pro ně samotné, aby byly schopny zamezit šíření hrozby do exponovaného segmentu v důsledku neznalosti hrozby. Příkladem šíření může být e-mail obsahující škodlivý kód, který je nepřímo určen pro segment administrativy. Doručen je pedagogovi, avšak jeho obsah žádá o přeposlání odpovědnému administrativnímu uživateli. Neznalost pedagoga tak může vést k velmi snadnému přesunu hrozby na požadované místo a administrativní pracovník může e-mail odeslaný pedagogem uvnitř domény vzdělávací instituce vyhodnotit jako zcela důvěryhodný.

### 3.4.1 Administrativa

Prvním, a zároveň stěžejním segmentem je administrativa. Úlohou tohoto segmentu je zejména správa dílčích databází, například databáze studentů či spravovaného majetku. Příznačný pro tento segment je pak fakt, že řada dat, se kterými pracuje, jsou data diskrétní povahy. Tato data jsou dále shromažďována v databázích, což z nich dále může činit data citlivé povahy.[41]

Administrativu Vzdělávací instituce lze podle povahy pracovní činnosti dále rozdělit na činnost řídící a rozhodovací, ekonomickou a asistenční. Je třeba podotknout, že pracovní činnosti administrativního segmentu se v prostředí informačních a komunikačních technologií často úzce prolínají, ať už z důvodu nutné spolupráce jednotlivých pracovníků na konkrétních pozicích, nebo také z důvodů znalostních – často je pracovník nucen učinit úkon, který před samotnou

[41] Kategorizace dat. *Univerzita Karlova* [online]. Praha: Univerzita Karlova, c2022, 2. říjen 2020 [cit. 15.2.2022]. Dostupné z: https://openscience.cuni.cz/OSCI-95.html

realizací raději konzultuje s jiným pracovníkem administrativy. Zde lze namítat uplatnění zásady „*need-to-know*“, avšak z jistých procesně provozních důvodů je tato zásada často zanedbávána. Omluvou ze strany administrativy je odkazování na komplikovanost a nutnost spolupráce jednotlivých pracovníků v daných oblastech s cílem zvýšit efektivitu a snížit chybovost. Toto je však činěno na úkor bezpečnosti v oblasti informačních a komunikačních technologií.[42]

Samotná IT infrastruktura administrativy je z pohledu uživatele provázána především na cloudové úrovni, případně prostřednictvím e-mailové korespondence. K dispozici je každému pracovníkovi z řad administrativy cloudové úložiště, přesněji Google Drive. Toto úložiště pak každý pracovník může využívat způsobem, který uzná vhodným a především dostatečně bezpečným. Na úložiště tohoto typu by se v žádném případě neměla dostat data diskrétní povahy a data citlivá, ať už by se mělo jednat o osobní údaje, interní informace či přístupové údaje.

Využívání cloudového řešení přináší určitá bezpečnostní rizika, zvláště ta spojená s možným únikem dat a informací. Cloudové úložiště je uživatelům přístupné i mimo fyzickou lokaci vzdělávací instituce Alfa a pouze na základě znalosti přístupových údajů, tedy přihlašovacího jména a hesla. Každý z uživatelů má možnost se samostatně rozhodnout, zda bude při přihlašování k účtu poskytující cloudové úložiště používat dvoufázové ověřování. Při přihlašování s aktivním dvoufázovým ověřováním musí uživatel kromě znalosti hesla poskytnout další faktor k ověření totožnosti. Dalšími faktory mohou být například elektronický token z mobilní aplikace, SMS zpráva s kódem, snímek obličeje, otisk prstu, fyzický ověřovací klíč nebo klíč odeslaný na e-mail. Užití dvoufázového ověřování je důrazně doporučeno, zejména proto, že při případném úniku přihlašovacích údajů nemusí nutně dojít ke kompromitaci daného účtu.[43]

Z pohledu hardware zabezpečení nelze jednoznačně stanovit, zda jsou dodržována všechna bezpečnostní pravidla k předcházení bezpečnostním

[42] Security: The Need-to-know principle. *Microsoft* [online]. Washington, USA: Microsoft, c2022, Feb 03 2021 [cit. 15.2.2022]. Dostupné z: https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393

[43] How Does Two-Factor Authentication (2FA) Work?. *Merchant Fraud Journal* [online]. Concord, Ontario: Merchant Fraud Journal, c2022, January 16, 2020 [cit. 17.2.2022]. Dostupné z: https://www.merchantfraudjournal.com/two-factor-authentication-work/

incidentům. Pracovníci administrativy mají možnost přistupovat k úložišti, e-mailu a k systému Bakaláři, jakožto i ke vzdálené ploše serveru Bakaláři, z jakéhokoliv zařízení na základě znalosti přihlašovacích údajů, popřípadě dalších údajů nutných pro ověření. Instituce Alfa však nemá kontrolu nad tím, z jakého zařízení uživatelé ke zmíněným službám přistupují, přesněji řečeno nemohou přímo ovlivnit dostatečné zabezpečení přístupu.

V potaz přichází použití VPN, fyzického tokenu nebo vynucení dvoufázového ověřování. Všechny tyto prvky mohou sloužit jako další nástavba zabezpečení. V případě VPN, kdy dochází k šifrování komunikace mezi uživatelem a cílovým systémem, by byla zajištěna šifrovaná komunikace a předcházeno možnému zachycování síťového provozu. Fyzický token lze užívat k ověřování identity uživatele při přihlašování k řadě služeb, vydávaný a kontrolovaný by byl vzdělávací institucí. Implementace vynuceného dvoufázového ověřování představuje další efektivní a uživatelsky přívětivou vrstvu zabezpečení, například v podobě aplikací poskytující autentizaci uživatele na základě náhodně generovaného číselného kódu s platností maximálně několik minut.

### 3.4.2 Pedagogický sbor

Pedagogický sbor tvoří méně než 10 % všech uživatelů vzdělávací instituce, a přesto je skupinou, která je značným potenciálním bezpečnostním rizikem. Znalosti a přístup ke kybernetické bezpečnosti se v řadách sboru značně liší. Na základě pravidelné kontroly všech zařízení ve vlastnictví vzdělávací instituce bylo zjištěno, že zhruba polovina všech uživatelů na kybernetickou bezpečnost nedbá dostatečným způsobem. Projevy tohoto jevu lze vnímat například na nejběžnějším způsobu zabezpečení počítače – ochrana uživatelského účtu uzamčením.

Každý z pedagogů je při nástupu do zaměstnání vybaven notebookem Microsoft Surface Laptop Go, který je primárně určen k vykonávání pedagogické činnosti, může však být využíván také k osobním potřebám pedagogů. Při předávání zařízení pedagogům je důrazně doporučováno, aby zařízení využívali obezřetně a zabezpečili jej proti možné ztrátě dat při fyzickém odcizení nebo ztrátě. Zhruba polovina uživatelů však těchto doporučení nedbá a z důvodu pohodlnosti nemá nastavené žádné zabezpečení přístupu k uživatelskému účtu. Zbylí pedagogové bezpečnostní doporučení plní, k přihlašování k uživatelskému

účtu využívají silná hesla, případně biometrické údaje ve formě otisku prstu a snímku tváře. Nevyužíváním žádné formy zabezpečení uživatelského účtu uživatel značně zvyšuje riziko možné kompromitace zařízení a dat na něm obsažených.

Aktualizace probíhají automaticky, tato funkce byla při prvotním nastavení všech těchto zařízení nastavena správcem. Uživatelé si pak mohou zvolit čas, ve kterém budou pravidelné aktualizace probíhat. Aktualizace software je výlučně na uživatelích, kterým však bylo v rámci proškolení zdůrazněno, aby všechny součásti systému včetně aplikací a software udržovali aktuální.

Vyjma výše uvedených bezpečnostních rizik se tato zařízení potýkají s hrozbou ve formě sdílení zařízení v osobním užití. Někteří z pedagogů zařízení sdílejí například s rodinnými příslušníky. Nutno podotknout, že se jedná o jednotky uživatelů, nelze však toto riziko považovat za nepodstatné. Sdílení pracovního notebooku, který může obsahovat citlivá data, přístup do databází a systémů vzdělávací instituce je kritickým rizikem a z těchto důvodů by nemělo být sdíleno s jinými uživateli. Pokud existuje nutnost zařízení sdílet, mělo by být sdíleno pouze se zabezpečeným primárním, pracovním uživatelským profilem. Následně by měl být vytvořen uživatelský profil hosta, který bude mít omezená práva a odepřen přístup ke všem částem uživatelského profilu pracovního.

Ve spojitosti s pedagogickým sborem se objevuje také riziko ve formě phishingu. Vzdělávací instituce Alfa za účelem komunikace zveřejňuje na svých stránkách e-mailové spojení na pedagogický sbor v celém rozsahu. Pro útočníky je tak velmi jednoduché získat kontakty, včetně informací o poli působnosti daného pedagoga. Phishing tak může být cílen přesně na konkrétní osoby, hovořit lze v této souvislosti o spear-phishingu. Důležité je poznamenat, že e-mailové schránky pedagogů nejsou vázány na konkrétní zařízení. Mohou k nim tedy přistupovat z libovolného zařízení a umístění, pouze na základě znalosti přístupových údajů. K otevření podvodného odkazu obsaženého ve phishingovém e-mailu tak může dojít na řadě zařízení, například na pracovním notebooku, vlastním soukromém stolním počítači, na mobilním telefonu nebo na počítači v kabinetu. Důsledky se budou přímo odvíjet od druhu obsaženého škodlivého kódu, avšak následky a způsobené škody budou závislé na místě a zařízení, ve

kterém došlo k prvotnímu spuštění. Škody tak mohou vznikat jak v domácí síti uživatelů, tak v síti vzdělávací instituce.[44]

### 3.4.3 Studenti a zákonní zástupci

Jak je uvedeno v předešlých částech práce, studenti tvoří nejpočetnější skupinu uživatelů vzdělávací instituce. Činnost studentů je v přímé souvislosti s činností jejich zákonných zástupců. Aktivity lze rozdělit na dvě části, přičemž nedochází k jejich oddělení. Obě níže zmíněné části se vzájemně prolínají a mají přímou návaznost na bezpečnostní rizika plynoucí z povahy těchto uživatelů.

První částí je aktivita mimo vzdělávací instituci. Lze sem zařadit běžně prováděné činnosti na počítači, prohlížení internetu, příjem a zasílání e-mailové korespondence, využívání software a aplikací, hraní počítačových her apod. Prováděny jsou na osobních zařízeních. Při těchto činnostech však mohou uživatelé narazit na celou řadu bezpečnostních hrozeb, malware, phishing, či na počítačové viry. Tyto hrozby mohou být odhaleny a zneškodněny antivirovým software, ale také se mohou na počítačích vyskytovat jako součást software bez vědomí uživatele. Zvláštní pozornost je třeba věnovat souborům .PDF, .DOCX a .XLSX, které jsou velmi běžně využívanými formáty. Útočníci jsou do těchto druhů souborů schopni schovat řadu skriptů, které po otevření souboru stáhnou z internetu malware, a následně jím infikují dané zařízení. Některé hrozby jsou velmi snadno odhalitelné a budou zablokovány běžným antivirovým programem, jiné se dokáží úspěšně skrýt, zůstat na infikovaném zařízení bez povšimnutí uživatele a dále se šířit. Rizikem je propojenost kyberprostředí osobního a vzdělávacího. Obě tato prostředí mohou navzájem mezi sebou šířit hrozby.[45]

Studenti využívají k výuce a komunikaci v prostředí vzdělávací instituce Alfa systém Bakaláři a doménový e-mail. Tyto služby umožňují zasílání příloh ve formě souborů s omezenou velikostí a nemožností zasílat spustitelné soubory s příponou .EXE. Součástí komunikace jsou však často také zákonní zástupci studentů, kteří disponují vlastním účtem ve službě bakaláři, ale k e-mailové

[44] Phishing/Spear phishing. *ENISA* [online]. European Network and Information Security Agency, c2005-2022 [cit. 17.2.2022]. Dostupné z: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

[45] TANNER, Jonathan. Threat Spotlight: Document-Based Malware. *Barracuda* [online]. Campbell, California: Barracuda Networks, c2022, April 4, 2019 [cit. 17.2.2022]. Dostupné z: https://blog.barracuda.com/2019/04/04/threat-spotlight-document-based-malware/

korespondenci využívají vlastní nebo pracovní schránky. Vezmeme-li všechny možné cesty, po kterých lze vést komunikaci, dostáváme vcelku komplexní komunikační model. Autor práce si dovoluje poznamenat, že z hlediska uživatelské přívětivosti a přehlednosti by se jevilo jako nejvhodnější řešení zvolit jednotný kanál komunikace mezi všemi zúčastněnými subjekty. Taktéž si ale uvědomuje, že uživatelský pohled se na danou problematiku liší, rozliční uživatelé mohou považovat za vhodný komunikační kanál jakýkoliv z dostupných. Nicméně je třeba konstatovat, že nejednoznačnost v komunikačních systémech vytváří prostor pro bezpečnostní hrozby. Na uživatele je kladen zvýšený nárok na pozornost při práci se všemi komunikačními kanály. Frustrace způsobená nejednotností využívaných komunikačních kanálů tak může vést k absenci obezřetnosti a následnému průniku bezpečnostní hrozby.

Druhou částí je aktivita uvnitř vzdělávací instituce, která je vázána zejména na využívání sítě a internetu k potřebám vzdělávání. Mezi tyto činnosti lze zařadit vyhledávání informací, sdílení materiálů, využívání cloudového úložiště, práce na sdílených počítačích v učebnách informační a výpočetní techniky, využívání WiFi sítě, účast na distanční výuce a e-mailová korespondence. Studenti využívají nejen v hodinách informační a výpočetní techniky cloudové úložiště a vlastní datové nosiče. Obsah cloudového úložiště je přímo monitorován ze strany poskytovatele, ale i přes tuto skutečnost lze skrze toto úložiště šířit škodlivý kód a soubory. Při přístupu, stažení a otevření infikovaného souboru uvnitř sítě instituce pak může docházet k jeho šíření mezi ostatní zařízení.

Vlastní datové nosiče studentů mohou obsahovat, vědomě či nevědomě, infikované soubory. Při práci v hodinách, například prezentování projektů, využívají studenti soubory uložené právě na tyto nosiče. Když student připojí daný nosič k počítači v některé z odborných učeben, dojde ke spuštění škodlivého kódu uvnitř souboru na datovém nosiči, který může následně zašifrovat celý obsah pevného disku, odstranit soubory, odeslat data útočníkovi, nebo také infikovat ostatní zařízení na síti.

Bezpečnost této skupiny uživatelů je z velké části mimo působnost vzdělávací instituce. Lze mít za to, že dostatečné vzdělání a osvěta v problematice kybernetické bezpečnosti se promítne do zodpovědného chování uživatele v prostředí kyberprostoru. Nelze však těmto uživatelům přímo zasahovat do

vlastních činností. Ze strany vzdělávací instituce tak dochází k šíření povědomí existenci kybernetických hrozeb a bezpečnostních rizik. Taktéž jsou stanovena konkrétní opatření. Těmito opatřeními je myšleno zejména vynucený požadavek silného ověřování uživatele při přístupu k doménovému účtu instituce, vyzdvihnutí nutnosti chovat se obezřetně, kriticky přemýšlet nad přijímaným a zasílaným obsahem a taktéž nutnosti uchovávat přístupové údaje na bezpečných místech.

Osobní a přístupové údaje skupiny studentů a jejich zákonných zástupců podléhají zvláštní pozornosti při zacházení. Neměly by být za žádných okolností sdíleny s někým dalším. Vzdělávací instituce nemůže být odpovědná za únik těchto údajů vinou studenta nebo jeho zákonného zástupce v souvislosti s nedodržováním bezpečnostních doporučení a zásad. V takovém případě se na instituci lze samozřejmě neprodleně obrátit a požádat o zrušení daných účtů a služeb, případně požádat o vydání nových přístupových údajů. V případě zapomenutí přístupových údajů je lze přes samoobslužné funkce obou služeb získat zpět.

### 3.4.4 Jídelna

Segment jídelny je zvláštní skupinou, která se vyznačuje velmi nízkým počtem uživatelů. Přesněji se jedná o dva hlavní uživatele, přičemž zbylí uživatelé mají na starosti pouze zapnutí výdejních zařízení, která jsou pro zajištění fungování systému výdeje stravování nutná. Provoz systému je následně zcela automatický. Pozornost kybernetické bezpečnosti v tomto segmentu je nutné věnovat uživateli, který vykonává pracovní činnost na stejném zařízení, jehož součástí je také server a software výdejního systému.

Součástí tohoto serveru je databáze s údaji studentů, pedagogů a ostatních zaměstnanců, kteří se účastní stravování. Stejné zařízení slouží k zasílání a čtení e-mailové korespondence spojené s provozem jídelny, vystavování čipových karet a editaci uživatelských záznamů v databázi. Tato databáze se může stát cílem útoku. Společnost poskytující systém, Barda SW, HW s.r.o. na svých stránkách pravidelně zveřejňuje možná bezpečnostní rizika spojená s výdejním systémem, které zároveň uživatelům zasílá e-mailem. V případě infekce malware tohoto zařízení může dojít ke ztrátě a krádeži dat nebo zašifrování disku serveru. Tento

útok by prakticky znemožnil provoz výdejního systému a tím pádem i celé jídelny. Tato rizika je nutné vnímat jako velmi závažná, proto jsou uživatelé vykonávající pracovní činnost na serveru důsledně obeznámeni s bezpečnostními riziky a možnými následky. V historii vzdělávací instituce Alfa nebyl doposud zaznamenán žádný útok cílený na provoz nebo součást výdejního systému. I přes tuto skutečnost je třeba přistupovat k práci s databází, systémem a všemi ostatními aplikacemi a software obezřetně. Vhodná je taktéž pravidelná kontrola integrity tohoto zařízení a aktualizace veškerého software včetně operačního systému.[46]

Druhým zařízením je počítač užívaný ke vzdálenému přístupu na server výdejního systému a k administrativní činnosti spojené s provozem jídelny. Administrativní činnost zahrnuje vzdálené ovládání výdejního systému, vyřizování objednávek surovin, přístup k internetovému bankovnictví včetně plateb a vyřizování e-mailové korespondence. Odpovědná osoba tak pracuje s několika systémy a aplikacemi, jejichž kompromitace může mít značné následky. Při práci s internetovým bankovnictvím je bezpečnost uživatelského účtu u bankovní instituce zajišťována silným ověřováním uživatele. Pro přístup nebo uskutečnění plateb je tak nutný vyjma přihlašovacích údajů další prvek zabezpečení, například otisk prstu a také potvrzení platby v ověřovací aplikaci.

Při plnění objednávek surovin a dalších potřeb pro zajištění stravování, lze předpokládat možnost podvodné objednávky na základě sociálního inženýrství, phishingu či podvodného webu. Využitím těchto technik se mohou útočníci vydávat za legitimní společnost či subjekt. Následně je uskutečněna objednávka a poukázání odpovídající částky na účet útočníka. Objednávka však nedorazí, finanční prostředky budou odcizeny a bezpochyby bude výpadkem dodávky surovin způsoben chaos a nepříjemnosti spojené s výdejem stravování. Objednávky by měly být uskutečňovány pouze z ověřených zdrojů. Využívány by měly být prověřené a důvěryhodné zdroje, u kterých existuje zkušenost s plněním předchozích objednávek a odpovědná osoba má jistotu, že poukázané finanční

[46] AKTUALITY - řazeno chronologicky. *BARDA SW, HW s.r.o.* [online]. Ohrobec: BARDA SW, HW [cit. 18.2.2022]. Dostupné z: https://www.barda.cz/

prostředky směřují na skutečný účet daného subjektu. Řada z nich veřejně dává k dispozici číslo účtu, což může sloužit jako faktor ověření pravosti účtu.

Bezpečnostní rizika v tomto segmentu nejsou ovlivněna žádným dalším zařízením vyjma pracovního mobilního telefonu osoby odpovědné za administrativní činnost spojenou s objednáváním a platbou. Toto zařízení by mělo být pravidelně aktualizováno s cílem zajistit všechny bezpečnostní záplaty na mobilní operační systém. Dalším doporučením je využívat co možná nejnovější verze mobilních operačních systémů, které jsou stále podporovány ze strany výrobce. Vydavatelé aplikací, zejména bankovní instituce, však tento problém často řeší znepřístupněním aplikace pro uživatele, kteří disponují mobilním zařízením se zastaralým operačním systémem. Uživatel je tak nucen přejít na bezpečnější, novější zařízení a operační systém.[47]

[47] Android Security Bulletins. *Android Open Source Project* [online]. Mountain View, CA, USA: Google [cit. 18.2.2022]. Dostupné z: https://source.android.com/security/bulletin/

# 4. Testování kybernetické bezpečnosti Alfy

Tato kapitola se zabývá praktickým využitím kybernetických útoků pro účely testování a stanovení úrovně kybernetické bezpečnosti vzdělávací instituce. Všechny výsledky budou dále využity ke zvýšení zabezpečení vzdělávací instituce na poli kybernetické bezpečnosti, jakožto i ke vzdělávání a osvětě uživatelů konkrétní vzdělávací instituce. Reálné příklady s konkrétními dostupnými daty mají dle názoru autora značně vyšší míru účinnosti vzdělávání na dotčené uživatele než čistě teoretická výuka bez nich.

Zvoleny byly takové typy útoků, které mohou být nejběžněji použity proti vzdělávací instituci. Před samotným provedením útoků byla provedena analýza všech částí systému a stanovení kritických míst, u kterých lze mít za to, že jsou potenciálním vektorem útoku. Útoky jsou realizovány nedestruktivním způsobem – nedochází k narušení integrity dat a po skončení útoku lze všechny dotčené systémy a zařízení nadále plnohodnotně využívat.

Níže je popsána příprava, postup, realizace, hrozby, následky a doporučení na ochranu před útoky ve formě podvodného přístupového bodu, phishingu, DoS a sociálního inženýrství.

## 4.1 Podvodný přístupový bod

Cílem tohoto útoku bylo stanovit, zda uživatelé budou přistupovat k nezabezpečenému přístupovému bodu vysílajícímu podezřelé SSID a také, jestli dojde k jeho fyzickému odhalení. Dále bylo zjišťováno, zda ze strany některé ze skupin uživatelů dojde k ohlášení podezřelého výskytu nezabezpečené WiFi sítě na území vzdělávací instituce.

Příprava útoku prostřednictvím podvodného přístupového bodu vyžaduje v řadě případů fyzický přístup k místu, kde má být útok realizován. V této fázi je útočníkem proveden průzkum oblasti, především vytipování míst vhodných pro umístění potřebného HW. Příprava dále vyžadovala aktivní prvek ve formě přístupového bodu nebo routeru, ke kterému se následně uživatelé připojí. Při volbě HW byly vybírány takové prvky, které je možné ukrýt, a zároveň nevzbuzují příliš mnoho nežádoucí pozornosti. Vzdělávací instituce využívá pro zajištění pokrytí WiFi prvky od výrobce Ubiquiti, z těchto důvodů byl zvolen přístupový bod

Ubiquiti UniFi AP. To umožňuje umístit přístupový bod prakticky kdekoliv v budově, aniž by jeho případné odhalení budilo větší pozornost.[48]

Dalším krokem bylo vytvoření názvu SSID podvodného bodu. Vzdělávací instituce je pokryta legitimním SSID s názvem „WiFi Gymnázium 2.0“. Při průzkumu prostředí bylo zjištěno, že stabilita připojení v některých denních hodinách kolísá, případně přístupové body neumožňují připojování nových klientů. Z těchto důvodů, zejména vzbudit v potenciálních obětech útoku pocit možnosti rychlejšího připojení, bylo vysílané SSID podvodného přístupového bodu pojmenováno „HyperSpeedWiFi“. Pokrytí bylo značně omezené, k podvodnému přístupovému bodu bylo možné se připojit vždy v okruhu zhruba 25 metrů od jeho umístění. Bod byl v průběhu útoku náhodně několikrát přesunut po vzdělávací instituci, a to takovým způsobem, kdy byl stávající aktivní přístupový bod zaměněn za přístupový bod podvodný. K jeho napájení sloužila funkce PoE (Power over Ethernet), ta umožňuje přístupový bod napájet a přenášet data po stejném UTP kabelu. Pro připojení k internetu byla využita stávající síťová infrastruktura. Vyjma přístupového bodu, napájecího zdroje pro PoE v některých místech a UTP kabelu pro propojení nebyl nutný žádný další HW.

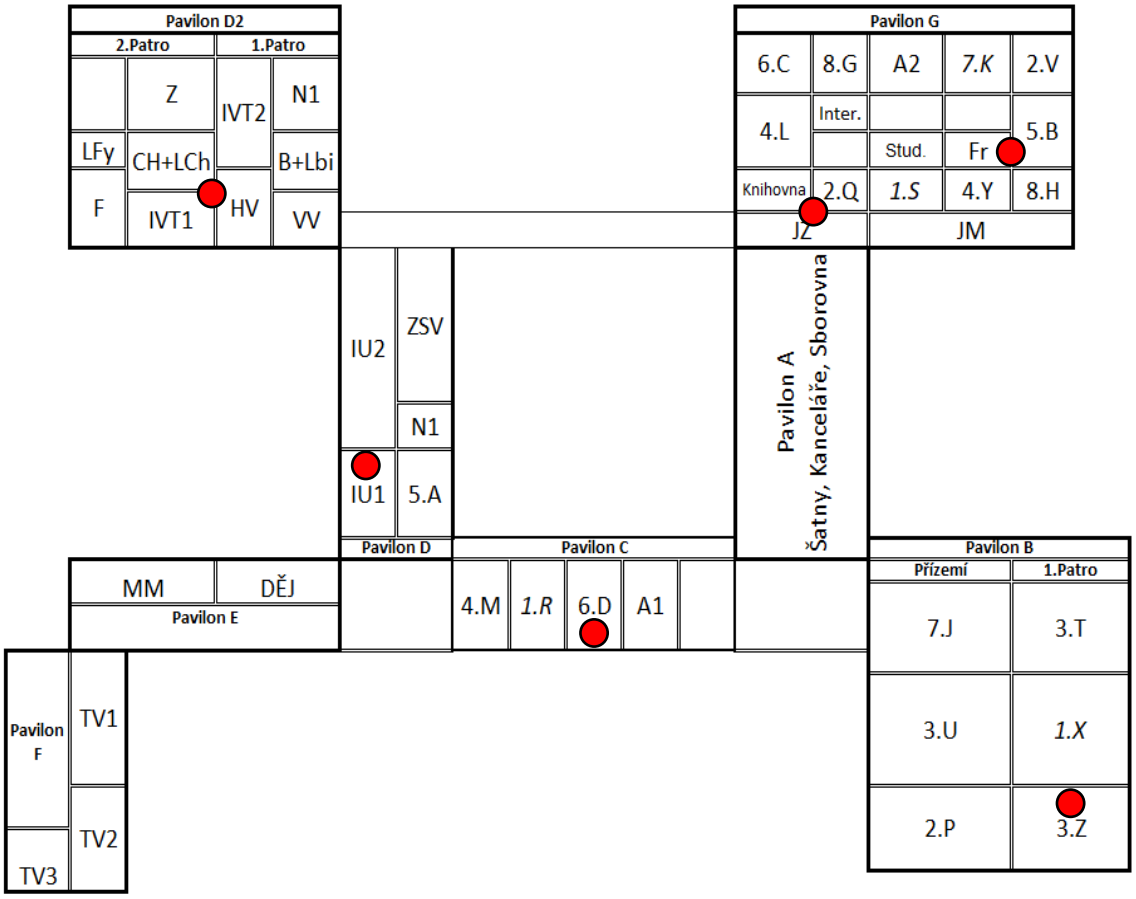
Autor si je však vědom, že při nesimulovaném útoku reálným útočníkem není pravděpodobné, že by útočník přímo využíval existující infrastruktury pro připojení podvodného bodu. Vhodným postupem útočníka je nastražení vlastní brány pro komunikaci s internetem a zvolení totožného názvu podvodného SSID s legitimním. Využíváno je často WiFi routerů a modemů, které umožňují připojení k internetu pomocí SIM karty. Ta je jednoduše vložena do tohoto prvku, který následně útočník nakonfiguruje dle potřeby, a k samotnému provozu postačí prvek napájet. Vhodným prvkem k realizaci útok je například TP-LINK TL-MR6400.[49]

Samotná realizace útoků probíhala umístěním, spuštěním přístupového bodu a zahájením vysílání SSID. Ve třech případech došlo k nahrazení vzhledově podobného přístupového bodu viditelně umístěného ve stropním podhledu na

[48] UniFi *Enterprise WiFi System: Models: UniFi AP (UAP), UniFi AP-Long Range (UAP-LR)* [online]. Ubiquiti Networks, c2011 [cit. 18.2.2022]. Dostupné z: https://www.wimoodshop.nl/downloads/54_UniFi_AP_Datasheet.pdf

[49] TL-MR6400: Bezdrátový router 300 Mbit/s Wireless N 4G LTE. *TP-Link* [online]. TP-Link, c2020 [cit. 18.2.2022]. Dostupné z: https://www.tp-link.com/cz/home-networking/3g-4g-router/tl-mr6400/

chodbách, zbylá umístění byla v datových zásuvkách uvnitř tříd. Jeho umístění bylo v průběhu realizace útoku náhodně měněno, celkem se jednalo o 6 umístění, která jsou červeně vyobrazena na schématu poskytnutém vzdělávací institucí níže.




*Obrázek 3: Schéma vzdělávací instituce Alfa*

Provoz podvodného bodu trval zhruba 26 dnů a 13 hodin. Za tuto dobu se k němu připojilo celkem 53 zařízení. Ve všech případech se, na základě záznamů MAC adres, jednalo o mobilní telefony. Vezmeme-li v potaz počet klientů legitimní sítě WiFi, který průměrně činí okolo 550 aktivních klientů za den, jedná se téměř o 10 % uživatelů instituce připojených k podvodnému bodu. Činnost uživatelů na přístupovém bodu byla monitorována pouze základní metrikou, tedy celkovým množstvím přenesených dat za posledních 24 hodin, objem odeslaných a přijatých paketů, a zda jsou momentálně aktivní či ne. Obsah komunikace nebyl žádným způsobem zachycován ani narušen. Relativně uspokojujícím faktem je zjištění, že žádné z připojených zařízení nebyl notebook zaměstnance vzdělávací instituce. Faktem mírně znepokojujícím je naopak neoznámení podezřelého SSID správci

sítě. Po celou dobu aktivity přístupového bodu bylo z řad studentů a pedagogů přijato jediné hlášení o potenciálně nezabezpečené síti.

Nejmenovaný pedagog Alfy si po 19 dnech všiml nového SSID a zjišťoval od kolegy vyučujícího informační a komunikační technologie, zda nemá k této síti nějaké informace. Jednalo se o značně strohý neformální rozhovor, při kterém byly přítomny další osoby. Kolega pouze vyjádřil nevědomost, čímž byl rozhovor přenesen na jiné téma a dále výskytu podezřelé sítě nebyla věnována žádná pozornost. Samotný správce sítě, který spravuje hardware Alfy a byl o činnosti informován v základní rovině bez podrobností, si sítě všiml náhodou při řešení nefunkčního připojení k internetu jednoho ze zařízení v administrativě. Tuto skutečnost sdělil autorovi společně s dotazem, zda se nejedná o činnost prováděnou v rámci testování bezpečnosti Alfy. Autor správci sdělil, že se opravdu jedná o součást testování a následně byl provoz podvodného bodu ukončen.

Samotnému ukončení předcházel rozhovor se správcem, který popsal postup přijatých opatření, vyhledání a zneškodnění hrozby:

„*SSID jsem si všiml v kanceláři zástupce. Síť mi přišla podezřelá a chtěl jsem to jít hned řešit, nicméně jsem si okamžitě vzpomněl na to testování, o kterém jsme se bavili. Kdyby to testování nebylo, šel bych podle síly signálu až ke zdroji, a protože vím, co jsem tady kde zapojil, tak bych ten bod odpojil. Pak bych se šel určitě poptat, nebo napsal hromadně e-mail, kdo všechno se k tomu připojil, a sdělil jim, že se mohli stát obětí útoku, tak ať si změní hesla a sledují, jestli se u nich neděje něco divného.*“

Pro účely této práce bylo samotné připojení klienta k podvodnému bodu dostačující, dále nebyly podniknuty z důvodu zachování bezpečnosti všech klientů žádné kroky útoku. Podstatné je však popsat další postup, který by útočníkem mohl být realizován. Síťový provoz klientů by po jejich připojení k podvodnému bodu a pohybu na internetu mohl být zaznamenáván útočníkem. Vyjma samotného záznamu je útočník schopen komunikaci zachycovat, pozměnit a následně odeslat v pozměněné podobě. K záznamu a čtení síťové komunikace lze využít metodu s názvem sniffing. Ta má za cíl zachytit všechny pakety, které nejsou zašifrované a mohou obsahovat informace využitelné útočníkem. Především se jedná o nezabezpečený síťový přenos dat, který obsahuje požadavky přihlášení k rozličným službám nebo webovým stránkám. Útočník je

schopen tato nezašifrovaná data zachytit a přečíst. Požadavky odeslané uživatelem mohou obsahovat údaje nutné k ověření uživatele, tedy přihlašovací jméno a heslo. Ty následně útočník může zneužít pro neoprávněný přístup k dané službě.[50]

Útočník dále může využít takzvaného SSL strippingu. Ke komunikaci s webovými stránkami je využíván protokol HTTPS, který vychází ze staršího protokolu HTTP. Komunikace prostřednictvím protokolu HTTPS je na rozdíl od komunikace po protokolu HTTP šifrovaná pomocí asymetrické šifry. Obě strany komunikace mají k šifrování jeden pár klíčů, veřejný a soukromý. Komunikace šifrovaná veřejným klíčem pak lze rozšifrovat pouze klíčem privátním. Tímto způsobem je zajištěna integrita datového toku při příjmu a odesílání. SSL stripping umožňuje útočníkům z komunikace vyřadit část, ve které dochází k zašifrování pomocí SSL. Následně proběhlá nezašifrovaná komunikace je přenesena ve formě prostého textu a plně čitelná. Útočník může taktéž využít metodu vynucování komunikace pouze přes nešifrovaný protokol HTTP, tuto komunikaci odposlouchávat a dále zneužít. Nicméně řada webových stránek je pod tímto protokolem nepřístupná a vynucuje si užití šifrovaného protokolu HTTPS. Jedná se zejména o webové stránky užívané k přístupu do služeb, internetového bankovnictví a dalších, u kterých je při komunikaci zacházeno s citlivými daty. I přes tuto skutečnost však existuje řada webových stránek, které pod nezabezpečeným protokolem nadále přístupné jsou a mohou být k tomuto útoku zneužity.[51]

Mezi základní postupy obrany proti tomuto útoku patří uživatelská obezřetnost. Nezabezpečené přístupové body a jejich sítě by nikdy neměly být využívány při přihlašování ke službám, webům a serverům, které mohou být na základě zachycené komunikace zneužity. Nešifrovaná komunikace je plně čitelný prostý text a lze z ní velmi jednoduše extrahovat druh požadavku obsahující přihlašovací údaje včetně hesla zadaného uživatelem. Indikátorem podvodného

[50] IRWIN, Luke. How to defend against man-in-the-middle attacks. *IT Governance* [online]. Bull Ring, Lagavooren, Drogheda: IT Governance, c2022, 21st December 2021 [cit. 19.2.2022]. Dostupné z: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks

[51] ZHANG, Xiaolu a Kim-Kwang Raymond CHOO, ed. *Digital Forensic Education* [online]. Cham: Springer International Publishing, 2020 [cit. 19.2.2022]. Studies in Big Data. ISBN 978-3-030-23546-8. Dostupné z: doi:10.1007/978-3-030-23547-5 str 125.

přístupového bodu je taktéž výskyt totožného, často nezabezpečeného SSID společně s legitimním, zabezpečeným SSID. Moderní spravovatelné WiFi sítě běžně pracují s technologií client roaming, která umožňuje uživatelům pohyb v celém pásmu pokrytí bez nutnosti opětovného připojení k přístupovému bodu ve stejné síti. Nejen že se jedná o podstatný prvek umožňující velmi uživatelsky přívětivé prostředí, ale taktéž o prvek bezpečnostní. Je velmi nepravděpodobné, že administrátor sítě vytvoří přístupový bod se stejným názvem SSID, které bude pokrytím dostupné pouze na malém území a nebude zabezpečené. V takovém případě se jedná o indikátor možnosti výskytu podvodného přístupového bodu.[52]

Dalším možným postupem obrany je kontrola komunikačního protokolu. Dnes již prakticky každý webový prohlížeč poskytuje uživateli možnost vidět, jaký protokol je využíván ke komunikaci s cílovou webovou stránkou. V případě, že je využíván nezabezpečený protokol HTTP, prohlížeč uživatele zpravidla graficky upozorní na možnost odposlechu komunikace. Pokud je to možné, vždy by měl být využíván zabezpečený protokol HTTPS.

Pokud uživatel používá otevřené, nezabezpečené a veřejně přístupné sítě, lze se proti odposlechu, odcizení a zneužití komunikace bránit prostřednictvím VPN. Virtuální privátní síť lze taktéž využít jako další vrstvu ochrany a nástavbu protokolu HTTPS. VPN umožní uživateli navázat zabezpečenou šifrovanou komunikaci mezi zařízením a cílovým serverem či webem. Vytvořen je pomyslný tunel, skrz který komunikace probíhá a pokud je jakýmkoliv způsobem zachycena, nelze ji číst. Obecně je VPN doporučováno využívat při připojení k veřejným sítím, kterou může být například síť pro návštěvníky nejen ve vzdělávací instituci.

Správci sítě ve vzdělávací instituci by měli podnikat kroky ke zjišťování, vyhledávání a zneškodňování možných podvodných přístupových bodů v teritoriu vzdělávací instituce. K tomuto účelu lze využít například funkce sousedních WiFi sítí a přístupových bodů, která je primárně určena k minimalizaci překrytí komunikačních kanálů a rušení. Pokud správce v tomto seznamu narazí na stejnojmennou vysílanou síť, může ji přesněji lokalizovat na základě metrik síly signálu, které poskytují jednotlivé přístupové body v síti. Pokud uživatel zjistí

[52] COLEMAN, David D. a David A. WESTCOTT. *CWNA Certified Wireless Network Administrator: Study Guide*. Sixth Edition. Indianapolis, Indiana: Wiley, c2021. ISBN 978-1-119-73450-5. Str 505.

přítomnost podezřelé WiFi sítě nebo fyzického přístupového bodu, měl by tuto skutečnost neprodleně oznámit správci sítě, aby mohly být učiněny kroky k odstranění potenciální hrozby.

## 4.2 Spear-Phishing

Druhým provedeným útokem byl spear-phishing cílený výhradně na zaměstnance vzdělávací instituce Alfa. Cílem bylo zjistit, jak se uživatel při doručení podezřelé a potenciálně podvodné zprávy zachová. Sledováno bylo, zda dojde k otevření odkazu, který byl součástí všech zaslaných zpráv. Každá zpráva měla unikátní odkaz určený k verifikaci jeho otevření uživatelem.

V přípravné fázi útoku bylo prvním krokem obstarat e-mailové kontakty na oběti útoku. Vzhledem ke skutečnosti, že vzdělávací instituce zveřejňují prakticky všechny e-mailové kontakty na zaměstnance Alfy na svých webových stránkách, byl tento proces velmi jednoduchý.

Dalším krokem bylo vytvořit sdělení, které uživatele donutí kliknout na odkaz přiložený k tělu zprávy. Zde bylo využito portálu aktualit, které Alfa na webu zveřejňuje. Aktuality zahrnují řadu důležitých informací, které lze však také snadno zneužít. Vzhledem k povaze útoku se jevilo jako nejvhodnější využít aktualit, které se týkají výsledků a úspěchů studentů ve školních soutěžích. Při účasti na školních akcích je prakticky vždy nutná účast pedagoga, který účast studentů zaštiťuje, organizuje a poskytuje o nich informace zbytku instituce a veřejnosti. Každá aktualita na webu je podepsána autorem, kterým je prakticky vždy zaštiťující pedagog. Vybráno bylo celkem 9 e-mailových adres na pedagogy, kteří se ve vybraných aktualitách vyskytovali jako autoři příspěvků.

Následně byla vytvořena e-mailová schránka odesílatele ve službě Google s uživatelským jménem *vysledky.info@gmail.com* a dále těla sdělení. Těla e-mailových sdělení ve všech případech odkazovala na určitou skutečnost spojenou s organizací školní soutěže, a dále samotný odkaz, na kterém by uživatel na základě zprávy měl dostat doplňující informace. Hypertextový odkaz byl zkrácen pomocí zkracovače a po jeho otevření se zobrazila uživateli stránka s upozorněním, že po kliknutí na aktivní prvek stránky bude přesměrován. Odkaz směřoval na korespondující aktualitu, zveřejněnou na webových stránkách Alfy. Oslovení bylo zvoleno v obecné neutrální rovině, bez konkretizace osoby. Zprávy

byly podepsány náhodnou, vymyšlenou identitou. Níže je uveden autentický příklad jednoho ze zaslaných sdělení, včetně chyby ve slově „*matematické*“.

> Dobrý den,
>
> dovolujeme si Vám touto cestou nabídnout možnost účasti v Internetové matematicvké olympiádě. 15. ročník soutěže se uskuteční 29. 11. 2022. Více informací naleznete zde.
>
> S pozdravem
>
> Tým IMO

K otevření odkazu došlo ve 3 z 9 případů útoku. Dva zaznamenané případy byly pouhé otevření odkazu a uživateli nebyly nahlášeny jakožto podezřelé. Ve třetím případě byl odkaz uživatelem otevřen, a ten hned vzápětí na zaslaný e-mail odpověděl. Uživatel také kontaktoval organizátora soutěže, ve kterém zjišťoval, zda je e-mail opravdu zaslaný organizátorem. V odpovědi organizátora se dozvěděl, že zprávu nezasílal. Mírně znepokojující je zjištění, že samotný organizátor odkaz otevřel také, a to dokonce dvakrát. Sdělení bylo tímto uživatelem dále oznámeno správci vzdělávací instituce Alfa, který jej vyhodnotil jako možný podvod. Uživatel správci na dotázání sdělil, že odkaz otevřel, ale byl přesměrován na webové stránky Alfy. Zde nic nevyplňoval a web okamžitě opustil.

Zmíněný případ, ve kterém došlo k oznámení útoku, včetně všech okolností a učiněných kroků lze taktéž považovat za nebezpečný. Důležité je však zmínit to, že uživatel byl upřímný, přiznal své pochybení a sdělil správci všechny okolnosti dle skutečného stavu. Ve zbylých dvou případech však k žádnému oznámení o možném podvodném jednání nedošlo. Zanedbání tohoto bezpečnostního postupu je značně znepokojující, protože při reálném útoku mohlo dojít k úniku dat či narušení integrity některého ze systémů.

Útok při testování nezpůsobil žádnou škodu, zaznamenáno bylo pouze kliknutí na odkaz a základní statistická data o zařízení uživatele. V případě reálného útoku se lze obávat především krádeže osobních a přihlašovacích údajů. Útočník pod odkaz, který dále ukryje zkracovačem, může nastražit podvodnou stránku s totožným vzhledem legitimní stránky, například informační vzdělávací systém, na které následně oběť zadá přihlašovací údaje. Ty jsou zaslány útočníkovi, který je může zneužít k přístupu do tohoto systému instituce. Za odkazem se však může skrývat prakticky cokoliv a uživatel by při sebemenším podezření neměl odkaz otevírat a zjištění neprodleně oznámit správci. Oznámení

lze učinit i formou hromadné korespondence všem ostatním uživatelům instituce, kteří se teoreticky také mohli stát cílem útoku.

Při předcházení škodám vzniklým v důsledku spear-phishingu by uživatelé měli dbát na základní pravidla spojená s rozpoznáním možných podvodných sdělení. Prvním indikátorem podvodného sdělení je e-mailová adresa, ze které bylo sdělení odesláno. Nejjednodušší způsob je ověřit autenticitu adresy na oficiálních stránkách subjektu, za který se osoba ve sdělení vydává. Dalším indikátorem je doména e-mailové adresy. Při oficiální komunikaci instituce využívají v drtivé většině vlastní doménová jména korespondující s názvem instituce, například *pacr.eu*, nikoliv *google.com*. Pokud je doména užitá k zaslání sdělení odlišná od domény domnělého subjektu, lze mít důvodné obavy o pravost sdělení.

Mezi další indikátory podvodného sdělení patří samotná identita podepsané instituce nebo osoby. Při oficiální komunikaci bude legitimní subjekt vystupovat vždy pod pravými jmény, která lze často dohledat ve veřejných kontaktech zveřejněných na webových stránkách konkrétní instituce. V případě pochybností lze danou instituci kontaktovat s dotazem, zda je osoba uvedená v podezřelém sdělení opravdu reálná a legitimní.

Pokud existuje důvod, kvůli kterému nelze ověřit legitimitu subjektu, lze k otevření odkazu využít bezplatnou službu VirusTotal, která umožňuje uživateli prověřit obsah odkazu na základě databází řady společností zabývajících se kybernetickou bezpečností. Po vložení odkazu zkráceného zkracovačem a proběhlé analýze odkazu se uživateli zobrazí vyjma výsledku také cesta přesměrování. Uživatel tak může vidět, kam bude po otevření odkazu přesměrován.[53]

Pokud se uživatel dopustí chyby v podobě otevření podvodného odkazu, nebo hůře vyplněním údajů na podvodné stránce, je nutné tuto skutečnost neprodleně oznámit. Prevence a obeznámenost s možnými hrozbami je zde nejlepší obranou, avšak v případech, kdy se uživatel dopustí chyby, je nutné překonat stud a celou skutečnost oznámit a popsat všechny podrobnosti.

[53] *VirusTotal* [online]. Minneapolis, MN, United States: Chronicle [cit. 20.2.2022]. Dostupné z: https://www.virustotal.com/gui/home/upload

## 4.3 DoS

Třetí útok měl za úkol prověřit odolnost systému a webových stránek užívaných vzdělávací institucí Alfa vůči DoS útoku. Jedná se o informační vzdělávací systém Bakaláři a oficiální webové stránky instituce. Oba zmíněné cíle útoku jsou podstatné pro řádné fungování Alfy a jsou jí poskytovány odlišným subjektem.

Přípravná fáze útoku zahrnovala analýzu cílů, výběr nástroje k provedení útoku a fakultativně zjištění IP adres obou cílů. Protože se jedná o útok na platformy provozované na webovém serveru, bylo vhodné v první řadě zjistit, o jaký webový server se jedná. K tomuto účelu byla využita bezplatná služba Builtwith, která na základě zdrojového kódu stránky přehledně analyzuje všechny komponenty kódu. Z podrobné analýzy bylo zjištěno, že stránky Alfy jsou provozovány na webovém serveru Apache. V případě informačního vzdělávacího systému se jednalo o webový server IIS provázaný se službou Cloudflare. IP adresy obou cílů nebylo nutné díky znalosti domén obou cílů zjišťovat. Avšak pro zjednodušení realizace útoku lze velmi snadno příkazem PING na cílovou doménu tyto adresy zjistit.[54]

Testování probíhalo prostřednictvím operačního systému Linux Kali. K realizaci útoku byly využity HTTP metody GET a POST. Obě tyto metody jsou naprosto běžné v komunikaci mezi klientem a cílovým serverem. Metodou GET vyžaduje klient od cílového serveru data, v případě metody POST naopak data cílovému serveru zasílá.[55]

Oba cíle byly v první vlně podrobeny útoku metodou POST. Ani v jednom případě nedošlo k odepření přístupu ke službě. Útok byl však veden pouze z jednoho stroje, přesto odpovídal přístupu zhruba pěti tisíc uživatelů zároveň. Server hostující webové stránky byl nedostupný pouze z IP adresy útočícího stroje, vrácen byl HTTP ERROR 429 odpovídající přílišnému počtu požadavků ze strany uživatele. Cílový server uživatele vyhodnotil jako potenciální útok, zasílaná data nepřijímal a byl tak dostupný. V případě serveru hostujícího informační

[54] Find out what websites are Built With. *BuiltWith* [online]. Sydney NSW Australia: BuiltWith [cit. 20.2.2022]. Dostupné z: https://builtwith.com/
[55] HTTP Request Methods. *W3Schools* [online]. Sandnes, Norsko: Refsnes Data, c1999-2022 [cit. 20.2.2022]. Dostupné z: https://www.w3schools.com/tags/ref_httpmethods

systém Bakaláři pravděpodobně došlo k rozložení síťového provozu mezi dílčí servery poskytované službou Cloudflare. Domnívat se tak lze na základě zjištění, že při přístupu z IP adresy, ze které byl veden útok, server nevracel chybu v podobě přílišného počtu požadavků. Cloudflare však také poskytuje ochranu před DoS útoky včetně filtrování a propouštění legitimního síťového provozu.[56]

V druhé vlně byly webové servery testovány metodou GET. Útok opět odpovídal přibližně pěti tisícům uživatelů. Webový server hostující informační systém Bakaláři útoku odolal v plném rozsahu. Zde lze předpokládat, že ochrana před DDoS útoky byla schopna bez obtíží rozpoznat, že se jedná o útok a cílový server zůstal zcela dostupný. Server hostující webové stránky však žádnou ochranu proti útoku metodou GET pravděpodobně nemá, a pokud ano, je značně neefektivní. Po spuštění útoku došlo k okamžitému odepření služby. Při snaze dostat se na webovou stránku se uživateli stránka po celou dobu trvání útoku nedokázala načíst. Po zastavení útoku trvalo zhruba dalších pět až deset vteřin, než opět došlo k obnovení standardní doby trvání přístupu.

DoS útoky nezpůsobují žádnou přímou škodu. V případě Alfy došlo pouze k nedostupnosti webových stránek a studijní informační systém zůstal během útoku plně funkční. Mimo testovací prostředí lze předpokládat realizaci DDoS útoku prostřednictvím sítě napadených počítačů, která se nazývá botnet. Ten umožňuje útočníkovi využít k útoku mnohonásobně vyšší výpočetní výkon, a tím pádem i maximalizovat účinky útoku. Hlavním rozdílem mezi útokem DoS z jediného zařízení a útokem DDoS prostřednictvím botnetu je počet útočících zařízení. Vzhledem k tomu, že botnet zahrnuje stovky, tisíce, někdy až desítky tisíc infikovaných zařízení, je filtrování síťového provozu na straně serveru velmi obtížné. Útok z jednoho zařízení, tedy z jedné IP adresy je velmi snadné detekovat a filtrovat. Botnet je však síť zcela legitimních zařízení, která jsou zneužita útočníkem pro zasílání požadavků na cílový server. Ten je vnímá jako legitimní a filtrování podvodného síťového provozu je v tomto případě značně složitější.[57]

[56] Security, Performance, and Reliability - all in one package. *Cloudflare* [online]. San Francisco, California, USA: Cloudflare, c2022 [cit. 20.2.2022]. Dostupné z: https://www.cloudflare.com/plans/#overview

[57] viz str. 30, JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

Provedený útok odepřením služby vzdělávací instituci Alfa uškodil zejména v oblasti předávání informací. Kritická část v podobě informačního systému Bakaláři zůstala plně funkční, nicméně při útoku značnějšího rozsahu prostřednictvím botnetu by mohlo dojít k odepření služby. Oba zmíněné cíle jsou služby poskytované subjektem odlišným od Alfy. Poskytované služby nejsou těmito subjekty provozovány na vyhrazeném, ale na sdíleném serveru. Poskytovatelé tak řeší problém přílišného množství fyzických zařízení a případnou nehospodárnost. Zařízení na straně poskytovatele je pouze z určité odpovídající části vyhrazeno pro provoz dané služby a zbylé vyhrazené části jsou poskytovány dalším stranám. Při útoku přímo na cílový server tak lze předpokládat, že k odepření přístupu ke službě může docházet na všech serveru přidružených službách.[58]

DoS ochrana informačního systému Bakaláři je díky službě Cloudflare filtrující možné podvodné požadavky dostačující. Tento systém je kritický a jeho odepření by mělo za následek vznik chaosu a obtíží při běžném provozu nejen vzdělávací instituce Alfa. Webové stránky jsou proti DoS útoku zabezpečeny nedostatečně. K odepření služby stačilo jedno jediné zařízení s průměrným výpočetním výkonem. Pro obranu lze doporučit aplikaci stejné ochrany proti DoS útokům, jako v případě informačního systému Bakaláři. V každém případě je vhodné s poskytovateli služeb konzultovat problematiku ochrany před DoS a DDoS útoky a pokud je to nutné, podniknout opatření pro jejich zamezení. Využít lze například zmíněnou službu Cloudflare, která poskytuje základní ochranu v transportní a síťové vrstvě zcela zdarma.[59]

[58] Subnet Calculator. *MXToolBox* [online]. Austin, TX, USA: MxToolbox, c2004-2022 [cit. 20.2.2022]. Dostupné z: https://mxtoolbox.com/subnetcalculator.aspx
[59] OSI Model: What Is the OSI Model. *Imperva* [online]. California, USA: Imperva, c2021 [cit. 20.2.2022]. Dostupné z: https://www.imperva.com/learn/application-security/osi-model/

## 4.4 Sociální inženýrství

Poslední útok měl za cíl otestovat resistenci uživatelů Alfy vůči útoku sociálním inženýrstvím. Zjišťována byla skutečnost, zda se uživatele podaří zmanipulovat k otevření nastraženého podvodného souboru, zda soubor zaregistrují, oznámí nebo z počítače odstraní.

Ke splnění účelu útoku byla autorem vytvořena samostatná aplikace v programovacím jazyce Go. Pro další úpravu zdrojového kódu do finální podoby byl využit programovací jazyk Python. Zjišťováno bylo, zda uživatel otevřel nastražený soubor, a to dle časového razítka. Další zjišťované parametry pouze demonstrují okruh informací, kterých může útočník využít pro další druhy útoků.

Samotný kód aplikace se skládá z několika částí. Aby nebylo nutné opakovaně přistupovat k infikovanému systému fyzicky, byla do zdrojového kódu vložena část umožňující zaslání všech zjištěných informací prostřednictvím

```
type SysInfo struct {
Time        string
Hostname    string   `bson:hostname`
Platform    string   `bson:platform`
CPU         string   `bson:cpu`
RAM         uint64   `bson:ram`
Disk        uint64   `bson:disk`
Username    string   `bson:username`
IP []net.Addr
OSBuild string
 }
```

konfigurace SMTP serveru, v tomto případě byl využit server poskytovatele Centrum.cz. Další část kódu má na starost získání základních údajů o cílovém systému. Mimo jiné je zjišťován aktuální čas SMTP serveru použitý jakožto časové razítko, společně s aktuálním časem zařízení. Část zdrojového kódu, která určuje strukturu informací získávaných o cílovém zařízení, je vyobrazena níže. Zdrojový kód v plném rozsahu včetně zkompilované aplikace samotné je k dispozici u autora práce. Z důvodu možného zneužití je zde vyobrazena pouze část zdrojového kódu.

Zkompilovaný zdrojový kód byl spustitelný soubor s příponou .EXE. Jeho ikona se však zobrazovala jako výchozí ikona pro spustitelné soubory, a proto došlo k její úpravě. Zobrazovaná ikona finálního spustitelného souboru byla převzata z ikony tabulkového kalkulátoru Microsoft Excel.

Soubor byl umístěn na plochu sdíleného počítače ve sborovně. Pedagogové tento počítač využívají mimo jiné ke čtení e-mailových zpráv, připojování ke vzdálené ploše vzdělávacího informačního systému, tisku a občasnému vyřizování osobních záležitostí. Frekvence využití tohoto počítače je relativně vysoká, denně se u něj na základě pozorování vystřídá kolem 15 pedagogů. Umístěny byly celkem tři verze podvodného souboru, které se však lišily pouze názvem. Snahou bylo zneužít zvědavosti a důvěřivosti uživatelů, proto byly soubory pojmenovány „*Termíny 2021*“, „*Bonusy učitelů*“ a „*Důležité vyplnit!*“. Soubory se na zařízení nacházely pod dobu 20 dnů.

Za celou tuto dobu nebyl ani jeden ze tří souborů otevřen, tedy nedošlo ke spuštění nastraženého kódu. Z jakých důvodů nebyly otevřeny nelze přesněji specifikovat. Lze se domnívat, že uživatelé využívající sdílený počítač jsou čestné osoby, které dbají na soukromí ostatních uživatelů. Můžeme tedy konstatovat, že žádný z uživatelů nebyl zmanipulován k otevření potenciálně nebezpečného souboru. K interakci se soubory však muselo nutně dojít. Zhruba v polovině doby, po kterou se soubory na zařízení nacházely, došlo ke změně umístění těchto souborů na ploše, přesunuty byly z prostřední části plochy k levému spodnímu okraji. Některý z uživatelů si tak souborů všimnout musel a určitým způsobem s nimi interagoval.

Zdrojový kód taktéž nebyl zaznamenán jako podezřelý antivirovým programem. Při jeho umisťování a testovacím spuštění nedošlo k jeho přesunu do karantény nebo upozornění na potenciální hrozbu. Pro účely této práce byly soubory umístěny ne příliš běžným způsobem. Jejich propagace do systému mimo testovací prostředí by tak probíhala bezpochyby jinými způsoby. Mezi tyto způsoby lze zařadit především zaslání souboru e-mailovou zprávou, umístěním na sdílené cloudové úložiště, či jej šířit přes odkaz na vlastní FTP server. Zde je nutné poznamenat, že subjekty poskytující tyto služby často nedovolují nahrání a šíření souborů s příponou .EXE, právě z důvodu možného zneužití k šíření hrozeb. Možné je však zasílat a nahrávat soubory komprimované, tedy archivy s příponou .ZIP a .RAR. Autor práce zamýšlel kód skrytý uvnitř souboru tabulkového kalkulátoru s příponou .XLSX šířit e-mailovou zprávou, a to takovým způsobem, kdy podvodný kód lze implementovat jakožto část kódu legitimního souboru či aplikace. Při spuštění tohoto kódu či aplikace pak dojde i ke spuštění

kódu podvodného. Ve spojitosti s aktuální situací, doznívající pandemií a válečnému konfliktu Ukrajinské republiky a Ruské federace se rozhodl autor nezvyšovat míru frustrace, obav a napětí mezi uživateli a vyvolávat chaos ve vzdělávací instituci Alfa.

Následky nebyly při tomto konkrétním útoku, vzhledem k jeho nespuštění, zaznamenány žádné. Při spuštění souboru by došlo k zaslání některých ze základních údajů o infikovaném zařízení e-mailem. Výstupem aplikace byl záznam na základě struktury kódu uvedené výše. Jedná se o IP adresu všech připojených síťových adaptérů, build a druh operačního systému, uživatelské jméno, velikost operační paměti, druh procesoru, hostname a velikost pevného disku. Zkrácený výpis je pro přiblížení uveden níže. Časové razítko bylo zaznamenáváno na úrovni SMTP serveru v zaslaném e-mailu mimo aplikaci.

```
"Time": "",
"Hostname": "DESKTOP-AN1T57U",
"Platform": "Microsoft Windows 10 Home",
"CPU": "Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz",
"RAM": 4009,
"Disk": 243570,
"Username": "DESKTOP-AN1T57U\\Sborovna",
"IP": [
  {
  "IP": "192.168.5.208",
  "Mask": "////AA=="
  },
  …
  {
  "IP": "169.254.221.212",
  "Mask": "//8AAA=="
  },
  {
  "IP": "127.0.0.1",
  "Mask": "/wAAAA=="
  }
  ],
  "OSBuild": "19043"
```

Do souboru lze schovat prakticky jakýkoliv druh kódu, záleží na zdatnosti útočníka. Získané informace o stroji oběti mohou být velmi jednoduše zneužity. Útočníci využívají pro ukrytí škodlivého kódu makra v textových a tabulkových dokumentech, a také instalační soubory. Vhodné je také u instalačních a spustitelných souborů ověřit platnost digitálního certifikátu, které vydávají oprávněné subjekty vydavatelům software. Soubory jsou následně podepsány tímto digitálním certifikátem a uživatel si může ověřit, že se doopravdy jedná

o legitimní software či soubor. Podobně lze využívat digitální certifikáty a podpisy pro e-mailovou komunikaci. Pokud uživatel komunikuje se subjektem, který zprávu digitálně podepíše, lze ji považovat za legitimní. Pokud však přijde od stejného uživatele zpráva bez digitálního podpisu, je třeba dbát opatrnosti a zjistit, zda zpráva byla skutečně zaslána daným subjektem.

Obranou proti tomuto druhu útoků je především uživatelská obezřetnost. Sociální inženýrství využívá k úspěšnému provedení lidskou důvěřivost, neznalost, zvědavost a manipulaci. Pokud uživatelé postupují obezřetně a využívají kritického myšlení, mnohonásobně tak snižují riziko vzniku škody tímto útokem. Mimo testovací prostředí dochází k propagaci škodlivého kódu různými způsoby. Mezi ty nejvyužívanější patří zasílání e-mailem a stažení na první pohled legitimního software, jehož součástí je i škodlivý kód. Pokud uživatel dostane podezřelý e-mail, který obsahuje odkaz nebo přílohu, neměl by jej nikdy otevírat. Stejný postup by měl být aplikován při nálezu podezřelého souboru. Před spuštěním jakéhokoliv neznámého souboru je vhodné si ověřit, zda se opravdu jedná o správný druh v jeho vlastnostech. Škodlivého kódu součástí legitimního software se lze vyvarovat nákupem a pořizováním plně legitimního software od distributora či autora. Nikdy by neměl být stahován software, jehož původ je neznámý.

# Závěr

Kybernetická bezpečnost vzdělávacích institucí se v recentní době stala velmi aktuálním tématem. Denně se v kyberprostoru odehraje nespočet druhů útoků, které mohou mít za cíl poškodit kteroukoliv jeho součást. Nejen v České republice je velký počet vzdělávacích institucí, které mohou do vývoje kybernetické bezpečnosti přímo zasáhnout, ale také být přímo zasaženy.

Vývoj informačních a komunikačních technologií je rapidní proces, jehož součástí se stal každý z nás. Dnes si již velmi obtížně dokážeme představit všední život bez možnosti využívání kyberprostoru pro běžné činnosti. Tyto činnosti zahrnují i vzdělávací proces, který je důležitým prvkem vývoje každého jedince.

Vzdělávání by mělo zaopatřit uživatele vhledem do problematiky kybernetické bezpečnosti, a to bez ohledu na stranu, na které se ve vzdělávacím procesu nachází. Studenti, pedagogové a všichni ostatní zaměstnanci těchto institucí se v kyberprostoru pohybují, vykonávají pracovní činnost, spolupracují, ale také tráví volný a soukromý čas. Jejich přístup formovaný a mezigeneračně předávaný bude udávat budoucí směr vnímání a rozpoznávání všech hrozeb. Lze se zcela oprávněně domnívat, že podíl času stráveného v kyberprostoru vůči času strávenému ve světě reálném bude mít stoupající tendence a uživatelé tak budou hrozbám vystavováni stále častěji.

Práce přináší vhled do specifické oblasti problematiky kybernetické bezpečnosti. Věnuje se vzdělávacím institucím jakožto celku, v potaz bere jejich podobnost na základě účelu, ale také je vzájemně rozděluje na základě specifik pro každou z nich. Teoretická část práce zpočátku vymezila pojem vzdělávací instituce, kybernetická bezpečnost, a následně tyto dva pojmy vymezila ve vzájemném propojení. Dále se věnovala vymezení a popsání kybernetických útoků, se kterými se lze ve spojení se vzdělávacími institucemi setkat nejběžněji, popsala možná rizika, škody a stanovila vhodná opatření.

Praktická část práce byla vyhrazena pro komplexní analýzu kybernetické bezpečnosti konkrétní vzdělávací instituce. Popsány a analyzovány z hlediska kybernetické bezpečnosti byly všechny její kritické a stěžejní části, infrastruktura a uživatelé. Stanovena byla vhodná doporučení pro minimalizaci vzniku nežádoucích účinků kybernetických útoků, slabá místa vhodná k dalšímu

zabezpečení a možné způsoby ochrany. Závěr praktické části experimentálně prověřil některé z kritických částí konkrétní vzdělávací instituce realizací kybernetických útoků. Popsána byla příprava, proces provedení a následně vzniklé nežádoucí účinky útoků.

Práce by měla sloužit především jako vhled do specifické problematiky kybernetické bezpečnosti vzdělávacích institucí. Využití této práce, aktuálních pramenů a reálných příkladů ke vzdělávání a rozšiřování povědomí o kybernetické bezpečnosti mezi jedinci ve vzdělávacím procesu autor považuje za vhodné a stěžejní pro vývoj budoucích generací. Právě v průběhu vzdělávacího procesu dochází k formování návyků, mezi kterými je i způsob chování v kyberprostoru, přístup k bezpečnosti a zodpovědnost.

Vzdělávání a osvěta by měly začínat již od doby, kdy uživatel poprvé vstoupí do kyberprostoru a trvat po celou dobu aktivního využívání kyberprostoru. Neměly by se však týkat pouze mladých jedinců, ale také ostatních věkových skupin, které se ve sféře vzdělávání pohybují. Právě tyto osoby mohou mladé generaci předat cenné zkušenosti a znalosti umožňující formovat zodpovědné, kriticky smýšlející jedince, kteří budou v kyberprostoru jednat s maximální opatrností, budou umět hrozbám odolávat a předcházet vzniku nežádoucích účinků.

# Seznam použité literatury

## Monografie


[1] AUGER, Gerald, Jaclyn SCOTT, Jonathan HELMUS a Kim NGUYEN. *Cybersecurity Career Master Plan: Proven techniques and effective tips to help you advance in your cybersecurity career*. Birmingham, UK: Packt, 2021. ISBN 978-1-80107-356-1.

[2] BHATTACHARYYA, Dhruba Kumar a Jugal Kumar KALITA. *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. Boca Raton: CRC Press, Taylor & Francis, c2016. ISBN 978-1-4987-2965-9.

[3] COLEMAN, David D. a David A. WESTCOTT. *CWNA Certified Wireless Network Administrator: Study Guide*. Sixth Edition. Indianapolis, Indiana: Wiley, c2021. ISBN 978-1-119-73450-5.

[4] CORNISH, Paul, ed. *The Oxford Handbook of Cyber Security*. New York, NY: Oxford University Press, c2021. ISBN 978-0-19-880068-2.

[5] DULANEY, Emmett a Chuck EASTTOM. *CompTIA Security+ Study Guide: SY0-401*. 6th Edition. Indianapolis, Indiana: Wiley, 2014. ISBN 978-1-118-87507-0.

[6] HADNAGY, Christopher, Michele FINCHER. *Phishing dark waters: the offensive and defensive sides of malicious e-mails.* Indianapolis: Wiley, 2015. ISBN 978-1-118-95849-0.

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

[8] KUMAR, Kamila N., ed. *Advancing Cloud Database Systems and Capacity Planning With Dynamic Applications*. Hershey, PA: IGI Global, 2017. ISBN 9781522520139.

[9] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[10] OZKAYA, Erdal. *Learn Social Engineering: Learn the art of human hacking with an internationally renowed expert*. Birmingham: Packt Publishing, 2018. ISBN 978-1-78883-792-7.

[11] SPAMMER-X, POSLUNS, Jeffrey, ed. *Inside the SPAM Cartel: Trade Secrets From The Dark Side*. Rockland, MA: Syngress, c2004. ISBN 1-932266-86-0.

[12] WHITMAN, Michael E. a Herbert J. MATTORD. *Principles of information security*. 2nd ed. Boston, Massachusetts.: Thomson Course Technology, c2005. ISBN 978-1-4239-0177-8.

## Zákonná úprava


[13] Zákon č. 106/1999 Sb., *Zákon o svobodném přístupu k informacím* ve znění k 15.2.2022

[14] Zákon č. 181/2014 Sb., *Zákon o kybernetické bezpečnosti* ve znění k 18.1.2022

[15] Zákon č. 370/2017 Sb., *Zákon o platebním styku* ve znění k 11.12.2021

[16] Zákon č. 561/2004 Sb., *Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání* ve znění k 18.11.2021


## Webové stránky a elektronické zdroje


[17] AKTUALITY - řazeno chronologicky. *BARDA SW, HW s.r.o.* [online]. Ohrobec: BARDA SW, HW [cit. 18.2.2022]. Dostupné z: https://www.barda.cz/

[18] Android Security Bulletins. *Android Open Source Project* [online]. Mountain View, CA, USA: Google [cit. 18.2.2022]. Dostupné z: https://source.android.com/security/bulletin/

[19] Back up and restore your PC. *Microsoft* [online]. Washington, USA: c2022 [cit. 10.2.2022]. Dostupné z: https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c

[20] Bakaláři. [Online]. Příbram: BAKALÁŘI software, c2022 [cit. 15.2.2022]. Dostupné z: https://bakalari.cz/

[21] BREJCHA, Pavel. Útoky na univerzity jsou v kybernetickém prostoru novým standardem. *Fakespace* [online]. Fakescape, c2021, 28. 12. 2021 [cit. 28.11.2021]. Dostupné z: https://www.fakescape.cz/blog/kyberneticke-utoky-univerzity

[22] *Buď pánem svého prostoru: Jak chránit sebe a své věci, když jste online* [online]. Praha: CZ.NIC, 2013. [cit. 1.2.2022]. ISBN 978-80-904248-6-9. Dostupné z: https://knihy.nic.cz/files/edice/bud_panem_sveho_prostoru.pdf

[23] Co všechno umíme?. *BAKALÁŘI* [online]. Příbram: BAKALÁŘI software, c2022 [cit. 4.12.2021]. Dostupné z: https://www.bakalari.cz/Static/WhatWeKnow

[24] ČERNÝ, Michal. *Informační systémy ve vzdělávání: od matrik k sémantickým technologiím a dialogovým systémům pro učení* [online]. Brno: Masarykova univerzita, 2016 [cit. 4.12.2021]. ISBN 978-80-210-9129-0. Dostupné z: https://is.muni.cz/el/1421/jaro2016/VIKMB39/um/kniha_Informacni_systemy_ve_vzdelavani_kor_MG.pdf

[25] ESET: Kybernetickou bezpečnost na školách v pětině případů řeší učitel informatiky. *ESET* [online]. Bratislava: ESET, c1992 – 2022, 21. 11. 2019 [cit. 28.11.2021]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-kybernetickou-bezpecnost-na-skolach-v-petine-pripadu-resi-ucitel-informatiky/

[26] Find out what websites are Built With. *BuiltWith* [online]. Sydney NSW Australia: BuiltWith [cit. 20.2.2022]. Dostupné z: https://builtwith.com/

[27] HÁJEK, Martin. Kurz základů kybernetické bezpečnosti. *Dávej kyber* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 4.12.2021]. Dostupné z: https://osveta.nukib.cz/mod/resource/view.php?id=1024

[28] How Does Two-Factor Authentication (2FA) Work?. *Merchant Fraud Journal* [online]. Concord, Ontario: Merchant Fraud Journal, c2022, January 16, 2020 [cit. 17.2.2022]. Dostupné z: https://www.merchantfraudjournal.com/two-factor-authentication-work/

[29] HTTP Request Methods. *W3Schools* [online]. Sandnes, Norsko: Refsnes Data, c1999-2022 [cit. 20.2.2022]. Dostupné z: https://www.w3schools.com/tags/ref_httpmethods

[30] Identity Theft. *ESET* [online]. Bratislava: ESET, c1992 – 2022 [cit. 18.2.2022]. Dostupné z: https://www.eset.com/uk/types-of-cyber-threats/identity-theft/

[31] IP Address. *TechTerms* [online]. Minneapolis, MN, United States: Sharpened, c2020 [cit. 8.1.2022]. Dostupné z: https://techterms.com/definition/ip_address

[32] IRWIN, Luke. How to defend against man-in-the-middle attacks. *IT Governance* [online]. Bull Ring, Lagavooren, Drogheda: IT Governance, c2022, 21st December 2021 [cit. 19.2.2022]. Dostupné z: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks

[33] Jaký je rozdíl mezi WPA2, WPA3, WPA, WEP, AES a TKIP?. *AIRWAYNET* [online]. Praha: AIRWAYNET, c2022 [cit. 12.2.2022]. Dostupné z: https://www.airwaynet.cz/jaky-je-rozdil-mezi-wpa2-wpa3-wpa-wep-aes-a-tkip/

[34] Kategorizace dat. *Univerzita Karlova* [online]. Praha: Univerzita Karlova, c2022, 2. říjen 2020 [cit. 15.2.2022]. Dostupné z: https://openscience.cuni.cz/OSCI-95.html

[35] KOLOUCH, Jan. *CyberCrime* [online]. Praha: CZ.NIC, 2016. [cit. 12.1.2022]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[36] KRČMÁŘ, Petr. DDoS útoky: jak se účinně bránit?. *Root.cz* [online]. Praha: Internet Info, c1998 – 2022, 16. 5. 2016 [cit. 15.1.2022]. Dostupné z: https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/

[37] KRESA, Dan. 3 výzvy kybernetické bezpečnosti ve vzdělávacím sektoru. *KYBEZ* [online]. Jihlava: GORDIC, c2021, 16. 5. 2018 [cit. 28.11.2021]. Dostupné z: https://www.kybez.cz/3-vyzvy-kyberneticke-bezpecnosti-ve-vzdelavacim-sektoru/

[38] NÚKIB. Online výuka a bezpečnost. *YouTube* [online]. 25. 3. 2021 [cit. 5.12.2021]. Dostupné z: https://www.youtube.com/watch?v=8y9Z-f97_3M

[39] OSI Model: What Is the OSI Model. *Imperva* [online]. California, USA: Imperva, c2021 [cit. 20.2.2022]. Dostupné z: https://www.imperva.com/learn/application-security/osi-model/

[40] Phishing. *Avast* [online]. Praha: AVAST, c1988-2022 [cit. 28.12.2021]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

[41] Phishing/Spear phishing. *ENISA* [online]. European Network and Information Security Agency, c2005-2022 [cit. 17.2.2022]. Dostupné z: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

[42] Rogue access point. *PCMag* [online]. New York, NY: PCMag, c1996-2022 [cit. 12.1.2022]. Dostupné z: https://www.pcmag.com/encyclopedia/term/rogue-access-point

[43] ROMANOSKY, Sasha a Zachary K. GOLDMAN. What Is Cyber Collateral Damage? And Why Does It Matter?. *Lawfare* [online]. The Lawfare Institute, c2022, November 15, 2016 [cit. 11.2.2022]. Dostupné z: https://www.lawfareblog.com/what-cyber-collateral-damage-and-why-does-it-matter

[44] Security Tip (ST04-001): What is Cybersecurity?. *Cybersecurity and Infrastructure Security Agency* [online]. Rosslyn, Arlington, Virginia: CISA, May 06, 2009 [cit. 28.11.2021]. Dostupné z: https://www.cisa.gov/uscert/ncas/tips/ST04-001

[45] Security, Performance, and Reliability - all in one package. *Cloudflare* [online]. San Francisco, California, USA: Cloudflare, c2022 [cit. 20.2.2022]. Dostupné z: https://www.cloudflare.com/plans/#overview

[46] Security: The Need-to-know principle. *Microsoft* [online]. Washington, USA: Microsoft, c2022, Feb 03 2021 [cit. 15.2.2022]. Dostupné z: https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393

[47] Select UniFi Access Point (AP) Models Obsoletion Date: March 1, 2021. *Ubiquiti* [online]. New York: Ubiquiti, c2022, March 1, 2019 [cit. 13.2.2022]. Dostupné z: https://community.ui.com/questions/Select-UniFi-Access-Point-AP-Models-Obsoletion-Date-March-1-2021/65487283-ce9d-49f4-85b9-b6aa54659ef7

[48] SHAH, Abhishek. Rogue access points. *Khan Academy* [online]. Kalifornie, USA: Khan Academy, c2022 [cit. 15.1.2022]. Dostupné z: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks

[49] Silné ověření klienta při poskytování platebních služeb. *Epravo.cz* [online]. EPRAVO.CZ, c1999-2022, 18. 9. 2019 [cit. 8.12.2021]. Dostupné z: https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html

[50] *SOCIAL ENGINEERING HANDBOOK: How to Take the Right Action* [online]. Bratislava:ESET, c1992 - 2021 [cit. 11.1.2022]. Dostupné z: https://datasecurityguide.eset.com/storage/download-widget-files/ESET_Data%20Security%20Guide_Social%20Engineering%20Handbook_UK.pdf

[51] Subnet Calculator. *MXToolBox* [online]. Austin, TX, USA: MxToolbox, c2004-2022 [cit. 20.2.2022]. Dostupné z: https://mxtoolbox.com/subnetcalculator.aspx

[52] TANNER, Jonathan. Threat Spotlight: Document-Based Malware. *Barracuda* [online]. Campbell, California: Barracuda Networks, c2022, April 4, 2019 [cit. 17.2.2022]. Dostupné z: https://blog.barracuda.com/2019/04/04/threat-spotlight-document-based-malware/

[53] TL-MR6400: Bezdrátový router 300 Mbit/s Wireless N 4G LTE. *TP-Link* [online]. TP-Link, c2020 [cit. 18.2.2022]. Dostupné z: https://www.tp-link.com/cz/home-networking/3g-4g-router/tl-mr6400/

[54] Understanding Rogue Access Points. *Juniper Networks* [online]. Sunnyvale, California, USA: Juniper Networks, c1999 - 2022, 5-Oct-18 [cit. 26.1.2022]. Dostupné z: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html

[55] UniFi *Enterprise WiFi System: Models: UniFi AP (UAP), UniFi AP-Long Range (UAP-LR)* [online]. Ubiquiti Networks, c2011 [cit. 18.2.2022]. Dostupné z: https://www.wimoodshop.nl/downloads/54_UniFi_AP_Datasheet.pdf

[56] VILLANUEVA, John C. An Introduction To Cipher Suites | SSL/TSL Cipher Suites Explained. *JSCAPE* [online]. Eugene, OR: JSCAPE, c2022, May 16, 2018 [cit. 15.1.2022]. Dostupné z: https://www.jscape.com/blog/cipher-suites

[57] *VirusTotal* [online]. Minneapolis, MN, United States: Chronicle [cit. 20.2.2022]. Dostupné z: https://www.virustotal.com/gui/home/upload

[58] What are the security risks of RDP? | RDP vulnerabilities. *Cloudflare* [online]. Kalifornie, USA: Cloudflare, c2022 [cit. 19.2.2022]. Dostupné z: https://www.cloudflare.com/learning/access-management/rdp-security-risks/

[59] What is a denial of service attack (DoS) ?. *Palo Alto Networks* [online]. Kalifornie, USA: Palo Alto Networks, c2022 [cit. 8.1.2022]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[60] What Is a VPN? - Virtual Private Network. *Cisco* [online]. San Jose, CA, USA: Cisco Systems, c2022 [cit. 18.11.2021]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[61] What is an SSL Certificate ?. *DigiCert* [online]. Lehi, Utah: DigiCert, c2022 [cit. 10.2.2022]. Dostupné z: https://www.digicert.com/what-is-an-ssl-certificate

[62] What Is Cybersecurity?. *Cisco* [online]. San Jose, CA, USA: Cisco Systems, c2022 [cit. 28.11.2021]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[63] WHAT IS IDENTITY THEFT?. *Terranova Security* [online]. Laval, Quebec, Canada: Terranova Worldwide, c2022 [cit. 2.2.2022]. Dostupné z: https://terranovasecurity.com/what-is-identity-theft/

[64] What Is Phishing?. *Phishing.org* [online]. Clearwater, Florida, USA: KnowBe4 [cit. 18.12.2021]. Dostupné z: https://www.phishing.org/what-is-phishing

[65] WINDER, Davey. Critical HP Printer Security Warning: 150 Models Exposed To Hack Attack. *Forbes* [online]. Jersey City, NJ: Forbes Media, c2022, Dec 4, 2021 [cit. 10.2.2022]. Dostupné z: https://www.forbes.com/sites/daveywinder/2021/12/04/critical-hp-printer-update-warning-150-models-open-to-hack-attack/

[66] ZHANG, Xiaolu a Kim-Kwang Raymond CHOO, ed. *Digital Forensic Education* [online]. Cham: Springer International Publishing, 2020 [cit. 19.2.2022]. Studies in Big Data. ISBN 978-3-030-23546-8. Dostupné z: doi:10.1007/978-3-030-23547-5

[67] Zkrácená cesta protokolu RDP služby Azure Virtual Desktop pro spravované sítě. *Microsoft* [online]. Washington, USA: Microsoft, c2022 [cit. 19.2.2022]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/virtual-desktop/shortpath

[68] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020.* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 26. 7. 2021 [cit. 21.12.2021]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

# Seznam obrázků