Návrh praktické úlohy z problematiky informační bezpečnosti

Jakub Pšenčík

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Pšenčík**
Osobní číslo:	**L21721**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Návrh praktické úlohy z problematiky informační bezpečnosti**

Zásady pro vypracování

1. Na základě provedené rešerše zpracujte teoretický vstup do problematiky.
2. Analyzujte aktuální obsah výuky informační bezpečnosti v kontextu ochrany obyvatelstva.
3. Zvolte vhodnou praktickou úlohu a navrhněte její zadání.
4. Zpracujte příkladové řešení navržené úlohy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CODINGS, Zach. *Cyber security: hacking with Kali linux, ethical hacking.* USA: Zach Codings, 2019. ISBN 9781701275560.
2. EVANS, Lester. *Cybersecurity: What you need to know about computer and cyber security, social engineering, the internet of thing + an essential guide to ethical hacking for beginners.* USA: Lester Evans, 2019. ISBN 9781794647237.
3. KOLOUCH, Jan a BAŠTA Pavel. *Cybersecurity.* CZ.NIC, Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168348.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 22.04.2024

Jméno a příjmení studenta: Jakub Pšenčík

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se věnuje návrhu úlohy pro praktické cvičení v oblasti informační bezpečnosti. V práci je zpracován teoretický úvod do problematiky informační bezpečnosti, na kterou navazuje zhodnocení současné výuky informační bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Následně je podle výsledků tohoto zhodnocená navrženo zadání úlohy, která odráží aktuální téma informační bezpečnosti, a pro tuto úlohu je také zpracováno vzorové řešení.

Klíčová slova: informační bezpečnost, phishing, sociální inženýrství

ABSTRACT

This bachelor thesis focuses on design of practical task in the field of information security. The thesis provides a teoretical introduction to the issue of information security, folowed by analysis of current teaching of information security on Faculty of Logistic and Crisis Management of Tomas Bata Univesity in Zlín. Based on previous analysis is proposed an assignment of task, which reflects the current trends in information security, and exemlpar solution si also prepared.

Keywords: information security, phishing, social engineering

Děkuji svému vedoucímu, panu Ing. Petru Svobodovi, Ph. D., za trpělivost.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Informace lze v dnešní době považovat za jeden z nejvýznamnějších zdrojů zajišťujících pokrok ve všech odvětvích lidské společnosti. Narušení nebo deformace toku informací, poruchy přenosu nebo další neoprávněné operace s informacemi mohou způsobit špatnou činnost procesů a rozhodování v podniku, státní správě či jiném organizačním systému. Proto je zásadní znalost, která umožní předcházet potenciálním útokům na informace nebo informační systémy, ať už osobní nebo v rámci organizace. Zejména pak osoby na řídících pozicích, nebo v bezpečnostním sektoru, by měli mít dostatečnou zkušenost se zajišťováním informační bezpečnosti.

Tato práce se tedy zaměřuje na výuku informační bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, kde studují budoucí nebo i současní pracovníci státní správy, bezpečnostních složek a dalších oblastí věnujících ze zajišťování bezpečnosti. Hlavním cílem této práce je zvýšit kvalitu výuky informační bezpečnosti na zmíněné fakultě, k čemuž povede několik dílčích cílů. Dílčí cíle této práce jsou tedy následující.

Prvním cílem je vypracování teoretického vstupu do problematiky informační bezpečnosti, který poslouží pro uvedení do terminologie a základních postupů a metod informační bezpečnosti a také jako výchozí bod pro další směřování práce.

Druhým cílem této práce je analyzovat současný obsah výuky, zejména potom to, jakým způsobem reflektuje současné trendy informační bezpečnosti v kontextu ochrany obyvatelstva.

Třetím cílem je návrh vhodného zadání pro novou praktickou úlohu, která bude zohledňovat výsledky a poznatky z předchozích cílů pro stanovení nejpřínosnějšího tématu a způsobu zpracování zadání úlohy.

Čtvrtým a posledním dílčím cílem je vytvoření příkladového řešení zvolené úlohy. Toto řešení poslouží k ověření přínosu, který má úloha přinést a také jako vzor pro budoucí zpracování úlohy při výuce.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY INFORMAČNÍ BEZPEČNOSTI

Informační bezpečnost je téma, které se zaměřuje zabezpečení informací před jejich ztrátou, poškozením či zneužitím. Informace jako takové musí být, ale někde uloženy. To může být na pevných médiích jakými jsou flash-disky, paměťové karty, pevné disky v počítači, ale také na cloudových úložištích nebo v databázích organizací, které s těmito informacemi dále nakládají. Vzhledem k rozmachu bezdrátových technologií a internetových služeb nabývají právě poslední dva zmíněné způsoby uložení informaci na důležitosti a s tím souvisí také rozvoj prostředí ve kterém pracují. Toto prostředí je možné označit jako kyberprostor. Kyberprostor jako takový je možné si představit jako určitou virtuální realitu téměř neomezených rozměrů, která je však velmi závislá na své materiální stránce, tedy technologiích, které ji udržují. Tento kyberprostor je tvořen prvky informačních a komunikačních technologií fungujících na sjednoceném protokolu TCP/IP jako globální síť složenou z jednotlivých zařízení které v ní interagují. Takto kyberprostor vytváří neustále rostoucí systém, vázaný jen technologickými možnostmi hardwaru. Mezi hlavní znaky kyberprostoru se řadí jeho necentralizovanost, otevřenost a s tím související globální dostupnost, velké množství dostupných informací a interaktivnost, díky které může být kyberprostor ovlivňován svými uživateli, ale i naopak uživatelé mohou být ovlivněni kyberprostorem. (Kolouch, Bašta, 2019)

Kybernetický prostor, na rozdíl od technologií, na kterých je provozován, není nikým vlastněn. Není pod plnou kontrolou žádného úřadu nebo národa či státu. Z toho důvodu musejí být aktivity usilující o udržení bezpečnosti kyberprostoru koordinovány různými subjekty na různých úrovních. Tyto subjekty by měly pro ideální efektivitu sdílet informace a postupy pro koordinaci opatření proti různým incidentům a bezpečnostním abnormalitám. (Doucek et al., 2019)

1.1 Vybrané pojmy informační bezpečnosti

Tak jako v jakémkoli specializovaném prostředí, i v oblasti informační bezpečnosti je nutné se seznámit se základními terminologickými pojmy. Pro přehlednost a jednodušší orientaci v terminologii ze zahraničních zdrojů jsou uvedené pojmy zapsány včetně jejich anglické alternativy.

Autorizace (Authorization) popisuje udělení přístupu na základě ověření přístupových práv. Projevuje se jako jakákoli činnost k oprávnění subjektu či uživatele k provádění vybraných aktivit v informačním systému. (Jirásek et al., 2015)

Aktivum (Asset) je jakýkoliv hmotný či nehmotný majetek, který má pro majitele tohoto aktiva hodnotu. Čím větší dopad by měla ztráta daného aktiva, tím větší má pro držitele cenu. Mezi nejcennější aktiva se řadí peníze, majetek, a právě data a informace. Pokud se jedná o peníze jako aktivum, nemusí to být pouze hotovost, ale v kontextu informační bezpečnosti se jedná zejména o peníze digitální, tedy na bankovních účtech, investičních fondech a dalších virtuálních prostředních. V případě majetku je možné si představit kromě materiálních statků také duševní vlastnictví, kterým jsou patenty, know-how e nebo třeba struktura procedur a procesů využívaných pro vykonávání činnosti objektu. (Kolouch, Bašta, 2019)

Bezpečnost (Security) je možné definovat jako stav, kdy jsou hrozby pro určitý objekt a zájmy tohoto objektu omezeny na nejnižší možnou míru, a daný objekt je svými prostředky vybaven k efektivnímu zvládnutí stávajících potenciálních hrozeb. Objektem se může myslet určitá organizace, instituce nebo stát či jednotlivec. Podstatné je, že bezpečnost je stav relevantní pro potřeby daného objektu a jeho komplexnosti. Ideálním stavem bezpečnosti by bylo, pokud pro daný objekt neexistují žádné hrozby nebo jsou zcela eliminovány, ale takový stav je z principu nedosažitelný, proto jsou bezpečností myšleny podmínky, při kterých byly učiněny dostupné opatření, které vedou ke snížení účinnosti hrozeb proti objektu na přijatelnou úroveň. (Kolouch, Bašta, 2019)

Vzdálený přístup (Cloud computing) je obecný termín pro poskytování služeb k využívání programů a dat bez jejich instalace nebo uložení na zařízení ze kterého jsou vyžádány. Uživatelé k těmto službám mohou přistupovat vzdáleně přes internet pomocí webového prohlížeče nebo klienta dané aplikace. Toto umožňuje přístup více uživatelů k jednomu zdroji služby, a tedy i snížení provozních nákladů a výdajů na hardware. (Pavlíček et al., 2017)

Hrozba (Threat) je negativním působením, které usiluje o nežádoucí změny systému. Může být účelným pokusem o narušení systému anebo nechtěnou příčinu působící škody na systému nebo organizaci provozující tento systém. Hrozbu lze vnímat taky jako pasivní působení, jakým je zpřístupnění informací bez změny stavu v systému. Obecně lze hrozbu popsat jako jev s negativním dopadem pro posuzovaný objekt. (Jirásek et al., 2015)

Hodnocení rizik (Risk assessment) je proces, při kterém dochází k hodnocení negativních aspektů neboli hrozeb, které působí na daný systém za účelem definovat míru ohrožení, kterému je systém vystaven. Výsledkem je zjištění, zda jsou současná bezpečnostní opatření dostatečná k tomu, aby snížila míru rizika na přijatelnou úroveň. (Evans, 2019)

Informační systém (Information system/IS) je možné popsat jako soustavu programů a technického vybavení, která má plnit úkoly nezbytné pro fungování organizace. K tomuto systému přistupují uživatelé najednou a mají k dispozici stejná data, se kterými mohou dále nakládat podle přidělených oprávnění. (Pavlíček et al., 2017)

Internet věcí (Internet of Things/IoT) je součástí internetu, složenou s fyzických a virtuálních věcí. Tyto věci mají svou identitu a jsou schopné komunikovat mezi sebou i se svým okolím a spouštět tak procesy bez nutnosti lidského zapojení. Propojení těchto zařízení nabízí možnost pokročilých služeb, které monitorují a řídí prvky ve svém okolí. (Pavlíček et al., 2017)

Opatření (Security measure) je prostředek navržený pro zmírnění vlivu hrozby na aktiva omezením zranitelností nebo možného dopadu hrozby. Opatření se navrhují jako způsob pro předcházení vzniku škody nebo pro usnadnění vyrovnání se z vzniklou škodou. Může být realizováno jako režimový či operační postup, procedura, technické řešení nebo jakýmkoliv jiným způsobem zajišťujícím dostatečnou efektivitu. Efektivita opatření se odvíjí od implementačních a provozních nákladů a schopnosti opatření minimalizovat hrozby. (Smejkal et al., 2019)

Riziko (Risk) je chápáno jako potenciál určité hrozby k páchání škod. Lze jej popsat jako pravděpodobnost, při které nastane nežádoucí jev, který působí na zranitelnost aktiva a má proto negativní dopad na informační systém, jeho prvky, uživatele nebo organizaci jako celek. Významnost tohoto rizika se vyjadřuje pravděpodobností jejího skutečného výskytu a možnými následky, které může způsobit. (Kolouch, Bašta, 2019)

Zranitelnost (Vulnerability), nebo také slabina, je nedostatek v posuzovaném systému, který může být zneužit k působení škod na aktivech či jejich úplnému zničení. Zranitelnost je tedy slabé místo, které může být využito hrozbou, a to může vést k neoprávněným přístupům ke zdrojům a aktivům daného subjektu. Lze rozlišovat typy zranitelností podle jejich původu či charakteru hrozby. Obecně může být zranitelnost fyzická, technická, nosičů dat, komunikační či personální. Fyzickou zranitelností se myslí prostorová zranitelnost, která zahrnuje prostředí, ve kterém jsou počítačové systémy uloženy. Technická zranitelnost se projevuje softwarovou chybou systému nebo poruchou zařízení. Zranitelnost nosičů dat může způsobit ztrátu dat, jejich nečitelnost či vymazání. Komunikační zranitelnost hrozí přerušením komunikačního spojení, odposlechem přenosu informací a jejich narušením. Personální zranitelnost je zapříčiněna lidskou chybou, úmyslným jednáním či nedbalostí. (Doucek et al., 2019)

1.2 Bezpečnost informačních systémů

Bezpečnost informací a informačních systémů lze chápat jako schopnost systému odolávat, na přiměřené úrovni, pokusům o narušení důvěryhodnosti, dostupnosti a integrity skladovaných, přenášených nebo zpracovávaných dat a k tomu přidružených služeb a procesů. Jako hlavní cíle informační bezpečnosti je možné chápat udržená těchto charakteristik informací:

Důvěrnost (Confidentiality) – Zajištění, že daná informace není přístupná osobám k tomu neautorizovaným. Toho se dosahuje zajištěním adekvátních omezení a ověření přístupu k informacím, případně jejich kontrolovaným zveřejňováním a procesy pro ochranu soukromí nebo chráněných informací.

Integrita (Integrity) – Zachování celistvosti a kompletnosti informací. Zaručení přesnosti a neporušenosti informací lze zajišťovat ochranou před jejich modifikací, nahrazením špatnou informací nebo zničením. Integrita informací zaručuje, že důvěrná a citlivá data nebudou upravena nepovoleným či nevědomým způsobem.

Dostupnost (Availability) – Informace musí být na vyžádání dostupná k využití autorizovanými uživateli. Zajištění včasné a spolehlivé dostupnosti informace je zásadní pro její užitečnost. Nedostupná informace má stejnou hodnotu, jako by žádná informace neexistovala, tedy žádnou. (ČSN EN ISO/IEC 27000)

Tyto klíčové charakteristiky informace jsou zásadní pro užitečnost a využitelnost informací a bývají také označovány jako CIA triáda. Při narušení kterékoliv z výše zmíněných vlastností dochází ke ztrátě spolehlivosti informace. Jelikož informace získává na významu právě pouze pokud je považována za spolehlivou, je potřeba tuto spolehlivost udržet. Z takového důvodu lze určit ještě další parametr informace, který pomáhá udržovat spolehlivost informací:

Autentičnost (Authenticity) – Stav, který je cílem bezpečnosti informací. Popisuje hodnověrnost informace a schopnost zajistit, že svěřenou informaci je možné sledovat zpět k jejímu původu, případně ověřit její pravost. (ČSN EN ISO/IEC 27000)

1.2.1 Klasifikace hrozeb

Hrozby pro informační systémy jsou v zásadě útoky na jeden či více zmíněných aspektů systému, které usilují o získání prospěchu ze slabin a zranitelností daného systému. Jejich původ může být z různých zdrojů a s různou mírou závažnosti, ale v každém případě je nezbytná určitá míra struktury a organizovanosti, která umožňuje se s hrozbami vypořádat. Základním bodem pro jakoukoliv snahu o eliminaci hrozeb je definování informačního systému, ke kterému je hodnocení rizik vztahováno. Je nezbytné určit funkční i fyzické hranice systému, stanovit za jakým bodem už se nejedná o odpovědnost určeného systému. Jsou-li jasně definované hranice systému, je možné se zaměřit na to, jakým hrozbám je systém vystaven na základě vnějších a vnitřních zranitelností. Tyto hrozby je možné velmi obecně zařadit do několika typů blíže popsaných v tabulce níže.

Tabulka 1 - Klasifikace hrozeb

Typ hrozby	Popis hrozby	Dotčená aktiva a struktury	Možná řešení, úpravy systému
Spoofing	Uvedení neplatné identity	Autentičnost dat Ověření uživatele	Přísnější rozpoznání uživatele
Manipulace	Neoprávněná úprava obsahu	Integrita dat Struktura dat	Změna oprávnění uživatele
Zveřejnění	Neautorizovaný přístup k datům	Důvěrnost dat Soukromí	Oddělení dat (data fencing)
Odepření přístupu	Znemožnění využití zdrojů systému	Dostupnost dat Přístup k systému	Filtrování přístupu (packet filtering)
Zvýšení výsad	Nepovolené zvýšení přístupových práv	Důvěrnost dat Autorizace přístupu	Ověření autorizace Kontrola přístupu

Zásadní je uvědomit si, jaké hrozby jsou pro kontext systému a jeho fungování hlavním nebezpečím, které může působit nejzávažnější škody. Po vybrání hrozeb je potřeba vyjasnit situace při kterých by mohl být stanovený typ útoku úspěšný a vytvořit obranný model pro každý z vybraných útoků. Následně proběhne výběr optimálních řešení založený na jejich efektivitě a požadavcích na zdroje. Výběr optimálního řešení by měl zohledňovat účinnost řešení vyváženou pravděpodobností výskytu hrozby a závažnosti důsledků, a také cenu vývoje a implementace daného řešení. Takovýto postup vyžaduje zapojení všech zúčastněných na bezpečném fungování systému a bude vyžadovat průběžné hodnocení a úpravy zohledňující nové informace a situace. (Kostopoulos, 2013)

1.2.2 Fyzická bezpečnost

Ačkoli to může působit jako samozřejmost, fyzická bezpečnost je základem, který není možné opomíjet, protože sebelepší programové zabezpečení bude k ničemu, pokud útočník přijde až k danému zařízení a fyzicky se na něj připojí. Z tohoto pohledu se fyzická bezpečnost informačních systémů skládá z několika prvků. Tím základním je zajištění perimetru, tedy stanovení oblasti, ve které se nachází chráněná aktiva. K určení optimálního zabezpečení se provádí analýza rizik, která umožňuje posouzení, jaká opatření jsou pro ochranu jednotlivých prostor a aktiv nejúčinnější. Zde se nabízí různé mechanické zábrany a elektronické poplachové systémy. Aby však byla tato opatření efektivní je potřeba zajistit kontrolu přístupu. Ta slouží k tomu, aby se do určeného perimetru dostaly pouze osoby oprávněné ke vstupu. Systémů pro kontrolu je k dispozici mnoho. Začínají klasickými zámky, přes elektronické přístupové systémy, až po fyzickou kontrolu ostrahou objektu při vstupu. Pro maximální zabezpečení aktiv je vhodné využívat kombinaci těchto systémů, kdy kromě kontroly přístupu dochází i k druhotné autentizaci, což může zabránit zneužití ztraceného klíče či přístupové karty. Je-li zamezen nežádoucí přístup do určeného perimetru, je třeba se zaměřit na vnitřní bezpečnost, kde se věnuje zabezpečení prostor, kde se jednotlivá aktiva nacházejí. Jedná se o přístup do jednotlivých místností, režim provozu v případě, že zůstává budova prázdná a bezpečné uložení nosičů dat. Za zmínku zde stojí takzvaně politika čistého stolu a prázdné obrazovky, která říká, že během nepřítomnosti uživatele v kanceláři by měl být jeho počítačový systém uzamčený a veškeré pracovní dokumenty uschovány tak, aby nehrozilo jejich zneužití. Dodržování výše zmíněných doporučení by mělo zabránit nepozorovanému průniku osob k počítačovým a informačním systémům, ale je žádoucí vnímat zabezpečení jako celek složený z několika samostatných vrstev, a proto není žádoucí spoléhat se pouze na jednu vrstvu. Je vhodné všem zařízením zajistit ochranu před rozebráním, úpravou nebo připojení škodlivých periferií. Běžné počítačové systémy, jakými jsou laptopy, tiskárny a stolní počítače se většinou nachází v prostorách, které nejsou trvale zabezpečené a monitorované. K jejich zabezpečení je možné využít uzamčení nebo šifrování pevného disku, které i v případě krádeže zabrání zneužití obsahu. Šifrování je do jisté míry možné i u tiskáren a dalších kancelářských přístrojů. Důležité je také myslet na zařízení, která umožňují odposlech přenášených dat. Taková zařízení se dají připojit mezi počítač a jeho periferie a jejich odhalení bez fyzické kontroly zařízení je téměř nemožné. (Kolouch, Bašta, 2019)

1.2.3 Programová bezpečnost

Software a jeho vývoj jsou silně závislé na zkušenostech, expertíze a dostupných nástrojích vývojáře. Jelikož je tento vývoj plně intelektuálním procesem, omezují jej lidské schopnosti. Z pohledu vývojáře lze stanovit tři základní parametry každého softwarového projektu. Jedná se o čas dodání, cenu a funkční kvalita. Tyto parametry jsou vzájemně propojeny a pokud má být jeden ze zmíněných parametrů na velmi vysoké úrovni, je nutné slevit z nároků ve zbylých dvou. Pro zajištění maximálního softwarového zabezpečení je proto brát ohled i na výše popsané a počítat s tím například při objednávání vlastního informačního systému. Žádný software není dokonalý a nástroje kybernetických útočníků se neustále vyvíjí, proto je naprosto zásadní udržovat veškeré programové vybavení na nejaktuálnější verzi. Ideální je využít možnosti vydavatele programu, který jistě pravidelně informuje o nových aktualizacích. Dalším podstatným opatřením je ověřování dat, a to ještě před jejich přijetím, stejně jako ověřování příjemce, které musí proběhnout před odesláním, aby nedošlo k úniku dat. Jsou-li data ukládána, měla by být ukládána do zabezpečeného úložiště. Pro případ selhání některého výše zmíněného opatření je důležité mít nastavený systém varování, který informuje o vzniklém problému, aby bylo možné zahájit jeho vyšetřování. Takový varovný systém by měl mít několik prostředků pro doručení varovné zprávy, například chybové hlášení přímo v aplikaci, email nebo SMS zpráva pro pověřené osoby. Pro ochranu před cíleným útokem se využívá anti malware programů, které jsou nezbytné na serverových zařízeních i počítačových systémech pro uživatele. Vzhledem ke vzniku nových útoků, založených na nově objevených zranitelnostech je potřeba anti malware programy aktualizovat a doplňovat o nové poznatky z databází malware a zranitelností. (Evans, 2019)

Za malware lze obecně považovat jakýkoli škodlivý software, který se zpravidla bez vědomí uživatele dostane do jeho zařízení, kde následně skrytě působí škody formou modifikace souborů a dat, sledováním a odesíláním dat na jiné zařízení, zobrazováním nevyžádaných reklam nebo dokonce žádáním výkupného pod hrozbou odstranění dat v zařízení. V případě, že je napadené zařízení zapojené do počítačové sítě, může se malwarový program pokusit rozšířit do dalších zařízení, proto je nutné tyto škodlivé programy odhalit co nejdříve, než jsou schopné napáchat nezvratné škody na napadeném zařízení. (Kolouch, Bašta, 2019)

1.2.4 Personální bezpečnost

Lidé jejichž činnost spočívá v práci s internetem nebo jiných způsobech nakládání s daty, se mohou velmi snadno stát slabým článkem v bezpečnostním systém. Každá aktivita, spojená s přístupem k informačnímu systému, by měla být prováděna s ohledem na bezpečnostní politiku a opatření organizace. Nezanedbatelná část útoků probíhá zevnitř nebo s interní pomocí, ať už je tak činěno úmyslně či nikoliv. Zranitelnosti v oblasti personálu mohu být rozděleny na dva základní typy. Tím prvním je osoba, které bylo svěřeno oprávnění k nakládaní s citlivými daty, ale svým přístupem a zanedbáním opatření tato osoba vystavuje informace nežádoucímu zveřejnění. Toto může být způsobeno ztrátou pracovních zařízení jako jsou mobily a laptopy, kompromitací přístupových hesel nebo nezabezpečení počítačových systémů při opuštění pracovního místa. Druhým typem jsou osoby, kterým byla svěřena oprávnění, ale tyto osoby jich následně zneužijí, pravděpodobně pro získání finančního prospěchu. Základním opatřením v tomto směru je poskytovat uživatelům informačního systému oprávnění k nakládání s daty pouze v rozsahu, který je pro ně nezbytně nutný. Zřízené oprávnění by měly mít stanovenou konečnou platnost, která zabrání v přístupu osobám bez aktuálního oprávnění. Podstatné je také vytváření záznamů o úspěšných i neúspěšných pokuse o přístup. Takové záznamy umožňují spuštění včasných varování při podezření na zneužití zranitelnosti nebo nestandardního chování. (Kostopoulos, 2013)

Kromě technických opatření týkajících se přímo informačních systémů je důležité myslet i na opatření režimová. Pravidelné školení umožňuje zaměstnance organizace nejen seznámit s bezpečnostními pravidly, ale také vysvětlit jakému slouží účelu a jaké může mít jejich nedodržování následky. Jestliže uživatelé neporozumí významu nastavených postupů, lze předpokládat, že je dříve či později začnou obcházet a ignorovat. V takovém případě je potom na místě zaměstnance informovat o důsledcích, které jejich jednání v rozporu s bezpečnostními pravidly může mít. V případně závažného nebo opakovaného porušování stanovených směrnic, a to nejen v oblasti bezpečnostní, bude nezbytné provést formální disciplinární řízení. V neposlední řadě je také potřeba zohlednit přístup k ukončení pracovního poměru. Je nezbytné mít stanovený jasný proces a odpovědnost za jeho průběh. Žádoucím výsledkem je vrácení pracovních předmětů a zrušení přístupových práv přidělených zaměstnanci pro výkon pracovní činnosti. Velmi podobně lze přistupovat ke změně pracovní pozice, kde je nutné revidovat aktuální nezbytný přístup pro výkon svěřené zaměstnanecké pozice. (Kolouch, Bašta, 2019)

1.2.5 Bezpečnost komunikačních sítí

Rizikem postihujícím komunikační sítě je možný odposlech přenášených dat a případně také modifikace těchto zpráv. Technikou k zabezpečení komunikace je takzvaně segmentace komunikační sítě. Jedná se o rozdělení sítě na samostatné zóny, které je možné odděleně řídit a monitorovat. S tím se pojí vytvoření virtuální sítě LAN (Local Area Netvork), kdy je pod existující fyzickou sítí vytvořena další, virtuální. Metody zařazení do této virtuální sítě je možné podle portu switche, MAC adresou nebo podle protokolu přenášeného paketu. (Smejkal et al., 2019)

Dále je možné využívat ochrany sítí na úrovni řízení komunikace sítě a kontroly přenášených dat pomocí ACL (Access Control List), fungujících na principu omezení prostupů z počítačové sítě a dovnitř počítačové sítě. Je to také způsob řízení přístupu jednotlivých uživatelů nebo jejich skupin k vybraný složkám a souborům. K účelu omezení přístupu slouží také například firewall, který má za úkol zabránit nežádoucí síťové komunikaci mezi různými sítěmi nebo rozhraním koncového počítače a sítí. Na každý paket, který přichází nebo odchází ze zařízení provozujícího firewall, je aplikován filtr, který podle nastavené bezpečnostní politiky povolí nebo zakáže přijetí nebo odeslání paketu. Dle typu fungování lze rozlišit dva typy firewallu. Prvním jsou paketové filtry, pracující na síťové vrstvě a umožňují tak pouze povrchní filtrování, představují ale levnou a velmi rychlou variantu zřízení firewallu. Druhou možností jsou Stavové paketové filtry, fungující podobně jako předchozí typ, ale umožňují ukládat informace o předchozích spojeních, díky čemuž nemusí firewall rozhodovat o každém paketu zvlášť, ale může využít uložené informace o povolených spojích. Možnost omezit, která strana zahájí spojení je potom další výhodou tohoto typu. Pakety pocházející z druhé strany firewall propustí pouze jako odezvu na zahájení komunikace první stranou. Současně ale stavové filtry obvykle umožňují kontrolou obsahu paketů nebo analýzu aplikačního protokolu. Specifickým využitím firewallu jsou takzvaně aplikační brány neboli proxy firewally, které slouží jako prostředník mezi dvěmi sítěmi. Probíhá to tak, že proxy přijme požadavek zdrojového systému, ten zpracuje a následně předá cílovému systému, který svou odpověď vátí proxy bráně, která ji následně předá zdrojovému systému. Tato funkce umožňuje odhalit útoky a chyby v protokolu, pro který je určena, nebo rozpoznat útoky hrubou silou a tyto data odstranit z komunikace. (Kolouch, Bašta, 2019)

1.3 Kybernetická kriminalita

Definování kybernetické kriminality jako pojmu je velmi obtížné, protože různé definice vznikají a následně se ruší při jejich zastarání z důvodu technologického pokroku. Z toho také vyplývá že to, co je v současné době považováno za kompletní definici kybernetické kriminality se může s dobou opět ukázat jako zastaralé, proto je vhodné u toho to pojmu volit spíše obecnější formulaci.

Pod pojmem kybernetická kriminalita, lze vnímat souhrn trestné činnosti týkající se počítačů, informačních systémů, internetu a síťových prvků. Jejím utvářejícím aspektem je, že se odehrává v kyberprostoru. Jedná se tedy o trestné činy proti důvěrnosti, celistvosti a dostupnosti počítačových údajů, projevující se blokováním a poruchami dat nebo zneužitím informačního systému či zařízení. Dále jsou to trestné činy spojené s počítačem, zejména podvody a padělání, trestné činy spojená s obsahem a trestné činy porušováním autorských práv. Z pohledu počítačové kriminality se s rozvojem digitální ekonomiky zvyšuje i počet kybernetických podvodů, mezi těmi nejčastějšími krádež identity. Ta se nejčastěji provádí zjištěním potřebných údajů metodami sociálního inženýrství, získáním údajů přímo z počítače oběti škodlivým kódem nebo vniknutím do databází informačního systému (například finančních společností). Mezi další rozšířené formy podvodů patří také falešné stránky obchodů a investiční podvody. (Završnik, 2017)

Informační systémy, výpočetní technika a další digitální technologie se postupně integrují do všech odvětví lidské činnosti. Do kyberprostoru se přesouvá čím dál více společenských a ekonomických vztahů, čímž vzniká potřeba právně regulovat jednání v tomto prostoru. Z pohledu kyberkriminality se jedná zejména o prostředky trestního práva, kde se ovšem naráží na to, že spáchá-li útočník svou činností útok, který není možné spojit s žádným ustanovením trestního zákona, nebude možné takový čin postihnout. Vzhledem k rychlému vývoji kybernetického prostředí, je obtížné včas reagovat změnou legislativy, která by odrážela současnou situaci, proto může docházet k prodlevě kvůli složitějšímu procesu přijímání úprav zákonů. Bohužel tak dochází k možnosti zneužívání těchto výsledků technologického pokroku pro páchání trestné činnosti, která je obtížně uchopitelná jak po stránce právní, tak i vyšetřování. (Kolouch, 2016)

1.3.1 Právní aspekty kyberkriminality

Jedním ze zásadních legislativních dokumentů, vztahujícím se k této oblasti je zákon o kybernetické bezpečnosti č. 181/2014 Sb., který se upravuje práva a povinnosti osob i orgánů veřejné moci v oblastní kybernetické bezpečnosti. Tento zákon reaguje na směrnici NIS Evropské unie o bezpečnosti sítí a informací. Dále také stanovuje systém zajištění kybernetické bezpečnosti, bezpečnostní opatření a postup kontroly. To vše slouží k nastavení společného standardu kybernetické bezpečnosti, zajišťující určitou míru kybernetické bezpečnosti. (Česko, 2014)

Zákon výše je míněn jako způsob prevence, ale samotné protiprávní jednání se posuzuje podle trestního práva, které rozlišuje několik druhů právní působnosti trestních zákonů, kde z pohledu kyberkriminality je zásadní působnost místní, tedy odpověď na otázku, kde byl trestný čin spáchán? Dle trestního zákoníku České republiky lze ve vztahu ke kyberkriminalitě využít především zásad teritoriality, pokud byl trestný čin spáchán v České republice a není tedy problém na něj vztáhnout české trestní právo. V případě, že došlo k trestnému činu mimo území České republiky, ale na palubě plavidla, letadla, nebo jiného vzdušného prostředku, registrovaného v České republice, posuzuje se jako by se stal na území České republiky. Podle zásady personality se také posuzuje čin spáchaný v zahraničí občanem české republiky anebo takový, který je spáchán na občanu České republiky. Rozhodujícím je tedy zejména místo, kde vznikl následek trestného činu, nebo místo kde došlo k jednání. (Česko, 2009)

Úkolem orgánů činných v trestném řízení je získat dostatek důkazního materiálu, aby bylo možné obžalovaného usvědčit nad veškerou pochybnost. V prostředí kybernetických zločinů se však tohoto stavu dosahuje velmi obtížně. Kyberprostor umožňuje jeho uživatelům zastírat či maskovat svou identitu, například pomocí sítě TOR nebo VPN služeb. Takto získaná anonymita ztěžuje jednoznačné určení útočníka, což komplikuje celý proces trestního stíhání. Protiprávní jednání ve virtuálním prostředí však nemusí mít pouze povahu trestného činu. Může se také jednat o přestupky podle zákona 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Skrze internet tak dochází nejčastěji k přestupkům v souvislosti s porušováním autorských práv a nakládáním s cizím duševním vlastnictvím nebo přestupky proti právu na ochranu osobnosti, kde se může jednat o narušení soukromí, ublížení na cti nebo také působení újmy pro příslušnost k etnické, náboženské či jiné skupině, případně pro jeho věk zdravotní stav politické a jiné smýšlení. (Kolouch, 2016)

1.3.2 Škodlivý kód

Za škodlivý kód neboli malware, se považuje libovolný software, který je využíván k narušení běžné činnosti počítačových systémů. Toto zahrnuje získávání informací nebo přístupu k danému systému. Podle účelu jsou rozřazovány malwary kategorií se samostatným pojmenováním. Konkrétní malware může plnit jeden nebo více funkcí.

1. **Adware:** Software, zobrazující uživateli na jeho počítačovém systému reklamy, se nazývá adware. Ačkoli se většinou jedná o program, který uživatele „pouze“ obtěžuje reklamními sděleními, může být tento typ malware spojen se spywarem.
2. **Spyware:** Právě spyware bývá často součástí jiných typů malware programů a zaměřuje se na získávání dat uživatele systému, na kterém se nachází. Zjištěná data jsou poté odesílána útočníkovi, který je dále zpracovává za účelem cílené reklamy nebo pro další typy útoku za pomoci sociálního inženýrství.
3. **Keylogger:** Specifickým typem spyware programu je keylogger, tedy program zaznamenávající jednotlivé stisky kláves na napadeném zařízení, který tímto způsobem získává přihlašovací údaje k účtům, na které se uživatel přihlašuje.
4. **Virus:** Další skupinou jsou viry, což je označení, které laická veřejnost používá pro jakýkoliv typ malwaru. Viry fungují na principu přidružení škodlivého kódu k jinému spustitelnému souboru. V momentě jeho spuštění se virus reprodukuje se snahou o rozšíření do co nejvíce zařízení. Kromě toho může mít virus různé účinky od neškodných audiovizuálních efektů, přes zahlcení systému, po celkové zničení napadeného systému.
5. **Červ:** Jako viry bývají občas označováni i takzvaní červi, kteří však na rozdíl od viru nepotřebují pro své rozšíření spustitelný soubor a dokáží se šířit samostatně. Červi využívají napadené zařízení k odeslání svých kopií do co největšího počtu zařízení pomocí sítové komunikace.
6. **Trojský kůň:** Následně existují programy označované jako trojské koně, jež bývají přidružené k jinému bezpečnému programu nebo samy na první pohled působí jako užitečný program, který si uživatel sám nainstaluje. Takový trojský kůň má ale kromě svého viditelného využití i skryté funkce o kterých uživatel neví a při jejich aktivování útočníkem mohou působit modifikace v systému a sítích ke kterým jsou připojeny.

7. **Rootkit:** K zamaskování všech výše zmíněných škodlivých programů v systému využívají útočníci rootkity. Rootkit označuje programy, a obecně i technologie, které umožňují změnu chování operačního systému tak, aby zabránily odhalení malwaru v zařízení.
8. **Ransomware:** V neposlední řadě patří do skupiny malware programů ransomware, sloužící k vymáhání výkupného po uživateli napadeného systému. K tomu dojde buď uzamčením uživatelských dat v zařízení nebo kompletním omezením funkčnosti systému. (Kolouch, 2016)

1.3.3 Sociální inženýrství

Jedná se o souhrnný název pro sociálně-psychologické metody, kterými útočníci získávají informace o svých obětech, které je následně možné zneužít. Prozrazení citlivých informací samotným uživatelem je častou formou, kterou útočníci získávají přístup do chráněných systémů, jakými jsou emailové schránky, sociální sítě, bankovní účty a další. Skrze sociální sítě a diskuzní fóra zjišťují data narození, jména dětí a domácích mazlíčků, které jsou často základem hesel uživatelů. Do kategorie sociálního inženýrství patří také phishing, jehož název vznikl jako složenina anglických slov „password“ a „fishinig“, v českém překladu jako „heslo“ a „rybaření“. Tato metoda prostřednictvím rozeslaných elektronických zpráv usiluje o získání přihlašovacích údajů tím, že napodobuje styl a grafiku vybrané společnosti od jejíhož účtu se snaží získat přihlašovací údaje. Klamavou zprávou, upozorňující na událost vyžadující ověření přihlášením k danému účtu, se snaží uživatele přesměrovat na stránku pod kontrolou útočníka, kde je možné ověření přihlášení provést a tím útočník získá údaje k účtu. Modifikovaná verze tohoto útoku nabízí příjemcům klamavé zprávy možnost získat významný benefit jako výhru v loterii, výhodné zaměstnání nebo provizi z finanční transakce. Po zahájení konverzace je z uživatele vylákána částka, která je údajně nezbytná pro nutné vstupní výdaje a následně útočník přestane jakkoliv reagovat. Podobných metod sociálního inženýrství je mnohem více, ale jejich společnými rysy je působení na lidské vlastnosti, zejména pak důvěřivost, které uživatele nevědomky vmanévrují do situace, kdy dobrovolně vydá své osobní údaje. Mezi hlavní motivátory, kterými útočníci manipulují svými oběťmi jsou vidina finančního zisku, strach ze ztráty majetku nebo financí a soucit s tíživou životní situací. (Pavlíček et al., 2017)

1.3.4 Kryptografie

Kryptografie je vědním oborem, který se zabývá zabezpečení zpráv, dat a informací pomocí matematických metod zajišťujících zachování důvěrnosti a autentičnosti, tedy zabraňuje přístupu neoprávněných osob k informaci a zajišťuje, aby byla informace zachována jako celistvá, neporušená a spolehlivá. S kryptografií je možné se setkat nejčastěji právě v informačních a komunikačních systémech a k zajištění správného chodu těchto systémů je potřeba chránit nejen prvky ze kterých se tyto systémy skládají, ale také informace, které jsou uloženy nebo přenášeny pomocí těchto systémů. K zajištění autentičnosti a důvěryhodnosti je možné v praxi využít několika způsobů. Optimálním cílem pro ochranu zpráv je pokud se útočník o existenci zprávy vůbec nedozví, k čemuž slouží metody pro skrytí zpráv. Pokud si útočník není vědom toho, kde se zprávy nacházejí, není schopen je odposlouchávat či manipulovat. Příkladem skrytí zprávy může být vložení zprávy do obrázku nebo jiný způsob maskování skutečného účelu. Pokud však není možno zprávu skrýt, pak je usilováno o zamezení přístupu k informaci. Pro zamezení přístupu k informaci se využívají techniky zamezení nebo řízení přístupu, které spočívají v tom, že přístup k informaci mají pouze osoby s příslušným oprávněním. Útočník tak nemá možnost takto chráněné zprávy číst ani modifikovat. To je možné aplikovat použitím přenosu informace komunikačním kanálem s omezenou dostupností nebo fyzickým zamezení přístupu neoprávněným osobám do prostor, kde je informace uložena. Posledním možným způsobem ochrany informací je takzvaně transformace informací. Pro účely zajištění důvěrnosti informace je původní posloupnost znaků, které představovaly danou informaci upravena na jinou posloupnost. K této nové posloupnosti může mít přístup i útočník, jelikož podstata této metody spočívá v nemožnosti využití informace, pokud není navrácena do původní posloupnosti. K tomu slouží další, zpravidla utajovaná informace, která umožňuje opětovné navrácení informace do původní posloupnosti. (Codings, 2019)

2 SOUČASNÉ TRENDY V INFORMAČNÍ BEZPEČNOSTI

Z pohledu uživatele patří, u poskytovatelů služeb v oblasti informačních technologií, mezi hlavní trendy současné doby personalizovaný přístup zaměřený na zákazníka, umožňující okamžitý přístup k požadovaným informacím a službám přes cloudové nástroje. Obecně je tedy čím dál více informací na dostupných online a množství těchto dat se neustále zvětšuje. Nejedná se přitom pouze o data, ke kterým si uživatelé přejí přistupovat, ale také jejich osobní data, umožňující výše zmíněnou personalizaci a doporučování dalších služeb podle analýzy preferencí a návyků uživatele. Specifickým aspektem současného nakládání s informacemi je, že jsou tyto informace roztříštěny po mnoha zdrojích a nosičích jakými jsou mobilní telefony, počítače, cloudová úložiště a také internet věcí (anglicky Internet of Things – IoT). Toto způsobuje, že zabezpečení všech zdrojů a nosičů je velmi komplikované, což následně vede riziku úniku informací v rámci narušení jejich důvěrnosti. Široká škála zdrojů a nosičů slouží pro usnadnění přístupnosti dat pro uživatele, což je sice potenciálním bezpečnostním rizikem, ale tato personalizace také umožňuje, při srovnání s běžnými návyky uživatele, zpozorovat abnormality a na základě toho vyžadovat vyšší míru ověření. (Zhou et al., 2018)

Pro úspěšné zajištění informační bezpečnosti institucí se považuje za klíčové adekvátně zabezpečit tři hlavní pilíře, kterými jsou lidé, procesy a technologie. Za nejslabší článek tohoto rozdělení jsou nejčastěji považováni lidé. Procesy se myslí připravenost organizace na realizaci bezpečnostních opatření a plánů, ať už formou školení zaměstnanců, režimových opatření, či vyhrazení části rozpočtu na zajišťování bezpečnosti informačních systémů. Technologickým aspektem je potom samotné použití bezpečnostních systémů, fyzické zabezpečení dat organizace a také využití vhodného hardware a software vybavení. Jednou z výzev při technologickém zabezpečení je nepochybně rychlý vývoj, který vyžaduje průběžnou aktualizaci všech opatření a jejich vzájemného propojení. Zde lze pozorovat, že značná část incidentů, které se dotýkají citlivých informací organizace, jsou silně ovlivněny zejména chováním uživatelů uvnitř instituce. Ačkoli jsou tedy útoky technického charakteru stále relevantní hrozbou, rozšiřujícím se trendem jsou útoky cílené přímo na uživatele, nikoliv jejich informační systémy jako takové. K takovému útoku je využíváno zanedbávání režimových opatření instituce nebo sociálního inženýrství. (Bhaharin et al., 2019)

2.1 Informační bezpečnost ve světě

Do segmentu informační bezpečnosti je zahrnuto široké odvětví činností, které zahrnuje technologické řešení, behaviorální, organizační a řídící přístupy. Současné trendy v oblasti informační bezpečnosti se zaměřují na několik aspektů:

1. **Detekce průniků** je oblast zaměřená na zjišťování slabých míst systému a jejich zabezpečení. Zjišťování externích útoků nebo vnitřního zneužití je podstatnou částí řádného zabezpečení informačního systému. Ke zmíněné detekci může docházet buď v reakci na zjištěný útok nebo způsobem neustálé kontroly, pro kterou se nabízí systém ověřování autorizace nebo systém hledání anomálií. Detekování průniků do systému si tedy klade za cíl odhalit slabá místa a eliminovat, případně minimalizovat možnost úniku informací, a tedy narušení jejich důvěrnosti a integrity.
2. **Ochrana soukromí** rezonuje v institucionálním i osobním prostředí jako jedno z hlavních bezpečnostních témat. Velké množství osobních informací je náchylné ke zneužití jako třeba finanční informace, osobní přístupové údaje, informace o poloze a zdravotní záznamy. Záměrem technologií v této oblasti je omezit dostupnost dat pro útočníka při zachování veškerých funkcionalit pro oprávněného uživatele. K tomuto účelu je možno využít několik metod šifrování dat, jejich směrování přes zabezpečenou síť v případě nebo anonymizací.
3. **Kryptosystémy**, zaměřené na převod běžného textu do šifrovaného textu, jsou složeny z šifrovacího algoritmu a infrastruktury nezbytné k jeho aplikaci. Z hlediska informační bezpečnosti plní kryptosystémy úkol zajištění soukromí, a tím i důvěrnosti informací, a také mohou potvrzovat jejich autentičnost a integritu. Tímto způsobem je zajištěno, že informace přenášená veřejnými kanály nebude dostupná neautorizovaným uživatelem a zároveň mohou často sloužit k ověření původu informace a její celistvosti.
4. **Zabezpečení datových služeb**, s rozvojem cloudových procesů získává na důležitosti. Tento způsob „outsourcingu“ úložiště a služeb nabízí uživatelům benefity okamžitého přístupu kdekoli, kde si je uživatel vyžádá a odstranění nutnosti starat se o uložení dat. Nicméně, tento přístup má i svá negativa ve formě odevzdání kontroly nad daty, kdy selhání cloudového systému může vést k porušení či ztrátě dat nebo jejich neautorizovanému zveřejnění. Může tedy být narušena důvěrnost, integrita i dostupnost dat.

5. **Malware** hrozby jsou software vytvořený za účelem působit škody. Čím dál atraktivnějším cílem pro tyto softwarové útoky se stávají chytré telefony, jelikož obsahují velké množství osobních informací uživatelů, které je možné nadále zneužít pro finanční zisk. Využívají se různé metody pro analýzu malware programů a implementaci opatření proti nim, ale při výskytu nového typu není možno předvídat, jaké zranitelnosti bude využívat, proto se jedná o náročný proces.
6. **Bezpečnostní management** zahrnuje činnosti od zajišťování režimových a procesních opatření na úrovni celé organizace, až po řízení jednotlivců. I po zohlednění všech předchozích kategorií je stále nejrozsáhlejším problémem závislost bezpečnosti informačního systému na lidském a řídícím faktoru. Proto je nezbytný vyrovnaný přístup po technické i personální stránce zabezpečení. Aby bylo možné hrozbám předcházet musejí si uživatelé informačního systému uvědomit jejich existenci, jinak nebudou schopni jim předcházet bez ohledu na implementovaná technická opatření. (Shiau et al., 2023)

Při zaměření na korporátní oblast velkých firem a státní organizace jsou dominantními problémy kybernetické a informační bezpečnosti ransomware a phishing. Dochází k rozvoji ransomware jako služby, kdy jedna samostatná skupina zajišťuje vývoj programového řešení pro vydírání, které následně poskytuje dalším skupinám, realizujícím samotný ransomware útok, za podíl na zisku. Tato distribuce významně rozšiřuje řady potenciálních útočníků. Ačkoli většina útočníků využívajících tuto metodu aplikuje ransomware na jakékoli systémy, ke kterým získají přístup, ti sofistikovanější si zaplatí za získání přístupu do vybrané sítě od jiných kybernetických kriminálníků, specializujících se na pronikání do systémů. Tuto zvýšenou spolupráci lze pozorovat napříč celým odvětvím kyberkriminality a kybernetická a informační bezpečnost tak získává čím dál více na důležitosti. Druhým zmíněným útokem je phishing, česky také rhybaření, které se projevuje zejména svou schopností působit na velké množství potenciálních obětí a kvůli tomu je svým celkovým dopadem řádově výše než jakákoliv jiná hrozba. Rozšířením práce z domu v letech 2020 a 2021 došlo k významnému nárůstu phishingových útoků cílených na měnící se pracovní prostředí. Jako u ransomware, i operátoři phishingu se snaží zajistit větší věrohodnost svých podvodů odesíláním zpráv z kompromitovaných účtů s vyšší mírou důvěryhodnosti než účty čerstvě založené, a za tímto účelem spolupracují s jinými útočníky na získání kontroly nad cizími účty, které následně využívají ke svým účelům. (Burt, 2022)

2.2 Informační bezpečnost v české republice

Podle dostupných dat dochází v České republice k nárůstu celkového počtu bezpečnostních incidentů. V roce 2023 to bylo 2 752 incidentů, řešených týmem CSIRT.CZ a oproti předchozím letům se jedná až o třetinový nárůst.

Tabulka 2 – Statistika bezpečnostních incidentů CSIRT.CZ

Typ útoku/rok	**2020**	**2021**	**2022**	**2023**
Phishing	738	1277	1485	2064
Malware	216	163	220	163
Spam	109	141	224	352
Jiné	86	56	63	35
Sbírání informací	68	67	69	105
DoS	0	0	0	12
Kompromitace	16	11	0	21
Celkem	**1267**	**1725**	**2067**	**2752**

Z výše uvedeného je patrné, že nejčastějším typem útoku je phishing, jehož nárůst je znatelný po celém světě. Ostatní incidenty mají v porovnání s phishingem výrazně nižší výskyt, ale například sbírání informací není vhodné opomíjet, protože umožňuje útočníkům identifikovat zranitelnosti systému pro zneužití při dalších typech útoků. Nárůst počtu incidentů je spojen s častější hrozbou APT (Advanced Persistent Threat), tedy dlouhodobou pokročilou hrozbou. Tyto hrozby jsou nebezpečné kvůli svému charakteru, který umožňuje útočníkům dlouhodobě udržovat nepozorovaný přístup do daného informačního systému, kde může následně shromažďovat data a provádět špionáž nebo sabotáž systému. (CSIRT.CZ, 2024)

Do budoucna lze očekávat další nárůst incidentů dle statistik výše, ale také další rozvoj ransomware, kde se očekává vyšší aktivita a distribuce ransomwarových prostředků širší skupině útočníků pro rozšíření útočných kampaní. Nicméně se dá předpokládat, že mezi významnými hráči na poli ransomware zůstanou stále stejné skupiny. Opomíjeným problémem je potom internet věcí, u kterého výrobci často přehlížejí doporučené bezpečnostní standardy, což vede ke zneužívání těchto zařízení pro anonymizační sítě nebo botnet sítě pro DDoS útoky. Trendem budoucnosti se také stává využívání umělé inteligence pro generování škodlivého obsahu a pro útoky využívající metody sociálního inženýrství jakými jsou například phishingové útoky. Umělá inteligence najde své uplatnění i při psaní škodlivých skriptů pro web skimming za účelem extrahování dat z HTML formulářů. V neposlední řadě jsou mobilní zařízení, zejména na platformě Android, kde se očekává nárůst hrozeb jako adware a skryté aplikace, generující příjmy z reklam. (ESET, 2024)

3 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V teoretické části této práce byl proveden úvod do problematiky informační bezpečnosti, v rámci kterého byly zakotveny základní pojmy této oblasti, včetně jejich významu a použití. Tato část se věnovala také základním metodám a postupům zajištění bezpečnosti informačních a počítačových systémů od počáteční klasifikace hrozeb přes jednotlivé typy zabezpečení, kterými jsou fyzické, programové personální a zabezpečení komunikací.

Dále se teoretická část práce věnovala aspektům kybernetické kriminality. Zde zkoumala právní zakotvení a důsledky kriminality ve virtuálním prostředí, typy kybernetických útoků, jakými jsou různé škodlivé programy a kódy, nazývané souhrnně ransomware, a také metody sociálního inženýrství, které se stává čím dál populárnějším nástrojem útočníků. V neposlední řadě byl popsán systém a obecný proces kryptografie, zabývající se ochranou dat šifrováním.

V druhé kapitole se práce věnovala současným trendům v informační bezpečnosti a hrozeb, které tato oblast zahrnuje. Z porovnání situace v zahraničí a České republice lze odvodit, že se globálně i u nás rozšiřuje množství kybernetických útoků. U těchto útoků je možné pozorovat nárůst případů, kdy cílem není zařízení nebo systém ale přímo uživatel. Do portfolia útočníků se čím dál častěji dostávají psychologické metody sociálního inženýrství a také se předpokládá rozšíření ransomwarových hrozeb, cílených na firemní prostředí.

II. PRAKTICKÁ ČÁST

4 VÝUKA INFORMAČNÍ BEZPEČNOSTI V OCHRANĚ OBYVATELSTVA

Pro účely této části práce bude prozkoumána výuka informační bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, konkrétně praktických seminářů následujících předmětů v bakalářské úrovni studia:

1. L2SIB – Informační bezpečnost
2. L4SKB – Kybernetická bezpečnost

Absolventi Fakulty logistiky a krizového řízení nacházejí uplatnění u složek integrovaného záchranného systému, orgánech krizového řízení územně samosprávných celků, ale také v soukromém sektoru, jako pracovníci bezpečnostního oddělení, projektového řízení a mnoha dalších odvětví. Z toho důvodu je pravděpodobné, že se ve své praxi setkají s oblastí informační bezpečnosti a budou se podílet na jejím zajišťování. (Univerzita Tomáše Bati ve Zlíně, 2024)

Z výše uvedeného vyplývá, že informační znalosti a dovednosti v oblasti informační bezpečnosti spadají do kompetencí, které by měli studenti této fakulty během studia získat. Ačkoli jsou informační technologie součástí každodenního života, je potřeba zdůraznit, že informační bezpečnost je komplexní oblast, která pro své plné pokrytí vyžaduje specialistu, věnujícího se čistě této oblasti. Proto nelze předpokládat, že studenti oborů, pro které je toto téma důležité, ale nikoli ústřední, se dokáží vyrovnat programátorům bezpečnostních systémů a výuka na této úrovni by o to ani neměla usilovat. Dle profilu absolventa zmíněného výše je žádoucí, aby měli studenti dostatečnou znalost pro pochopení významu doporučených opatření a byli schopni zhodnotit jejich přínos.

4.1 Předmět L2SIB – Informační bezpečnost

Tento předmět si klade za cíl zvýšit povědomí studentů o datové bezpečnosti, hodnotě informací a jejich významu ve společnosti založené na znalostech. Dále si klade za cíl seznámit studenty se současnými informačními systémy a riziky, které s nimi souvisí a také naučit studenty realizovat bezpečnostní politiku organizace v souladu se současnými technologiemi. Obsah předmětu je stanoven následovně:

Úvod do problematiky informační bezpečnosti – základní pojmy.

Legislativa – legislativní rámec a normy informační bezpečnosti.

Teoretický základ – aktuální témata informační bezpečnosti (Cloud, internet věcí, kryptoměny a další).

Systém řízení bezpečnosti informací – specifikace, problematika bezpečnostní politiky informačních systémů.

Řízení informačních aktiv – pojem, specifikace aktiv, hodnocení, zranitelnost.

Hrozby v informační bezpečnosti – specifikace současných hrozeb, vyhodnocení, opatření.

Bezpečnost desktopových operačních systémů Windows, Linux, OS X – historie a současnost.

Bezpečnost mobilních operačních systémů Android, iOS – historie a současnost.

Analýza rizik informační bezpečnosti – vyhodnocení rizik informační bezpečnosti vybraného subjektu.

Řízení přístupu k informacím a informačním systémům, fyzická bezpečnost a bezpečnost zařízení.

Kryptografie – historie, současná kryptografická opatření pro zajištění informační bezpečnosti.

Bezpečnost provozu a komunikací – ochrana proti malwaru, monitorování, bezpečnost přenosu informací, síťová bezpečnost.

Kyberkriminalita a kyberterorismus – počítačové trestné činy, postihy, prevence.

Řízení incidentů bezpečnosti informací – vymezení problematiky, odpovědnost. (STAG UTB, 2024)

Na současných seminářích předmětu Informační bezpečnost se vyučují úlohy, jejich cílem je předat studentům znalost konkrétního způsobu práce s daty nebo bezpečnostními opatřeními. Jednotlivé úlohy, které jsou na seminářích předmětu probírány a následně studenty zapracovány do protokolů, jsou následující:

1. **Vytvoření a požívání virtuálního počítače** jako izolovaného prostředí pro další práci se škodlivým kódem. Toto virtuální prostředí slouží k oddělení části výpočetního výkonu počítače pro vytvoření bezpečného prostoru k experimentování a zkoumání hrozeb oblasti informační bezpečnosti bez ohrožení skutečného počítače. Studenti vytvoří v programu VirtualBox nový virtuální počítač, na který následně nainstalují operační systém typu Linux.
2. **Práce s malwarem ve virtuálním počítači** je další oblast zkoumání, které se semináře věnují. V rámci této úlohy studenti vědomě stáhnou do virtuálního počítače vybraný druh malware, pozorují jeho chování v systému, a nakonec jej vyhledají a odstraní pomocí antivirového programu.
3. **Práce s Cloudovými úložišti** je trendem současné doby, a proto je také zařazena jako úloha, ve které studenti prakticky vyzkouší využití cloudu pro přenos souborů mezi více zařízeními a možnosti nastavení nebo omezení sdílení těchto souborů.
4. **Práce se správcem hesel** jako metoda zabezpečení přístupových údajů. Studenti si v této úloze vyzkoušení práci s programem KeePass, který umožňuje generování a ukládání hesel v zašifrovaném úložišti. Správci hesel umožňují ukládáním hesel a jejich vkládáním do přihlašovacích formulářů snížit nároky na jejich zapamatování, což umožňuje používání obsáhlejších a komplikovanějších hesel.
5. **Deepweb a darkweb** jsou pojmy úzce spojené s informační bezpečností. Jelikož se kybernetiční útočníci často snaží získat přístupové údaje k účtu vedoucímu na deepweb anebo své aktivity skrývají přes darkwebový prohlížeč, studenti se v tomto úkolu naučí rozlišovat tyto pojmy a pomocí prohlížeče TOR se pokusí připojit k webové stránce provozované na darkwebu.
6. **Obnovení smazaných souborů** je úloha, která má za úkol naučit studenty obnovovat soubory, které byly z počítače zdánlivě odstraněny. K tomu využívají programový nástroj Photorec, který dokáže obnovit smazaný soubor, který doposud nebyl přepsán jinými daty, a tudíž ještě má svou stopu na disku počítače.

7. **Analýza rizik v domácnosti** je cvičení, během něhož studenti pomocí nově získaných znalostí hodnotí stav zabezpečení vlastní domácnosti z pohledu informační bezpečnosti. K tomu si stanovují aktiva a hrozby ohrožující tato aktiva. Následně navrhují změny vedoucí k lepšímu zabezpečení těchto aktiv. (Moodle UTB, 2024)

Z výše uvedeného je možné soudit, že tento předmět slouží jako úvod do oblasti informační bezpečnosti, a proto se také zaměřuje na základní bezpečnostní činnosti. Tomu odpovídá také jeho zařazení do druhého semestru prvního ročníku studia, stanovené cíle předmětu. Dle profilu absolventa tohoto předmětu dokáže student prokázat po úspěšném ukončení předmětu tyto znalosti a dovednosti:

Definovat problematiku moderní informační bezpečnosti.

Popsat legislativní ukotvení informační bezpečnosti.

Charakterizovat útoky za účelem narušení bezpečnosti informací.

Charakterizovat problematiku malwaru, jeho druhy a cílení.

Vysvětlit souvislosti ICT pojmů s informační bezpečností.

Navrhnout bezpečné pracovní prostředí v rámci pracovní stanice.

Identifikovat realizované útoky proti informační bezpečnosti v subjektu.

Identifikovat kategorii malwaru a navrhnout způsoby ošetření napadené pracovní stanice.

Zpracovat pojednání o problematice informační bezpečnosti.

Efektivně aplikovat nabyté znalosti z oblasti informační bezpečnosti. (STAG UTB, 2024)

Při porovnání osnov předmětu s náplní seminářů lze vidět, že probíraná témata se prolínají, případně na sebe navazují. Studenti si tak mohou vyzkoušet praktická cvičení vztahující se k tématice probírané na přednáškách a tím hlouběji pochopit danou problematiku. Takový postup se zdá odpovídající úvodnímu charakteru předmětu.

4.2 Předmět L4SKB – Kybernetická bezpečnost

Předmět Kybernetická bezpečnost má za cíl osvojit u studentů principy systémového přístupu ke kybernetické bezpečnosti, pochopení využití kybernetického zákona pro reálné prostředí, a role systémových prostředků bezpečnosti a ochrany obyvatelstva v kyberprostoru. Předmět se také zaměřuje na používání projektovaných prostředků systémů CAD a dalšího programového vybavení laboratoře kybernetické bezpečnosti. Studenti během semestru také zpracují případovou studii na vybrané téma. Obsah předmětu je anotován následovně:

Vymezení bezpečnosti.

Teorie systémů.

Teorie modelů a modelování.

Kybernetika a informatika.

Informační a kybernetická bezpečnost.

Definování kybernetického prostoru.

Modelování kybernetického systému a kybernetické bezpečnosti.

Kybernetický útok, obrana a bezpečnost.

Možnosti systémového rozpoznávání agresivního kyberprostoru.

Zdroje světa o moderním pojetí informační a kybernetické bezpečnosti.

Ochrana informačních a kybernetických systémů a možnosti modelování a simulací.

Vývoj a užití nových prostředků kybernetiky a jejich bezpečnosti.

Řešení projektu kybernetické bezpečnosti prostředky modelování (CAD a další).

Shrnutí látky předmětu a konzultace. (STAG UTB, 2024)

Z výše uvedených osnov vyplývá, že by měl tento předmět navazovat na obsah předmětu L2SIB – Informační bezpečnost. Témata tohoto předmětu pokrývají mnohem širší oblast než předmět předchozí. Jedná se tedy o pokračování pro podrobnější pochopení problematiky informační a kybernetické bezpečnosti. Tyto osnovy také odkazují na seznámení s větším počtem technických prostředků zajišťování kybernetické bezpečnosti jako například modelovací a CAD systémy.

Na současných seminářích předmětu Kybernetická bezpečnost se vyučují následující úlohy:

1. **Definice základních pojmů** kybernetické bezpečnosti je úloha, která má studenty seznámit s terminologií oblasti kybernetické bezpečnosti. Jedná se tedy o úvodní úlohu předmětu.
2. **Logické obvody** využívající pro vizuální popis své činnosti hradla. Studenti se seznámí se základními prvky Boolovy algebry a naučí se vytvářet pravdivostní tabulky podle předložených schémat.
3. **Šifrování** jako způsob zabezpečení informací. Studenti jsou seznámeni se základními principy šifrování a následně si vyzkouší zašifrovat vlastní zprávu pomocí vybraných druhů šifer. Postup šifrování sepisují do protokolu.
4. **Kódování** jako proces rozložení zprávy na jednotlivé bity. Studenti ze své zašifrované zprávy vytvoří takzvaně binární strom, se kterým budou pracovat v následujících úlohách.
5. **Zabezpečení přenosu** pro zajištění správnosti a celistvosti přenášené informace. Toho studenti dosáhnou stanovením parity kódového slova a využitím takzvané křídlové značky.
6. **Přenos** zprávy je simulován zakódováním zprávy dle vybraného typu kódování a průběh přenosu je následně zakreslen do grafu.
7. **Legislativa a normy** v oblasti kybernetické bezpečnosti jsou studenty zpracovány do protokolu popisujícího příslušné zákony a normy, jejich obsah, povinnosti a opatření která stanovují.
8. **Práce s umělou inteligencí** je aktuálním tématem, proto je zařazena i do poslední úlohy kybernetické bezpečnosti. Studenti mají za úkol najít logický rozpor v tvrzeních jazykového modelu ChatGPT.

Velké část seminárních úloh se zaměřuje na jedno téma, a to přenos zašifrované zprávy. Toto téma je probráno tak podrobně, že vzniká pochybnost, jestli student krizového řízení potřebuje znalost rozkládání informace na jednotlivé bity a nejedná se komplexností spíše o úlohu vhodnou pro fakultu či obor věnující se čistě informačním technologiím. Úlohy týkající se legislativy kybernetické bezpečnosti a práce s umělou inteligencí jsou velmi aktuální a pokud by se část času věnovaného šifrování a přenosu zpráv věnovala například kybernetickým útokům a obraně, bylo by to nejspíš přínosnější.

Výsledky učení v tomto předmětu by měly vést k hlubšímu pochopení problematiky kybernetické bezpečnosti. Student, který úspěšně splnil tento předmět by měl být schopný prokázat následující znalosti a dovednosti:

Charakterizovat obsah a souvislosti Zákona o kybernetické bezpečnosti.

Definovat základní pojmy oblasti kybernetické bezpečnosti.

Specifikovat příklady historických kybernetických bezpečnostních incidentů.

Pojednat o problematice teorie systémů.

Pojednat o problematice teoretické kybernetiky.

Zpracovat instrumentální a deskriptivní případovou studii.

Identifikovat teoretické aspekty v reálném kybernetickém bezpečnostním incidentu.

Posoudit povinnosti subjektu v rámci Zákona o kybernetické bezpečnosti.

Identifikovat chráněné zájmy subjektu v oblasti kybernetické bezpečnosti a možné zranitelnosti.

Navrhnout postupy pro zvýšení kybernetické bezpečnosti subjektu.

4.3 Analýza bezpečnostního prostředí

Pro co nejobjektivnější porovnání současných hrozeb v informační bezpečnosti budou všechny hrozby zmíněné v kapitole o současných trendech zpracovány do matice rizik. Porovnávanými parametry budou pravděpodobnost výskytu a závažnost důsledků podle vzorce:

$$R_i = P_i * D_i$$

Kde:

R_i je celková míra rizika *i*,

P_i je pravděpodobnost vzniku rizika *i*,

D_i je dopad způsobený rizikem *i*.

Jednotlivá kritéria budou hodnocena na stupnici od 1 do 5 podle závažnosti, kdy číslo 1 značí nejméně závažné položky a číslo 5 nejvíce závažné položky.

Tabulka 3 – Hodnocení rizik informační bezpečnosti

i	Riziko	Pi	Di	Ri
1	Phishing	5	5	25
2	Ransomware	4	5	20
3	Ostatní malware	3	3	9
4	Sbírání informací, spyware	2	4	8
5	Kompromitace	1	5	5
6	Spam	4	1	4
7	DoS	1	2	2

Z hodnocení lze vyčíst, že nejzávažnějšími útoky jsou zcela bezkonkurenčně phishing a ransomware. Položky v tabulce byly seřazeny podle závažnosti rizika a vysvětlení jednotlivých hodnot je popsáno níže:

1. **Phishing** je statisticky nejčastějším útokem, z čehož lze soudit, že také nejúspěšnějším. Důsledky jsou závažné, jelikož útočník získá kompletní přístup k napadenému účtu oběti, který může nadále vytěžit o data nebo finanční prostředky.
2. **Ransomware** není možné aplikovat tak plošně jako phishing, ale v porovnání s jiným malwarem je jeho popularita významně vyšší. Škody, které může způsobit nejen výkupným, ale současným zničením nebo kopírováním souborů je velmi závažné.

3. **Ostatní malware** ani kolektivně nemá taková počet výskytů jako předchozí dvě položky. Možné důsledky také nejsou v porovnání srovnatelné svou závažností. Zobecněním a seskupením se ztrácí možnost posuzovat specifika jednotlivých typů, ale při jejich rozčlenění by byla pravděpodobnost jednotlivých útoku v měřítku hodnocení zanedbatelná, proto byla přiřazena střední hodnota.
4. **Sbírání informací** a spyware se většinou vykytuje jako součást jiného malwaru, proto je i pravděpodobnost výskytu omezená. Důsledkem však může být ztráta osobních informací a v kombinaci s keyloggerem také přístupových údajů. Tento útok má potenciál působit škody zejména ve spojení s jiným typem útoku.
5. **Kompromitace**, tedy proniknutí do systému hrubou silou je samo o sobě nepravděpodobné, ale možné důsledky úspěšného útoku jsou srovnatelné s phishingem. Pravděpodobnost tohoto útoku se může zvýšit v kombinaci se sbíráním informací, které je následně možné zneužít pro cílený útok.
6. **Spam** je svým výskytem poměrně rozšířený díky možnosti rozeslat jej na velké množství adres, ale jeho dopady jsou velmi malé a nedá se ve spojitosti se spamem mluvit o závažných, pokud vůbec nějakých, škodách.
7. **DoS** útoky se v porovnání s ostatními hrozbami objevují minimálně a v případě výskytu se dají jejich následky relativně snadno minimalizovat, nejedná se tedy v dnešní době o relevantní typ útoku, ačkoli zcela jej zanedbávat by také nebylo vhodné.

Z výše uvedených popisů vyplývá, že hodnotit jednotlivé typy útoku je poměrně složité, protože se jejich metody vzájemně prolínají a doplňují, dá se proto předpokládat, že moderní útočník bude při svém útoku kombinovat několik typů hrozeb. Dle tohoto výčtu by se nejspíš jednalo o systém sběru informací za účelem uzpůsobení dalšího typu útoku speciálně na cíleného uživatele, který má následně vyšší šanci útoku podlehnout. S ohledem na výsledky hodnocení analýze zcela dominují phishing a ransomware. Oba tyto útoky mají společnou vlastnost, kterou je vyvíjení tlaku na uživatele, kterým jej vyzívají k vydání osobních údajů a finančních prostředků. Ačkoli ransomware působí na vybavení počítačového systému, cílí často také na uživatele vytvářením časového tlaku, aby donutil uživatele zaplatit výkupné, například místo kontaktování specialisty. Oba útoky tak zneužívají naivity, nebo neznalosti uživatele a jelikož jsou řádově výše než ty ostatní, vede to k myšlence, že hlavní problém bude ve skutečnosti nedostatečná informovanost o možném nebezpečí.

4.4 Komparace výuky se současnými bezpečnostními trendy

V rámci komparace budou srovnávány hrozby z oblasti informační bezpečnosti se současnou náplní výuky v obou popisovaných předmětech Fakulty logistiky a krizového řízení univerzity Tomáše Bati ve Zlíně. Bude hodnoceno, jestli se dané hrozbě, nebo alespoň podobnému tématu věnuje výuka předmětů zaměřených na informační bezpečnost. Hrozby v tabulce jsou seřazeny od nejzávažnější po nejméně závažnou.

Tabulka 4 – Komparace hrozeb s výukou informační bezpečnosti

Hrozba	**Zařazení do výuky**
Phishing	Není zařazeno do výuky
Ransomware	Není zařazeno do výuky
Ostatní malware	Je zařazeno v rámci L2SIB – práce s malwarem
Sbírání informací, spyware	Okrajově v rámci L2SIB – řízení přístupu k informacím
Kompromitace	Není zařazeno do výuky
Spam	Není zařazeno do výuky
DoS	Není zařazeno do výuky

Ve výuce jsou do určité míry zmíněny všechny výše uvedené hrozby a minimálně v rámci přednášek jsou teoreticky popsány a vysvětleny. Tato komparace zohledňuje pouze úlohy, kterým se věnují praktické semináře, kde není z časových možností obsáhnout všechna témata. Nezařazení všech těchto tedy neznamená nedostatečně aktuální náplň výuky. Jak bylo ale shrnuto na konci předchozí podkapitoly, hrozbám v informační bezpečnosti dominují útoky phishing a ransomware spoléhající na neznalost a naivitu uživatele, proto je vhodné toto zohlednit při určování náplně vyučovaných předmětů informační bezpečnosti. Z průzkumu současných trendů v informační bezpečnosti vyplývá, že útoky využívající sociální inženýrství jako svou hlavní metodu se čím dál více rozšiřují. To je pravděpodobně způsobeno rychlým vývojem informačních technologií a nedostatečném vzdělávání veřejnosti, což vede k nízké míře informační gramotnosti a vysoké pravděpodobnosti, že tito nezkušení uživatelé snadno naletí útočníkovi, kvůli své nepozornosti, nedbalosti nebo útočníkem navozenému stavu naléhavosti. U ransomware útoků lze očekávat podobné důvody pro jeho úspěšnost, s tím rozdílem, že ransomware program musel být nějak vpuštěn do počítačového systému uživatele, kde se ale dá předpokládat, že se tak stalo v domnění, že uživatel stahuje bezpečný soubor či program, který se následně ukázal být ransomwarem. V takovém případě se dá do určité míry spoléhat na antivirový program, pokud je instalován, ale i ten může být ošálen pomocí rootkitu nebo nestihnout reagovat včas. Proto je nejdůležitější prevence a respektování režimových opatření, která mají za úkol předcházet těmto krajním situacím.

5 NÁVRH PRAKTICKÉ ÚLOHY

Z předchozích částí práce vyplynula jako nejzávažnější aktuální hrozba phishing, proto se bude návrh úlohy věnovat tomuto typu útoku. Pro kvalitní zpracování úlohy je podstatné správně porozumění pojmu phishing jako takovému, možným typům a variacím tohoto útoku a jeho základním projevům, podle kterých jej lze identifikovat.

Navrhovaná úloha je zaměřena na výuku informační bezpečnosti v oblasti ochrany obyvatelstva, konkrétně pak pro použití na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Svým rozsahem a složitostí proto měla reflektovat toto zadání jakožto úloha pro studenty oborů, které nejsou primárně zaměřeny na informatiku či programování. Z tohoto důvodu je vhodné předem nastavit parametry či technická omezení, které vymezí úlohu do podoby, která bude přínosná, pochopitelná a zvládnutelná pro studenty bez předchozí zkušenosti s programováním nebo jinými pokročilými technikami z oblasti informatiky.

Aby byla úloha přínosná, měla by mít adekvátní rozsah, který zachová dostatečnou podrobnost tématu, ale zároveň studenty nezahltí informacemi, které nejsou pro jejich působení v krizovém řízení nezbytně nutné.

5.1 Znaky phishingu

Nejběžnějším typem phishingového útoku je emailový phishing. Takový email není adresovaný konktrétnímu uživateli, ale velké skupině adresátů a spoléhá na to, že se některý z nich nechá nachytat. Pokud je phishing cílený na konkrétní osobu či organizaci, jedná se o takzvaný spear phishing. Spear phishingové zprávy jsou zpravidla vytvářeny na míru pro konkrétní cíl. Specifickými případy phishindu jsou vishing, který se provádí přes telefonní hovor, a smishing, což je podvodná zpráva na mobilní telefon.

Mezi hlavní znaky phishingu patří neočekávanost, kdy phishingová zpráva neodpovídá pravidelné komunikaci, a požadavek na poskytnutí osobních údajů. Osobní údaje by žádná seriózní firma po svých klientech nevyžadovala do emailové zprávy, proto lze už v tento moment předpokládat, že jde o podvod. Dalšími znaky jsou přílišná naléhavost a tlak na co nejrychlejší odpověď, aby uživatel neměl čas nad obsahem zprávy přemýšlet, a podezřelá emailová adresa, zejména pak doména, ve které bývá překlep oproti originálu, za který se vydává, nebo podezřelé odkazy přímo v emailu. (Eset, ©2024)

5.2 Parametry navrhované úlohy

Pro maximální užitek úlohy je nutné mít stanoveno, jaký má být výsledek z pohledu studentů. Jaké znalosti mají získat? Jaké dovednosti si úlohou osvojí? Za tímto účelem je potřeba definovat cíle výuky, které má úloha předávat. Za optimálních podmínek by se navrhovaná úloha měla vztahovat k jednomu specifickému tématu a je tedy žádoucí, aby bylo možné dosáhnou uceleného pochopení problematiky během jednoho vyučovacího bloku v délce 100 minut. Zároveň, pokud by úloha trvala déle než dva vyučovací bloky, je pravděpodobné, že studenti budou svou práci odkládat v přesvědčení, že úlohu stihnou dokončit během posledního bloku. Jestliže má být možné úlohu samotnou splnit na jednom semináři, bude nezbytné studenty předem seznámit s probíranou problematikou, aby měli základní povědomí o obsahu úlohy. K tomuto účelu může sloužit předem zveřejněné zadání úlohy, teoretická příprava během přednášky nebo vzdělávací materiál, popisující problematiku vztahující se k úloze. Ideálním řešením je kombinace všech zmíněných prvků, pro co největší připravenost studentů na praktickou úlohu. Vzhledem k charakteru úlohy bude teoretická příprava v rámci přednášky komplikovaná, proto se jako jednodušší možnosti nabízejí zveřejnění zadání úlohy, které nevyžaduje žádnou další přípravu, a příprava a zveřejnění pomocného materiálu. Takový materiál by měl být stručný a využitelný během řešení úlohy studenty, takže jeho důkladné nastudování by nemělo trvat déle, než 30 minut. Nízkým rozsahem a přehledným zpracováním lze zvýšit procento studentů, kteří přijdou do výuky připraveni. Stanovená omezení pro tuto úlohu jsou tedy následující:

1. Úloha má jasně stanovené cíle výuky.
2. Časová příprava studentů před výukou musí být maximálně 30 minut.
3. Samotnou úlohu musí být možné zpracovat během 100 minut na semináři.
4. Pro úlohu bude vypracována pomocný materiál, zadání, a vzorové řešení.

Tyto parametry úlohy budou postupně rozebrány v jednotlivých částech přípravy. Vzhledem k podstatě úlohy není zcela podstatné studenty naučit detailní postup phishingového útoku, ale spíše vysvětlit princip na jakém tyto útoky fungují, aby si dokázali představit, jaké jsou možné nedostatky a chyby útoku. Tato vědomost by měla být studentům prospěšná v případě, že se setkají se skutečným phishingovým útokem.

5.3 Výukové cíle navrhované úlohy

Pro kvalitní zpracování úlohy je důležité vědět, čeho se má jejím zpracováním dosáhnout. Obecně lze říct, že úloha by měla vést k pochopení principu, na kterém funguje phishingový útok, seznámení s metodou sociálního inženýrství a osvojení ostražitého přístupu k nedůvěryhodným zprávám. To jsou ale velmi obecné předpoklady a je tedy nutné si stanovit poněkud přesnější cíle, kterých má být úlohou dosaženo. Z tohoto důvodu bude pro úlohu stanoven cíl znalostní, dovednostní a postojový, kdy:

1. **Znalostní cíl** určuje, jaké teoretické znalosti student tímto cvičením získá.
2. **Dovednostní cíl** určuje, jakou získá praktickou dovednost.
3. **Postojový cíl** určuje, jak sám student vnímá danou problematiku. (Blyth et al., 1966)

Tyto cíle budou formulovány metodou SMART, tak aby byly specifické, měřitelné, akceptovatelné, reálné a termínované, ačkoli termínem je v tomto případě konec vyučovací hodiny, proto bude tento parametr vynechán. (ProjectSmart, ©2023)

Teoretický obsah této úlohy by měl odrážet povědomí o tom, jak se phishingový útok projevuje a jak jej rozeznat, naopak není podstatná detailní znalost všech jeho specifik. Znalostní cíl bude proto formulován jako:

1. **Student rozpozná charakteristiky podvodné zprávy.**

Po stránce dovednostní je žádoucí, aby si student vyzkoušel, jak se takový phishingový útok připravuje a porozuměl tomu, jak působí na uživatele. Dovednostní cíl bude tedy formulován následovně:

2. **Student dokáže vykonat simulovaný phishingový útok.**

Nejhůře uchopitelný je postoj, jelikož ten není možné někoho jen tak naučit. Studenti by měli chápat proč je podstatné předcházet těmto útokům a jaké mohou mít následky. Postojový cíl bude formulován následovně:

3. **Student si uvědomuje dopady úspěšného útoku a jeho následky.**

Splněním úlohy by měl student prokazovat znalost, dovednost a postoj k probírané problematice. Pro řádné ověření, jestli toho skrze tuto úlohu opravdu dosahuje, musí být tyto cíle zohledněny při zpracování zadání úlohy, aby bylo při jejím splnění možno vyhodnotit naplnění cílů.

5.4 Zadání úlohy

Pro splnění této úlohy se předpokládá, že se student předem seznámí se zadáním a pomocným materiálem, který je přílohou P I této práce. Tato příprava před vyučovací hodinou je odhadována na méně než 30 minut, během kterých si student přečte zadání, aby se ujistil, že mu rozumí a případně si sám nastudoval nejasnosti.

Kromě přípravy studenta bude potřeba, aby bylo na počítačích v učebně nainstalován program pro editování zdrojového kódu jako Notepad ++, Visual Studio Code nebo podobný, případně je potřeba studentům umožnit takový program instalovat. Ačkoli teoreticky není nezbytný, jelikož je možné pracovat s HTML i v poznámkovém bloku, který je před instalován v počítači, ale toto řešení není komfortní.

S ohledem na dříve formulované cíle je zadání úlohy stanoveno následovně:

1. **Během tohoto cvičení nasimulujte phishingový útok. Postup zaznamenejte pomocí snímků obrazovky a zapište do protokolu.**
   1.1. V internetovém prohlížeči vyhledejte libovolnou přihlašovací stránku (email, moodle, banka, atp.)
   1.2. Pomocí klávesy F12 nebo pravým kliknutím myši v prohlížeči otevřete nástroj „Prozkoumat“.
   1.3. Pravým kliknutím na horní řádek zobrazeného kódu (začínající <html lang=“cs“ dir=“ltr“> nebo podobně) vyberte možnost „Editovat jako HTML“.
   1.4. Zkopírujte celý kód a vložte jej do prázdného textového dokumentu v programu Notepad ++.
   1.5. Tento soubor uložte s příponou **.html** a následně otevřete.
2. **Porovnejte Vaši verzi stránky s originálem a popište podle čeho lze rozpoznat phishingový útok a jak se mu bránit.**
   2.1. Porovnejte snímky obrazovky původní stránky a Vaší verze. Popište, čím se liší.
   2.2. Na konci protokolu vysvětlete, proč jsou phishingové útoky nebezpečné a jak se jim bránit.

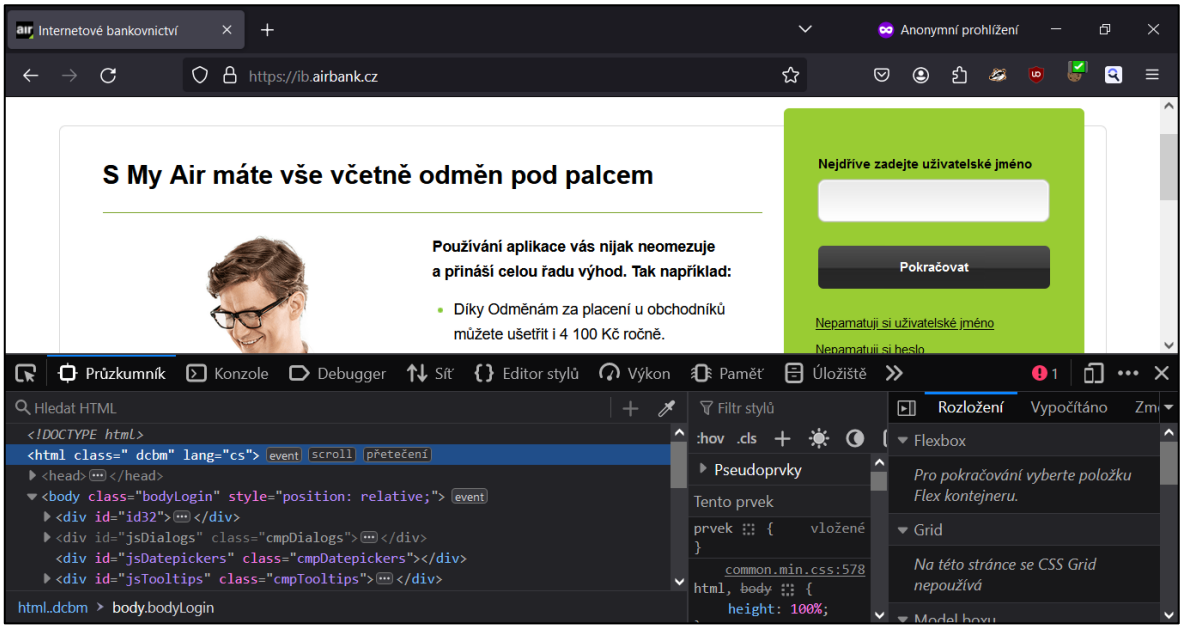
Během první části si studenti vytvoří vzor vlastní webové stránky, aby si vyzkoušeli, jak mohou postupovat praví útočníci. V druhé části zkoumají studenti rozdíly mezi stránkami a zamýšlí se nad riziky, které tento útok vytváří.

6 VZOROVÉ ZPRACOVÁNÍ ÚLOHY

Pro vzorové zpracování této úlohy byla vybrána webová stránka banky Airbank, konktrétně pak přihlašovací stránka do jejího internetového bankovnictví. Banka byla vybrána, protože se jedná o pravděpodobný cíl útoku.

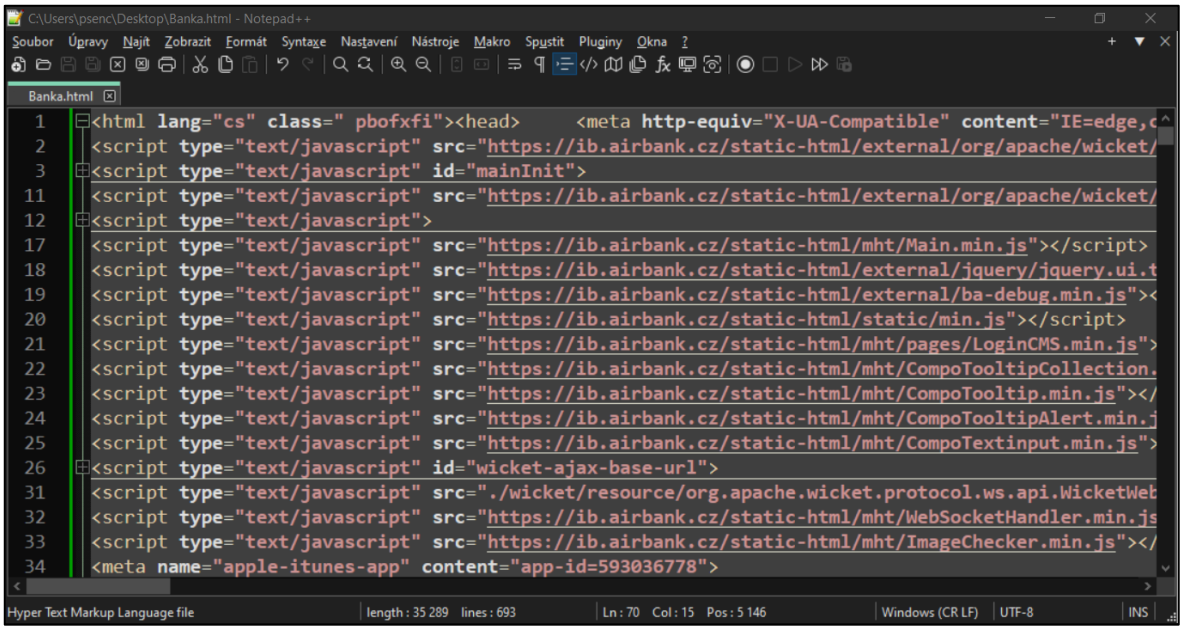
Obrázek 1 – Přihlašovací stránka internetového bankovnictví (Airbank.cz)

V dalším kroku je pomocí nástroje „Prozkoumat“ otevřeno okno zobrazující HTML kód webové stránky.



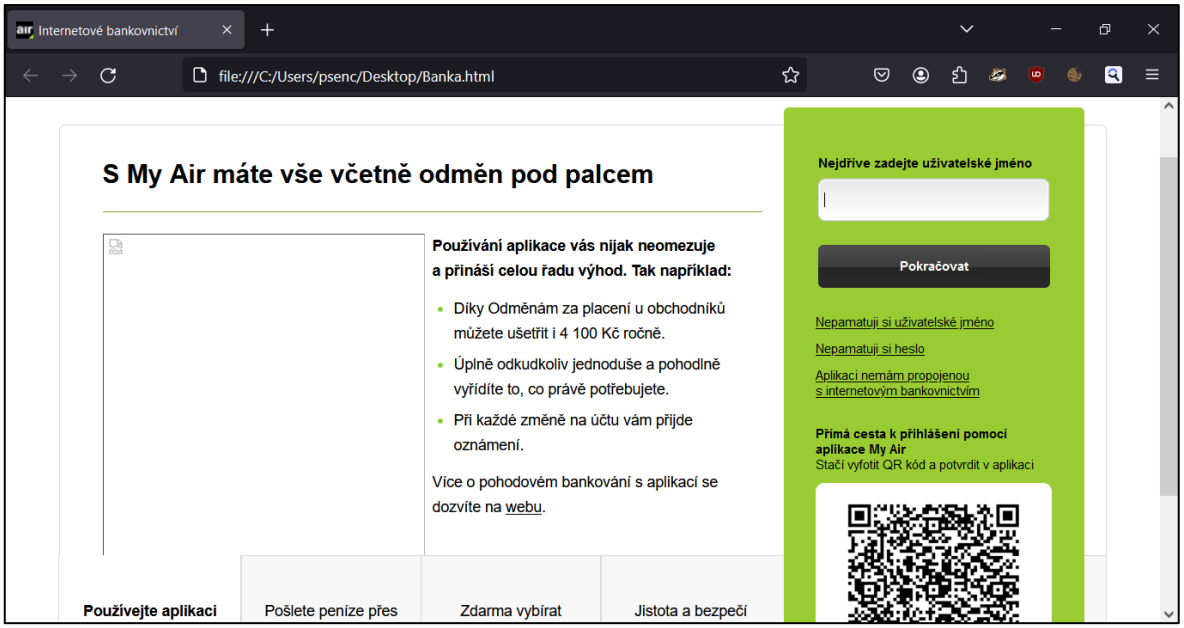
Obrázek 2 – Zobrazení HTML kódu webové stránky (Airbank.cz)

Dále bude pravým kliknutím myši vybrán první řádek kódu, z něhož bude následně možné pomocí klávesové zkratky Ctrl+A možné vybrat veškerý kód stránky. Po vybrání veškerého HTML kódu stránky je tento kód překopírován do programu Notepad ++, kde je následně soubor uložen ve formátu HyperText Markup Language, pro který je zvolena přípona .html.



Obrázek 3 – Kopírování kódu do programu Notepad ++ (Vlastní)

Po otevření uloženého souboru je vidět, že svou strukturou odpovídá ortogonální verzi. Na první pohled schází pouze grafické prvky jako jsou obrázky, vložené do webové stránky.



Obrázek 4 – Lokální verze webové stránky (Vlastní)

Porovnání webových stránek:

Po grafické stránce je jediným rozdílem mezi prvním snímkem (originál webové stránky) a posledním snímkem (lokální verze webové stránky) je chybějící fotka muže v zeleném svetru, jinak jsou tyto dvě webové stránky k nerozeznání. Při podrobnějším zkoumání obou snímků obrazovky je možné si všimnout, rozdílu v adresním řádku, kdy u kopie stránky je adresa lokálního umístění souboru na disku. Je možné bez problému procházet informační karty, které se přepínají na spodní části webové stránky, pouze opět chybí vložené obrázky.

Co se týká funkčnosti stránky, tak většina odkazů je plně funkční a přesměrují uživatele zpět na internetovou verzi. Výjimkou jsou pak přihlašovací odkazy a odkazy pro obnovení hesla, což je pravděpodobně způsobeno specifickým nastavením těchto odkazů ze strany banky.

Z toho vyplývá, že pokud by bylo věnováno přípravě tohoto útoku více času, falešná stránka by mohla být téměř k nerozeznání od originálu.

Nebezpečí phishingu a jak se mu bránit:

Hlavním nebezpečním, které phishing představuje, je ztráta kontroly nad osobními údaji a jejich následné zneužití útočníkem. Díky možnosti rozesílat tyto phishingové zprávy hromadně velkému počtu osob je vysoká pravděpodobnost, že se podvodná zpráva dostane k někomu, kdo ji neodhalí a umožní tak útočníkovi přístup ke svým údajům. Zpracovaná úloha poukazuje na to, že příprava takového útoku není příliš složitá, a proto je nejspíš tak rozšířenou metodou.

Obranu před phishingem mohou do určité míry zprostředkovat například spamové filtry v emailové schránce uživatele, ale i přesto je důležitá ostražitost a povědomí uživatele. V rámci prevence phishingových útoků je vhodné neotvírat a nereagovat na podezřelé zprávy, před zadáním přihlašovacích údajů nebo jiných osobních informací si zkontrolovat adresu webové stránky.

Pro případ, že by se útočníkovi podařilo získat přihlašovací údaje k určitému účtu, je vhodné používat dvoufaktorové ověřování všude, které zabrání proniknutí do účtu bez znalosti bezpečnostního kódu nebo potvrzení identity na jiném zařízení.

7 DÍLČÍ ZÁVĚR

V rámci praktické části této práce byla zhodnocena výuka informační bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, konkrétně předmětů Informační bezpečnost s označením L2SIB a Kybernetická bezpečnost s označením L4SKB, které se vyučují v bakalářském stupni studia. Byla shrnuta studijní náplň obou předmětů a vyhodnoceno, že ačkoli náplň praktických seminářů odpovídá očekávání, nereflektuje současné trendy mezi hrozbami v oblasti informační bezpečnosti, které jsou výsledkem analýzy bezpečnostního prostředí v České republice.

Další část práce se zabývala návrhem praktické úlohy z oblasti informační bezpečnosti, která se zabývá phishingem, jakožto aktuálně nejčastějším typem útoku. Pro tento účel byly určeny hlavní znaky phishingového útoku, ze kterých se následně vycházelo při tvorbě výukových cílů i úlohy samotné. Cíle výuky, které má vybraná úloha předávat byly rozděleny na znalostní, dovednostní a postojový, každý vztažený k určité oblasti úkolu. Na základě výukových cílů bylo stanoveno zadání úlohy, která má představit zjednodušený průběh phishingového útoku.

Pro tuto úlohu bylo zpracováno vzorové řešení, zaměřené na vybranou bankovní instituci, skrze kterou bylo demonstrováno, jak by mohla probíhat příprava phishingového útoku. V druhé části úlohy byly pozorovány rozdíly mezi originální webovou stránkou a kopií, podle čehož bylo následně sepsáno krátké zamyšlení, jak odhalit phishingový útok a jak se před ním bránit.

ZÁVĚR

Tato práce se zaměřila na návrh konkrétní úlohy z oblasti informační bezpečnosti v kontextu ochrany obyvatelstva. Hlavním cílem práce je tedy zvýšit kvalitu výuky informační bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně návrhem praktického cvičení, které zde může být v budoucnu vyučováno. Pro dosažení tohoto cíle bylo stanoveno několik dílčích cílů, popsaných níže.

Prvním dílčím cílem práce je vypracování teoretického vstupu do problematiky informační bezpečnosti, který poslouží jako výchozí bod pro další směřování práce. V teoretické části práce byly popsány základní terminologické pojmy, včetně vysvětlení jejich významu a využití. Dále byly zpracovány základní metody a postupy zajišťování informační bezpečnosti a rozbor nejčastějších kybernetických hrozeb s jejich návazností na současné trendy informační bezpečnosti ve světě i České republice.

Druhým dílčím cílem je analyzovat současný obsah výuky a zejména to, jakým způsobem odráží současné trendy informační bezpečnosti. V souvislosti s tím bylo provedeno zhodnocení obsahu výuky a následná komparace s výsledky analýzy současného bezpečnostního prostředí.

Třetím dílčím cílem je návrh vhodného zadání pro novou praktickou úlohu, která bude zohledňovat výsledky předchozích dvou cílů. K tomu proběhlo stanovení tématu úlohy, jejích výukových cílů a následná formulace zadání.

Posledním dílčím cílem je vytvoření příkladového řešení zvolené úlohy, které poslouží jako ověření přínosnosti úlohy a vzor pro budoucí zpracování úlohy při výuce. Toto bylo splněno přípravou protokolu zaměřeného na tvorbu kopie webové stránky vybrané finanční instituce. Na tomto řešení byla ověřena časová i technická náročnost a úloha by měla být splnitelná ve stanovených parametrech bez jakýchkoliv problémů.

Výsledky práce lze shrnout tak, že bylo dosaženo všech dílčích cílů a tím i cíle hlavního. Výsledná úloha by tedy měla být přínosná pro výuku informační bezpečnosti a svým zadáním a zpracováním pozitivně ovlivnit znalosti, dovednosti i postoje studentů v dané problematice.

SEZNAM POUŽITÉ LITERATURY

BHAHARIN, Surayahani Hasnul; MOKHTAR, Umi Asma'; SULAIMAN, Rossilawati a YUSOF, Maryati Mohd. Issues and Trends in Information Security Policy Compliance. Online. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. 2019, s. 1-6. ISBN 978-1-7281-6726-8. Dostupné z: https://doi.org/10.1109/ICRIIS48246.2019.9073645. [cit. 2024-04-13].

BLYTH, W. A. L.; BLOOM, B. S. a KRATHWOHL, D. R. Taxonomy of Educational Objectives. Handbook I: Cognitive Domain. Online. *British Journal of Educational Studies*. 1966, roč. 14, č. 3, s. 119. ISSN 00071005. Dostupné z: https://doi.org/10.2307/3119730. [cit. 2024-04-20].

BURT, Tom et al. *Microsoft Digital Defense Report 2022: Illuminating the threat landscape and empowering a digital defense*. Online. Microsoft, 2022. Dostupné z: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us. [cit. 2024-04-04].

CODINGS, Zach. *Cyber security: hacking with Kali Linux, ethical hacking. learn how to manage cyber risks using defense strategies and penetration testing for information systems security*. Publikováno nezávisle, 2019. ISBN 9781701275560.

CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2023*. Online. 2024. Dostupné z: https://csirt.cz/media/filer_public/1b/b2/1bb2354c-ad7f-4691-a4fe-893b8d21a88e/240327_csirt_vyrocni_zprava_2023.pdf. [cit. 2024-04-13].

ČSN EN ISO/IEC 27000, *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*.

ČESKO. Zákon č. 40/2009 Sb.: Trestní zákoník. In: *Sbírka zákonů České republiky*. 2009, 11/2009. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-40.

ČESKO. Zákon 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, 75/2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181/.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

ESET. *Co je phishing?* Online. Eset. ©2024. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2024-04-20].

EVANS, Lester. *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. Bravex Publications, 2019. ISBN 9781794647237.

IS/STAG UTB, 2024. *Informační bezpečnost*. Online. Portál IS/STAG. Dostupné z: https://stag.utb.cz/portal/studium/prohlizeni.html?pc_pagenavigationalstate=AAAAAQAFMTMzMDcTAQAAAAEACHN0YXRlS2V5AAAAAQAULTkyMjMzNzIwMzY4NTQ3NzM1NzEAAAAA#prohlizeniSearchResult. [cit. 2024-04-25].

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

KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Brusel, 2022. Dostupné také z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf.

PAVLÍČEK, Antonín; GALBA, Alexander a HORA, Michal. *Moderní informatika*. Druhé, rozšířené vydání. [Praha]: Professional Publishing, 2017. ISBN 978-80-906594-6-9.

PROJECTSMART. *A Brief History of SMART Goals*. Online. ProjectSMART. ©2023. Dostupné z: https://www.projectsmart.co.uk/smart-goals/brief-history-of-smart-goals.php. [cit. 2024-04-20].

SHIAU, Wen-Lung; WANG, Xiaoqun a ZHENG, Fei. What are the trend and core knowledge of information security? A citation and co-citation analysis. Online. *Information and Management*. 2023, roč. 60, č. 3, s. 1-17. ISSN 03787206. Dostupné z: https://doi.org/10.1016/j.im.2023.103774. [cit. 2024-04-04].

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. 2019. ISBN 978-80-7380-765-8.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Naše obory*. Online. 2024. Dostupné z: https://flkr.utb.cz/studium/moznosti-studia/bakalarske-studium/. [cit. 2024-04-17].

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ, 2024. *Kybernetická bezpečnost*. Online. IS/STAG UTB Zlín. Dostupné z: https://stag.utb.cz/portal/studium/moje-studium/index.html?pc_pagenavigationalstate=AAAAAQAFMTMyNTYTAAAAAAA*#prohlizeniAnchor. [cit. 2024-04-28].

MOODLE UTB, 2024. *Kurz: Informační bezpečnost#2021#*. Online. Moodle UTB. Dostupné z: https://moodle.utb.cz/course/view.php?id=26598. [cit. 2024-04-25].

MOODLE UTB, 2024. *Kurz: Kybernetická bezpečnost#2022#*. Online. Moodle Univerzita Tomáše Bati ve Zlíně. Dostupné z: https://moodle.utb.cz/course/view.php?id=28112. [cit. 2024-04-25].

ZHOU, Linqi; GU, Weihong; HUANG, Cheng; HUANG, Aijun a BAI, Yongbin. Research on information security in big data era. Online. *AIP Conf. Proc*. 2018, roč. 1967, č. 1, s. 020020-. Dostupné z: https://doi.org/10.1063/1.5038992. [cit. 2024-04-13].

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Access Control List
APT	Advanced Persistent Threat
CSIRT	Computer Security Incident Response Team
HTML	HyperText Markup Language
IoT	Internet of Things
LAN	Local Area Netvork
MAC	Media Access control
SMART	Specifický, měřitelný, akceptovatelný, reálný, termínovaný (cíl)
TOR	The Onion Router
VPN	Virtual Private Network

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁVOD PRO PRÁCI S HTML

HTML neboli HyperText Markup Language je název jazyka pro tvorbu jednoduchých webových stránek. Tento kód je možné si zobrazit u libovolné webové stránky stisknutím klávesy F12 nebo pravým kliknutím myši a výběrem možnosti „Prozkoumat“.

Každý HTML soubor by měl obsahovat několik základních tagů hlavičky a těla. Tím se zaručí, že všichni klienti (zejm. prohlížeče) pochopí, o co v dokumentu vlastně jde. Tag je značení, kterým se udává, jak se má daná část stránky chovat. Většina tagů se zadává v páru při syntaxi **<tag>** na začátku funkce a **</tag>** na konci funkce.

Každý dokument by měl obsahovat tuto základní strukturu:

Tag	Význam	Výskyt
<!doctype>	Udává verzi HTML, které dokument odpovídá.	Před značkou <html>.
<html> </html>	Označuje začátek a konec celého HTML dokumentu.	Na začátku souboru.
<head> </head>	Hlavička dokumentu platná pro celý soubor.	Na začátku souboru.
<body> </body>	Tělo stránky obsahující hlavní část kódu.	Navazuje na hlavičku.

Pro potřeby úlohy bude stačit veškerou další syntaxi zaznamenat do těla dokumentu, tedy mezi <body> a </body>. Pro úpravy textu dokumentu lze využít možností formátování:

Tag	Význam
** **	Tučné písmo.
** **	Kurzíva.
<big> </big>	Zvětšení písma.
** **	Zmenšení písma.

Pro práci s jednotlivými bloky dokumentu je potom možné využít následující tagy:

Tag	Význam
** **	Konec řádku.
** **	Vycentrování na střed.
** **	Nadpis 1. úrovně. Lze použít i pro další úrovně.
<hr>	Vodorovná čára

Podrobný popis práce v HHTML poskytuje například webová stránka *Jak psát web* na adrese: https://www.jakpsatweb.cz/html/