VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

Porovnání výuky informační a kybernetické bezpečnosti v České republice a Jižní Koreji s návrhy na zlepšení

Comparison of education information and cybernetic security in Czech republic and South Korea with suggestions for improvement

AUTOR PRÁCE — Bc. Marcel Šisler
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Marcel Šisler**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Porovnání výuky informační a kybernetické bezpečnosti v České republice a Jižní Koreji s návrhy na zlepšení

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Analyzovat stávající stav výuky informační a kybernetické bezpečnosti v České republice a Jižní Koreji, posoudit tento stav a připravit návrhy na zlepšení.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací, Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá návrhem na zlepšení současného stavu výuky informační a kybernetické bezpečnosti v České republice. Tyto návrhy pramení ze srovnání výuky na Vysokém učení technickém v Brně - Fakultě podnikatelské a Hallym University v Jižní Koreji. Dalším podkladem je analýza trendů v oblasti kybernetických útoků a srovnání této oblasti mezi Českou republikou a Jižní Koreou.

Abstract

This diploma thesis deals with a suggestions to improve the current state of education information and cyber security in the Czech Republic. These suggestions are from a comparison of education at the Brno University of Technology - Faculty of Business and Hallym University in South Korea. Another part is the analysis of trends in the field of cyber attacks and comparison of this area between the Czech Republic and South Korea.

Klíčová slova

informační bezpečnost, kybernetická bezpečnost, systém řízení bezpečnosti informací, ISO/IEC 27000, NIST SP 800, výuka informační bezpečnosti, digitální forenzní analýza

Key words

information security, cyber security, information security management system, ISO/IEC 27000, NIST SP 800, education of information security, digital forensics

Bibliografická citace

ŠISLER, Marcel. Porovnání výuky informační a kybernetické bezpečnosti v České republice a Jižní Koreji s návrhy na zlepšení [online]. Brno, 2020 [cit. 2020-04-11]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/127745. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2020

……

Bc. Marcel Šisler

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce Ing. Petru Sedlákovi, za ochotu při konzultacích a odborné rady, které mi pomohli nejen při psaní této diplomové práce, ale taktéž je zcela jistě využiji v budoucím životě. Dále bych rád poděkoval panu profesoru Joshua I. Jamesovi, který mi vypomáhal s moji prací při mém pobytu v Jižní Koreji, stejně tak Fakultě podnikatelské VUT, která mi tento studijní pobyt umožnila.

OBSAH

ÚVOD

Tato diplomová práce se věnuje porovnání výuky informační bezpečnosti v České republice a Jižní Koreji, společně s návrhy na zlepšení stávající situace. Tyto návrhy pramení převážně ze studijního pobytu Freemover, který jsem absolvoval V jižní Koreji na Hallym University. Zde mi bylo umožněno studium předmětů souvisejících s informační a kybernetickou bezpečností, kde jsem měl možnost pozorovat určité odlišnosti ve směru výuky, které nakonec vedli právě k napsání této diplomové práce.

Problematika informační a kybernetické bezpečnosti je v dnešní době velice aktuální téma, kterému se musí věnovat každý stát. Největším problémem, se kterým se potýká i Česká republika, je nedostatek kvalifikovaných lidí v této problematice. Proto jsem se rozhodl sestavit doporučení, která by mohla dopomoci ke zlepšení výuky a tím i k získání více kvalifikovaných lidí.

Abychom lépe chápali problematiku této diplomové práce, obsahu první část této práce teoretická východiska informační a kybernetické bezpečnosti, včetně legislativy a certifikačních autorit.

V další části nalezneme analýzu současné situace, ve které uvádím příklady vysokých škol a univerzit, které se věnují této problematice. Ty poté porovnáme se školami a univerzitami v Jižní Koreji a vysvětlíme si důvody případných odlišností.

Poslední část se zaměřuje na doporučení, která by mohla vypomoci doplnit možné mezery ve výuce informační bezpečnosti pro Českou republiku, primárně pak v oblasti vyšetřování a digitální forenzní analýzy.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem této diplomové práce je provést analýzu současné situace výuky informační a kybernetické bezpečnosti. Tento stav bude vyhodnocen na základě vybraných vysokých škol a univerzit a nimi nabízených oborů.

Pro analytickou část taktéž využijeme trendy v oblasti kybernetické bezpečnosti a kulturní odlišnosti, které vysvětlí rozdílnost výuky v České republice a Jižní Koreji.

Výstupem této práce bude doporučení pro nalezení optimální kombinace výuky informační bezpečnosti na základě analýzy výuky v České republice a v Jižní Koreji.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Pro lepší pochopení následujících částí práce, je zapotřebí objasnění základních pojmů a termínů, které budeme používat. Pokusíme se objasnit si, co je to kybernetická a informační bezpečnost a jaké jsou její součásti. Popíšeme si kybernetickou trestnou činnost. Představíme si normalizační instituce, normy a také legislativu. Stručně si představíme principy řízení informační bezpečnosti. Dále si představíme metody pro aplikování kybernetické a informační bezpečnosti včetně jejich slabých a silných stránek.

1.1 Kyberprostor

Tento pojem má vícero definicí, z čehož vyplývá, že jeho chápání nemusí být zcela jednotné a jednoznačné.

Lze jej chápat jako něco, co je tvořeno prvky informačních a komunikačních technologií, které s využitím protokolu TCP/IP vytvářejí celosvětovou, globální počítačovou síť. Jednotlivé počítačové systémy jsou do této sítě připojeny a interagují v ní. Tato interakce je umožněna díky zásahu jednotlivých uživatelů, a to buď administrátorů, případně koncových uživatelů (1).

Máme tedy vytvořen dynamický, neustále se měnící a vyvíjející se systém, který je závislý na hardware, zároveň však vytvářející těžko definovatelný a prakticky neomezený kyberprostor (2).

Dle Cyberspace Operations: Concept Capability Plan 2016–2028 lze kyberprostor rozdělit do tří vrstev, které jsou následně složeny dohromady z pěti složek.

Vrstvy jsou:

1) fyzická,
2) logická,
3) sociální (3).

Co se týče komponent, tak ty nalezneme ve fyzické vrstvě dvě. První komponentou jsou fyzické síťové komponenty, tedy infrastruktura v podobě kabelů, síťových prvků, a dalších zařízení a tou druhou umístění fyzických prvků v reálném světě (3).

V logické vrstvě je pak třetí, logická síťová komponenta, tedy logická propojení mezi síťovými uzly. Jako uzly můžeme chápat nejen počítače, ale také telefony a další síťová zařízení (3).

Sociální vrstva je tvořena komponentou kyberosobnost a osobnost. Kyberosobnost nám vymezuje identifikaci osoby na síti, tedy například IP adresu, emailovou adresu, číslo telefonu a podobně. Osobnost je pak skutečná osoba připojená do sítě. Jedna osobnost může mít vícero kyberosobností. Stejně tak jedna kyberosobnost může být sdílena mezi více osobností (3).

Nejvýznamnějšími znaky kyberprostoru jsou decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost, ale také možnost ovlivňovat mínění skrze uživatele (2).

1.2 Kybernetická bezpečnost

Vymezit pojem kybernetické bezpečnosti je velice důležité, především proto, že se řada lidí mylně domnívá, že se tato problematika týká pouze oddělení informačních a komunikačních technologií. Ta se ovšem týká každého, kdo využívá jakékoliv prvky ICT v každodenním životě. Tato mylná domněnka může zvyšovat pravděpodobnost úspěchu kybernetických útoků (2).

Dle národní strategie pro kybernetickou bezpečnost pro roky 2015-2020 je definice kybernetické bezpečnosti tato:

„Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka“ (4, s. 5).

O významnosti kybernetické bezpečnosti se můžeme přesvědčit i ve zprávě o kybernetické bezpečnosti pro ČR:

„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení“ (5, s. 4).

Z tohoto tvrzení lze zcela jednoznačně vidět důležitost kybernetické bezpečnosti. Navýšení digitální gramotnosti a odolnosti vůči hrozbám je dlouhodobý proces, zvlášť pokud se jedná o navýšení napříč celou společností. Díky úsilí národního úřadu pro kybernetickou a informační bezpečnost proniká výuka této problematiky i do školní výuky (6).

„Gestorem v oblasti kybernetické bezpečnosti České republiky je Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem pro kybernetickou bezpečnost, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galleo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 2015/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., a kybernetické bezpečnosti a o změně souvisejících zákonů. Jeho součástí se stalo Národní centrum kybernetické bezpečnosti, které před tím působilo pod Národním bezpečnostním úřadem (NBÚ)“ (6, s. 8).

Dle Evropské agentury ENISA je kybernetická bezpečnost taková, která se zaměřuje na bezpečnost kyberprostoru, kde kyberprostor představuje soubor propojení a vztahů mezi objekty, které jsou přístupné skrze všeobecnou telekomunikační síť, a také seskupení objektů jako takových, kde jejich dostupní rozhraní umožňuje vzdálené ovládání, vzdálený přístup k datům, případně jejich zapojení do řídících akcí v kyberprostoru (7).

Dalším pohledem, který bychom neměli opomíjet, je pohled právnický. Dle směrnice Evropského parlamentu a rady EU 2016/1148 je bezpečnost sítí a informačních systémů schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které by mohli narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat případně souvisejících služeb, které tyto sítě a informační systémy nabízejí, případně takové, které jsou jejich prostřednictvím přístupné (8).

Na základě výše uvedených definic, můžeme kybernetickou bezpečnost chápat jako:

„souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů, schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených“ (2, s. 44).

Zároveň musíme pamatovat na to, že kybernetická bezpečnost je realizována nejen v kyberprostoru, ale také mimo něj (2).

1.3 Informační bezpečnost

Nazývána taktéž bezpečnost informací, má za úkol chránit data před zničením, poškozením, krádeží a ztrátou. K bezpečnosti informací je velmi často vztahována triáda CIA (9).

V organizaci dosáhneme informační bezpečnosti pomocí zavedení vhodných bezpečnostních opatření. S výběrem těchto opatření nám může pomoci proces řízení rizik. Následně jsou řízena pomocí systému řízení bezpečnosti informací (10).

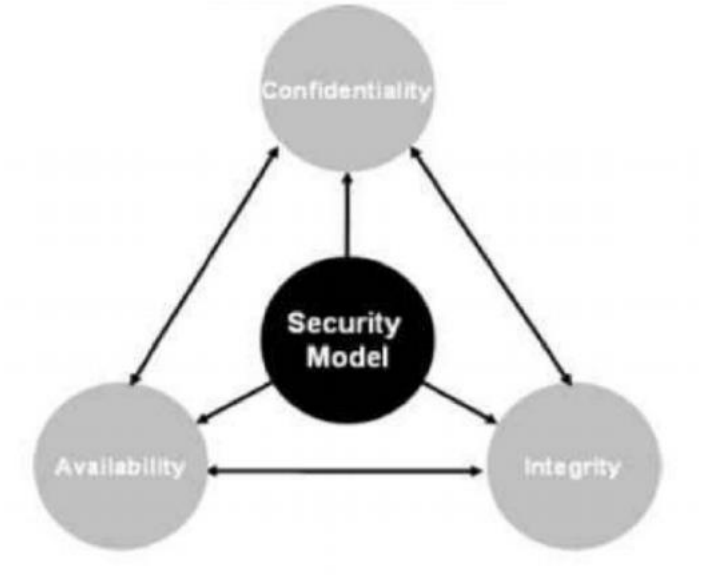
1.4 Triáda CIA

Jedná se o nejvýznamnější a nejpoužívanější triádu kybernetické bezpečnosti.

C - confidentiality, neboli důvěrnost, tedy poskytování informací pouze těm procesům, entitám a uživatelům, kteří jsou k tomu oprávnění (9).

I - integrity, neboli integrita, tedy zajistit úplnost a správnou informací (9).

A - availability, neboli dostupnost, tedy to, že budou data oprávněnému uživateli přístupná v okamžiku jejich vyžádání (9).



Obrázek č. 1: Triáda CIA
(Zdroj: 11, s. 5)

1.5 Důvěrnost

Dle bezpečnostních standardů ISO/IEC 27000 by:

„Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost“ (2, s. 49).

Dále také:

„Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací“ (2, s. 49).

A nakonec:

„Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání“ (2, s. 49).

Informace na základě důvěrnosti se v komerční sféře klasifikují na:

Chráněné – neoprávněné zacházení s takovýmito informacemi by mohlo způsobit závažné poškození či zničení organizace. Může se jednat například o únik hesel (11).

Interní – neoprávněné zacházení s interními informacemi by mohlo způsobit poškození organizace. Například únik smluv či osobních údajů (11).

Citlivé – neoprávněné nakládání s informacemi citlivými, by mohlo mít negativní dopad na organizaci. Příkladem budiž informace o dosud nezveřejněné akci (11).

Veřejné – neoprávněné nakládání s veřejnými informace by nemělo nijak poškodit jak společnost, tak ani nikoho dalšího (11).

Dle ust. § 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů se informace klasifikují na:

„a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,

b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,

d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky“ (12).

1.6 Integrita

Lze chápat jako vlastnost přesnosti a úplnosti. Tedy určitá jistota, že data nebyla změněna. Pro její zjišťování se využívá kontrolních součtů a hashovacích funkcí, případně redundancí, samoopravnými kód a podobně (13).

„O nežádoucí modifikaci (alteration) se proto v informační bezpečnosti hovoří jako o narušení integrity“ (11, s. 22).

1.7 Dostupnost

Bývá definována jako vlastnost přístupnosti a použitelnosti na základě žádosti oprávněné entity (13).

Můžeme ji také chápat jako možnost přístupu k informacím, datům, či počítačovým systémům a to v okamžiku potřeby. Samotná integrita a přístup tedy nestačí, pokud není splněna podmínka spolehlivé přístupu dle potřeby (14).

1.8 Parkerian hexad

Jedná se o rozšíření CIA triády o tři další prvky. Jedná se o P/C, neboli držení/kontrola. Dále A – authenticity, tedy autentičnost, a nakonec U – utility, tedy užitečnost (15).

Obrázek č. 2: Parkerian hexad
(Zdroj: 11, s. 7)

1.9 Prvky kybernetické bezpečnosti

Abychom nastolili kybernetickou bezpečnost, je zapotřebí tří základních prvků, respektive jejich vzájemné interakce. Těmito prvky jsou lidé, technologie a procesy. Je důležité si uvědomit, že v praxi není reálné vytvořit absolutně zabezpečený systém. Pokud by totiž takový systém existoval, znamenalo by to i to, že je zároveň nepoužitelný (2).

1.9.1 Lidé

Lidé jsou často nejslabším článkem v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů (16).

Na tuto složku z pohledu kybernetické bezpečnosti můžeme nahlížet jako na:

- strůjce bezpečnosti, tedy někdo, kdo se snaží prosadit a implementovat prvky kybernetické bezpečnosti,
- příjemce pravidel kybernetické bezpečnosti, tedy osoby, které se rozhodly, případně jsou nuceny, implementovat existující pravidla kybernetické bezpečnosti,
- subjekty, které musíme chránit před kybernetickými útoky,
- subjekty, které musíme informovat a proškolit v rámci kybernetické bezpečnosti,
- rizika a hrozby v rámci kybernetické bezpečnosti (2).

V souvislosti se Zákonem o kybernetické bezpečnosti je třeba definovat a zajistit pozice:

- *„výbor kybernetické bezpečnosti,*
- *manažer kybernetické bezpečnosti,*
- *architekt kybernetické bezpečnosti,*
- *auditor kybernetické bezpečnosti,*
- *tým kybernetické bezpečnosti,*
- *garant primárních aktiv,*
- *garant podpůrných aktiv,*
- *věcný správce,*
- *technický správce,*
- *provozovatel/dodavatel,*
- *administrátor,*
- *uživatel“* (2, s. 58).

Ať už se jedná o jakoukoliv bezpečnost, lidé vždy představují klíčový prvek. V případě kybernetické bezpečnosti se tato klíčovost ještě umocňuje. Jsou proto nejslabším článkem a zároveň nejčastějším cílem kybernetických útoků (2).

Americký odborník na kryptografii a kybernetickou bezpečnost Bruce Schneier prohlásil: *„Amateurs hack systems, professionals hack people“* (17).

Lidé pohybující se v kyberprostoru by měli chápat základní principy a pravidla kybernetické bezpečnosti. Rozumět základním funkcím počítačových systémů. Zanalyzovat si činnosti a smluvní podmínky aplikací, které využívají. Vzdělávat se v oblasti kybernetické bezpečnosti (2).

1.9.2 Technologie

Technologie jsou z pohledu běžného uživatele často pouze koncová zařízení, která mu umožňují přístup k internetu, sociálním sítím, emailové komunikaci a podobně, o technologické vrstvy, díky kterým je připojen do kyberprostoru, se povětšinou nezajímá. Pro organizace už je tento pohled značně rozsáhlejší, kromě koncových zařízení vnímají i kompletní infrastrukturu sítě, služeb, prvky zajišťující bezpečnost, monitoring a jiné (2).

Aby bylo možné zajistit kybernetickou bezpečnost, je zapotřebí technologické prvky udržovat aktualizované a zabezpečené. Bez správně nastavených procesů a lidí, kteří tyto procesy dodržují, jsou však sebelepší bezpečnostní technologické prvky neúčinné (2).

1.9.3 Procesy

Pod procesy můžeme chápat činnosti, které je zapotřebí vynaložit, aby bylo možné technologie včetně jejich procesů využívat lidmi. Jako příklady procesů důležitých v rámci kybernetické bezpečnosti můžeme sledovat:

- řízení aktiv a jejich rizik,
- implementování ICT technologií a aplikací,
- správu uživatelů a jejich rolí,
- autorizaci a autentizaci,
- údržbu včetně aktualizací u systémů a služeb,
- průběžné testování počítačových systémů a služeb v rámci zabezpečí,
- analýzu případných nápravných opatření,
- realizaci takovýchto opatření,
- audit kybernetické bezpečnosti,
- detekci kybernetických útoků,
- reakci na kybernetické útoky,
- procesy zajišťující kontinuitu,

- školení zaměstnanců (2).

Správné nastavení procesů, údržba, modifikace a dodržování představuje nejnáročnější část budování kybernetické bezpečnosti. Dále je vhodné zavést procesy pro pravidelné aktualizace hardwaru a softwaru, provádět simulace typických kybernetických útoků, jako jsou například podvodné emaily, penetrační testování a podobně. Zároveň by se ovšem organizace měla primárně zaměřit na oblast lidských zdrojů, zejména na jejich edukaci (2).

1.10 Životní cyklus kybernetické bezpečnosti

Je třeba si uvědomit, že kybernetická bezpečnost je nikdy nekončící cyklus. Zjednodušeně by se dalo říci, že se jedná o neustálou analýzu rizik, která navíc obsahuje procesy podporující kybernetickou bezpečnost v organizaci (2).

Obrázek č. 3: Životní cyklus kybernetické bezpečnosti
(Zdroj: 18)

1.11 Riziko

Dle výkladového slovníku kybernetické bezpečnosti můžeme riziko definovat jako nebezpečí, možnost škody či ztráty a nezdaru. Dále také účinek nejistoty na dosažení cílů a také možnost, že hrozba využije zranitelnosti aktiva a způsobí organizaci škodu (13).

Jako základní rámec pro zjištění rizik můžeme například využít tří základních otázek:

- *„co špatného (nežádoucího) se může stát, co může selhat,*
- *jaká je možnost / pravděpodobnost, že se to stane,*
- *jak závažné (intenzita, velikost apod.) mohou být účinky (dopady, následky)“* (18, s. 73)

Analýza rizik je obtížná činnost, pro kterou je zapotřebí znát příslušná aktiva, hrozby, ale také mít v dané oblasti určité zkušenosti. Při správné analýze rizik je poté možné sestavit příslušná opatření, která vedou k minimalizaci nebo i úplnému odstranění rizika (2).

Pro výpočet významnosti rizika se využívá vzorce:

Významnost rizika *= Dopady rizika* ******* *Pravděpodobnost výskytu rizika* (2, s. 70)

1.12 Aktivum

Definice dle Výkladového slovníku kybernetické bezpečnosti je aktivum cokoliv, co má nějakou hodnotu pro jednotlivce, organizaci, či veřejnou správu (13).

Jako aktivum můžeme vnímat věc hmotnou, například budovu, počítačový systém, sítě, energii, zboží, ale také věci nehmotné, jmenovitě například informace, znalosti, data, programy. Může se jednat ale i o vlastnost. Dostupnost, funkčnost systému a dat a jiné, nám tedy taktéž mohou představovat aktivum. Stejně tak dobré jméno společnosti, reputace, zaměstnanci, uživatelé (2).

Vyhláška o kybernetické bezpečnosti dělí aktiva do dvou skupin:

- podpůrná aktiva,
- primární aktiva (19).

1.12.1 Podpůrné aktivum

Představuje aktivum technické, zaměstnance a dodavatele, kteří se podílejí na provozu, rozvoji, správě a bezpečnosti informačního a komunikačního systému (19).

1.12.2 Primární aktivum

V tomto případě se jedná o informaci či službu, která je zpracovávána případně poskytována informačním a komunikačním systémem (19).

1.13 Zranitelnost

„Zranitelnost (vulnerability) označuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami“ (2, s. 72)

V kybernetické bezpečnosti se využívá dělení na:

- zranitelnosti známé,
    - opravené – někdy také ošetřené, kupříkladu software, který obsahoval zranitelnost, nicméně ji výrobce již záplatoval pomocí aktualizace,
    - neopravené – jedná se o zranitelnost, o které výrobce již ví, ale zatím nebyla opravena,
- zranitelnosti neznámé,
    - skryté,
    - neobjevené (2).

V případě bezpečnostní zranitelnosti se jedná o potenciální bezpečnostní hrozbu. Takováto zranitelnost lze do jisté míry eliminovat, například důslednými aktualizacemi a záplatováním veškerého softwaru (13).

Ve vyhlášce o kybernetické bezpečnosti se jako příklady zranitelností uvádí:

1. nedostatečná údržba informačního a komunikačního systému,

2. zastaralost informačního a komunikačního systému,

3. nedostatečná ochrana vnějšího perimetru,

4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,

5. nedostatečná údržba informačního a komunikačního systému,

6. nevhodné nastavení přístupových oprávnění,

7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,

9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,

10. nedostatečná ochrana aktiv,

11. nevhodná bezpečnostní architektura,

12. nedostatečná míra nezávislé kontroly,

13. neschopnost včasného odhalení pochybení ze strany zaměstnanců (19, s. 1143).

1.14 Hrozba

Ministerstvo vnitra definuje hrozbu jako:

„Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby“ (20).

V případě výkladového slovníku kybernetické bezpečnosti se můžeme dočíst o bezpečnostní hrozbě, která:

„Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb“ (13, s. 25).

1.14.1 Aktivní hrozba

„Jakákoliv hrozba úmyslné změny stavu systému zpracování dat nebo počítačové sítě. Hrozba, která by měla za následek modifikaci zpráv, vložení falešných zpráv, vydávání se někoho jiného nebo odmítnutí služby“ (13, s. 16).

1.14.2 Pasivní hrozba

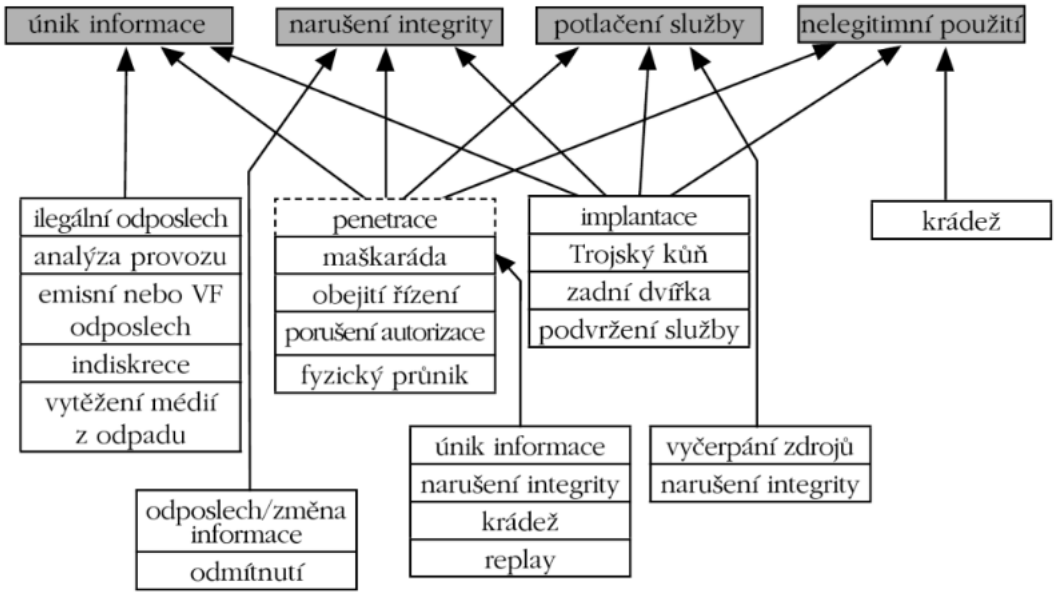
„Hrozba zpřístupnění informací, aniž by došlo ke změně stavu systému zpracování dat nebo počítačové sítě“ (13, s. 81).

1.14.3 Pokročilá a trvalá hrozba

„Typickým účelem APT je dlouhodobé a vytrvalé infiltrování a zneužívání cílového systému za pomoci pokročilých a adaptivních technik (na rozdíl od běžných jednorázových útoků)“ (13, s. 87).

1.15 Základní rozlišení hrozby

V knize Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství uvádí Jirovský čtyři základní rozlišení hrozeb, ke kterým přiřazuje hrozby aktivační a podkladové. Ve schématu níže můžeme vidět jednotlivé propojení těchto hrozeb (21).



Obrázek č. 4: Vztah základních a podkladových hrozeb
(Zdroj: 22, s. 23)

Tento výčet hrozeb není pochopitelné zcela úplný, nicméně nám pokrývá velkou část nejpoužívanějších hrozeb (21).

1.16 Klasifikace kybernetických hrozeb

Klasifikací můžeme nalézt celou řadu. Nejběžnější dělení bývá podle zdroje hrozby, zdroje působení, cíle hrozby, motivace a typu hrozby (2).

1.16.1 Zdroje hrozby

Hrozby způsobené člověkem – v tomto případě se také doporučuje zjistit, jaká byla forma zavinění, která vedla k dané hrozbě. Tyto formy jsou:

- úmyslné:
    - vědomé smazání dat, konfigurace systému,
    - fyzické poškození prvku ICT, případně počítačového systému,
    - odcizení dat či informací,
    - běžné kybernetické útoky, například DoS, malware, phishing (2).
- nedbalostní:
    - neúmyslné smazání dat,
    - neúmyslné poškození prvku ICT, případně počítačového systému, například pádem,
    - poškození systému či dat z důsledku nedostatečného seznámení s interními akty, ať už právnickými, či technickými,
    - ostatní chyby uživatele (2).

Hrozby způsobené z důvodu technické chyby – například defekt hardwaru, chyba v softwaru, opotřebení materiálu a podobně (2).

Hrozby způsobené z důvodu působení vyšší moci – do těchto chyb můžeme zařadit například:

- neočekávaný výpadek napájení,
- přírodní katastrofy a události, například zásah bleskem, zemětřesení,
- požár, který nebyl zapříčiněn člověkem (2).

1.16.2 Zdroje působení hrozby

Jsou děleny na:

- vnitřní hrozby,
- vnější hrozby (22).

1.16.3 Cíle hrozby

Cíle hrozby můžeme dělit na:

Útoky na triádu CIA:

- útoky na **důvěrnost**, například krádeže přístupových údajů, klíčů, dat,
- útoky na **integritu**, například chyby v databázích, konfigurace oprávnění,
- útoky na **dostupnost**, kupříkladu Dos a DDoS útoky, fyzické poškození serveru, kabeláže, útoky na dodávku energií (2).

Útoky na prvky kybernetické bezpečnosti:

- útoky na **lidi**, nejčastěji prostřednictvím sociálního inženýrství, phishingem, malwarem či krádeží,
- útoky na **technologie**,
    - hardware – servery, síťové prvky, koncové počítačové systémy,
    - databáze,
    - sít a síťovou infrastrukturu,
    - software – operační systémy, programové vybavení,
    - data a informace – uložená v počítačových systémech,
- útoky na **procesy**, například neoprávněné testování funkčnosti procesů či zabezpečení (2).

1.16.4 Motivace hrozby

V případě, že se jedná o úmyslně způsobenou hrozbu člověkem, je taktéž vhodné znát motivaci tohoto jednání. Dle Kybez máme dělení hrozeb s ohledem na motivaci na:

- *hrozby za získání finančního prospěchu,*
- *hrozby za účelem získání konkurenční převahy,*
- *hrozby za účelem dokázání svých schopností,*
- *hrozby za účelem odplaty,*
- *hrozby z důvodu neplnění povinností* (23).

1.16.5 Typ hrozby

Jako typy hrozeb můžeme mít například:

- *sociální inženýrství,*
- *botnet,*
- *malware,*
- *ransomware,*
- *spam/scam*
- *podvodné nabídky,*
- *phishing, pharming, spear phishing, vishing, smishing,*
- *hacking,*
- *sniffing,*
- *DoS, DDoS, DRDoS útoky,*
- *šíření závadového obsahu,*
- *identity theft,*
- *APT (Advanced Persistent Threat),*
- *kyberterorismus,*
- *kybernetické výpalné či vydírání (cyber extortion)* (2, s. 79).

Dle Vyhlášky o kybernetické bezpečnosti, přílohy č. 3, můžeme za hrozbu označovat:

- *porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,*
- *poškození nebo selhání technického anebo programového vybavení,*
- *zneužití identity,*
- *užívání programového vybavení v rozporu s licenčními podmínkami,*
- *škodlivý kód (například viry, spyware, trojské koně),*
- *narušení fyzické bezpečnosti,*
- *přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,*
- *zneužití nebo neoprávněná modifikace údajů,*
- *ztráta, odcizení nebo poškození aktiva,*
- *nedodržení smluvního závazku ze strany dodavatele,*
- *pochybení ze strany zaměstnanců,*

- *zneužití vnitřních prostředků, sabotáž,*
- *dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,*
- *nedostatek zaměstnanců s potřebnou odbornou úrovní,*
- *cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,*
- *zneužití vyměnitelných technických nosičů dat,*
- *napadení elektronické komunikace (odposlech, modifikace)* (19, s. 1143).

1.17 Kybernetická bezpečnostní událost

Takovouto událost můžeme chápat jako počítačový útok, případně počítačový trestný čin. Jedná se o nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, ve které figuruje počítačový systém či počítačová síť. Může se jednat o spam, krádeže osobních údajů, zpronevěru a podobně (24).

Dle Jiráska je bezpečnostní událost taková událost, která může způsobit, případně vést, k narušení informačních systémů a technologií, nebo také pravidel definovaných k jeho ochraně, takzvané bezpečnostní politiky (13).

V článku 3.5 ISO/IEC 27001 se můžeme dočíst, že bezpečnostní událost znamená:

„identifikovatelný stav systému, služby, nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací“ (25, s. 258).

1.18 Kybernetický bezpečnostní incident

Dle Výkladového slovníku kybernetické bezpečnosti je kybernetický bezpečnostní incident:

„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie“ (13, s. 25).

Norma ISO/IEC 27001 ve článku 3.6 uvádí, že informační bezpečnostní incident je:

„jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací“ (25, s. 258).

Kybernetický bezpečnostní incident také definuje zákon o kybernetické bezpečnosti v § 7 odstavce 2, a to jako:

„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“ (26, s. 7).

Jak můžeme vidět, tak ze zákona vyplývá, že kybernetický bezpečnostní incident může být způsobem nejen úmyslným, ale také nedbalostním jednáním člověka či vyšší mocí. V případě, že nám takový incident nastane, dojde k narušení bezpečnosti informací, případně služeb a informačních a komunikačních systému s nimi spojených. Představuje tedy skutečné narušení informačního nebo komunikačního systému s negativním dopadem (2).

1.19 Kybernetický útok

Ve výkladovém slovníku se můžeme dočíst, že kybernetický útok je:

„*Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků*“ (13, s. 71).

Tato definice se však jeví jako neúplná, jelikož nepostihuje všechny negativní aktivity uživatelů kyberprostoru. Nepokrývá například sociální inženýrství, DoS a spoustu dalších. Je nutné si uvědomit, že kybernetický útok oproti kybernetickému bezpečnostnímu incidentu bude mít vždy úmyslné zavinění člověkem (2).

Přesnější definice by mohla být například taková, že kybernetický útok je:

„jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby“ (2, s. 82).

1.20 Digitální forenzní analýza

Digitální forenzní analýza, taktéž známa jako počítačová a síťová forenzní analýza, má vícero definicí. NIST uvádí, že se jedná o aplikování vědy k identifikaci, sesbírání, zkoumání a analýze dat, zatímco je zachována integrita informací a dochází k udržování tzv. **chain of custody** pro data. Data zde představují jednotlivé části digitální informace, která byla formátována specifickým způsobem. Organizace mají stále se zvyšující množství dat z mnoha zdrojů. Například mohou být data uložena, případně přenesena ze standardních počítačových systémů, síťových prvků, počítačových periferií, chytrých mobilních telefonů a spoustu dalších typů médií (27).

Jelikož máme data z různých zdrojů, techniky digitální forenzní analýzy mohou být použity pro mnoho využití, jako například vyšetřování zločinů a porušení interních politik, rekonstrukce počítačových bezpečnostních incidentů a obnovování po náhodném poškození systému. Prakticky každá organizace potřebuje zvládat digitální forenzní analýzu. Bez ní by totiž měli velké problémy se zjišťováním, jaké události nastali v jejich systému a sítích, jako například vyzrazení citlivých dat (27).

Proces digitální forenzní analýzy se skládá z těchto základních fází:

- **sběr**: identifikace, označení, nahrávání, sbírání dat z možných zdrojů souvisejících dat, zatímco jsou dodržovány procedury k zajištění integrity dat,
- **přezkoumání**: forenzní postupy jsou aplikovány na sesbíraná data pomocí automatizovaných i ručních metod, posouzení a extrakce žádaných dat, zatímco jsou dodržovány procedury k zajištění integrity dat,
- **analýza**: analýza výsledků přezkoumání, využitím legálně akceptovatelných metod a technik, k zajištění užitečných informací, které pomohou odpovědět na otázky, které byli impulzem k zahájení vyšetřování,
- **reporting**: reporting výsledků analýzy, které mohou obsahovat popisy využitých metod, vysvětlení jak byli vybrány nástroje a procedury, určení jaké další akce jsou potřeba vykonat, doporučení pro vylepšení politik, procedur, nástrojů a dalších aspektů forenzní analýzy (27).

1.21 Volatilita dat

Při sbírání dat z místa činu musíme umět určit, která data sesbírat jako první. Na správnou prioritizaci dat využíváme právě pojmu volatilita dat. Zjednodušeně se jedná o nestálost dat. Čím vyšší hodnotu volatilit paměťové médium má, tím dříve z něj musíme data získat, než o ně přijdeme. Postupovat bychom měli v následujícím pořadí:

- procesor, cache paměti a obsah registrů,
- routovací tabulka, ARP cache, procesní tabulka, kernel statistiky,
- RAM paměť,
- dočasné soubory,
- data na pevném disku,
- vzdálená data,
- data na archivačním médiu (28).

1.22 Chain of custody

„popisuje podrobnou dokumentaci celého životního cyklu stopy tak, aby nevznikly pochybnosti o potenciální objektivnosti její vypovídající schopnosti a tedy nevzniklo podezření, že se stopou bylo možné nekontrolovaně manipulovat nebo ji bylo možné pozměnit“ (29, s. 16).

1.23 Incident response

Systémy jsou předmětem široké oblasti událostí hrozeb, od nakažených datových souborů, přes viry, až po přírodní katastrofy. Slabiny na některé tyto události hrozeb mohou být zmírněné, pakliže má organizace relevantní standardní operační procedury, které mohou být následovány v době incidentu. Například často se objevující událost, jako je nechtěné smazání souboru, může být obvykle napraveno obnovou ze zálohovacího souboru. Více závažné události hrozeb, jako jsou výpadky způsobené přírodními katastrofami, jsou obvykle řešeny v náhradních plánech organizace (30).

Příklady nástrojů pro incident response mohou být:

- incident response trénink,
- incident response testování,

- vypořádávání se s incidenty,
- monitorování incidentů,
- reportování incidentů (30).

Ve fázi incident response je zapotřebí detekovat podezřelý incident a zahájit před investigativní odpověď. Primární zaměření je na identifikaci a ohodnocení aktiv a také vyhodnocení takzvaného response plánu pro podezřelý bezpečnostní incident. Dále se v této fázi vyvíjí plán související s vyhrazením, eliminací, obnovou a vyšetřováním. Také zvládnutí koordinace lidí, právní a legislativní stránka věci a formulování vhodného vyšetřování (31).

1.24 Hashovací funkce

„Je jednosměrná matematická transformace vstupních dat (textu) do souboru (otisk, hash). Matematicky je prakticky nereálné získat z otisku zpět vstupní data. Tato funkce je využívána v aplikacích zabezpečení dat (například autentizace, digitální podpis, kontrola integrity). Narušení bezpečnosti hash funkce je označováno jako kolize„ (13, s. 50)

1.25 Logy a logování

Při provozování systémů, služeb a aplikací bychom neměli zapomenout na správné logování, tedy na jejich zaznamenávání činnosti a běhu. Tyto záznamy mohou být ukládány v různých podobách, nejčastěji pak textový dokument či databáze. Dále se může jednat o formáty syslog, XML, CSV, W3C, ale mohou se nacházet i v binární podobě. Detailnost logu závisí na konkrétní aplikaci či systému, přičemž často máme možnost nastavit si určité úrovně logování podle potřeby. Je třeba ovšem pamatovat, že logování může generovat obrovské množství dat. Tím nám vznikají velké požadavky na úložiště, zároveň však také na výpočetní výkon při procházení takovýchto logů. Výstupy logů bývají velmi častým zdrojem informací pro digitální forenzní analýzu (2).

1.26 Image file

Image file je soubor, který vznikl kopírováním bit po bitu z logického či fyzického disku, flash disku, paměti mobilního telefonu, CD či DVD a podobně. V případě digitální forenzní analýzy se často používá termín forensic image.

1.27 BotNet

„Síť infikovaných počítačů, které ovládá jediný cracker, který tak má přístup k výpočetnímu výkonu mnoha tisíců strojů současně. Umožňuje provádět nezákonnou činnost ve velkém měřítku – zejména útoky DDoS a distribuci spamu“ (13, s. 30).

1.28 Počítačová zombie

„Infikovaný počítač, který je součástí sítě botnetů“ (13, s. 135).

1.29 Distributed denial of service - DDoS útok

„Distribuované odmítnutí služby je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků“ (13, s. 40).

1.30 Normalizační instituce

Jelikož je v této práci uvedeno několik norem, je třeba si také uvést normalizační instituce, které se o tyto normy starají.

1.30.1 ISO – International Organization for Standardization

Jedná se o nezávislou, nadnárodní organizaci. Její působení je celosvětové a podporuje rozvoj standardizačních činností. Zaměřuje se na spolupráci na úrovni jak technických, ekonomických, tak i vědeckých a intelektuálních aktivit, dále také na usnadňování mezinárodních směn zboží a služeb (9).

1.30.2 IEC – International Electrotechnical Comission

Další rozsáhlá, celosvětová instituce. Stará se o přípravu a publikování norem pro veškeré ekonomické, elektrotechnické a jiné technologie, které s nimi souvisí (9).

1.30.3 ITU - International Telecommunications Union

Společně s ISO a IEC tvoří tři největší globální normalizační instituce. Tato instituce dopomohla růstu mnoha technologií. Jako příklad můžeme uvést mobilní technologie

a internet. Zaujímá vedoucí postavení při rozdělování a správě spekter rádiových frekvencí (9).

1.30.4 ČAS – Česká agentura pro standardizaci

Tato státní příspěvková organizace byla zřízena Úřadem pro technologickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ). Je zodpovědná za všechny činnosti v rámci tvorby, vydáváním a distribucí technických norem (32).

1.30.5 ČSN - Česká technická norma

Dříve taktéž známa jako Česká státní norma, přejímá evropské a mezinárodní normy. Dále také o původní normy, a to v případě, že vyplývají z národních potřeb (9).

1.30.6 NIST – National Institute for Standards and Technology

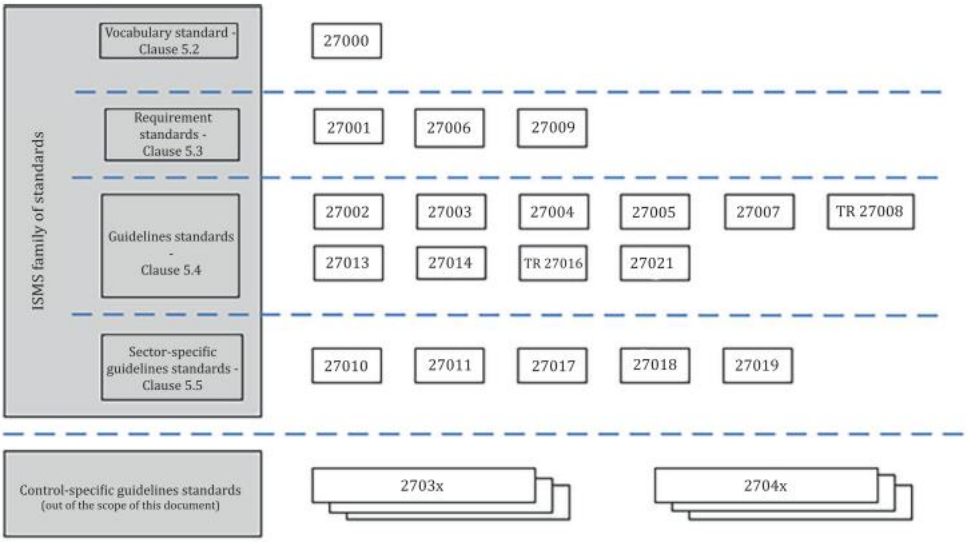
V případě této normalizační organizaci se jedná o organizaci americkou. Stará se o vývoj a podporu standardů, technologií, ale také měřících technik, které by měli zlepšovat úroveň života, zvyšovat produktivitu a dopomáhat k usnadňování obchodu (9).

1.31 Normy související s kybernetickou bezpečností

Norma, neboli doporučení jak danou problematiku, případně daný standard řešit. Standard oproti tomu přesně popisuje konkrétní kritéria a technické specifikace (9).

1.31.1 ISO/IEC 27000:2018

Mezinárodní norma na informační technologie, bezpečnostní techniky, zaměřující se na ISMS, neboli norma na řízení bezpečnosti informací. Obsahuje přehled a slovník využívaných termínů a ostatních norem pro ISMS. Popisuje základní principy, které napomáhají organizacím pochopit a provozovat ISMS. Dále představuje systémy řízení informační bezpečnosti jako takové a seznamuje s rodinou standardů ISMS (10).



Obrázek č. 5: Rodina norem ISMS
(Zdroj: 10, s. 19)

1.32 Normy ISO popisující požadavky

1.32.1 ISO/IEC 27001

Další norma na řízení bezpečnosti informací, nyní zaměřena na požadavky, které je potřeba dodržet při zakládání, implementaci, provozování, monitorování, vyhodnocování, revidování, údržbu a zlepšování ISMS v kontextu celkových business rizik organizace. Tuto normu mohou využívat organizace všech zaměření, velikostí i podstat. Vymezuje požadavky na bezpečnostní opatření, které jsou přizpůsobeny potřebám části, případně celé organizaci (10).

1.32.2 ISO/IEC 27006

Norma, která specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikace systému systémů řízení bezpečnosti informací. Doplňuje tedy požadavky z norem ISO/IEC 17021-1 a ISO/IEC 27001. Její primární určení je podpora procesu akreditace certifikačních orgánů poskytujících certifikace ISMS. Požadavky z této normy musí být prokázané ve smyslu odborné způsobilosti a spolehlivosti kteréhokoliv orgánu poskytující certifikaci ISMS (33).

1.32.3 ISO/IEC 27009

Zaměřuje se na používání ISO/IEC 27001 ve specifických odvětvích. Definuje požadavky dle oboru, oblasti aplikace, případně sektoru trhu. Vysvětluje, jak zavést dodatečné požadavky v souladu s ISO/IEC 27001 (10).

1.33 Normy ISO popisující obecné směrnice

Nyní si představíme jednotlivé normy, jež se zabývají popisem obecných směrnic.

1.33.1 ISO/IEC 27002

Tato norma obsahuje doporučení pro organizace při výběru opatření v rámci procesu zavádění systému řízení bezpečnosti, který je založen na normě předchozí, tedy na ISO/IEC 27001. Případně může pomoci organizacím při zavádění obecně přijatých opatření bezpečnosti informací. Také se využívá při vyvíjení směrnic pro řízení bezpečnosti informací specifických pro průmysl a organizace, kde se zároveň přihlíží na jejich konkrétní prostředí rizik pro bezpečnost informací (34).

1.33.2 ISO/IEC 27003

Tato norma představuje pokyny k požadavkům na systémy řízení bezpečnosti informací tak, jak je specifikován v ISO/IEC 27001 a poskytuje doporučení – měl by, může, smí ve vztahu k těmto požadavkům. Neposkytuje obecné pokyny související se všemi aspekty bezpečnosti informací. Také nepřidává žádné nové požadavky na ISMS a s ním související termíny a definice (35).

1.33.3 ISO/IEC 27004

Tato norma pomáhá organizacím při hodnocení výkonnosti bezpečnosti informací a efektivnosti systému řízení bezpečnosti informací tak, aby splnily požadavky plynoucí z normy ISO/IEC 27001, zaměřené na monitorování, měření, analýzu a hodnocení. Výsledky těchto monitorování a měření systému řízení informační bezpečnosti mohou zlepšovat rozhodování týkající se správy, managementu, provozní efektivnosti a neustálého zlepšování ISMS. Interpretace této normy by měla být upravena tak, aby vyhovovala konkrétní situaci konkrétní organizace (36).

1.33.4 ISO/IEC 27005

Norma poskytující směrnice pro řízení rizik bezpečnosti informací v organizaci. Neobsahuje specifické metody pro řízení rizik. Každá organizace si musí sama definovat vlastní přístup k řízení rizik, například v závislosti na rozsahu systému, odvětví a podobně. Je založena na metodě identifikace rizika aktiv, hrozeb a zranitelností (37).

1.33.5 ISO/IEC 27007

Tato norma obsahuje pokyny pro řízení programu auditu systému řízení bezpečnosti informací, provádění interních a externích auditů ISMS v souladu s ISO/IEC 27001 a také kompetence a hodnocení auditorů ISMS (38).

1.33.6 ISO/IEC TR 27008

Tato technická zpráva slouží k přezkoumání, zavedení a provozování opatření. Současně zde nalezneme kontrolu technické shody opatření informačního systému dle norem stanovených konkrétní organizací (10).

1.33.7 ISO/IEC 27013

Jedná se o pokyn pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1. Napomáhá k lepšímu pochopení obou výše uvedených norem (10).

1.33.8 ISO/IEC 27014

Se zabývá správou a řízením bezpečnosti informací. Navádí k principům a procesům, díky kterým tyto skutečnosti mohou organizace hodnotit, řídit a monitorovat řízení bezpečnosti informací (10).

1.33.9 ISO/IEC TR 27016

Je technická zpráva popisující řízení bezpečnosti informací se zaměřením na organizační ekonomiku. Napomáhá organizacím lépe porozumět ekonomickému ohodnocení jejich informačních aktiv, vyhodnotit rizika k těmto aktivům, ocenit hodnotu, kterou kontrola ochrany bezpečnosti přináší k těmto aktivům a stanovit optimální úroveň zdrojů aplikovaných při ochraně těchto aktiv (10).

1.33.10 ISO/IEC 27021

Tato norma specifikuje požadavky na kompetence ISMS profesionálů, kteří vedou, případně jsou součástí zakládání, implementace, správy a postupného vylepšování ISMS které podlého požadavkům ISO/IEC 27001 (10).

1.34 Normy ISO popisující směrnice specifické pro odvětví

Další skupinou jsou normy, které jsou určeny pro specifické odvětví.

1.34.1 ISO/IEC 27010

V této normě nalezneme směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi (10).

1.34.2 ISO/IEC 27011

Obsahuje směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002 (10).

1.34.3 ISO/IEC 27017

Obsahuje praktiky řízení bezpečnosti informací založené na ISO/IEC 27002 pro cloudové služby (10).

1.34.4 ISO/IEC 27018

Tato směrnice se zaměřuje na ochranu osobních údajů ve veřejných cloudech, působících jako zpracovatelé osobních údajů (10).

1.34.5 ISO/IEC 27019

Směrnice řízení informační bezpečnosti se zaměřením na energetický průmysl (10).

1.34.6 ISO/IEC 27799

Normy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002 (10).

1.35 Normy NIST

Normy americké agentury se zabývají různými problematikami. Pro určení této práce nás budou nejvíce zajímat normy, zabývající se kybernetickou a informační bezpečností.

1.35.1 NISTIR 7298

Tato norma popisuje pojmy používané v Národním institutu pro normy a publikace Technology (NIST) a Výboru pro národní bezpečnostní systémy (CNSS). Využívá databázi termínů extrahovaných z NIST Federal Information Processing Standard Publications (FIPS), NIST Special Publication (SP) 800 series, NIST Interagency, vnitřní zprávy (NISTIR) a výboru pro instrukce národních bezpečnostních systémů 4009 (CNSSI-4009) (39).

1.35.2 NIST SP 800-12 An Introduction to Information Security

Tato publikace slouží jako úvod do informační bezpečnosti. Obsahuje přehled principů, které můžou vést k efektivnímu zabezpečení systém a informací v organizacích. Popisuje a uvádí výhody řízení bezpečnosti. Představuje možné techniky, které mohou organizace

využít. Veškeré techniky a principy jsou ověřené na federálních informačních systémech a organizacích (30).

1.35.3 NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

Tyto normy jsou katalogem bezpečnostních opatření a dopomáhá vybrat vhodné opatření k ochraně organizace, včetně ochrany mise, funkce, reputace a image, organizačních aktiv, zaměstnanců, ale také jiných organizací. Dále také pomáhá chránit stát před hrozbami, jako například nepřátelskými kybernetickými útoky, přírodními katastrofami, lidskými chybami a chybami struktur. Řízení je přizpůsobitelné a implementované jako součást procesů napříč organizací, které se starají o informační bezpečnost a soukromá rizika. Adresuje bezpečnost z pohledu jak funkčního, tak i ujišťujícího. Dodržování těchto dvou pohledů zaručuje, že společnosti, které dodržují principy tohoto katalogu, jsou z pohledu informační bezpečnosti důvěryhodné (40).

1.36 Legislativa

V souvislosti s informační a kybernetickou bezpečností je třeba vnímat taktéž legislativní oblast, která je zachycena právními předpisy.

1.36.1 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Tento zákon vstoupil v platnost dne 29. srpna 2014 a jeho účinnost započala od 1. ledna 2015. Upravuje práva a povinnosti osob, stejně tak pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Reaguje na příslušné předpisy Evropské unie, které jsou transpozicí směrnice NIS, a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů (41).

Hlavním cílem tohoto zákona je:

- stanovení základní úrovně bezpečnostních opatření,
- zlepšení detekcí kybernetických bezpečnostních incidentů,
- zavedení hlášení kybernetických incidentů,

- zavedení systému opatření, který by reagoval na kybernetické bezpečnostní incidenty,
- upravení činností dohledových pracovišť (41).

Změny a novelizace:

- zákon č. 104/2017 Sb.,
- zákon č. 205/2017 Sb.,
- novelizace zákonem č. 183/2017 Sb.,
- zákon 35/2018 Sb.,
- zákonem č. 111/2019 Sb.,
- zákonem č. 12/2020 Sb. (41).

Zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi (26).

1.36.2 Směrnice Evropského parlamentu a Rady (EU) 2016/1148

Tyto směrnice z 6. července 2016 pojednávají o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (41).

„Tato směrnice má za cíl harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu“ (41).

Určité oblasti z této směrnice NIS již řeší zákonem č. 181/2014 Sb., o kybernetické bezpečnosti. Rozšiřuje navíc okruh subjektů, kterých se týkají povinnosti v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty. Do tohoto rozšířeného okruhu spadají provozovatele základní služby a poskytovatele digitálních služeb, tedy například internetové vyhledávače, cloudové služby a online tržiště. Tyto požadavky pro ČR zapracovává novela zákona o kybernetické bezpečnosti cestou zákona č. 205/2017 Sb. (41).

1.36.3 Vyhláška o kybernetické bezpečnosti

Zpracovává příslušný předpis Evropské unie a upravuje pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační

systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb:

- co je obsahem a jakou strukturu má bezpečnostní dokumentace,
- co je obsahem a v jakém rozsahu jsou bezpečnostní opatření,
- jaké typy, kategorie a hodnocení významnosti jsou pro kybernetické bezpečnostní incidenty,
- jaké náležitosti a způsoby hlášení jsou pro kybernetické bezpečnostní incidenty,
- jaké náležitosti musí obsahovat oznámení o provedení reaktivního opatření a jeho výsledku,
- jak vypadá vzor pro oznámení kontaktních údajů a v jaké je formě,
- jakým způsobem likvidovat data, provozní údaje a informace včetně kopií (19).

1.36.4 Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Tato vyhláška stanovuje významné informační systémy a také kritéria, podle kterých se určují. Kritéria se dělí na dopadová určující a oblastní určující (42).

1.36.5 Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Toto nařízení definuje průřezová a odvětvová kritéria, která určují, zdali je prvek součástí kritické infrastruktury či nikoliv (41).

1.36.6 Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Tato vyhláška byla vydána 15. prosince 2017. Byla zpracována Národním úřadem pro kybernetickou a informační bezpečnost ve spolupráci s odbornou veřejností. Zapracovává Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele požadavky Směrnice Evropského parlamentu a Rady (EU) 2016/1148, které se týkají opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Upravuje odvětvová a dopadová kritéria, které určují provozovatele základní služby a vymezují

významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti (41).

1.36.7 Prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb

V tomto provádějícím nařízení nalezneme bližší upřesnění bezpečnostních opatření, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, kterým jsou sítě a informační systémy vystaveny. Dále upřesňuje parametry pro posouzení významnosti dopadu incidentů. Pro poskytovatele digitálních služeb je toto nařízení závazné (41).

2 ANALÝZA PROBLÉMU A SOUČASNÁ SITUACE

V této kapitole se podíváme na současnou situaci výuky informační bezpečnosti v České republice. Představíme si konkrétní obory s předměty, které jsou zde vyučovány. Provedeme analýzu a pokusíme se vyhodnotit, zdali je aktuální situace uspokojující, případně v jakých oblastech by bylo vhodné výuku posílit. Dále si vysvětlíme, proč je výuka informační bezpečnosti v České republice zaměřena jiným směrem, než je tomu v Jižní Koreji. Porovnáme si tyto dvě zaměření a ukážeme si, co mohou být silná a co naopak slabá místa obou zaměření. Taktéž využijeme analýzu trendů kybernetických útoků.

2.1 Situace středních škol v České republice

Když se podíváme na aktuální situaci středních škol, máme zde velké množství škol, které se snaží následovat trend a nabízet studentům obor v oblasti informačních technologií. Na těchto oborech by se studenti měli dozvědět především základy z velice rozsáhlé oblasti, kterou informační technologie jsou. Tyto obory nebývají příliš úzce zaměřeny, tudíž má student ještě prostor rozmyslet si, jakým směrem v oblasti informačních technologií by se mohl vydat, ať už se jedná o počítačové sítě, programování, webové stránky a podobně, většina středních škol předá studentům alespoň základy do všech těchto oblastí. Bohužel se díky tomu často nenajde prostor na předměty, které by v dnešní době našli uplatnění, jmenovitě například právě kybernetická a informační bezpečnost.

2.1.1 Obor Informační technologie – 1820M01

Tento obor je nejběžnější v rámci středních škol v oblasti informačních technologií. Jedná se o čtyřletý obor zakončený maturitní zkouškou. Aktuálně je dle informací serveru stredniskoly.cz nabízen na 139 vzdělávacích institucí.

Dle Národního ústavu odborného vzdělávání, se absolventi tohoto oboru mohou uplatnit, s ohledem na příslušnou specializaci, v oblastech:

- *návrhů a realizace HW řešení odpovídajících účelu nasazení,*
- *údržby prostředků IT z hlediska HW,*
- *programování a vývoji uživatelských, databázových a webových řešení,*

− *instalací a správy aplikačního SW,*

− *instalací a správy OS,*

− *návrhů, realizace a administrace sítí,*

− *kvalifikovaného prodeje prostředků IT včetně poradenství,*

− *obecné i specializované podpory uživatelů prostředků IT.*

Možnými uplatněními absolventů jsou technik IT, pracovník uživatelské podpory, programátor, správce aplikací, správce operačních systémů, správce sítí, obchodník s prostředky IT aj (43, s. 12).

Pokud si rámcový vzdělávací program pro tento obor prohlédneme podrobněji, zjistíme, že o oblasti bezpečnosti se zmiňuje pouze v souvislosti s bezpečnostní v počítačových sítích. Chybí nám zde tedy jakékoliv širší pojetí informační bezpečnosti jako takové.

2.2 Situace vysokých škol a univerzit v České republice

Zde si uvedeme vybrané vysokých školy a univerzity, na kterých se vyučuje informační a kybernetická bezpečnost. Seznámíme se se způsobem, jak kybernetickou bezpečnost konkrétně vyučují, přesněji jaké předměty mají zaměřeny na tuto problematiku.

2.2.1 Vysoké učení technické v Brně - Fakulta podnikatelská

Obrázek č. 6: Logo VUT FP
(Zdroj: 45)

Na fakultě podnikatelské se díky odborníkům v oboru, kteří na této fakultě vyučují, dozvídají studenti o informační kybernetické bezpečnosti již dlouhá léta. Je pravdou, že dnes již máme vícero vysokých škol s obory na informační a kybernetickou bezpečnost, nicméně se jednalo o dlouhou dobu přehlíženou problematiku. Fakulta podnikatelská ale reagovala včasně a do výuky zařadila předměty jako kryptografie, bezpečnost ICT,

management informační bezpečnosti, oborové managementy bezpečnosti IS, a technologická bezpečnost ICT.

Díky těmto předmětům může student získat znalosti v oblasti informační a kybernetické bezpečnosti, včetně oblasti infrastruktury, která bývá často opomíjena jinými školami (44).

2.2.2 Vysoké učení technické v Brně - Fakulta elektrotechniky a komunikačních technologií

Obrázek č. 7: Logo VUT FEKT
(Zdroj: 45)

Tato fakulta nabízí bakalářský studijní program informační bezpečnost. Reaguje tím na zvýšenou poptávku po odbornících v oblasti informační bezpečnosti. Velkou výhodou tohoto oboru je to, že se nevztahuje pouze na technickou stránku oblasti informační bezpečnosti, ale také přidává právní a ekonomické souvislosti, které jsou stejně podstatné jako stránka technická. Akreditace tohoto oboru byla získána 29. 6. 2018, jedná se tedy o velice mladý obor. Na tento program také navazuje magisterský studijní program informační bezpečnost. Absolventi tohoto programu najdou uplatnění převážně v technických pozicích zaměřených na návrh, budování, správu informačních a komunikačních systémů. Konkrétně může jít o bezpečnostní administrátory, auditory, IT bezpečnostní konzultanty, manažery bezpečnostních týmu a podobně (44).

2.2.3 Vysoké učení technické v Brně - Fakulta informačních technologií

Obrázek č. 8: Logo VUT FIT
(Zdroj: 45)

Fakulta informačních technologií VUT nabízí specializaci na kybernetickou bezpečnost, nicméně až od magisterského studia. Pro studium bakalářské si uchazeč musí vystačit s oborem informační technologie. Tudíž musí student absolvovat i ostatní předměty, o které by nemusel mít zájem, pokud by mu šlo čistě o studium informační bezpečnosti (44).

„Absolvent oboru uplatní získané vzdělání ve vývojových a výzkumných odděleních firem a institucí zabývajících se vývojem programových systémů s důrazem na bezpečnost a u firem, které informační systémy provozují, například v institucích státní a místní správy, v armádě, ve zdravotnictví a prakticky ve všech průmyslových podnicích“ (44).

2.2.4 Masarykova univerzita – fakulta informatiky

Obrázek č. 9: Logo Masarykovy univerzity – fakulty informatiky
(Zdroj: 46)

Tato fakulta nabízí bakalářský program s názvem počítačové systémy, komunikace a bezpečnost, který má návaznost v magisterském programu. V něm si studenti mohou

zvolit informační bezpečnost. Ta je dle webových stránek Masarykovy univerzity specifikována takto:

„Specializace se zaměřuje na oblasti bezpečnosti počítačových systémů a sítí, kryptografie a jejich aplikací. Cílem je připravit takového absolventa, který bude schopen pracovat v řadě úloh, které jsou rozhodující pro zajištění bezpečnosti profilů specifických pro IT (např. směrem ke kryptografii, technologickým aspektům nebo řízení bezpečnosti)“ (45).

Dále nabízí magisterský program Řízení softwarových systémů a služeb, který umožňuje specializaci na řízení kyberbezpečnosti. Tu popisují jako:

„Specializace Řízení kyberbezpečnosti zohledňuje aspekty přesahu počítačového zpracování dat mimo pevně definované systémové perimetry (např. s dopadem na kritické infrastruktury), reflektované v oblasti tzv. kybernetické bezpečnosti a umožňující specifický víceoborový přesah jak technických, tak společenských a právních aspektů kybernetické bezpečnosti.“ (46).

I zde tedy můžeme vidět důraz nejen na technickou stránku informační bezpečnosti, ale taktéž na společenské a hlavně právní aspekty.

2.2.5 Fakulta informačních technologií ČVUT v Praze

Obrázek č. 10: Logo FIT ČVUT
(Zdroj: 49)

Na FIT ČVUT lze studovat bakalářský obor Bezpečnost a informační technologie. V tomto oboru lze studovat mimo jiné předměty Bezpečný kód, Hardwarová bezpečnost a Systémová a síťová bezpečnost. Co zde ovšem chybí, je bezpečnost z pohledu právního. Dále je k dispozici magisterské studium oboru Počítačová bezpečnost, který nabízí

předměty, jako jsou Algoritmy informační bezpečnosti, Síťová bezpečnost a také Systémová bezpečnost a forenzní analýza (47).

Právě forenzní analýza bývá v České republice často opomíjena a není na ni kladen příliš velký důraz.

2.2.6 Fakulta vojenských technologií Univerzity obrany v Brně

Obrázek č. 11: Logo fakulty vojenských technologií Univerzity obrany v Brně
(Zdroj: 50)

Na této univerzitě, v rámci katedry informatiky a kybernetických operací, jsou k dispozici dva magisterské studijní programy. Jedním z nich je Kybernetická bezpečnost, a tím druhým Informační technologie v rámci fakultního studijního programu Vojenské technologie. V těchto oborech je kladen důraz na administrativní a fyzickou bezpečnost, kryptografické techniky, řízení a bezpečnost komunikačních a informačních systémů (48).

2.2.7 Univerzita Tomáše Bati ve Zlíně – fakulta aplikované informatiky

Obrázek č. 12: Logo Univerzity Tomáše Bati – fakulty aplikované informatiky
(Zdroj: 51)

Tato univerzita nabízí bakalářský obor Bezpečnostní technologie, systémy a management. Ten nabízí zajímavou kombinaci předmětů, jelikož zahrnuje vícero aspektů bezpečnosti, například právní, technickou, ale také kriminalistickou. Právě poslední zmíněná oblast je v České republice velmi málo pokryta (49).

V rámci magisterského studia taktéž nabízí obor Bezpečnostní technologie, systémy a management, který je tedy navazující na bakalářské studium. K předchozím předmětů, přidává navíc Kybernetickou bezpečnost, Bezpečnostní technologie ochrany informačních systémů, Provoz počítačových sítí, ale také forenzní vědy. Jako jedna z mála tedy pokrývá jak technologickou stránku informační bezpečnosti, tak i právní, kriminalistickou a taktéž nabízí studium forenzních věd. Dále také nabízí magisterský obor Informační technologie se specializací Kybernetická bezpečnost (49).

2.3 Situace vysokých škol a univerzit v Jižní Koreji

V této podkapitole si pokusíme lehce přiblížit situaci vysokých škol a univerzit v Jižní Koreji s ohledem na kybernetickou a informační bezpečnost. Především půjde o Hallym University, jelikož na této univerzitě jsem měl možnost osobně studovat po dobu jednoho semestru. Dále se podíváme na pár dalších, namátkou vybraných vysokých škol a univerzit, zejména pak na předměty, které vyučují.

2.3.1 Hallym University

Obrázek č. 13: Logo Hallym University
(Zdroj: 52)

Na této univerzitě jsem prostřednictvím Fakulty podnikatelské VUT díky programu Freemover studoval po dobu jednoho semestru. Díky tomu jsem mohl poznat odlišný způsob výuky bezpečnosti, především také hlavní zaměření. Předměty, které bych rád vyzdvihl, jsou Network Security & Forensics a Introduction to Digital Forensics. V další části této práce oba předměty detailně přiblížím, ale abychom více chápali další část této kapitoly, je třeba si stručně představit jejich náplň. Popis předmětu Introduction to Digital Forensics je následující:

„Tento předmět je představením do digitálního forenzního vyšetřování. Naučíme se co digitální forenzní vyšetřování je a kdy se používá. Zaměření bude na užívání nástrojů pro sběr, analýzu a zkoumání dat forenzní analýzy. Dále bude zaměřen na obnovu a analýzu disků a pamětí, také na malware analýzu, vyšetřování databází a emailů a digitální forenzní analýza mobilních telefonů“ (50).

Předmět Network security & forensics je popsán následovně:

„Tento předmět představí studentům síťovou bezpečnost, incident response techniky a forenzní vyšetřování sítí. Studenti se naučí jak naplánovat a nakonfigurovat senzory pro monitorování sítí a zároveň jak odpovědět na detekované incidenty. Také se naučí základní koncepty související s vyšetřováním kyberzločinu“ (50).

Jak můžeme vidět na obou těchto předmětech, jejich zaměření je vždy nějak spjato s vyšetřováním.

2.3.2 Korea University - School of Information Security

Obrázek č. 14: Logo Korea University
(Zdroj: 54)

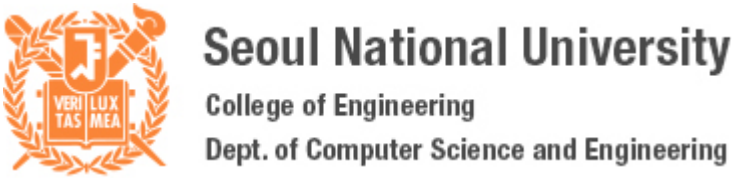
Důvod, proč bychom se měli podívat na tuto univerzitu, je především proto, abychom si dokázali lépe představit Korejské národní cítění. V popisu ústavu kybernetické bezpečnosti uvádí, že byl založen pomocí ministerstva pro národní bezpečnost, pro výcvik 1% nejlepších důstojníků kybernetické bezpečnosti. Studenti mají zaplacené celé čtyři roky studia a po dostudování musí nastoupit po určitou dobu do služby kybernetické bezpečnosti státu. Cílem oddělení pro kybernetickou bezpečnost je vycvičit zkušené odborníky v oblasti kybernetické bezpečnosti, kteří dokáží ochránit Koreu od kyber teroru a kybernetických válek. Dále nabízí ústav Digital Forensics, který byl otevřen pro složky státní policie, kde získávají zkušenosti v oblasti kriminálního práva, forenzních věd a inženýrství. Také ústav Kybernetické národní bezpečnosti, který byl zřízen na rekvalifikaci zaměstnanců pracujících ve složkách kybernetické bezpečnosti státu. Dále má oddělení pro kybernetickou obranu a ochranu pro big data. Nejblíže k této univerzitě by teoreticky mohla mít Univerzita obrany v Brně, ale jak můžeme vidět, jejich zaměření na kybernetickou bezpečnost státu je výrazně vyšší.

2.3.3 Sejong Cyber University

Obrázek č. 15: Logo Sejong University
(Zdroj: 55)

Ústav informační bezpečnosti nabízí vzdělání v oblasti hackování a virů, kybernetického vyšetřování a průmyslové bezpečnosti. Spolupracuje se státním zastupitelstvím a národním policejním sborem na procvičování praktických dovedností, které pomáhají s různými kyberzločiny páchanými v kyberprostoru (51).

2.3.4 Seoul National University – department of Computer Science and Engineering



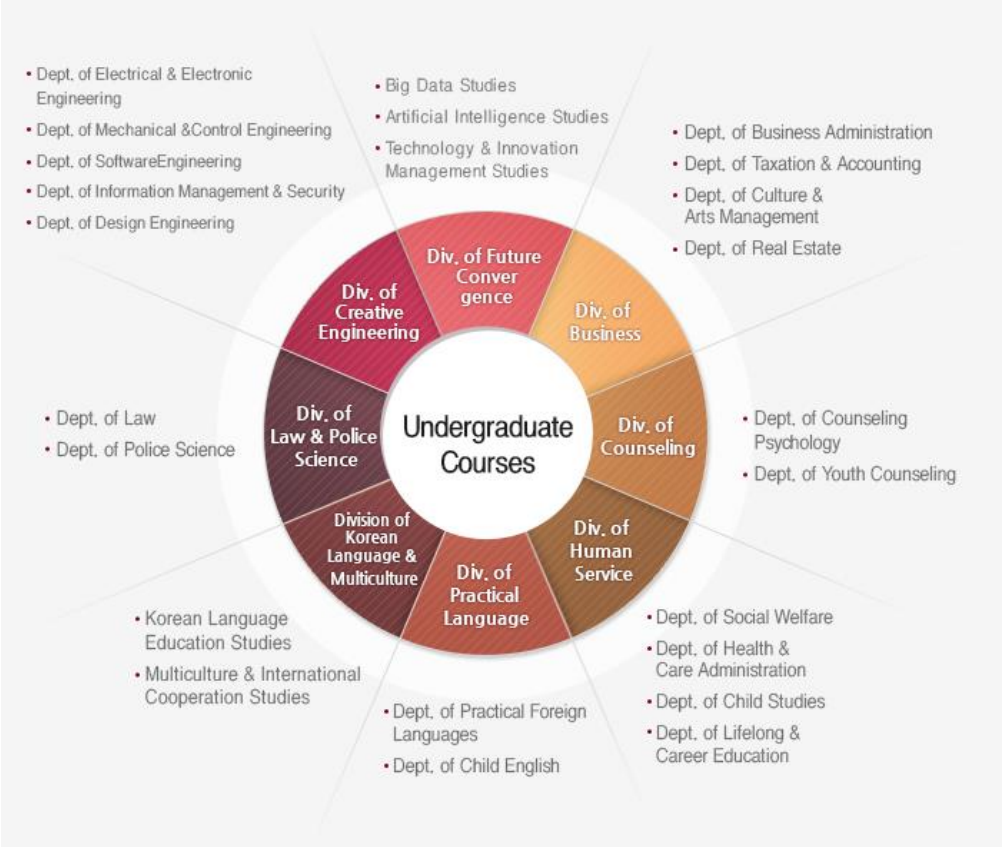
Obrázek č. 16: Logo Seoul National University
(Zdroj: 56)

Jedná se nejprestižnější státní univerzitu v Jižní Koreji. Intenzivně se věnuje výzkumu v oblasti Computer Science. Je taktéž mezinárodně uznávaná. Mimo předměty kryptografie a nabízí taktéž předmět, zaměřený na případové studie bezpečnostních systémů. Mimo tyto předměty se ale kybernetickou informační bezpečností příliš nezabývá. Důvod, proč tuto univerzitu uvádím, je proto, abych ukázal, že ne všechny univerzity a vysoké školy v Jižní Koreji se zabývá bezpečností do hloubky. Na druhou stranu ovšem mají několik škol, které jsou na bezpečnosti přímo zaměřeny (52).

2.3.5 The Cyber University of Korea

Obrázek č. 17: Logo The Cyber University of Korea
(Zdroj: 57)

Tato univerzita byla založena v roce 2001 vyčleněním od Korea University. Jedná se o univerzitu, která pokrývá vícero oblastí informační a kybernetické bezpečnosti. To můžeme vidět mimo jiné například na schématu níže:



Obrázek č. 18: Předměty The Cyber University Of Korea
(Zdroj: 57)

Přímo související je ústav informačního managementu a bezpečnosti, nicméně prvky bezpečnosti můžeme nalézt i v dalších ústavech.

2.3.6 Hanyang Cyber University

Obrázek č. 19: Logo Hanyang Cyber University
(Zdroj: 58)

Tato univerzita je silně zaměřena na průmysl, konkrétně automobilový. Tomu se v Jižní Koreji velice daří, stačí jen jmenovat značky jako Hyundai nebo Kia. Svým ústavem Computer and Information Security připravuje studenty taktéž na trendy moderní doby, jako je bezpečnost IoT. Velice zajímavá, je specializace v tomto oboru nazvaná Hacking and Security. V tomto oboru je spoustu zajímavých předmětů, které dle mého názoru naneštěstí chybí na jiných univerzitách, hlavně těch v České republice, ale přitom by pozvedli studium informační a kybernetické bezpečnosti na zcela jinou úroveň. Jmenovitě například Practical Cyber Attack response, kde si student prakticky vyzkouší jak reagovat na kybernetické útoky, jak takový útok vlastně probíhá. Dále nabízí praktické penetrační testování systémů, techniky síťových útoků, kryptografické programování, metody na analýzu virů, aplikační bezpečnost, digitální forenzní analýzu a mnoho dalšího. Věřím tomu, že to, co často schází na zdejších univerzitách, jsou právě praktické ukázky a cvičení v oblasti bezpečnosti (53).

Náplň tohoto oboru si můžeme prohlédnout na následujícím schématu:

Obrázek č. 20: Schéma oboru Hacking and Security
(Zdroj: 58)

2.4 Srovnání výuky v České republice a Jižní Koreji

Když se podíváme na výše vypsané vysoké školy a univerzity z obou zemí, všimneme si dvou zásadních rozdílů. Zatímco v České republice se informační a kybernetická bezpečnost vyučuje v relativně širokém, obecném měřítku, v Jižní Koreji se zaměřují

často na dvě specifické věci. Prvním zaměřením bývá orientace na vyšetřování kybernetických zločinů a předměty s touto problematikou spojené. Druhé zaměření pak na kybernetickou bezpečnost státu.

Pokud porovnáme údaje o počtu odhalených a řešených případů kybernetických zločinů z Jižní Koreji a České republiky, které uvedu níže, vezmeme v potaz počet obyvatel a vypočítáme počet odhalených případů na 1 obyvatele, dostaneme tyto hodnoty:

- **0.00039511737** odhalených kybernetických případů na jednoho obyvatele ČR za polovinu jednoho roku
- **0.00166446553** odhalených kybernetických případů na jednoho obyvatele Jižní Koreji za polovinu jednoho roku

I když se možná tyto hodnoty zdají na první pohled nic neříkající, dovolte mi jej přeformulovat. Při zvážení počtu obyvatel nám vychází, že Jižní Korea má zhruba **4,2 krát** více odhalených případů kyberkriminality na hlavu nežli Česká republika.

2.4.1 Orientace na vyšetřování kybernetických zločinů

Při pohledu na předměty z korejských univerzit můžeme vidět opakující se například Digital Forensics, tedy forenzní analýzu digitálních dat, které mohou pomoci při hledání důkazů v digitální podobě. Učí jak využívat nástroje pro sběr a zkoumání dat. Jak s takovými daty manipulovat aby byl zachován Chain of Custody. Dále Network Forensics, tedy forenzní analýzu sítí, která zase vypomáhá s hledáním důkazů a celkově vyšetřováním ze síťového prostředí. Jak odhalit probíhající incident a jak na něho reagovat. Dále předměty zabývající se právní stránkou této problematiky, která je pro vyšetřování naprosto nezbytná, například jak manipulovat s důkazy, jak vhodně psát dokumentaci k vyšetřování a podobně.

2.4.2 Orientace na kybernetickou bezpečnost státu

Obyvatelé Jižní Koreji, ostatně jako ve většině asijských zemí, mají obrovské národní cítění. Toho si můžeme povšimnout i při pohledu na programy některých univerzit v tomto státě. Například Korea University má za cíl trénovat špičky v oboru kybernetické bezpečnosti, proto jak jsem již uváděl, mají studenti oboru na kybernetickou bezpečnost plně hrazené školné, za podmínkou toho, že poté budou po určitou dobu pracovat v rámci

kybernetické bezpečnosti státu. Tímto, a dalšími podobnými kroky, si Korea zajišťuje dostatek odborně vzdělaných lidí v této oblasti. Obdobný model můžeme vidět u Sejong Cyber University, kdy univerzita úzce spolupracuje s policejními složkami státu. Studenti tak mohou zlepšovat svoje dovednosti na praktických příkladech, se kterými policejní složky přicházejí denně do styku.

2.4.3 Důvod odlišného zaměření kybernetické bezpečnosti

Abychom pochopili odlišné zaměření kybernetické bezpečnosti, musíme si taktéž vysvětlit jiné smýšlení obyvatel České republiky a Jižní Koreji. V tomto srovnání smýšlení vycházím z průzkumů, které jsem provedl formou rozhovoru se studenty vysokých škol a univerzit v obou zemích. Odpovědi jsem poté shrnul, abych získal odpověď na otázku odlišného smýšlení o bezpečnosti.

Je zde třeba pochopit, že odlišné smýšlení se nejedná pouze kyberbezpečnosti, ale bezpečnosti jako takové. Když jsem přiletěl do Jižní Koreji, ihned jsem si všiml něčeho velice zajímavého. Ve všech restauracích, kavárnách a ostatních podnicích si lidé zcela běžně nechávají svůj mobilní telefon, laptop, peněženku na stole, zatímco si jdou odskočit na toaletu, případně ven, zapálit si cigaretu. Když jsem se pak bavil s korejskými studenty, zdali se nebojí, že by jim tyto věci někdo ukradl, dostal jsem vždy stejnou odpověď. Ne. Oni na druhou stranu nedokázali pochopit, že v České republice by toto nikdo neudělal, protože by mu dané věci s velkou pravděpodobností někdo odcizil. To mě donutilo přemýšlet a dále se vyptávat, proč se o svoje věci nebojí. Ukázalo se, že Jižní Korea je velice bezpečným státem. Nejen že není běžné, aby Vám někdo ukradl věci. Ale také v případě, že by se tak stalo, budou obyvatelé Jižní Koreji spoléhat na policejní složky v tom, že jejich věci získají zpátky. Jak je tedy vidět, mají velkou důvěru v místní policejní sbor.

Zeptal jsem se tedy i studentů z České republiky, zdali si myslí, že v případě ukradených věcí jim je policie získá zpět. Nejčastěji jsem dostal odpověď, kterou si dovolím citovat:

„Pokud by mi ukradli věci, které jsem nechal na stole v restauraci, ani bych na policii nešel. Nejspíš by se mi vysmáli a řekli, že je to moje chyba“.

Když jsem pak tuto odpověď sdílel s korejskými studenty, nedokázali to pochopit. Řekli mi, že něco takového by se v Koreji stát nemohlo.

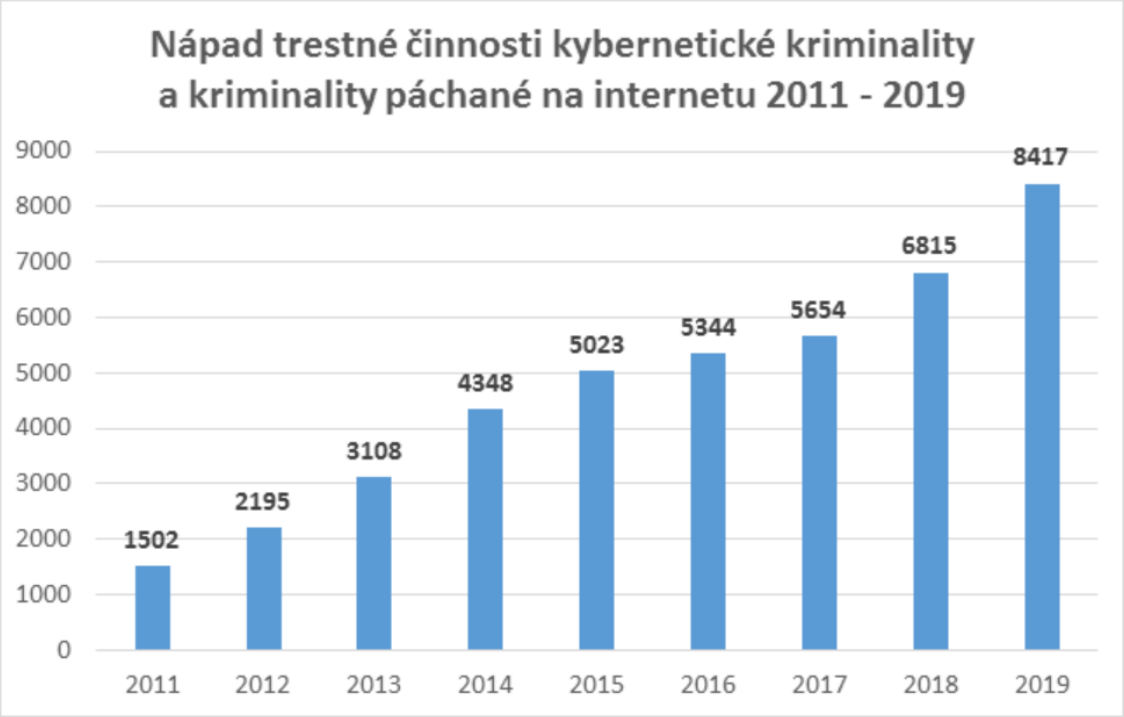
I když se uvedený příklad může zdát jako nesouvisející s kybernetickou bezpečností, opak je pravdou. Pokud se pozorně podíváme na české vysoké školy a univerzity, můžeme vidět jejich zaměření na zabezpečení dat, informačních systémů a podobně. Zjednodušeně řečeno celkové zabezpečení je děláno tak, abychom pokud možno eliminovali riziko bezpečnostního incidentu. A právě tak to probíhá i praxi. Organizace se snaží zabezpečit svoje systémy, sítě a data tak, aby byli co nejvíce chráněny. Ale pokud už k incidentu dojde, příliš se nezabývají vyšetřováním. Většinou se pouze pokusí zjistit, co bylo slabé místo, kvůli kterému k incidentu došlo a to následně záplatovat tak, aby k incidentu znovu nedošlo.

Pro Jižní Koreu platí stejná analogie, jako v případě ukradených věcí, i pro kybernetickou bezpečnost. Při konzultacích s profesorem Joshua I. Jamesem, který vyučuje kybernetickou bezpečnost na Hallym University v Jižní Koreji, mi bylo sděleno, že korejské společnosti nekladou příliš velký důraz na zabezpečení svých sítí a dat, často kybernetickou bezpečnost téměř neřeší. Spoléhají opět na místní policejní složky, které v případě bezpečnostního incidentu případ vyšetří.

Pokud si shrneme výše uvedené informace, vyjde nám tedy, že v České republice organizace velmi dbají na samotné zabezpečení, ale v případě bezpečnostního incidentu se již příliš nepočítá s vyšetřením daného případu. V Jižní Koreji máme situaci opačnou, organizace kybernetickou bezpečnost často zanedbávají, ale v případě bezpečnostního incidentu spoléhají na to, že případ bude prošetřen.

2.4.4 Slabé stránky přístupu České republiky

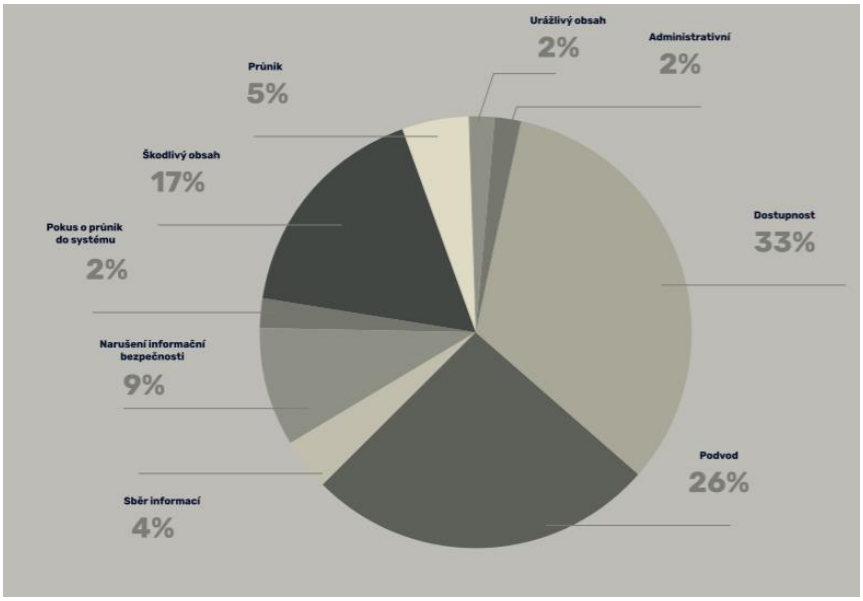
Je nutné si uvědomit, že i kybernetické útoky je nutné vyšetřovat. Když se podíváme na statistiku řešených kybernetických útoků v ČR, můžeme vidět, že se situace postupně zlepšuje, viz graf níže:



Obrázek č. 21: Vyšetřované kyberkriminální případy ČR
(Zdroj: 59)

Nastává však otázka, zdali bude mít Česká republika dostatek kvalifikovaných vyšetřovatelů pro kybernetickou bezpečnost, jelikož se samotné vyšetřování kybernetické bezpečnosti na českých školách nevyučuje.

Klasifikace hlášených útoků na GovCERT.CZ je následující:



Obrázek č. 22: Klasifikace útoků hlášených na GoVCERT.CZ
(Zdroj: 6)

Vzpomeneme-li na filosofii českých organizací, tedy maximální zabezpečení, primárně zaměřené na průnik, můžeme vidět, že byl pouhých 5% z celkových útoků. Podvod tvořil 26%. Tím se nám jenom potvrzuje nutnost kvalitních bezpečnostních politik organizací. Dle mého názoru může vysoké procento podvodů souviset právě s tím, že útočníci, v tomto případě podvodníci, spoléhají na to, že případ nebude nijak vyšetřován.

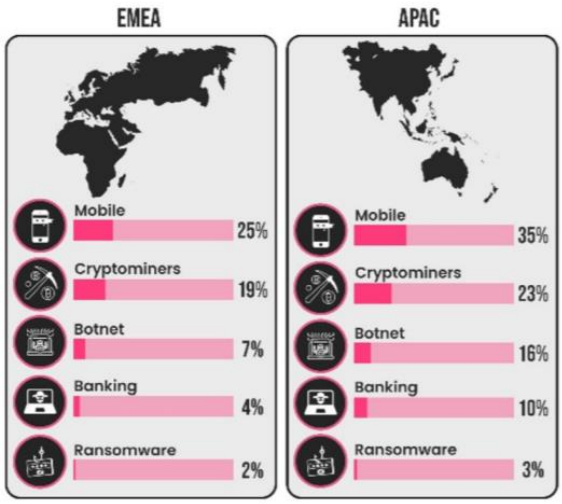
2.4.5 Slabé stránky přístupu Jižní Koreji

Vzhledem k tomu, že Jižní Korea je světový leader v internetové konektivitě, s nejrychlejším připojením k internetu na světě a nejvyšším využitím internetu na osobu, stává se lákavým cílem pro různé druhy útoků, stejně tak jejich zdrojem. Internet zde využívá přes 85% obyvatel, chytrý mobilní telefon potom přes 80% obyvatel (54).

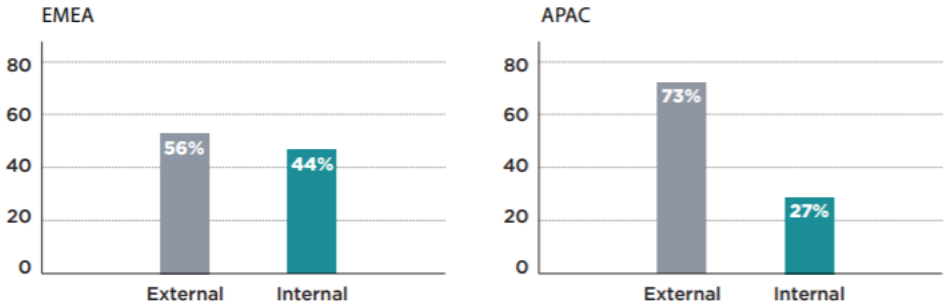
Vezměme si kupříkladu takový botnet. Pokud organizace nebudou mít dostatečně zabezpečené sítě, stávají se pro útočníky snadným zdrojem počítačových zombie, tedy počítačů v síti botnet. Problémem je, že se často nepodaří odhalit to, že je počítač napaden a spadá do takovéto sítě. O to spíš, když se jedná o ne příliš dobře zabezpečenou organizaci. Když si k tomu připočteme nejrychlejší připojení na světě, může útočník snadno získat velice silnou botnet síť, kterou následně může využít pro různé druhy útoků, například DDoS.

Proto je zapotřebí, aby organizace v Jižní Koreji nezanedbávali kybernetickou bezpečnost a nespoléhali se pouze na vyšetřovací metody. Problém ovšem je, že na vysokých školách a univerzitách se právě vyšetřovací metody vyučují primárně. Zabezpečení samotné již méně.

Výše uvedená tvrzení potvrzují dvě schémata. Na prvním si můžeme všimnout, že pro region, ve kterém se Jižní Korea nachází, máme výrazně vyšší podíl útoků typů botnet než je tomu v Evropě. Na stejném schématu taktéž vidíme vysoké procento útoků na mobilní telefony. Na druhém vidíme výrazně nižší četnost odhalení útoku interně, tedy samotnou organizací, pro tentýž region oproti Evropě.



Obrázek č. 23: Srovnání typů útoků v EMEA a APAC
(Zdroj: 61, s. 9)



Obrázek č. 24: Zdroj odhalení útoku v EMEA a APAC
(Zdroj: 62, s. 10)

Když se podíváme na statistiky kybernetických zločinů v Jižní Koreji, konkrétně na údaje za první polovinu roku 2019, máme zde 85 953 odhalených případů, což je 22,4% nárůst proti první polovině roku 2018. Z toho 1 734 kategorizovaných jako cybersecurity

incident crime, z nichž 1 294 byli případy hackingu. Cyber-enabled crime tvořil 72 139 případu, z nichž 65 238 byl internetových podvodů, 4 142 kyber finančních zločinů a 1 208 porušování licenčních práv. Nelegální obsah tvořil 12 080 případů, z toho 7 664 případů z kategorie osobní újmy, 3 155 online hazardu (který je v Jižní Koreji nelegální) a 1 115 případů nemravného obsahu. (55).

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole si ukážeme, jakým způsobem by mohla být výuka v České republice rozšířena. Uvedu zde příklady úkolů a cvičení, které jsem absolvoval v Jižní Koreji na Hallym University, včetně komentáře, proč si myslím, že by bylo vhodné jej začlenit do výuky i v českých školách, jaké výhody by to mohlo studentům přinést. Tyto úkoly a cvičení jsou inspirovány předměty Network Security & Forensics a Introduction to Digital Forensics, které jsou velmi často zaměřeny právě na vyšetřovací problematiku kybernetické bezpečnosti.

3.1 Dokumentace USB zařízení

Tento úkol se může jevit na první pohled jako příliš prostý a zbytečný. Nicméně si brzy ukážeme, že často opomíjené věci, jako je tahle, mohou znamenat velký rozdíl.

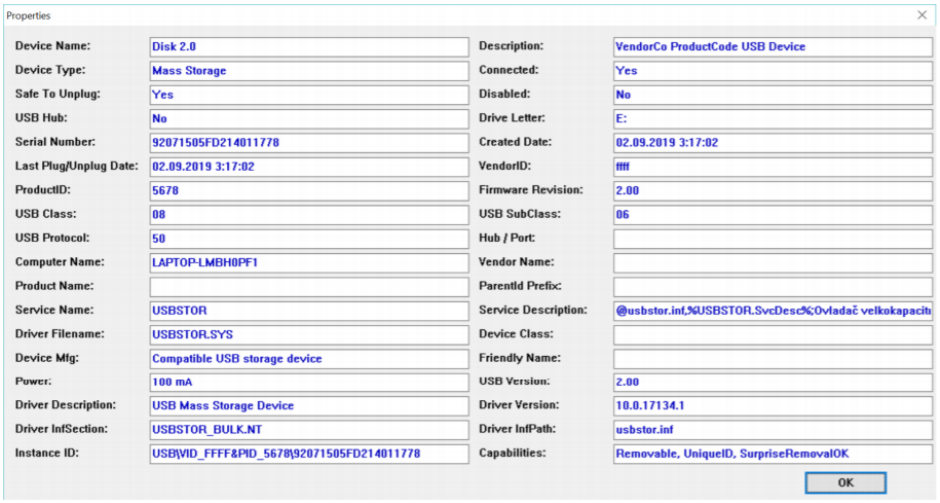
3.1.1 Zadání úkolu:

S vaším USB diskem:

- Zdokumentujte sériové číslo
- Zdokumentujte aktuální souborový systém
- Naformátujte disk na FAT32
- Opět zdokumentujte souborový systém

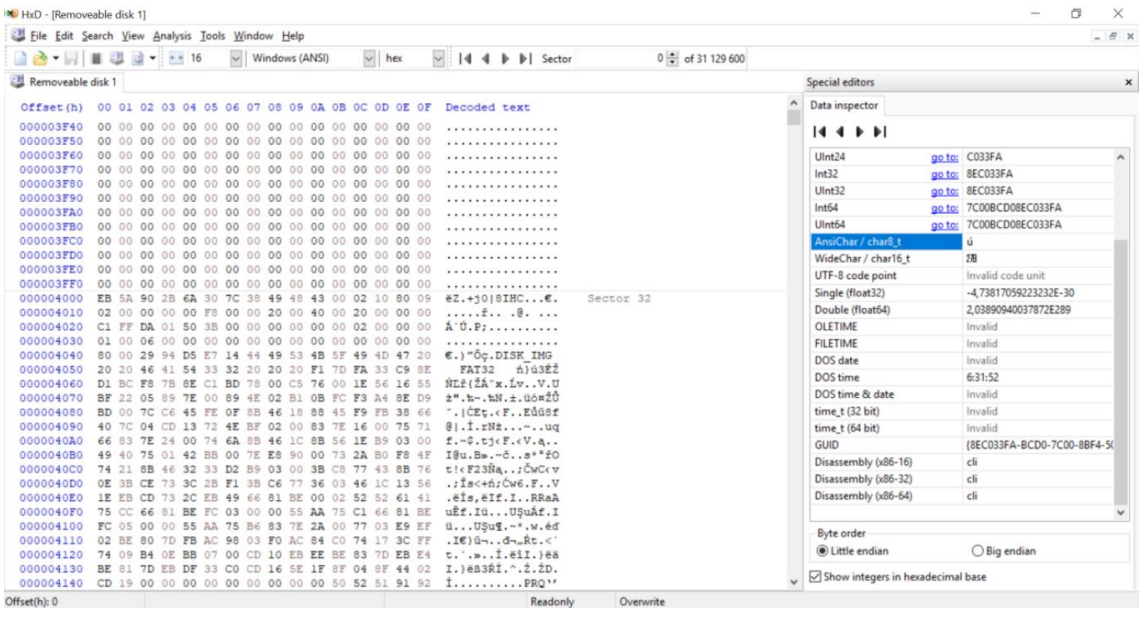
3.1.2 Vypracování úkolu:

I když se může zdát úkol zbytečně jednoduchý, primární důležitost byla na dokumentaci. Ta musela být v souladu s pravidly digitální forenzní analýzy, nakládáním s důkazy a s chain of custody. Pro vypracování tohoto úkolu jsem zvolil program USBDeview.



Obrázek č. 25: USB Deview – úkol 1
(Zdroj: vlastní zpracování)

Dalším úkolem bylo zjistit souborový systém. Na to jsem využil programu HxD. Zkušenější uživatel by si mohl říci, že je zbytečné zabývat se dodatečným program. Vždyť stačí použít Windows a pravé tlačítko myši, zobrazit si vlastnosti a souborový systém uvidím. Ale právě to je špatně z pohledu forenzní analýzy. Za prvé, tato metoda nemusí být dostatečně přesná a za druhé, může být USB disk přeformátován tak, že se například ve Windows bude tvářit jako FAT32, ale reálně bude mít souborový systém NTFS.



Obrázek č. 26: HxD screenshot – úkol 1
(Zdroj: vlastní zpracování)

Toto, ostatně jako všechny ostatní cvičení, mají studenty naučit primárně zacházet s dokumentací tak, aby byla využitelná při vyšetřování. Tedy i u soudu. Vyšetřovatel musí vždy naprosto přesně a neomylně prokázat kdy a jak daný důkaz získal. Stačí malá nejasnost v dokumentaci a celý důkazní materiál je neplatný. Musí taktéž naprosto správně odpovědět na otázky, které u soudu mohou zaznít. V tomto případě by například mohlo zaznít: „Jste si jistý, že má tento USB disk formát souborů FAT32?“. Uvedu zde dvě odpovědi, které by mohli zaznít:

„Ano, dal jsem pravé tlačítko myši v průzkumníku Windows a psalo to, že je systém souborů FAT32“.

A Druhá:

„Ano jsem si jistý, jak můžete vidět v dokumentaci, pro zobrazení obsahu důkazu číslo 1 v případě číslo xy, nalezeném na adrese x, na stole v kanceláři obžalovaného a to 3. května, 2018 v 11:30, tedy zde zobrazeného USB disku, jsem využil software HxD verze 2.3 a v sektoru 32 na adrese 000004050 tohoto zařízení jsem našel stopy, poukazující na formátování FAT32. To jsem taktéž poznamenal v dokumentaci, stejně jako hash tohoto disku, který je shodný po celou dobu trvání chain of custody, tudíž je prokázáno, že data na tomto zařízení nebyla změněna.“

I když se může jevit druhá verze jako zbytečně složitá a nadbytečná, rozhodně má nesrovnatelně vyšší šance uspět u soudu jako důkaz nežli verze první. Je třeba myslet na to, že v případě digitálních dat stačí i malé zaváhání a celý důkaz může být zneplatněn.

Zbytek úkolu by byl obdobný, tudíž jej není třeba dále rozvádět. Hlavním smyslem tedy bylo uvědomění si, že i k drobnostem, které využíváme každý den, je zapotřebí přistupovat zcela odlišně v případě vyšetřování kyberkriminálních případů.

3.2 Image disku a verifikace

V tomto úkolu jde především o zvládnutí správného vytvoření image disku či jiného zařízení, se všemi náležitostmi potřebnými pro vyšetřování. Pokud by vyšetřovatel pochybil v této části, zbytek vyšetřování je v podstatě zbytečný. Mělo také naučit studenty pracovat s hojně využívaným programem, primárně určeným právě pro tvorbu image souborů.

3.2.1 Zadání úkolu:

- Stáhněte si FTK imager
- Stáhněte si MD5 Sum portable

Vytvořte forenzní dokumentaci zobrazující následující proces:

- Vytvořte textový soubor pomocí poznámkového bloku. Vložte do něho text „Forensics is cool!“ a uložte soubor
- Použijte MD5 Sum k vytvoření hashe tohoto souboru a uložte jej
- Textový soubor nyní upravte na „Digital forensics is cool!“ a uložte jej
- Opět využijte MD5 Sum k vytvoření hashe a uložte jej
- Nyní znovu upravte text na původní text a uložte jej
- Pomocí MD5 Sum znovu udělejte hash a uložte jej

Dále:

- Vložte tento textový soubor na váš USB disk
- Vypočtěte MD5 hash vašeho USB disku
- Vytvořte physical disk image vašeho USB disku
- Vypočtěte MD5 hash této vytvořené image
- Odpojte USB disk
- Otevřete image v FTK imager
- Rozbalte váš textový soubor, vypočtěte jeho hash a ujistěte se, že se nezměnila

3.2.2 Vypracování úkolu:

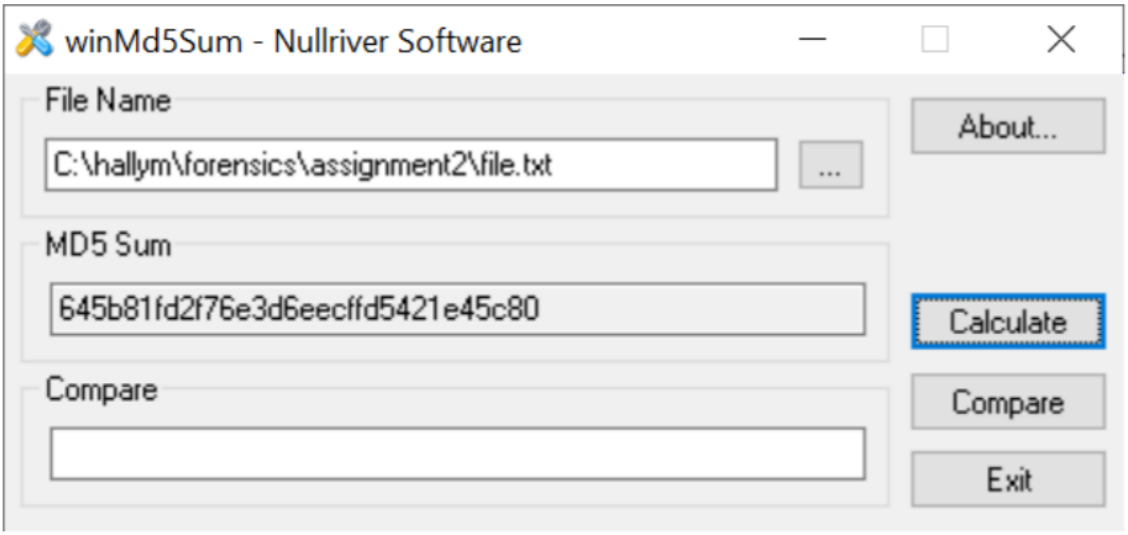
Nejdůležitější částí tohoto úkolu je právě forenzní dokumentace. Student si musí osvojit principy, které pro takovouto dokumentaci platí. Co patří do hlavičky takového souboru, jaké náležitosti musí obsahovat, na co se nesmí zapomenout.

Jmenovitě například využívání časových razítek – při vytvoření souboru, při každé editaci souboru, při každé manipulaci s důkazy. Dále dodržování chain of custody, uvádění zodpovědných osob, kde, kdy a jak získal informace či data a podobně.

Dále na tomto úkolu student pochopí fungování hash souboru.

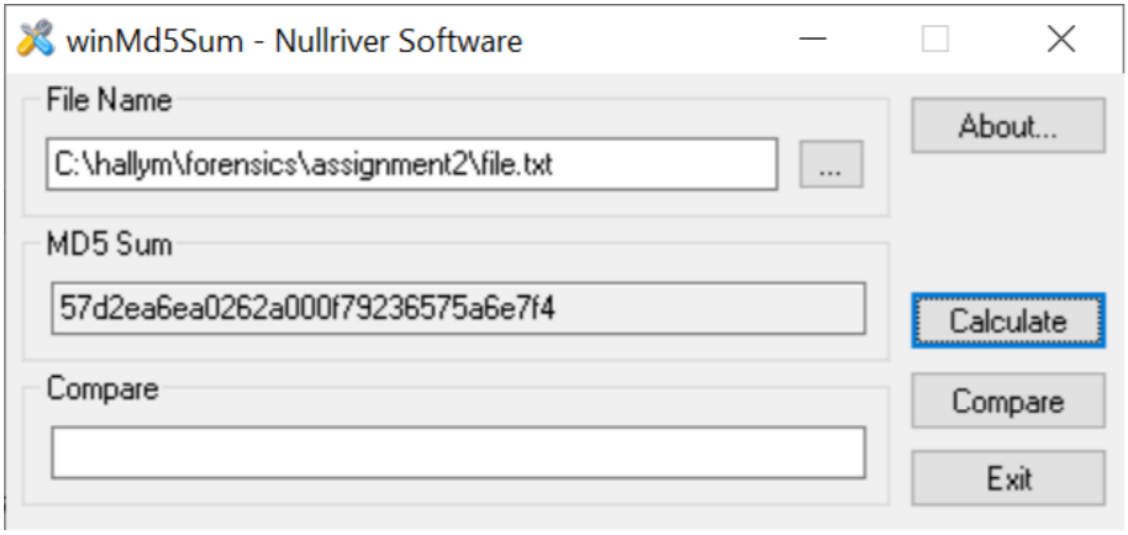
Některé nedůležité části přeskočím, abychom se dostali k tomu podstatnému.

Níže můžeme vidět využití softwaru MD5 Sum, který využijeme k vytvoření MD5 hashe. Při práci na digitální forenzní analýze je znalost a ovládání hashů naprostou nezbytností.



Obrázek č. 27: MD5 Sum – první hash
(Zdroj: vlastní zpracování)

Na dalším screenshotu máme vytvořený hash pomocí stejného softwaru, jen byl text uvnitř souboru pozměněn. Vidíme, že i malá změna způsobila vytvoření naprosto odlišeného hashe souboru.

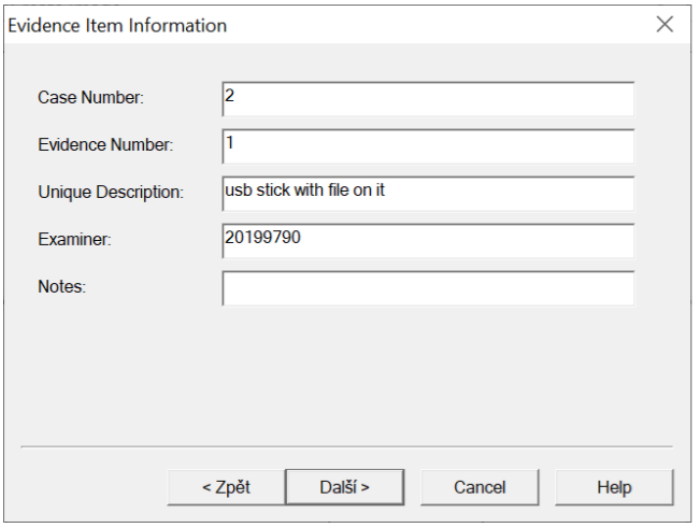


Obrázek č. 28: MD5 Sum – druhý hash
(Zdroj: vlastní zpracování)

Nakonec byl text v souboru opět pozměněn na původní hodnotu a porovnán s první hodnotou. Hodnoty byli totožné. Jak můžeme tedy vidět, meta data, tedy údaje o vytvoření souboru, název a podobně, nemají žádný vliv na podobu hashe souboru.

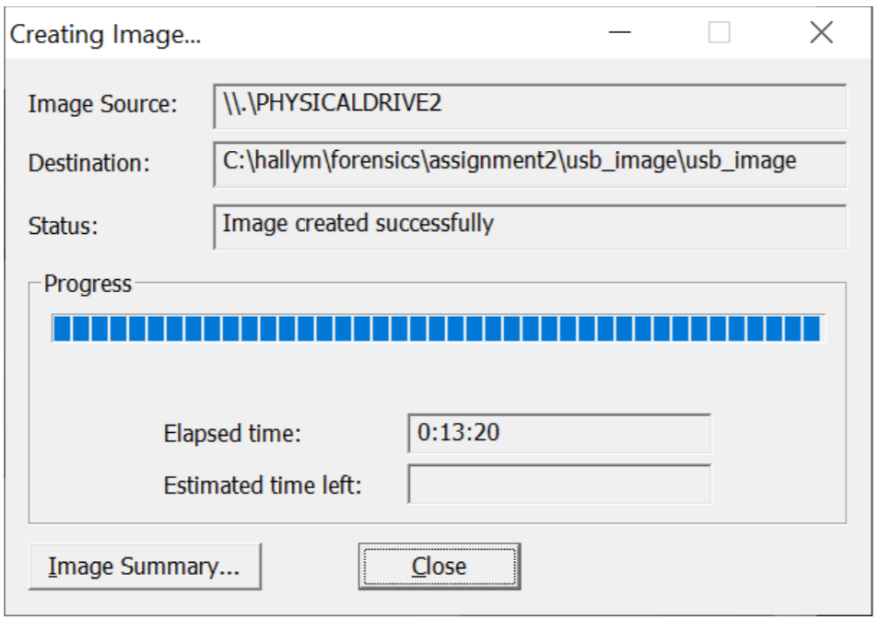
Dále jsem uložil textový soubor na flash disk. Spočítal jeho hash, který byl stále stejný. Nyní bylo zapotřebí vytvořit physical disk image. Pro tento účel jsem využil doporučený software FTK imager.

V něm přes záložky File -> Create disk image -> Physical drive -> Select my device jsem zvolil můj USB disk. Další okno nám naznačuje, že se opravu jedná o software využívaný pro vyšetřování, máme zde totiž položky číslo případě, číslo důkazu, unikátní popis a vyšetřovatel.



Obrázek č. 29: FTK imager – možnosti
(Zdroj: vlastní zpracování)

V dalším okně se pak zadává cesta uložení výsledného souboru, případně jeho rozdělení na více menších souborů. Poté se již vytvoří samotná image.



Obrázek č. 30: FTK imager – vytváření image
(Zdroj: vlastní zpracování)

O tomto procesu nám program zobrazí také kompletní logy. Ty jsou další důležitou součástí dokumentace pro forenzní analýzu, tudíž i s nimi se student musí naučit pracovat. FTK imager sám při vytváření image vytvoří hash této image a to jak MD5, tak SHA1. To jen potvrzuje jeho určení při práci na vyšetřování digitální forenzní analýzy.

Po odpojení USB disku bylo dalším úkolem připojit image soubor. Ten se poté chová stejně, jako bychom doopravdy připojili fyzické USB zařízení.

Student si tedy v tomto úkolu osvojí práci nejen s image soubory ale i hashem a dokumentací. Také mu to umožní pochopit, že při digitálních forenzní analýzách nikdy nepracuje se samotnými důkazy, pouze v případě vytváření image těchto důkazů, poté již veškeré činnosti provádí právě nad vytvořenou image. Veškeré kroky samozřejmě musí být zaneseny do dokumentace ve vhodné podobě a se všemi náležitostmi.

3.3 Průzkum cloudových služeb

Tento úkol je dosti odlišný od předchozích. Jedná se o průzkum cloudových služeb, konkrétně jejich smluvních podmínek. I když se může zdát, že s vyšetřováním kybernetických zločinů nijak nesouvisí, opak je pravdou. Mějme situaci, kdy je při vyšetřování nalezen jako důkaz prvek IoT, kupříkladu hlasový asistent – tedy zařízení, které po celou dobu vyčkává na hlasové příkazy uživatele. Nahrává tedy hlasovou stopu. Velmi malá část této stopy je ovšem uložena v samotném zařízení. Naprostá většina těchto dat je v cloudu. Proto by měl vyšetřovatel znát principy těchto služeb, stejně tak rozumět smluvním podmínkám. Měl by vědět, kde zjistí, jaká data daná cloudová služba uchovává, jak je získat zdali je to možné a podobně. Často tato data mohou hrát klíčovou roli v případu. Například případ vraždy, kdy potřebujeme přesně stanovit čas úmrtí. Dříve by se jednalo pouze o odhad, ale díky dnešním moderním technologiím můžeme čas stanovit klidně s přesností na vteřiny, pokud měla oběť chytré hodinky či náramek. Ty totiž zaznamenávají pohyb v podobě kroků, ale také prudký pohyb, v tomto případě pád na zem, po kterém pohyb skončí. Tato data bývají většinou synchronizována do mobilního telefonu, ale také na cloud. Pokud se nepodaří dostat k obsahu telefonu, může být cloud jediným možným zdrojem důkazů.

3.3.1 Zadání úkolu:

Vyberte 5 cloudových služeb které využíváte a pro každé odpovězte na následující:

- Která data cloudová služba uchovává
- Ke kterým datům má uživatel přístup
- Uchová cloudová služba data i po smazání či nikoliv

3.3.2 Vypracování úkolu:

Při vypracovávání úkolu jde především o to, aby si student uvědomil, jak může cloudové služby využít pro získávání důkazů. Dále také to, že většina cloudových služeb si ukládá více dat, než ke kterým má uživatel přístup. Vede to také k zamyšlení, zdali by daná služba tato data poskytla pro potřeby vyšetřování. Zde je nutné se také zamyslet nad tím, kde mají dané cloudové služby svoje data uložena, jelikož na tyto data poté platí zákony podle státu, ve kterém jsou fyzicky uloženy. Například cloudová služba, která má data v USA, nejspíše nebude příliš ochotně poskytovat data při vyšetřování případu z Číny. I to ovšem musí vyšetřovatel brát při vyšetřování v potaz.

3.4 Dokumentace místa činu

Vyšetřovatel nepracuje pouze s počítačem a daty, ale taktéž fyzicky sbírá důkazy na místě činu. Tento úkol dopomůže názorně si představit, co vše by něco takového mohlo obnášet a také na co si dát pozor, jak postupovat.

3.4.1 Zadání úkolu:

Proveďte dokumentaci vašeho pracovního místa tak, jako by se jednalo o místo činu. Berte v potaz každé zařízení a také to, jak by s ním mělo být zacházeno.

3.4.2 Vypracování úkolu:

Pro lepší představu zde přiložím částečné vypracování úlohy:

„23.09.2019 10:22

Vyšetřovatel: 20199790

Místo: Pracovní stůl na pravé straně (zády k tabuli) v první řadě

Číslo případu: 0001

Počet lidí v místnosti: 16

Číslo soudního příkazu: 675678

Podezřelý: John Madman, v místnosti

Oběť: Lady Victim, není na místě činu

Žádný nález na stropě, zdi neotevíratelné, jsou na ní dvě zásuvky, síťový adaptér, kovový předmět ležící na podlaze, vedle levé nohy stolu, u levé strany stolu další kovový předmět a plastová lišta – možná místo pro úkryt nějakých věcí, na stole klávesnice se silikonovým obalem, vedle ležící černá čepice – nejspíše by v ní mohli být nějaké vlasy k získání DNA, prázdná láhev od pomerančového džusu – taktéž by mohla sloužit ke zjištění DNA, na stole stopy od rozlité kávy, pod stolem otevřený kryt se síťovými kabely – možná s nimi bylo manipulováno…"

I když se může zdát, že tato dokumentace je přehnaná, nemusí být. Často i na první pohled zbytečné detaily mohou vést k důležitému důkazu – kupříkladu víme, že podezřelý nepije kávu? Tak se můžeme domnívat, že toto místo u stolu nebylo jeho, ale i tak to nevíme jistě. Je důležité si dávat pozor také na předsudky a předčasné závěry.

Další důležitou součástí tohoto úkolu bylo uvědomit si, že na místě činu má vyšetřovatel často velmi omezený čas. Musí tedy pracovat systematicky a efektivně. Často si musí dělat pouze stručné poznámky, ale i ty musí obsahovat veškeré náležitosti, aby byl poté schopen sepsat kompletní dokumentaci.

Nástroj, který mu v tom může silně pomoci, jsou fotografie. Na nich je důležité uchovávat časová razítka. I přes časový nátlak nesmí pokud možno vynechat jediný důležitý důkaz. Dále je důležité zajistit při vyšetřování místnost, osoby v ní, zjistit zdali je v místnosti pachatel a podobně. Nejdůležitější věc, na kterou musí totiž vyšetřovatel vždy pamatovat jako první je jeho vlastní bezpečí.

Nesmíme ani zapomínat na podstatu nalezených důkazů – kupříkladu zapnutý počítač na místě činu. Ten může obsahovat velice důležitá data – ovšem může o ně také velmi brzo přijít. Může být připojen k sítí, přes kterou díky vzdálenému přístupu, může pachatel data smazat. V určitých případech se naopak může stát, že potřebujeme nechat běžet síťový provoz, abychom získali určitý důkaz. Často se však vyšetřovatel dostane do velmi složité situace – mějme kupříkladu případ nelegálního sdílení filmů pomocí sítě torrent. Vyšetřovatel je ze zákona povinen ihned této nelegální činnost při zjištění zabránit. Pokud tak ovšem učiní, přijde například o spojení na další počítače, které by mohli být dalším důkazem. Pokud tak neučiní, neřídí se zákonem. Dostáváme se tedy do velice složité situace, kdy nám celé vyšetřování začíná silně komplikovat právní stránka věci. Proto je taktéž zapotřebí, aby vyšetřovatel první stránku znal, věděl jak si počínat a jak se

zachovat. Kupříkladu může nechat běžet síťový provoz pro zjištění dalších důkazů, ale musí být schopen toto jednání obhájit před soudem.

Další problematika, které musí vyšetřovatel věnovat pozornost, je volatilita dat. Pokud vidí na místě činu zapnutý počítač či jiné zařízení, může se mu s využitím vhodného vybavení podařit získat důkazy z například z cache paměti procesu či RAM paměti. Ovšem při manipulaci s počítačem, který je vlastně důkazním materiálem, musí zacházet s maximální opatrností – každá činnost, kterou provede, mění obsah paměti, jinak řečeno manipuluje s důkazy. To by za normálních podmínek bylo nepřípustné, ale pokud dokáže odůvodnit vyšetřovatel svoje počínání před soudem, je to povoleno. Musí například dokázat, jakou část RAM paměti znehodnotil jeho software pro vytváření image z RAM paměti a jaká část dat zůstala nezměněna. Při této činnosti musí vyšetřovatel perfektně znát veškerou činnost jeho nástrojů, na jakém přesně principu fungují, jaká data po sobě zanechávají a podobně.

Pokud možno by se ovšem měl snažit nemanipulovat s daty a jako první věc by měl vytvořit image všech disků a dalších paměťových zařízení. Po celou dobu by pak měl udržovat hash jak originálního paměťového média, tak image souboru, která musí být shodná.

3.5 Zajištění paměťového média na místě činu

Tento úkol navazuje na úkol předchozí a naučí studenty, jak se zachovat, pokud najdou paměťové médium na místě činu. Na co si musí dát pozor, jakým chybám se vyvarovat.

3.5.1 Zadání úkolu:

Našli jste zapnutý počítač na místě činu a v něm zasunutý USB disk. Jak sesbíráte data podle principů forenzní analýzy? Vytvořte dokumentaci.

3.5.2 Vypracování úkolu:

K tomuto úkolu přidávám vypracované řešení pro větší názornost:

„9/25/2019 10:14 AM

Nacházíme zapnuté PC na místě činu, ve kterém je zasunutý USB flash disk. Po zabezpečení místa činu a ujištění se, že je místo činu bezpečné, jsem zdokumentoval celé místo činu pomocí fotografií. Nyní se zaměřuji na samotný flash disk. Od pohledu můžeme vidět, že se jedná o USB flash disku značky iCube, 16GB paměť, modrá barva. USB disk nebudu vyšetřovat v počítači, ve kterém se právě nachází, aby nedošlo k žádným změnám a tím k porušení důkazu. Abych jej ale mohl vysunout z počítače, musím se ujistit, že neprobíhá na USB disk žádný zápis a že není šifrovaný. Pokud jsou všechny tyto okolnosti v pořádku, vysunu USB disk do správně označené složky na důkazní materiál, který následně převezeme na stanici, kde bude pokračovat další postup, tedy vytvoření image a samotná forenzní analýza.

9/25/2019 15:18 AM

Vkládám USB flash disk do mé forenzní stanice a pomocí softwaru FTK imager verze 1.3 vytvářím image.

Ta je ukládána do složky: D:\cislopripaduXY\images\dukaz1\dukaz1.dd. Po celou dobu mám nasazené rukavice, aby nedošlo k poškození otisků prstů. Po dokončení image uložím USB flash disk zpět do určené složky a předám k dalším analýzám. Vše je zaznamenáno do chain of custody. Ukládám hash samotné image a pokračuji s vyšetřováním obsahu disku…“

Je důležité všímat si drobných detailů, jako je zacházení s důkazem, veškerá dokumentace a další nutné náležitosti, bez kterých by důkaz neobstál u soudu.

3.6 Přepsání dokumentace

Tento úkol studenta opět zdokonaluje v sepisování dokumentace, která je pro vyšetřování klíčová. Jedná se taktéž o sepsání žádosti o soudní příkaz. I to je součástí práce vyšetřovatele, proto je nutné si tuto problematiku osvojit. Student si musí nastudovat dle

vzorů veškeré náležitosti dokumentace a osvojit si je. Dále si vyzkouší správnou práci s chain of custody, naprosto nezbytným nástrojem v oblasti digitální forenzní analýzy.

3.7 Analýza mobilních dat

Pro tento úkol student obdrží již vytvořenou image. Jedná se o image mobilního telefonu. To znamená, že některé principy a metody z běžné digitální forenzní analýzy nemusí fungovat a bude potřeba použít metody jiné. Pro analýzu využijeme software Autopsy, který je určen přímo na digitální forenzní analýzu. Navíc, obsahuje speciální nástroje pro analýzu chytrých mobilních telefonů. Naučit se správně pracovat s takovýmto softwarem je pro vyšetřovatele stejně klíčové, jako dokumentace. Pochopitelně je na každém vyšetřovateli, jaký nástroj zvolí, nicméně já bych rozhodně Autopsy doporučil – jedná se o volně dostupný nástroj, který vyšetřovací práci dokáže značně usnadnit.

3.7.1 Zadání úkolu:

Student obdržel scénář vyšetřovaného případu a image mobilního telefonu. Na základě scénáře měl sestavit hypotézy, které pomocí analýzy následně zkusí vyvrátit či potvrdit.

Scénář vypadá následovně:

„15:31 on 2017-07-17 obdržela Chuncheonská tísňová linka telefonát od místního správce budovy. Muž, který v této budově žije, tvrdí, že jeho žena (Betty) byla v jejich bytě. Policie reaguje.

15:40 2017-07-17 přijíždí policie na místo činu a nachází manžela (Simon H.) a manažera budovy (KIM Kil W.) před budovou. Byt je zajištěn a žena je nalezena na podlaze v obývací místnosti. Nedýchá a nemá puls. Z prvního ohledání se ukazuje, že utržila několik bodných ran. Přijíždí lékařská služba a potvrzuje, že úmrtí oběti.

15:50 2017-07-17 vyšetřovatel 1 vyslýchá správce budovy (pana Kima) a manžela (pana Simona H.). Správce budovy tvrdí, že pan Simon H. seběhl dolů po schodech s křikem a voláním po policii. Výslech Simona H. uveden níže v příloze A.

15:50 2017-07-17 prohledání bytu odhaluje následující digitální zařízení:

- *Senzor u hlavních dvěří*
- *Pohybový senzor na polici*
- *Chytrý náramek na zápěstí oběti*
- *Mobilní telefon u těla oběti*
- *Amazon Echo zařízení*
- *Google OnHub wifi router připojen k SmartThings Hub a IPTime switchi*
- *Samsung SmartThings hub*
- *IPTime switch hub*
- *Modem*
- *Raspberry Pi připojen pomocí HDMI k TV*
- *Bluetooth sluchátka*
- *Senzor dveří v ložnici*
- *Telefon oběti – Samsung Note II, černé barvy - /002-BettyNote2Black/SHV-E250L_Physical_20170717/*

Příloha A: Vyšetřování Simona H.

15:49 2017-07-17

1. Jaké je vaše celé jméno? – Simon Hall.

2. Vaše zaměstnání? – Jsem programátor.

3. Žijete v tomto bytě? – Ano, žiji s Betty, moji manželkou.

4. Mohl byste popsat, co se stalo? – Díval jsem se na film. Když skončil, vešel jsem do obývacího pokoje a našel ji na ležet na podlaze.

5. Víte o někom, kdo by chtěl ublížit vaší ženě? – Ne, o nikom.

6. Měla nějaké přátele v okolí? – Myslím, že ne. Nedávno jsme se přistěhovali.

7. Kde jste se díval na film? – V naší ložnici.

8. Dokázal byste si vzpomenout kdy? – Myslím, že téměř tři. Nevím to jistě, možná okolo třetí.

9. Když jste sledoval film, neslyšel jste nic? – Poslouchala hudbu, takže jsem měl sluchátka, nic jsem neslyšel.

10. Dokážete si vzpomenout, na co jste se díval? – Jednalo se o drama z Youtube.

11. Všimli jsme si, že máte chytrou domácnost. Máte přístup k těmto datům? – Ano, mám je v telefonu.

12. Mohl bych požádat o přístup do vašeho telefonu? – Ano, samozřejmě.

13. Mohl bych dostat přístup k datům vaší chytré domácnosti? - Ano.

14. Mohl byste identifikovat tento černý Samsung Note II a Mi step náramek? – Ano, ty jsou Betty.

15. Znáte hesla do jejího telefonu? – Neznám.“

3.7.2 Vypracování úkolu:

Klíčový poznatek pro tuto úlohu je, naučit se pracovat se všemi dostupnými informacemi, efektivně a správně využít zdroje a možnosti. Je zapotřebí si všímat detailů, být důkladný. Vyšetřovatel musí uvažovat o všech možných zdrojích dat, musí si uvědomit, jaká data může z jednotlivých zařízení získat a jak mu mohou pomoci vyřešit případ.

Na začátku každého případu by si měl vyšetřovatel stanovit hypotézy – těch bývá zpravidla více. Při tvoření takovýchto hypotéz musí pamatovat na jednu věc – žádná hypotéza nemá 100% jistotu, dokud případ nevyřeší. Jsou zde samozřejmě určité pravděpodobnosti, se kterými může pracovat. Je třeba ale také pamatovat na to, že tyto pravděpodobnosti nejsou konstantní, budou se měnit s každým nalezeným důkazem. Dále všeobecně platí, že čím zkušenější vyšetřovatel, tím přesnější hypotézy může zvládnout sestavit.

Pro tento případ jsem sestavil následující hypotézy:

1) Vrahem je manžel. V takovýchto případech je partner nejčastější pachatel. Rozhodně měl příležitost tento zločin spáchat. Jeho odpovědi z výslechu se zdají příliš klidné a racionální. Při forenzní analýze dat musíme pamatovat, že je počítačový programátor. Tudíž je šance, že data budou zmanipulována. Dále zde máme určité nepřesnosti v jeho odpovědích – prvně tvrdí, že se díval na film. Později však odpověděl, že se jednalo o drama z youtube, což film tak úplně není. Na druhou stranu souhlasil s prohledáním jeho telefonu, buď tedy zmanipuloval

data, nebo za smrtí jeho ženy stojí někdo jiný. Další zvláštní věcí je to, že než aby sám zavolal policii, běžel pro správce budovy. Proč nezavolal ihned sanitku či policii?

2) Vzhledem k tomu, že manžel běžel za manažerem budovy místo hovoru na policii, můžeme se domnívat, že je manažer spolupachatel.
3) Mohla spáchat sebevraždu – i když v případě vícero bodných ran se to zdá nepravděpodobné, nicméně ne nemožné.
4) Taktéž to mohla způsobit úplně jiná osoba, například náhodný zloděj, kterého přistihla při krádeži, a on ji v panice zavraždil. Měli bychom zjistit, zdali nebylo něco ukradeno.

Určitě bychom dokázali vymyslet spoustu dalších hypotéz, hlavní ale je, pokusit se na daný zločin dívat z různých pohledů. Vyšetřovatel pak lépe určí, kam a jak se na data dívat.

Dále přejdeme k analýze image mobilního telefonu oběti. Pokud pracujeme s image, je třeba vnímat taktéž její formát. Nejběžnějšími formáty jsou E01(E02-E-03-…) a DD. Můžeme se ale setkat třeba i s formáty jinými, například MDF. Na takovouto image bychom běžně potřebovali proprietární software, ale i to lze obejít. Stačí jednoduše přepsat koncovku souboru na E01 a můžeme jej otevřít i v ostatních softwarech.

Je taktéž důležité pamatovat na to, že i uložení image musí mít správnou strukturu. Na to existují různá doporučení a každý vyšetřovatel si nakonec může zvolit vlastní systém. Důležité je, aby cesta souboru byla systematická. Může se kupříkladu stát, že u soudu zazní otázka o uložení souboru.

„Kde přesně jste měl uložený soubor s image tohoto důkazu? Jste si jistý, že nemohli vaše ostatní soubory znehodnotit tento důkaz?“

Uvedu dvě odpovědi, abych demonstroval opět důležitost připravenosti na podobné otázky.

Odpověď první:

„Měl jsem to uložené někde na disku, nejspíš ve stažených souborech. Ale nemělo by se mi to pomíchat s ostatními soubory, alespoň myslím.“

Odpověď druhá:

„Image k případu ze dne 4. 11. 2019 související s důkazem 4 jsem měl uloženou na fyzicky odděleném disku. Byla překopírována z USB disku zajištěného na místě činu do mé forenzní stanice, která není připojena do žádné sítě, aby nedošlo k možnému poškození jinými soubory či viry.

Cesta tohoto souboru byla: D:\case_001_04_11_19\images\exhibit04.mdf.*

Využil jsem pochopitelně jiný disk nežli systémový, abych zamezil pomíchání dat.“

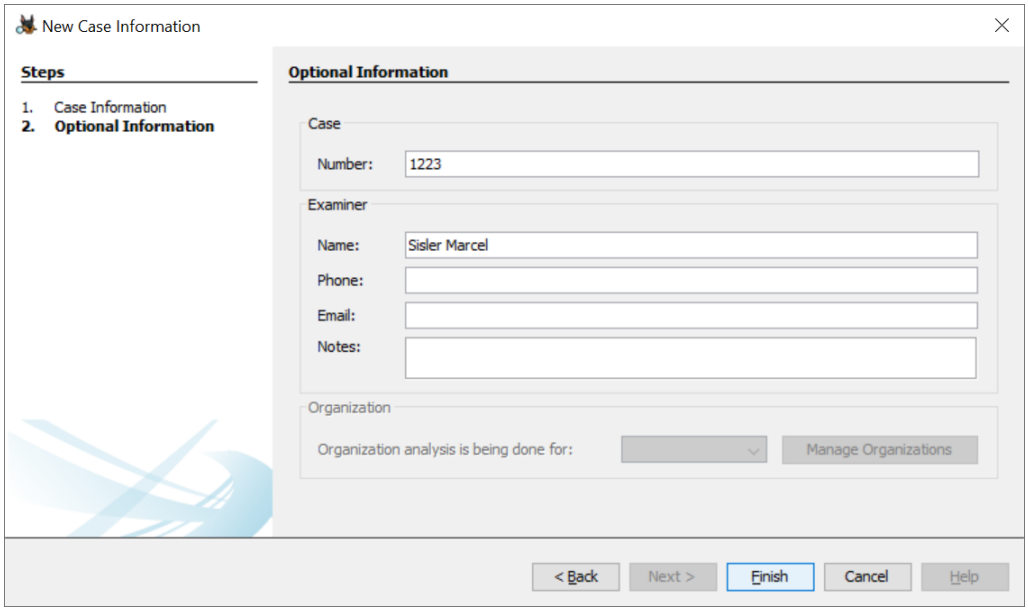
Nemusím asi vysvětlovat, která z daných dvou odpovědí by u soudu obstála lépe. I když se může zdát, že jsou občas tyto odpovědi přehnané, není tomu tak. Čím vyšší důvěryhodnost získáte jako vyšetřovatel, tím vyšší šance budete mít s obhájením důkazu.

Všimněme si taktéž systematicky zvolené cesty souboru. Můj systém je tedy:

Disk:\případ_číslo_den_měsíc_rok\images\důkaz_číslo\samotné soubory.

Pokud bude vyšetřovatel dodržovat určitý systém, jako například výše uvedený, tak i v případě že se ho někdo zeptá o 10 let později, kde měl uložený daný soubor, je schopen snadno a sebevědomě odpovědět.

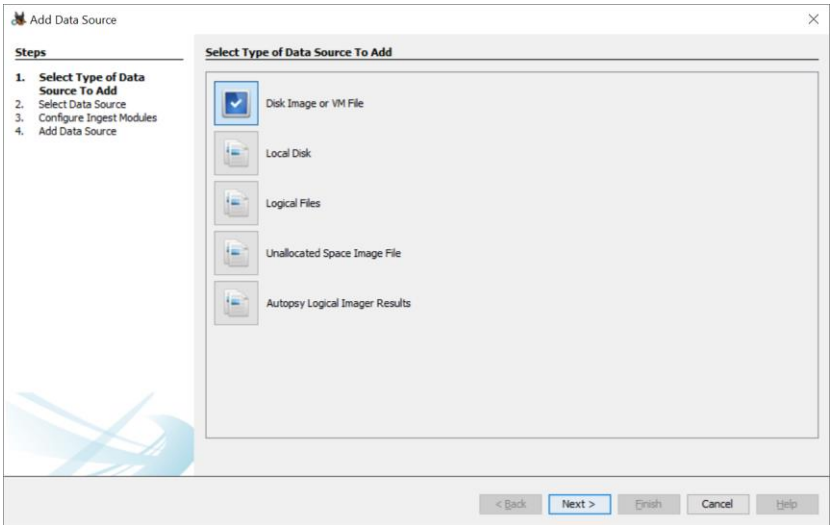
Nyní tedy k samotnému zpracování digitální forenzní analýzy. Využíval jsem softwaru Autopsy. Nejprve si vytvoříme nový případ. Dle doporučení o cestě souboru vytvoříme správnou strukturu složek. Dále zadáme údaje o případu:



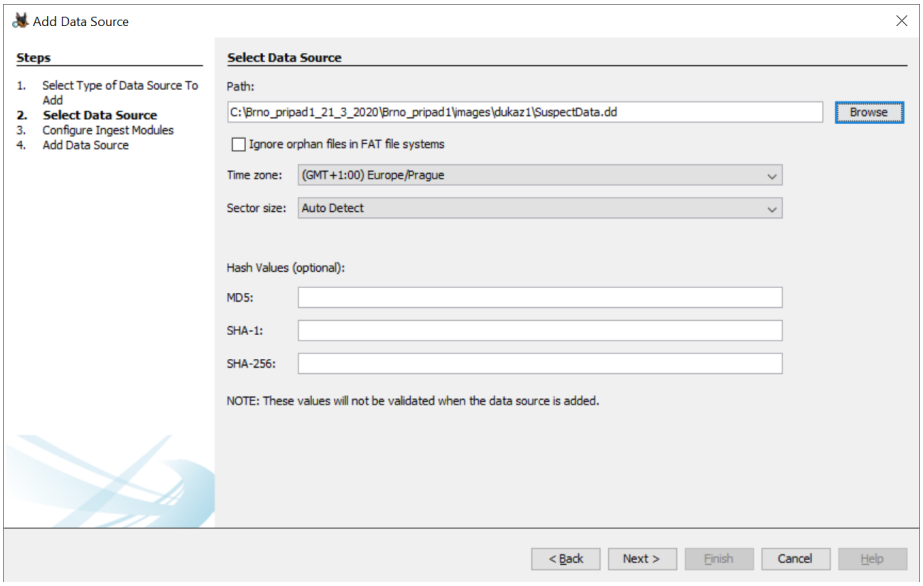
Obrázek č. 31: Autopsy – vytváření případu
(Zdroj: vlastní zpracování)

Jak můžeme vidět, jedná se opět o software přímo navržen na vyšetřování. Tím nám umožňuje využít spoustu nástrojů a taktéž usnadnit práci s dokumentací. Ve výše uvedeném okně zadáváme například číslo případu a údaje o vyšetřovateli.

Dále přidáme do případu soubor image:



Obrázek č. 32: Autopsy – přidání image 1
(Zdroj: vlastní zpracování)



Obrázek č. 33: Autopsy – přidání image 2
(Zdroj: vlastní zpracování)

Zde bych rád upozornil na údaj Time zone, neboli časové pásmo. Jedná se o podstatný a často přehlížený údaj. Při vyšetřování si musíme dávat pozor, z jakého časového pásma

data jsou, abychom byli schopni správně sestavit časovou osu. Ta nám může velice pomoci s vyšetřováním případu.

V dalším kroku přidávání dat nám Autopsy umožňuje spustit moduly, které spustí analýzu nad přidávanými daty. Tyto moduly pochopitelně můžeme spustit i dodatečně. Některé z nich jsou opravdu užitečným pomocníkem.

Například Extension Mismatch Detector, který zkontroluje přípony souboru s reálným typem souboru. Je totiž častým nálezem, že kriminálníci či hackeři se snaží maskovat například EXE soubory tím, že jim dají příponu JPG, tedy obrázku. Spustitelný soubor EXE potom nejde standardně otevřít ve Windows, jelikož se jej tento operační systém snaží otevřít jako obrázek. Tento modul tyto soubory identifikuje a vypíše nám jejich seznam. To může opravdu urychlit hledání souboru, protože tyto soubory budou s velkou pravděpodobností podezřelé.

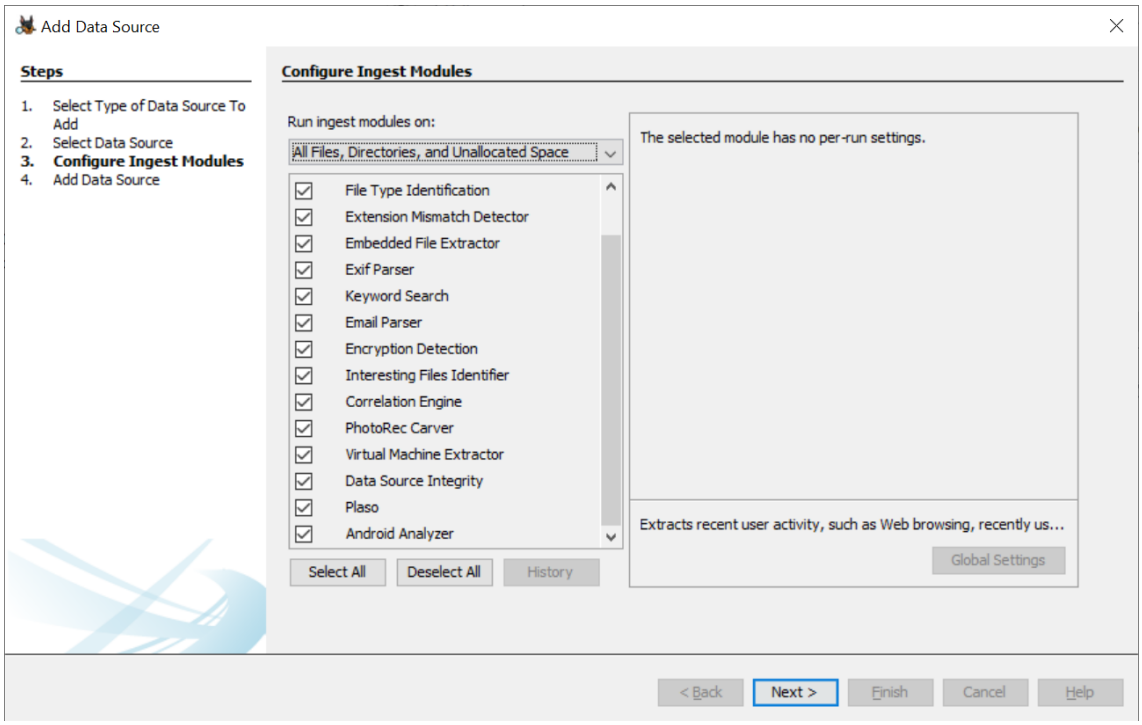
Exif Parser se nám pokusí získat EXIF informace z JPEG souborů, tedy například z fotografie údaje o času pořízení, lokaci a podobně.

Keyword search je jedním z nejužitečnějších nástrojů vůbec, proto se mu budu věnovat až později.

PhotoRec Carver nám dokáže „vydolovat“ obrázkové soubory z nealokovaného místa. Často se totiž stává, že kriminálníci od-alokují část paměti s nelegálními fotkami. Pomocí tohoto nástroje se nám tyto fotky najdou a vyextrahují.

Plaso zase pomocí časových značek u souborů sestaví časovou osu.

Pro tento případ je ovšem nejzajímavějším nástrojem Android Analyzer. Tento modul si poradí s image souborem Androidu, zná strukturu jeho dat, jak se ukládají aplikace, zprávy, kontakty a podobně. Proto velmi rychle dostaneme slušný přehled o datech, které tento telefon má.



Obrázek č. 34: Autopsy – moduly
(Zdroj: vlastní zpracování)

Vraťme se tedy nyní ke konkrétnímu úkolu. Známe přibližný čas vraždy a máme data z telefonu. Pomocí plaso analýzy jsme získali časovou osu. Při její analýze se díváme na časy okolo 15:31 dne 2017-07-17. Po důkladném hledání objevíme soubor s konverzací z nástroje pro instantní komunikaci.

Icon,"Date/Time","Description","Event Type"
true,"2017) Status: READ Type: RECEIVED","Other"
true,"2017-07-17 13:41:54","Sender: John Macron Body: How are you? Status: READ Type: RECEIVED","Other"
true,"2017) Status: READ Type: SENT","Other"
true,"2017-07-17 13:47:12","Sender: John Macron Body: Ugh. Work sucks Status: READ Type: RECEIVED","Other"
true,"2017-07-17 13:47:17","Sender: John Macron Body: I wanna see you later Status: READ Type: RECEIVED","Other"
true,"2017-07-17 15:03:45","Sender: Hallym Betty Body: I cant keep doing this Status: READ Type: SENT","Other"
true,"2017s too late now! U promised Status: READ Type: RECEIVED","Other"
true,"2017-07-17 15:04:18","Sender: Hallym Betty Body: Evwryone suspectbs Status: READ Type: SENT","Other"
true,"2017-07-17 15:04:36","Sender: Hallym Betty Body: It feels like they are warching us Status: READ Type: SENT","Other"
true,"2017re just paranoid.... Status: READ Type: RECEIVED","Other"
true,"2017-07-17 15:05:09","Sender: Hallym Betty Body: I cannot take it anymore Status: READ Type: SENT","Other"
true,"2017-07-17 15:05:22","Sender: John Macron Body: ... Status: READ Type: RECEIVED","Other"
true,"2017-07-17 15:05:25","Sender: Hallym Betty Body: Its over dont msg me Status: READ Type: SENT","Other"
true,"2017-07-17 15:05:40","Sender: John Macron Body: Who the fuck do you think k you are! Status: READ Type: RECEIVED","Other"

Obrázek č. 35: Autopsy – nalezená konverzace
(Zdroj: vlastní zpracování)

Jak vidíme, časy zpráv jsou chvíli před vraždou. Z obsahu se dovídáme nové informace – máme zde další osobu – John Macron. Z konverzace můžeme usoudit, že je dost velká

šance na to, že on a Betty spolu měli poměr. Taktéž můžeme usoudit, že Betty tento poměr chtěla ukončit, načež se J. M. rozhněval a začal ji vyhrožovat.

Tato nová informace může značně pozměnit hypotézy. Do dalšího vyšetřování z důvodu rozsahu a tématu této práce není nutno zacházet.

Důležité je, že si student v tomto úkole prakticky vyzkouší práci vyšetřovatele. Naučí ho, jak pracovat s hypotézami, dokumentací a nástroji pro digitální forenzní analýzu.

3.8 Analýza časové osy

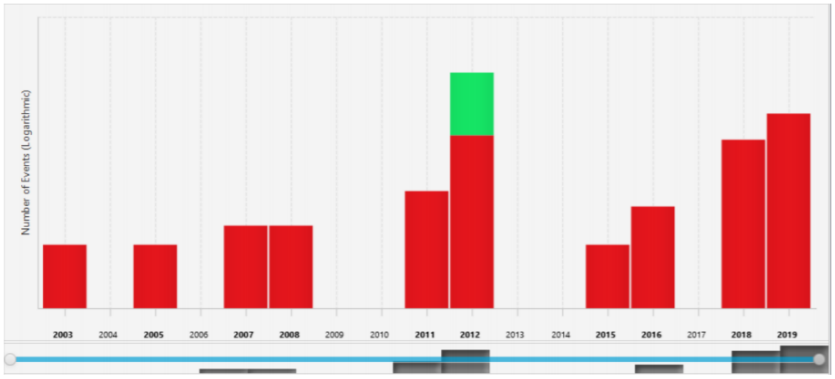
Jak jsem již zmínil, analýza časové osy je velice důležitá součást digitální forenzní analýzy. V tomto úkolu si student osvojí práci právě s časovou osou a pokusí se sestavit „příběh“ z nalezených dat.

3.8.1 Zadání úkolu:

Z USB disku sestavte v softwaru Autopsy časovou osu. Na základě této osy se poté pokuste sestavit scénář relevantní k datům na disku. Dále sestavte dokumentaci s náležitostmi digitálních forenzních dokumentací.

3.8.2 Vypracování úkolu:

Pro vypracování toho úkolu jsem opět využil Autopsy, který pomocí Plaso modulu vypomůže se sestavením časové osy. Výsledek může vypadat nějak takto:



Obrázek č. 36: Autopsy – časová osa
(Zdroj: vlastní zpracování)

Zde poté může vyšetřovatel filtrovat data, zobrazit si pro něho relevantní výsledky pomocí klíčových slov, změn souborů a podobně. Správné zvládání práce s časovou osou

je nezbytnou dovednostní při provádění digitální forenzní analýzy. Stejně je zapotřebí hlídat si časová pásma, jelikož bez nich by nalezené výsledky postrádali smysl.

3.9 Hashe a analýza klíčových slov

Nejen časová osa je mocný nástroj při digitální forenzní analýze. Když například děláme několikátý případ, zaměřený na stejnou problematiku, víme, jaká klíčová slova budou v případu hrát roli.

Například mějme organizovanou skupinu zakládající požáry. Získali jsme přístup souborům jednoho člena této skupiny. Než abychom pomalu procházeli jednotlivé soubory, což by zabralo příliš mnoho času a do té doby by se mohlo stát další neštěstí, využijeme klíčových slov. V tomto případě bychom nejspíše hledali slova jako požár, zapálit, hoří a podobně. Znát případ nám při vytváření slovníků klíčových slov značně pomůže. Je také dobré využít slovníky ze starších, podobných případů.

Hashe nám zase pomohou rychle a přesně odhalit a nalézt požadovaný soubor. Mějme například hackerskou skupinu, která šíří určitý vir. My už budeme znát jeho přesnou podobu, tedy soubor, který využívali na distribuci tohoto viru. Pokud jej budeme hledat v dalším zařízení, jednoduše využijeme hash vygenerovaný z toho souboru a budeme hledat shodu v novém médiu.

3.9.1 Zadání úkolu:

Úkol na procvičení něčeho takového může vypadat například takto:

Stáhněte si následující image soubor.

Z něho vhodnými forenzními technikami získejte hash klíče všech obrázků, na kterých je kočka.

Vytvořte z těchto hash klíčů databázi hashů.

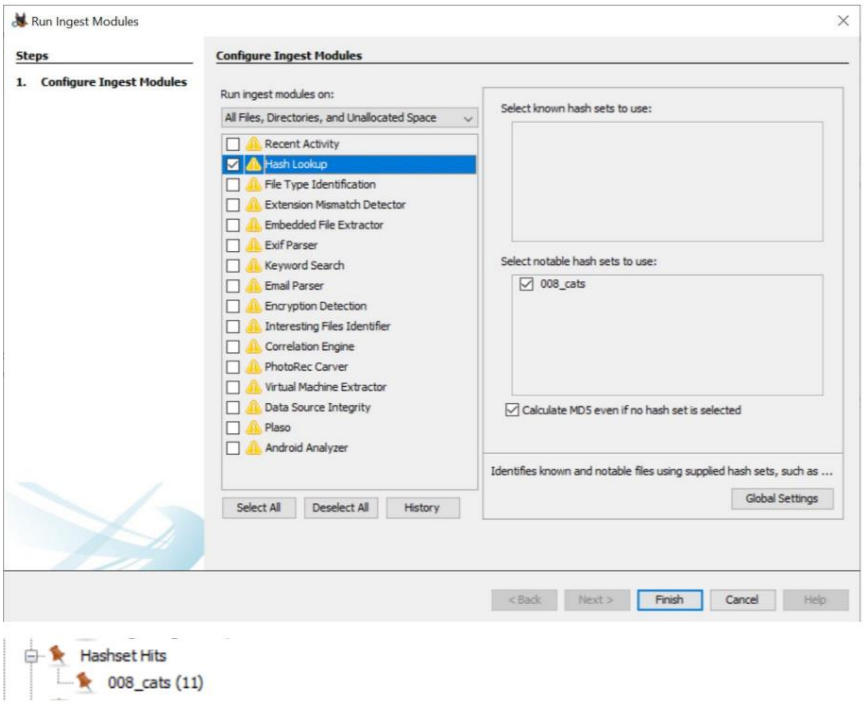
Využijte Autopsy modul pro práci s hashy a automaticky nalezněte všechny obrázky.

Dále vytvořte list klíčových slov a pomocí nástrojů nalezněte:

- Coffee, Meme
- 1 regulérní výraz

3.9.2 Vypracování úkolu:

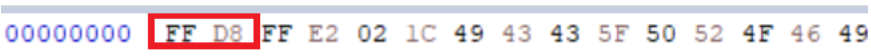
Zaprvé jsem si sestavil v Autopsy z nalezených souborů hash databází a poté využil nástroje Hash Lookup.



Obrázek č. 37: Autopsy – Hash Lookup
(Zdroj: vlastní zpracování)

Jak můžeme vidět, Autopsy nám poté vytvoří pro daný hash list odrážku se všemi shodami.

Zhruba stejně bychom postupovali u klíčových slov. Co se týče regulérních výrazů, mají zajisté své využití. Kupříkladu při hledání telefonních čísel v datech, využijeme zastupující znaky pro číslice, sestavíme přesný výraz pro telefonní číslo a zbytek práce za nás již udělá software. V tomto úkolu také stojí za zmínku, že některé soubory mohou být v nealokovaném prostoru. V některých případech musí vyšetřovatel vyhledávat v hexadecimálních hodnotách konkrétní předpony souboru, například pro JPG je to FF D8.



Obrázek č. 38: HxD – JPG předpona
(Zdroj: vlastní zpracování)

3.10 Případ Hackingu

Pro správný trénink vyšetřovatelů a pro trénink digitální forenzní analýzy, poskytuje taktéž NIST vhodné úkoly. Věřím tomu, že obdoba takové úkolu by mohla být vhodným testem do předmětů vyučující digitální forenzní analýzu. Tyto úkoly jsou volně dostupné na webu NIST, včetně správných odpovědí a **návodů** jak se k odpovědi mělo dojít.

3.11 Příklad závěrečného úkolu

Nyní uvedu příklad, ve kterém jsem využil veškeré dosud uvedené techniky. Ty mi dopomohli vypracovat se k možnému řešení případu. Musíme si ovšem uvědomit, že málokdy můžeme dojít k řešení, u kterého bude 100% jistota, že je správné. Pochopitelně se zvýšeným počtem důkazů roste také pravděpodobnost, že se jedná o správné řešení, proto se vyšetřovatel musí vždy snažit nalézt takovýchto důkazů co nejvíc. Musíme ale brát v potaz také to, že je často proti velice silnému nepříteli a tím je čas. Nejsou výjimkou případy, kdy má vyšetřovatel na případ pouze pár hodin a v případě, že jej nevyřeší včas, může dojít k tragickým událostem, například teroristickému útoku a podobně.

3.11.1 Zadání úkolu:

Podezřelý: Jim Cloudy

Obyvatel státu Alexandria, VA, USA

Bratr Jima, Paul, nahlásil na policii podezřelé dokumenty. Tvrdí, že dokumenty byli napsány Jimem. Policie získala povolení k prohlídce domu Jima a získala jeho laptop. Z něho byla vytvořena image, která vám je k dispozici.

Vyšetřete tuto image a posuďte, zdali podezřelý plánoval extremistické aktivity. Vaše tvrzení potvrďte důkazy.

3.11.2 Vypracování úkolu:

Jak jsem již uvedl, pro tento úkol je nutné využít všech výše uvedených technik, včetně správně sestavené dokumentace. Pokusím se přiblížit určité důležité kroky, ovšem celé vypracování zde není zapotřebí uvádět vzhledem k rozsahu práce.

Jako první si nachystáme strukturu složek, pochopitelně systematicky.

Zkontrolujeme si hash dané image a poté sestavíme hypotézy.

Poté začneme s analýzou v softwaru Autopsy. Při přidávání image si nezapomene nastavit správné časové pásmo, vzhledem k tomu že známe místo bydliště podezřelého tak to není problém. Sestavíme si vhodné slovníky klíčových slov vzhledem k povaze případu – například slova jako: zbraň, vražda, extremista, zastřelit, zapálit a podobně. Využíváme také všech možných tvarů těchto slov, což je bohužel nevýhoda českého jazyka.

Postupným prohledáváním možných souborů, historií prohlížečů, cloudových úložišť a podobně, postupně se můžeme dopracovat k důkazům, že daná osoba opravdu chystala extremistické aktivity. Nalezené výsledky musíme správně zanést do dokumentace. Opět se snažíme pracovat s každou informací, kterou máme k dispozici. Nesmíme zapomenout na závěr, kde shrneme výsledky a proneseme konečné prohlášení.

3.12 Detekce ARP poisonu

Tento úkol je zaměřen na síťovou problematiku, konkrétně na detekci ARP poisonu, což je druh útoku který zneužívá protokolu ARP, kdy se útočník v místní sítí vydává za počítač jiný pomocí falešné MAC adresy. Naučit se konkrétní síťové útoky může být obrovskou výhodou pro studenta v budoucí praxi. Taktéž dostane příležitost vidět, jak takový útok vypadá z pohledu pohybu na síti.

3.12.1 Zadání úkolu:

Ve dvojici určete jeden útočící systém a jeden cílový systém. Útočník provede ARP poison směrem na cíl. Vše zaznamenejte v softwaru Wireshark.

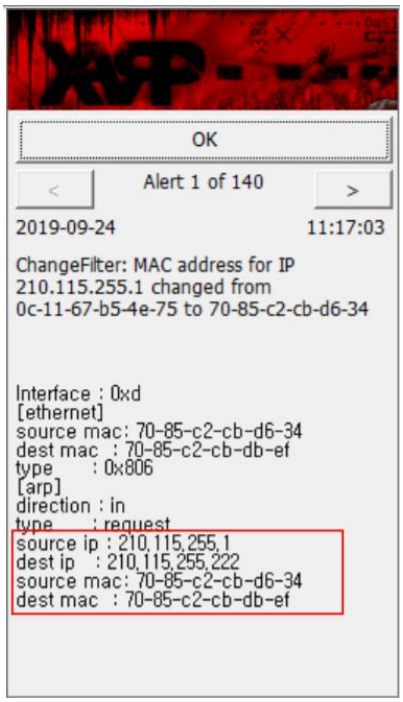
3.12.2 Vypracování úkolu:

V roli útočníka si jako první zjistíme IP adresu cíle, poté můžeme využít různé softwary již připravené pro ARP poison. Útok potom může vypadat velmi jednoduše, například zde v příkazové řádce:

```
C:¥Users¥user¥Desktop>arpspoof.exe 210.115.255.222
Resolving victim and target...
Redirecting 210.115.255.222 (70:85:c2:cb:db:ef) ---> 210.115.255.1 (0c:11:67:b5:4e:75)
        and in the other direction
Press Ctrl+C to stop
```

Obrázek č. 39: ARP poison – útok
(Zdroj: vlastní zpracování)

V roli obránce si můžeme zavést pomocný software pro detekci ARP poisonu, například XARP. Ten nás při útoku okamžitě varuje:



Obrázek č. 40: ARP poison – XARP
(Zdroj: vlastní zpracování)

Můžeme vidět, že došlo ke změně MAC adresy z 0c-11-67-b5-4e-75 na 70-85-c2-cb-d6-34, tudíž vidíme, že bylo manipulováno z ARP tabulkou. Útočníkova IP adresa zde byla 210.115.255.225 a MAC adresa byla 70-85-c2-cb-d6-34.

Pro zjištění stejného útoku v softwaru Wireshark můžeme využít filter:

arp.duplicate-address-detected

3.13 Analýza místní sítě

V tomto úkolu si student vyzkouší základní analýzu sítě. Podobné analýzy se velice hodí při vyšetřování, kdy jako první krok musíme zjistit, jak vlastně místní síť vypadá. Bez tohoto kroku bychom nemohli pokračovat s další analýzou, například tím jak probíhal nějaký útok.

3.13.1 Zadání úkolu:

Proveďte analýzu místní sítě a odpovězte na následující otázky:

- Kolik počítačů se nachází v místní síti
- Které služby jsou spuštěny v síti
- Která zařízení přenáší nejvyšší množství dat

3.13.2 Vypracování úkolu:

Pro analýzu místní sítě jsem využil software Wireshark a Nmap.

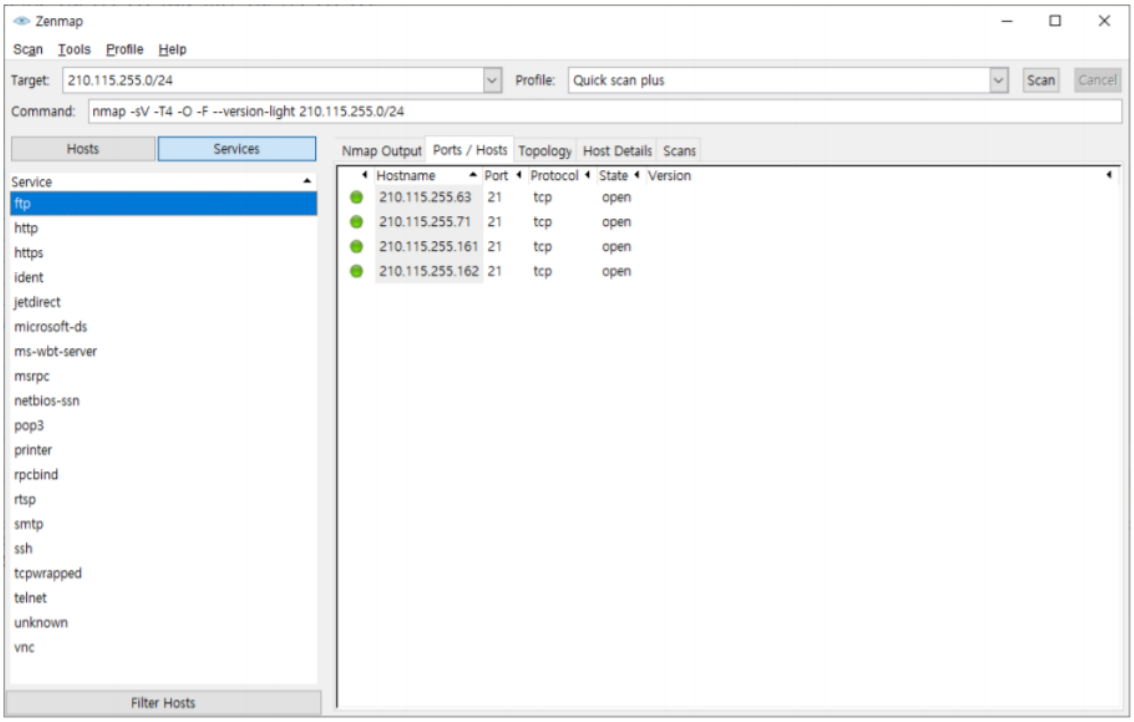
Nejprve jsem zadal do příkazu Nmap následující kód:

„nmap -sP 210.115.255.0/24“

Tím jsme získali informaci o počtu počítačů v místní síti:

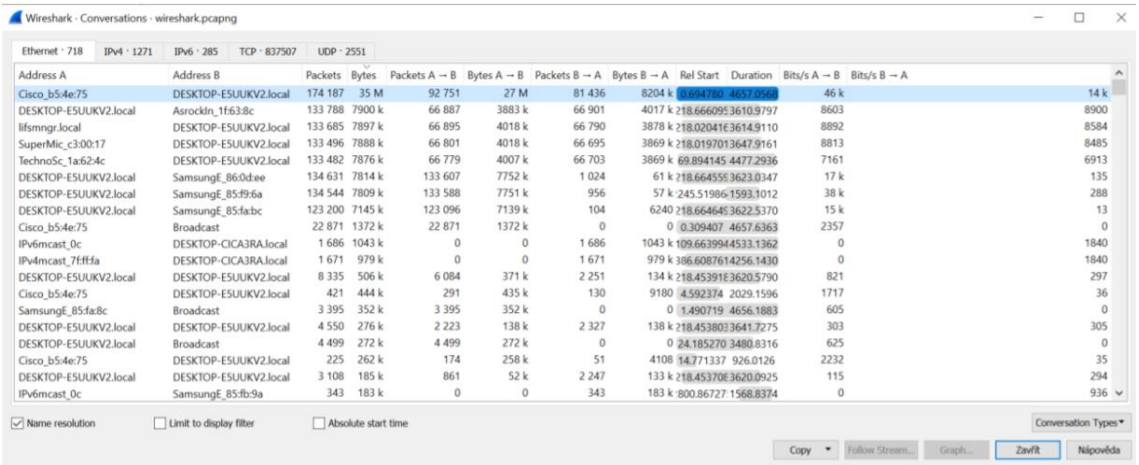
„Nmap done: 256 IP addresses (74 hosts up) scanned in 1.04 seconds“

Dále zjistíme, jaké služby běží v síti. Toho můžeme docílit vícero metodami, například opět v Nmap:



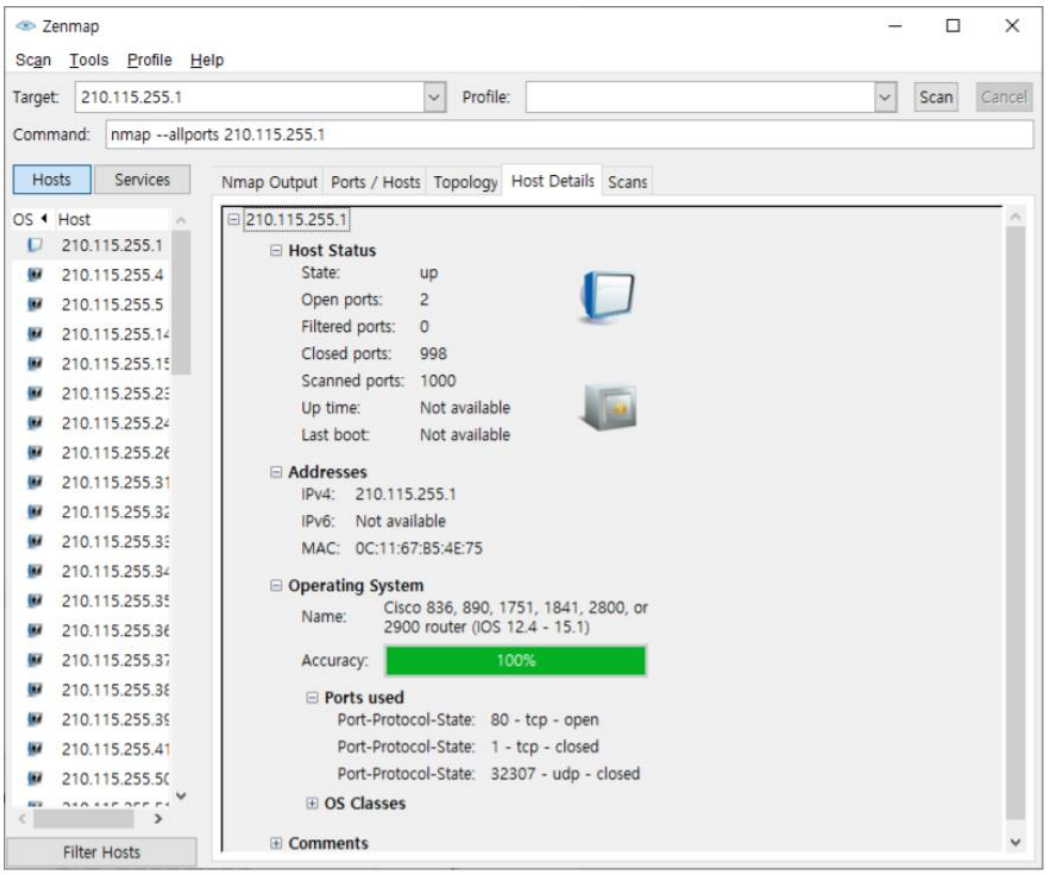
Obrázek č. 41: Nmap – FTP služba
(Zdroj: vlastní zpracování)

Takto můžeme zjistit otevřené porty pro jednotlivé služby. Můžeme taktéž analyzovat logy třeba v programu Wireshark. Ten využijeme hlavně v dalším úkolu, kdy zjišťujeme, které zařízení v sítí přenáší nejvíce dat.



Obrázek č. 42: Wireshark – objem dat
(Zdroj: vlastní zpracování)

Výše uvedenou tabulku získáme přes kartu conversations a můžeme si jej seřadit dle Bytes k zjištění největšího objemu dat. K zjištění bližších informací o tomto zařízení můžeme využít opět Nmap:



Obrázek č. 43: Nmap – adresa s největším objemem dat
(Zdroj: vlastní zpracování)

3.14 Práce s logy

Logy mohou být dalším, velice zajímavým zdrojem informací při digitální forenzní analýze. Proto je velice vhodné si práci s nimi osvojit. V následujícím cvičení student získá představu o struktuře i umístění, dále také pochopí základní principy logování a jak je může využít.

3.14.1 Zadání úkolu:

Odpovězte na následující otázky:

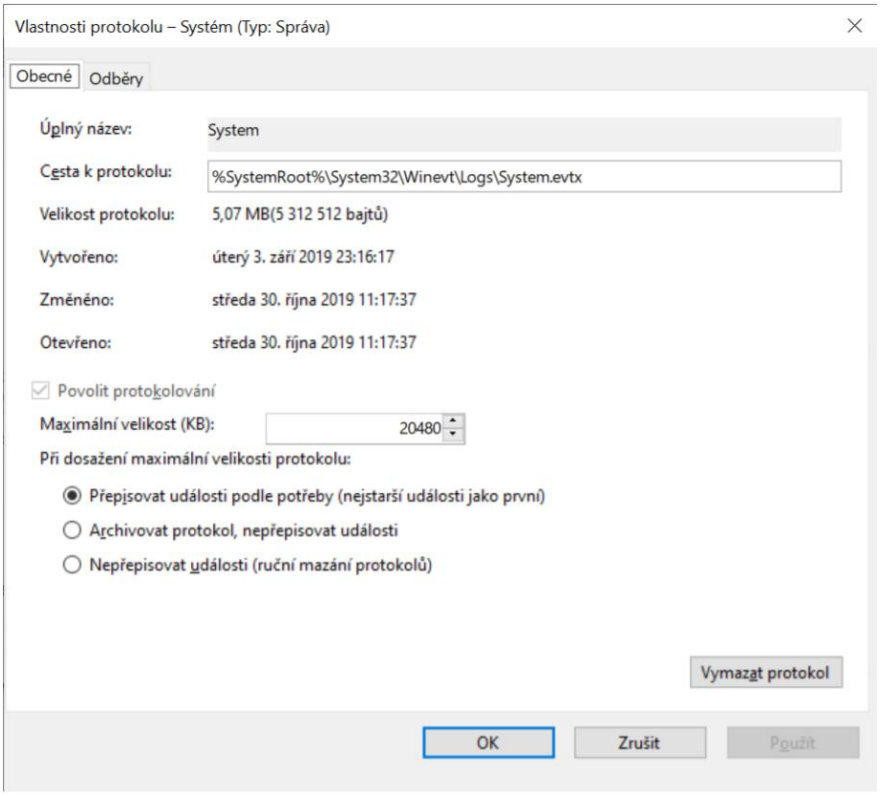
- Kde jsou ve vašem počítači uchovány systémové logy
- Kolik záznamů je momentálně v systémových lozích
- Jaké typy informaci v nich můžeme nalézt
- Kde je ve vašem počítači uložen firewall log
- Kolik záznamů obsahuje

- Nalezněte jakýkoli aplikační log
- Co se v něm můžete dočíst

3.14.2 Vypracování úkolu:

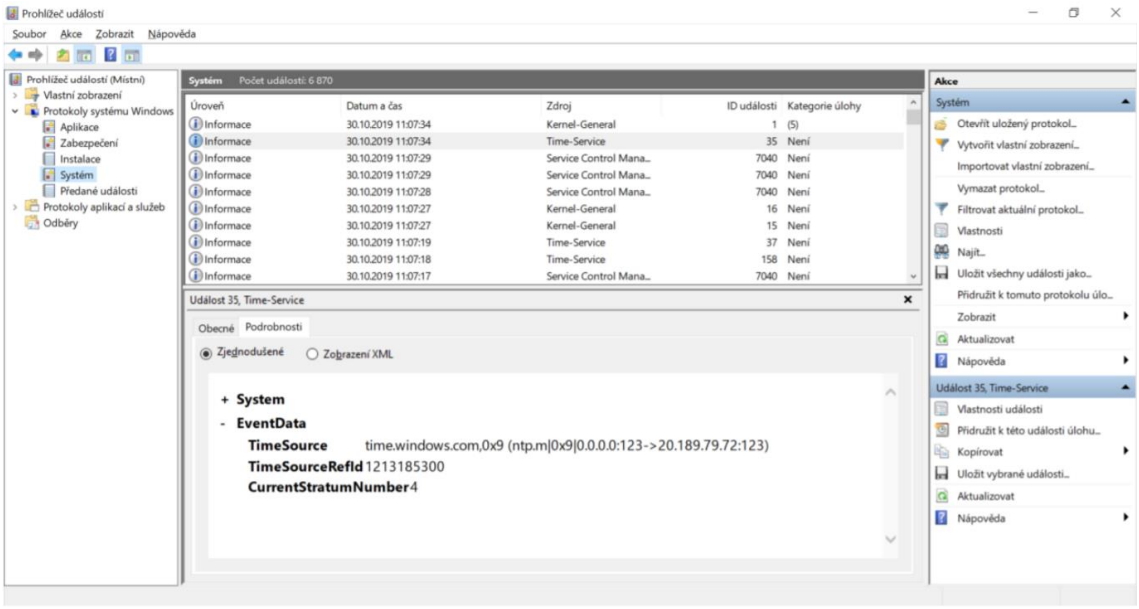
Systémové logy nalezneme na cestě:

%SystemRoot%\System32\Winevt\Logs\System.evtx



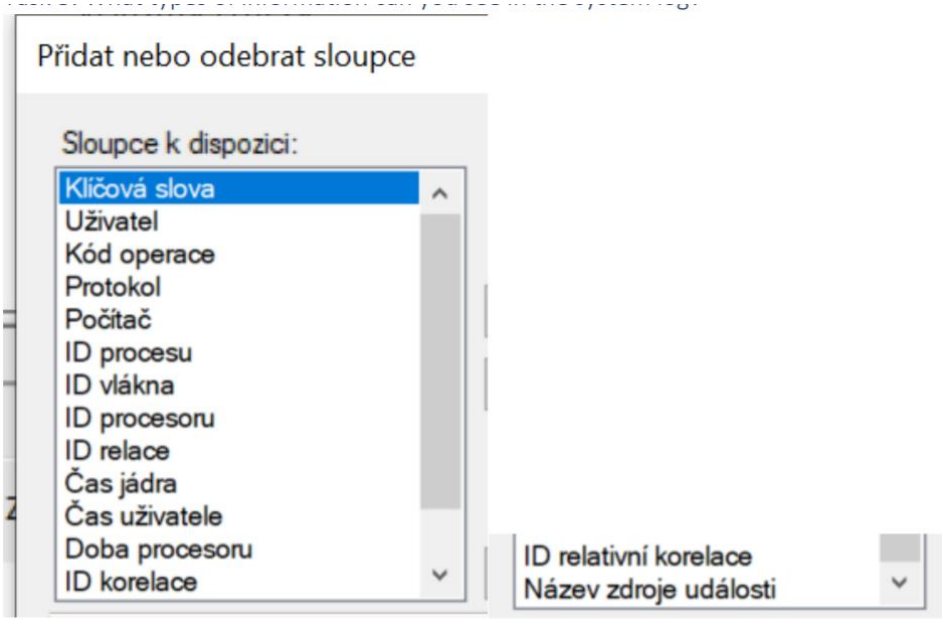
Obrázek č. 44: Systémové logy
(Zdroj: vlastní zpracování)

Logy si můžeme ve windows otevřít v prohlížeč událostí, viz níže:



Obrázek č. 45: Prohlížeč událostí
(Zdroj: vlastní zpracování)

V tomto prohlížeči událostí můžeme snadno pod položkou počet událostí zjistit počet logů. Níže vidíme taktéž veškeré dostupné informace.



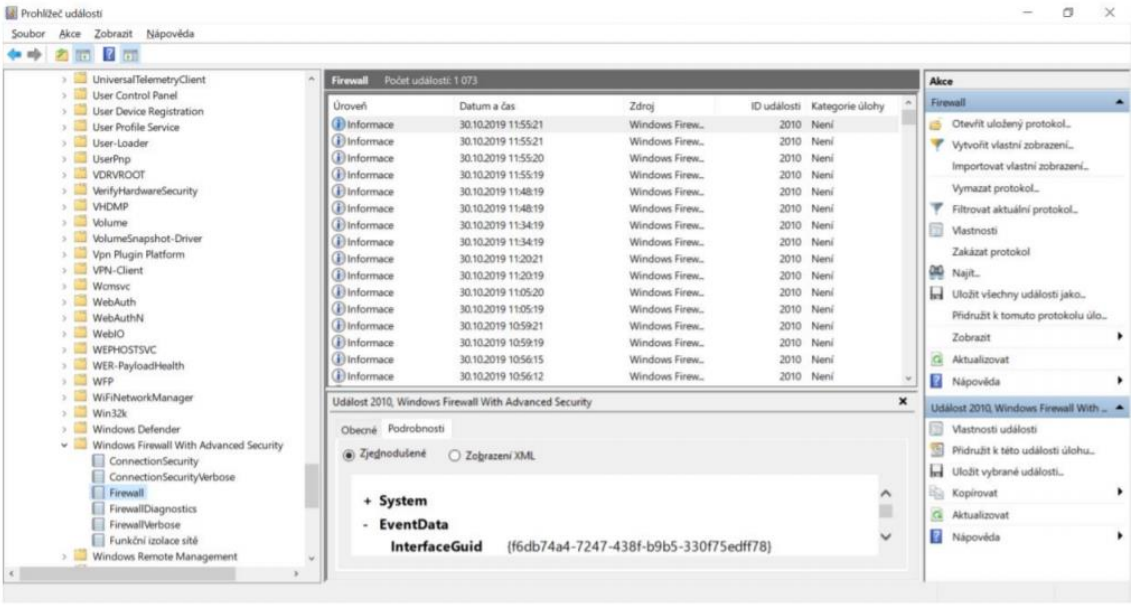
Obrázek č. 46: Atributy systémových logů
(Zdroj: vlastní zpracování)

Logy firewallu nalezneme na cestě:

%systemroot%\system32\LogFiles\Firewall\pfirewall.log

%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx

Zobrazit si je můžeme opět v prohlížeči událostí:



Obrázek č. 47: Firewall logy
(Zdroj: vlastní zpracování)

Příklad logu aplikace máme například zde:

Obrázek č. 48: Aplikační log
(Zdroj: vlastní zpracování)

Tento log vypovídá o tom, že Microsoft Office 32-bit Components 2013:

File C:\windows\SysWOW64\msvcr100.dll je využíván aplikací Microsoft Word.

Z tohoto cvičení vidíme alespoň základní práci s logy. Pochopitelně je nutné tuto znalost hlouběji rozvíjet, umět je správně filtrovat a vyhledávat v nich. Pro názornou ukázku je toto cvičení však dostačující.

3.15 Odhalení útoků – vytvoření časové osy

Ať už v reálném čase, či potom zpětně z uložených logů, často musíme provádět analýzu síťového provozu. Pokud bychom ovšem měli procházet jednotlivé záznamy, nikdy se nám to z důvodu obrovského objemu dat nemůže podařit. Proto je nutné naučit se správně a vhodně volit filtry a využívat další nástroje, které nám pomohou zobrazit pouze ta data, která jsou pro nás relevantní.

3.15.1 Zadání úkolu:

Detekujte útoky a vytvořte časovou osu útoků pomocí nástroje Wireshark.

Analyzujte útočníka.

3.15.2 Vypracování úkolu:

Pro tuto analýzu využijeme kartu statistiky -> I/O graph. Tím získáme provoz na sítí. Vybereme postupně nejvyšší vrcholy. Zjistíme, z jakých byli adres a ty potom využijeme při tvorbě filtru. Ten vypadá následovně:

ip.src == x , kde x představuje nalezené adresy.

Obrázek č. 49: Wireshark – časová osa s útoky
(Zdroj: vlastní zpracování)

Na obrázku výše můžeme vidět výsledná vyfiltrovaný graf, přesněji tedy časovou osu, s nejvyšším provozem na síti. Ten byl o tolik vyšší nežli standardní provoz na síti, že můžeme usoudit, že se s velkou pravděpodobností jednalo o útoky.

Tuto metodu můžeme využít při vyšetřování provozu na síti, ale taktéž při incident response, kdy můžeme odhalit adresu útočníka a následně ji zablokovat.

3.16 Plán a realizace malé sítě

Opět bych rád vyzdvihl důležitost a užitečnost možnosti praktického vyzkoušení. V tomto úkolu si studenti sami navrhnou jednoduchou síť z dostupných síťových prvků a vyzkouší si základní konfigurace. V české republice se sítě vyučují velmi často, nicméně výrazně méně mají studenti možnost si tyto znalosti vyzkoušet v praxi. Dle mého názoru je to škoda, protože tímto způsobem mnohem lépe a rychleji pochopí principy a zároveň odhalí souvislosti, které by jim bez praktické části mohli uniknout.

3.16.1 Zadání úkolu:

Ve skupině vytvořte plán na síťovou strukturu, včetně bezpečnosti a monitoringu.

- Plán musí obsahovat síťovou mapu infrastrukturu

- Dále musí obsahovat 4 služby, které na síti poběží
- Všechny služby musí být dostupné jak uvnitř tak i zvenčí sítě

3.16.2 Vypracování úkolu:

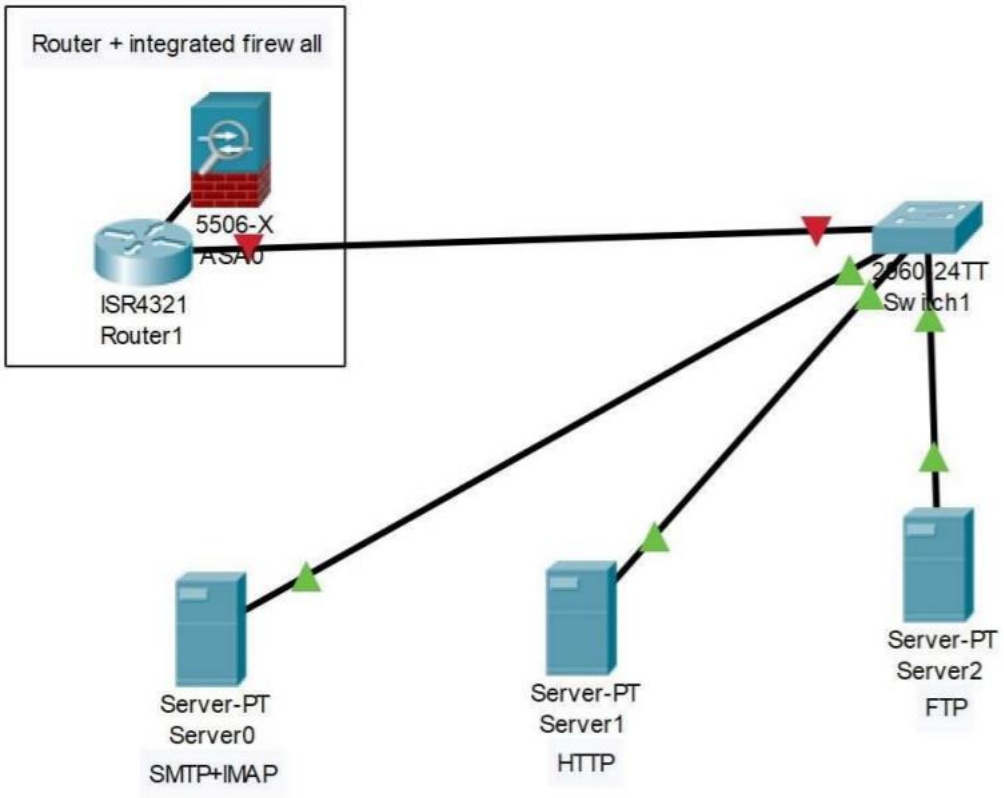
Určíme si, které služby bychom chtěli na naší síti zprovoznit. Může jít například o:

- http, pro webovou stránku
- FTP, pro úložiště dat
- SMTP/IMAP - pro emailové služby, odesílání a přijímání

Další možnosti můžou být:

- DNS a DHCP z důvodu bezpečnosti
- SNORT / IPS pro bezpečnost v lokální síti

Infrastruktura může vypadat například takto:



Obrázek č. 50: Infrastruktura navržené sítě
(Zdroj: vlastní zpracování)

Po vytvoření schéma následuje samotné zapojení a konfigurace prvků, včetně instalace OS a podobně.

Takovýto typ úkolu studentovi nejen propojí praktickou část s teoretickou, ale taktéž mu dá příležitost nad sítí přemýšlet.

3.17 Testování vytvořené sítě

V předchozím úkolu jsme vytvořili funkční síť. Proto je na místě ji řádně otestovat. Tento úkol skvěle kombinuje oba úhly pohledu na sítě, tedy útočníka i obránce, jelikož proti sobě staví dvě skupiny, každá má vlastní síť s vlastními službami.

3.17.1 Zadání úkolu:

V rámci obou týmu propojte vzájemně vaše sítě. Celý proces dokumentujte a monitorujte.

Vaším úkolem je zajistit bezproblémové fungování vašich služeb a zároveň se pokusit omezit nebo naprosto zastavit provoz služeb týmu druhého.

3.17.2 Vypracování úkolu:

Vzhledem k rozsáhlosti úkolu, zde uvedu pouze důležité a zajímavé části.

Nejprve je nutné sestavit si dobrý plán. Na to, abychom správně naplánovali útok, musíme znát služby soupeře. V nich se pak snažíme najít slabé stránky a ty napadnout. Například bude mít soupeř služby:

- Apache2
- SSH
- Telnet

Můžeme se tedy pokusit například o tyto útoky:

- Skript na vypínací smyčku v Apache
- Útok hrubou silou na SSH
- DDoS

Na obranu využijeme:

- Firewall
- Monitorování softwarem Wireshark, Nmap, případně ještě Snort

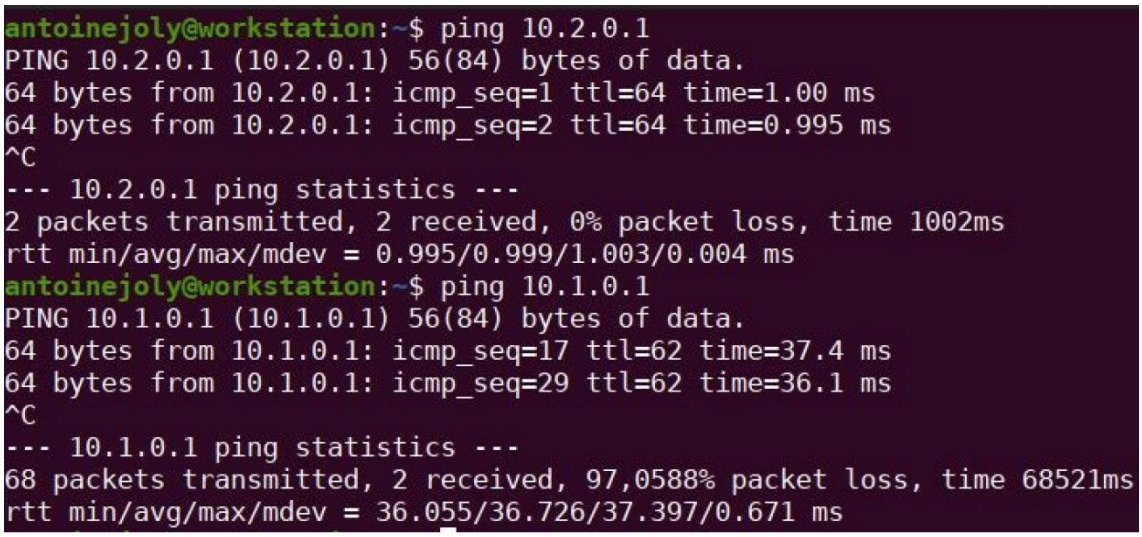
Abychom monitorovali provoz celé sítě, využijeme Mirrorport.

Monitorování soupeřovi sítě můžeme provádět čistým testováním jeho služeb, případně příkazy v terminálu.

Zkusíme spustit například DDoS útoky pomocí Pentmenu – Echo Flood útokem:

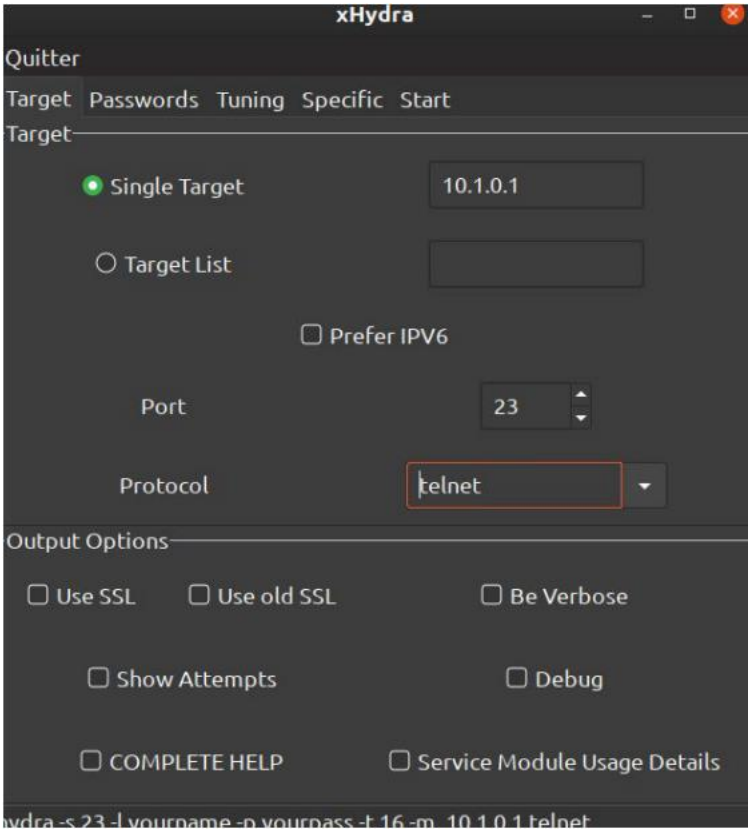
Obrázek č. 51: Pentmenu – Echo Flood
(Zdroj: vlastní zpracování)

Výsledkem je 97% ztracených paketů:



Obrázek č. 52: Výsledek Echo Flood útoku
(Zdroj: vlastní zpracování)

Dalším útokem může být útok hrubou silou na telnet:



Obrázek č. 53: xHydra bruteforce útok
(Zdroj: vlastní zpracování)

Pokud jsme úspěšní, můžeme zkusit podstrčit náš skript, který může vypadat takto:

```
1 #!/bin/bash
2 while true
3 do
4         sudo service apache2 stop
5         sleep 1
6 done
```

Obrázek č. 54: příklad skriptu pro vypínací smyčku
(Zdroj: vlastní zpracování)

Pro monitoring naší sítě můžeme využít například Nmap pomocí tohoto příkazu:

root@kali:~# nmap -v -A 10.2.0.1

Pomocí tohoto a dalších podobných úkolů, se studenti taktéž naučí jednu důležitou věc a tou je spolupráce. Většinou se v praxi setkají s tím, že infrastrukturu a služby provozují odlišní lidé. Musí se naučit mezi těmito skupinami komunikovat, jak se domluvit, jak si předat informace efektivně.

Dále si student vyzkouší chování sítě v případě útoku, jak se takový útok projeví v monitoringu a podobně. Další poznatek, který si tímto cvičením osvojí, je ten, často je mnohem snazší být v pozici útočníka nežli obránce.

3.18 Vyšetřování na místě činu – praktická zkouška

Tento úkol byl z mého pohledu ten nejzajímavější. Jednalo se o nasimulování situace z praxe, kdy si student mohl vyzkoušet, jak by mohlo probíhat vyšetřování a sbírání důkazů. Díky tomu získá opravdu cenné zkušenosti, kterým se samotná teorie nikdy nemůže vyrovnat.

3.18.1 Zadání úkolu:

Zadání v tomto případě bylo vcelku prosté. Vytvořil se tým po čtyřech studentech. Cvičení začínalo ve třídě, kde byli studenti seznámeni se scénářem. Ten byl v tom cvičení následující:

„Bylo hlášeno, že z IP adresy xy byli provedeny pokusy o hackování banky. Z IP adresy byla zjištěna adresa, kam se nyní vydáte s vaším týmem a provedete zajištění důkazů na místě činu.“

Taktéž zde studenti žádali o soudní příkaz. Zde museli uvést veškeré náležitosti, které takové povolení musí obsahovat.

Dále si musel každý tým určit role. Tato část je taktéž velice důležitá. Každý člen musí přesně vědět, co dělat.

Poté byl tým doveden na místo činu. Odtud si vše řídil sám.

3.18.2 Vypracování úkolu:

Popíši zde, jak probíhalo moje cvičení, abych demonstroval hlavní body tohoto cvičení.

V mém týmu jsme si rozdělili role na vyšetřovatel, který řídí celou operaci, fotograf, dokumentarista a poslední člen se staral o bezpečnost samotné operace a výslech.

Poté co jsme vešli do místnosti, ihned jsme vyfotili místo činu – tato první fotografie je velice důležitá – zachytíte totiž přesnou polohu podezřelého. Máte pak důkaz, zdali například seděl u konkrétního počítače a podobně. Ihned musíte zpacifikovat podezřelého, dostat ho dál od počítače a dalších zařízení, aby nemohl rychle zmanipulovat či odstranit data.

Každý člen týmu se musí po celou dobu držet své role, tudíž po zajištění bezpečnosti začne jeden člen s výslechem, zatímco ostatní postupně, systematicky, procházejí celou místnost a hledají možné zdroje informací. Každé digitální zařízení nám může sdělit určité informace, každý senzor, každý počítač, mobilní telefon a podobně. Je nesmírně důležité taktéž po celou dobu hlídat bezpečnost celé operace a zároveň dávat pozor na podezřelého.

Zde se dostáváme k jedné důležité věci – abyste byli schopni takovouto operaci zvládnout úspěšně, musíte taktéž znát zákony daného státu. Kupříkladu v našem případě byla podezřelou osobou žena – ale náš člen určený na zajištění podezřelého byl muž. Vzhledem k tomu, že podezřelá nechtěla spolupracovat, musel zasáhnout i fyzicky a posunout ji dál od počítače. V tu chvíli by ovšem podezřelá mohla podat stížnost za sexuální obtěžování. Kdyby náš člen na zajištění podezřelé byla žena, vše by bylo v pořádku. Je třeba pamatovat, že tato situace se mění dle daného státu.

Celou situaci bedlivě pozoruje vyučující, který po skončení cvičení podává zpětnou vazbu, sdělí případné chyby, na co si dát pozor a podobně.

Jak jsem již uvedl, velký důraz je taktéž na samotnou dokumentaci, proto zde uvedu její náhled:

1. **Informace o místě činu:**

Lokace:

Group Study Room 5 (1st floor)

Dohan Global School, Hallym University

Chuncheon, Kangwon Do, South Korea

Čas příjezdu: 10:19 AM 2019-10-16

Počet policistů: 4

Počet podezřelých: 1

Počet nalezených důkazů: 8

Čas odjezdu: 11:04 AM 2019-10-16

Soudní příkaz:

Číslo případu: Case 004

Typ: Search and Seizure Warrant

Zařízení k zabavení:

- Všechna zařízení s připojením k síti
- Všechna paměťová média
- Bezpečnostní tokeny
- Papírové důkazy a fotografie

Platnost do: 2019-10-24

Informace o podezřelé:

Popis osoby:

- Žena, asijského původu
- Okolo 20 let
- Světlé vlasy
- Kulatý obličej
- Okolo 165cm výška
- Mluví korejsky a anglicky

Chování:

Obrázek č. 55: Foto podezřelé při vstupu na místo činu
(Zdroj: vlastní zpracování)

Při vniknutí do místnosti seděla za stolem a měla ruce v kapsách.

Když ji byla vysvětlena situace, pokusila se vzít svůj mobilní telefon a nechtěla ho vydat.

Obrázek č. 56: Foto podezřelé, když se snažila získat telefon
(Zdroj: vlastní zpracování)

Nejprve se snažila utéct, poté začala spolupracovat a podvolila k výslechu. Když jsme se snažili zajistit laptop, přiskočila a pokusila se jej rozbít.

Zvláštnosti:

- nemá občanský průkaz
- nechce prozradit svoji identitu
- odmítá jakoukoliv souvislost se zločinem
- pokusila se utéct
- pokusila se zničit důkazy

Chain of custody:

Číslo případu: Case 004

Čin: Online hacking do bankovního systému

Zodpovědná osoba: (Name/ID#) Marcel Sisler / 20199790

Datum a čas získání důkazů: 2019-10-16, 11:04 AM

Lokace: Group Study Room 5, Dohan Global School, Hallym University, Chuncheon, Kangwon-Do, South Korea

Popis důkazů:

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	**Mobile Phone**: Samsung Galaxy Note (4G LTE), White, Cracks on screen and camera lens, painting peeled off
2	1	**Tablet PC**: Silver cover, black body, power on (charging), stickers (NASA, chemical, etc.), one USB connected,
3	1	**USB Drive**: SanDisk Cruser Glide, 16GB, black and red, connected to tablet PC
4	1	**USB Drive**: Dell, 128MB, black and silver, disconnected (next to tablet PC)
5	1	**Samsung TV**: Black, power off
6	1	**Yellow Folder**: Documents, written "그룹스터디룸 사용대장-23102 호-도헌글로벌스쿨 교학팀"
7	1	**Remote Control** (Samsung TV): Black
8	1	**Air Conditioner Control**: Air conditional was turned off

Obrázek č. 57: Seznam nalezených důkazů
(Zdroj: vlastní zpracování)

Obrázek č. 58: Foto důkaz 1
(Zdroj: vlastní zpracování)

Čas: 2019-10-16@10:33 A. M.

Telefon fyzicky zkontrolován:

-Výrobce: Samsung

- Model: Galaxy Note

- Color: White

Telefon chráněn pinem, ale stále zapnutý – musíme zajistit, aby se nevypl, pak už se s největší pravděpodobností nepodaří získat z něho data. Telefon v módu letadlo.

Obdobně by byly popsány i ostatní důkazy, ale jako ukázka bude stačit jeden.

Jak můžeme vidět na tomto cvičení, vyšetřování je velmi komplexní činnost, při které si musí vyšetřovatel hlídat spoustu věcí. Proto věřím, že je zapotřebí praktické cvičení.

3.19 Shrnutí přínosů představených návrhů

Hlavním přínosem z doporučených návrhů spatřuji především v oblasti vyšetřování kybernetických zločinů. Student by díky nim dokázal lépe pracovat s důkazy a vhodně provádět dokumentace potřebné pro vyšetřování a chain of custody. Základy digitální forenzní analýzy by mohli silně přispět při hledání důkazů z digitálních médií, počítačů, mobilních telefonů a podobně.

Práce s časovou osou by zase dopomohla k lepší rekonstrukci možných příčin při bezpečnostním incidentu, ale taktéž při vyšetřování.

Je taktéž nutné znát legislativu a umět se orientovat ve smluvních podmínkách, zejména pak při vyšetřování cloudových služeb.

Znalost principů hashe je naprostou nezbytností při práci s chain of custody a zajištění integrity důkazů.

Při vyšetřování je často nutné hledat důkazy i v logovacích souborech, proto je jejich znalost velmi důležitá.

Realizace vlastní sítě zase umožní lepší propojení teoretických znalostí na souvislosti a umožní snazší orientaci v budoucí praxi.

3.20 Doporučení

V České republice je výuka informační bezpečnosti na slušné úrovni, nicméně doporučuji zařadit výše uvedené návrhy k zacelení výuky, kterého bude dosaženo obohacením stávajících studijních programů o cvičení na digitální forenzní analýzu, vyšetřování a praktické testování sítě.

ZÁVĚR

Cílem této diplomové práce bylo porovnat výuku informační a kybernetické bezpečnosti v České republice a Jižní Koreji. Na základě analýz a zkušeností ze studijního pobytu Freemover poté představit návrhy na zlepšení současné situace.

V první části této práce byla představena teoretická východiska, pojmy a definice z oblasti informační a kybernetické bezpečnosti. Dále také legislativa pro tuto problematiku v České republice a certifikační autority.

Druhá část se zabývala současnou situací škol a univerzit v České republice a Jižní Koreji. Tyto školy a univerzity byli představeny, včetně jejich oborů, které byli posouzeny. Nakonec bylo provedeno srovnání České republiky a Jižní Koreji, včetně odůvodnění pramenícího z kulturních rozdílů a trendů v oblasti informační a kybernetické bezpečnosti.

Následně jsem představil návrhy na zlepšení současné situace. Ty pramenili především ze zkušeností posbíraných na studijním pobytu na Hallym University. Jednalo se především o doporučení na úkoly v oblasti digitální forenzní analýzy, vyšetřování kybernetických zločinů a bezpečnosti sítí.

Nakonec byli shrnuty přínosy pro výuku plynoucí z představených návrhů.

SEZNAM POUŽITÝCH ZDROJŮ

(1) KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-8.

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

(3) *Cyberspace Operations: Concept Capability Plan 2016–2028* [online]. In: . b.r., s. 77 [cit. 2020-04-11]. Dostupné z: https://fas.org/irp/doddir/army/pam525-7-8.pdf

(4) *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. b.r. [cit. 2020-04-11]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

(5) *Zpráva o stavu kybernetické bezpečnosti ČR 2017* [online]. In: . b.r., s. 49 [cit. 2020-04-11]. Dostupné z: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2017.pdf

(6) *Zpráva o stavu kybernetické bezpečnosti ČR 2018* [online]. b.r., , 68 [cit. 2020-04-11]. Dostupné z: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

(7) *Definition of Cybersecurity - Gaps and overlaps in standardisation* [online]. b.r., , 35 [cit. 2020-04-12]. DOI: 10.2824/4069. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

(8) *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148* [online]. In: . b.r. [cit. 2020-04-12]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN#d1e688-1-1

(9) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(10) *ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems — Overview and vocabulary* [online]. Fifth edition. 2018, 23 s. : il., tab. [cit. 2020-05-12]. Dostupné z: https://standards.iso.org/

(11) ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 9788073807375.

(12) *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů* [online]. In: . b.r. [cit. 2020-04-12]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/

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

(14) *Standards for Security Categorization of Federal Information and Information Systems* [online]. 2004, , 13 [cit. 2020-04-12]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

(15) PENDER-BEY, Georgie. *THE PARKERIAN HEXAD* [online]. In: . b.r., s. 31 [cit. 2020-04-12]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

(16) SCHNEIER, Bruce. *Secrets and lies: digital security in a networked world*. Fifteenth Anniversary Edition. Indianapolis, Indiana: John Wiley & Sons, Inc., 2015. ISBN 978-1-119-09243-8.

(17) *SCHNEIER, Bruce* [online]. In: . b.r. [cit. 2020-04-14]. Dostupné z: https://www.azquotes.com/quote/570035

(18) VALÁŠEK, Jarmil a František KOVÁŘÍK. *Krizové řízení při nevojenských krizových situacích: účelová publikace pro krizové řízení*. Vyd. 1. Praha:

Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. ISBN 978-80-86640-93-8.

(19) *Sbírka zákonů Česká republika*. Břeclav: Moraviapress, b.r., 2018. ISSN 1211-1244.

(20) *Hrozba: Ministerstvo vnitra České republiky* [online]. b.r. [cit. 2020-04-17]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

(21) JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. ISBN 9788024715612.

(22) POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace* [online]. In: . b.r. [cit. 2020-04-17]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

(23) *Motivace hrozeb: KYBEZ* [online]. b.r. [cit. 2020-04-17]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

(24) PEPE, Matthew, Jason LUTTGENS, Ryan KAZANCIYAN a Kevin MANDIA. *Incident response & computer forensics: Jason T. Luttgens, Matthew Pepe and Kevin Mandia*. Third edition. New York: McGraw-Hill Education, 2014. ISBN 9780071798686.

(25) NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. První vydání. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

(26) *Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. b.r. [cit. 2020-04-14]. Dostupné z: https://www.govcert.cz/download/legislativa/2020/2020-02-01_novelizace_zneni_zakona_181_2014_final.pdf

(27) *NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response* [online]. b.r. [cit. 2020-04-17]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

(28) *Volatile Evidence: ScienceDirect* [online]. b.r. [cit. 2020-04-20]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/volatile-evidence

(29) *Digital forensic review: Časopis institutu pro Digitální Forenzní analýzu*. Oškobrh: Institut pro Digitální Forenzní Analýzu, 2018, 2018(1). ISSN 2570-5040.

(30) *NIST SP 800-12: An Introduction to Information Security* [online]. b.r. [cit. 2020-04-13].

(31) JOSHI, R.c. *Fundamentals of network forensics: a research perspective*. New York, NY: Springer Berlin Heidelberg, 2016. ISBN 9781447172970.

(32) *Česká agentura pro standardizaci* [online]. 2017 [cit. 2020-04-13]. Dostupné z: http://www.agentura-cas.cz/

(33) *ČSN ISO/IEC 27006: Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací* [online]. b.r. [cit. 2020-04-13]. Dostupné z: http://www.technicke-normy-csn.cz/

(34) *ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací* [online]. In: . b.r. [cit. 2020-04-13]. Dostupné z: http://www.technicke-normy-csn.cz/

(35) *ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny* [online]. In: . b.r. [cit. 2020-04-13].

(36) *ČSN ISO/IEC 27004: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení* [online]. In: . b.r. [cit. 2020-04-13]. Dostupné z: http://www.technicke-normy-csn.cz/

(37) *ČSN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací* [online]. b.r. [cit. 2020-04-13]. Dostupné z: http://www.technicke-normy-csn.cz/

(38) *ČSN ISO/IEC 27007: Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací* [online]. b.r. [cit. 2020-04-13]. Dostupné z: http://www.technicke-normy-csn.cz/

(39) *NISTIR 7298: Glossary of Key Information Security Terms* [online]. b.r. [cit. 2020-04-13].

(40) *NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations* [online]. b.r. [cit. 2020-04-14]. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-53r4

(41) *Legislativa: Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2020-04-14]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

(42) *317/2014 Sb.: Vyhláška o významných informačních systémech a jejich určujících kritériích* [online]. b.r. [cit. 2020-04-14]. Dostupné z: https://www.govcert.cz/download/kii-vis/VVIS_UZ.pdf

(43) *Rámcový vzdělávací program pro obor vzdělání 26 – 47 – M/01 Informační technologie: MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY* [online]. In: . b.r. [cit. 2020-04-18]. Dostupné z: http://zpd.nuov.cz/RVP_kategorie_ML/RVP_2647M01_Informacni_technologie.pdf

(44) *VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://www.vutbr.cz/

(45) *Informační bezpečnost: Masarykova univerzita* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://www.fi.muni.cz/admission/mgr/computer-systems-communication-and-security.html

(46) *Řízení softwarových systémů a služeb: Masarykova univerzita* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://www.fi.muni.cz/admission/mgr/software-systems-and-services-management.html

(47) *Fakulta informačních technologií ČVUT v Praze* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://fit.cvut.cz/

(48) *Fakulta vojenských technologií Univerzity obrany v Brně* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://www.unob.cz/fvt/Stranky/default.aspx

(49) *Univerzita Tomáše Bati ve Zlíně – fakulta aplikované informatiky* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://fai.utb.cz/

(50) *Smart Campus - Hallym University* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://smart.hallym.ac.kr/

(51) *Sejong Cyber University* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://home.sjcu.ac.kr/

(52) *Seoul National University – department of Computer Science and Engineering* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://cse.snu.ac.kr/

(53) *Hanyang Cyber University* [online]. b.r. [cit. 2020-04-18]. Dostupné z: http://en.hycu.ac.kr/

(54) *South Korea - crime & safety report: Overseas Security Advisory Council* [online]. b.r. [cit. 2020-04-19]. Dostupné z: https://www.osac.gov/Country/SouthKorea/Content/Detail/Report/6d2ced24-cc8e-4077-8b75-15f4aeb80d5f

(55) *Cyber Threat Analysis Report (First half of 2019): Cyber Bureau, Korean National Police Agency* [online]. In: . b.r. [cit. 2020-04-21]. Dostupné z: http://cyberbureau.police.go.kr/board/boardView.do?board_id=news&id=6234&page=1&mid=

(56) *Životní cyklus kybernetické bezpečnosti: KYBEZ* [online]. b.r. [cit. 2020-04-14]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

(57) *Fakulta informatiky: Masarykova univerzita* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://www.fi.muni.cz/

(58) *Hallym University* [online]. b.r. [cit. 2020-04-18]. Dostupné z: https://english.hallym.ac.kr/

(59) *Korea University - School of Information Security* [online]. b.r. [cit. 2020-04-18]. Dostupné z: http://gss.korea.edu/

(60) *The Cyber University of Korea* [online]. b.r. [cit. 2020-04-18]. Dostupné z: http://eng.cuk.edu/

(61) *Kyberkriminalita: Policie ČR* [online]. b.r. [cit. 2020-04-19]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

(62) *CYBER ATTACK TRENDS: 2019 MID-YEAR REPORT: CHECK POINT RESEARCH* [online]. b.r. [cit. 2020-04-19]. Dostupné z: https://www.ispin.ch/fileadmin/user_upload/partner/pdf/CP-mid-year-report-2019.pdf

(63) *FIREEYE MANDIANT SERVICES | SPECIAL REPORT: Fireeye* [online]. b.r. [cit. 2020-04-19]. Dostupné z: https://content.fireeye.com/m-trends/rpt-m-trends-2020

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

IS - informační systém

IT – informační technologie

ICT – informační komunikační technologie

ISO - International Organization for Standardization

HW – hardware

SW – software

CIA – Confidentality, integrity, availability

NIST - National Institute of Standards and Technology

IEC - International Electrotechnical Comission

ITU - International Telecommunications Union

ČAS - Česká agentura pro standardizaci

ČSN - Česká technická norma

DoS – Denial of service

DDoS – Distrubuted denial of service

SEZNAM POUŽITÝCH OBRÁZKŮ