VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ŘEŠENÍ KYBERNETICKÉ BEZPEČNOSTI A INCIDENT HANDLINGU NA FP VUT

CYBERSECURITY AND INCIDENT HANDLING SOLUTIONS ON FBM VUT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Jiří Valtr

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Petr Sedlák

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jiří Valtr**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2021/22
Studijní program:	Informační management

Garant studijního programu 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:

Řešení kybernetické bezpečnosti a incident handlingu na FP VUT

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrh řešení a přínos práce
Závěr

Cíle, kterých má být dosaženo:

Návrh pracovního rámce pro zajištění kybernetické bezpečnosti na podnikatelské fakultě VUT v Brně.

Základní literární prameny:

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

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

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

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

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

ABSTRAKT

Diplomová práce se věnuje návrhu rámce pro řešení kybernetické bezpečnosti ve vybrané organizaci. První část představuje teoretická východiska, nutná pro pochopení bezpečnostní situace v ČR a ve světě. Následná kapitola pak obsahuje výsledky analýz současného stavu kyberbezpečnosti v organizaci, pro kterou pak v části třetí sestavuji vhodný pracovní rámec, včetně doporučených nástrojů a postupů k zajištění kvalitního řešení kyberbezpečnosti a její udržitelnosti.

ABSTRACT

The diploma thesis deals with design of cyber security solution in given organisation. The first part describes theoretical basis needed for basic understanding the security question in CZ and in the world. The following chapter then contains analysis outcome of current state of organisation, for which in the third part I compile a suitable framework, including needed tools and procedures, to settle a proper cyber security solution and its sustainability.

KLÍČOVÁ SLOVA

kybernetická bezpečnost, incident handling, perimetr, kybernetická hrozba

KEYWORDS

cyber security, incident handling, perimeter, cyber threat

BIBLIOGRAFICKÁ CITACE

VALTR J. Řešení kybernetické bezpečnosti a incident handlingu na FP VUT. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 20122. 79 s. Vedoucí diplomové práce Ing. 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 5. května 2022

PODĚKOVÁNÍ

Chtěl bych poděkovat svému vedoucímu Ing. Petru Sedlákovi za jeho odborné vedení mé diplomové práce, za jeho cenné připomínky a rady a především za prvotní impulz na začátku mých studií, který probudil můj zájem o oblast kybernetické bezpečnosti.

OBSAH

ÚVOD

Síť internet se během posledních dekád proměnila takovým způsobem, jaký nikdo koncem sedmdesátých let, když se rodily první verze rodiny TCP/IP protokolů, nemohl předvídat. Tato rozsáhlá decentralizovaná síť v současnosti představuje základní stavební pilíř kyberprostoru, jak jej dnes známe. Od skutečného světa se však tento prostor diametrálně odlišuje hned několika principy. Nejdůležitějším z nich je běžná absence hranic mezi jednotlivými uživateli, organizacemi nebo státy. Další odlišností je též vysoká míra anonymity, kterou internet svým uživatelům poskytuje. A v neposlední řadě též neexistence státních výkonných orgánů, které by měly mít nad bezpečností svého kyberprostoru plnou kontrolu. Z těchto i mnoha dalších charakteristik plyne jediné: naše bezpečnost v kyberprostoru je vždy pouze v našich rukou.

Tuto zodpovědnost si v posledních letech čím dál více uvědomuje jak veřejnost, tak státní i soukromé organizace. Počet vyšetřovaných kyberkriminálních případů v ČR vzrostl za posledních 10 let na více než pětinásobek a neočekává se v budoucnu jiný než rostoucí trend. Otázka, která se kvůli tomu v mnohých společnostech probírala u ředitelského stolu, tedy „zda“ dojde v organizaci ke kyberbezpečnostnímu incidentu, se v posledních letech klade spíše formou „kdy“ k němu dojde. Váha této otázky se ale naštěstí čím dál více odráží v zavádění interních bezpečnostních procesů a ve zvyšování investic do odbornosti pracovníků a do potřebných technologií.

Ve své práci objasním, proč by se touto otázkou měla zabývat i Fakulta podnikatelská Vysokého učení technického v Brně a vysvětlím, jakým způsobem by se proti kybernetickým hrozbám měla moderní organizace bránit.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

1.1 Cíle práce

Hlavním cílem mé práce je navrhnout nové řešení kybernetické bezpečnosti na míru dané organizaci. Toto řešení vychází čistě z analýzy a zhodnocení současného stavu kybernetické bezpečnosti v organizaci a zohledňuje jak použití konkrétních nástrojů, metodik a postupů, tak i implementace celého rámce z hlediska procesního.

1.2 Metody a postupy zpracování

Tato práce je rozdělena do tří hlavních částí. Část teoretická, část analytická a část návrhu a implementace bezpečnostního řešení. V první části vymezuji pojmy potřebné pro získání přehledu o fungování různých typů kyberbezpečnostních týmů, jejich členů a komunikace mezi nimi. Představuji širokou škálu nástrojů, které jsou v kyberbezpečnostní komunitě považovány za stavební kameny jejich činnosti a nastiňuji základní pracovní rámec SOC analyst pracovníka nebo incident handlera. V části druhé, tedy analytické, je rozebírán současný stav kybernetické bezpečnosti. Nejprve v obecné rovině, tedy kdo má tuto činnost v gesci, poté i v té technické rovině s praktickými ukázkami konkrétních bezpečnostních nedostatků. Část poslední pak na část druhou přímo navazuje a je v ní obsažena sada návrhů a doporučení, jak celou kybernetickou bezpečnost na fakultě zlepšit s důrazem na proveditelnost a udržitelnost řešení.

2 TEORETICKÁ VÝCHODISKA

V této části diplomové práce Vás seznámím s potřebnými teoretickými znalostmi, které budou využity v části analytické a při návrhu řešení.

2.1 Seznam zkratek / pojmů

Backdoor – je to typ malwaru, který umí ve fázi delivery (dle Cyber Kill Chain) obejít authentizační obrané mechanismy.

C&C – neboli Command and Control je označení pro vzdálené kontrolování infikovaných strojů. Jde též o poslední krok v Cyber Kill Chain a zkratkou C&C se též označují servery, které byly identifikovány, jako řídící servery v rámci kybernetických útoků. Kromě C&C se můžeme setkat i se zkratkou C2.

CVSS – neboli Common Vulnerability Scoring System je systém vyvinutý společností MITRE, který pomocí několika klíčových metrik počítá skóre závažnosti zranitelnosti na škále od 1 do 10. V současnosti se používá jeho třetí iterace (v. 3).

Intel – odvozeno ze slova intelligence je informace nebo její část, relevantní pro obránce v rámci Cyber Threat Intelligence.

Leak site – jedná se o stránky provozované operátory ransomwarových skupin, na níž jsou zveřejňovány informace ohledně úspěšných ransomwarových útoků. Jména obětí, počet ukradených dat, ceník, informace o aukci, případně data samotná. Leak sites jsou ve většině případů na darknetu.

Man-in-the-middle – označení pro typ kybernetického útoku, kde se útočník dostane v rámci komunikačního kanálu mezi dvě komunikující strany a prezentuje se jako legitimní protistrana oboum účastníkům. S oběma stranami si také vymění klíče a komunikuje s nimi šifrovaně.

Modus operandi – v rámci kybernetické bezpečnosti jde o pojem využívaný převážně ve spojitosti s kyberzločineckými aktéry a označuje jejich charakteristický styl, způsob jednání, postup činností nebo typické cíle útoků.

OSINT – je zkratka Open Source Intelligence. Jde o typ analýzy, která využívá především veřejně dostupné zdroje informací. Tuto analýzu například provádí útočníci v rámci reckon fáze (první fáze v Cyber Kill Chain) před provedením spear-phishing útoku.

NIS – Network and Information Security. Směrnice, vydaná evropskou organizací ENISA.

Payload – neboli „náklad“. Označení pro dopravovaný malware na zacílenou stanici útočníky.

PoC – Proof of Concept. V oblasti kybernetické bezpečnosti nás zajímají především PoC popisující úspěšné zneužívání zranitelnosti. Zranitelnost, ke které je veřejný volně dostupný PoC se stává mnohem nebezpečnější. PoC se v oblasti komunikace zároveň rozumí jako Point of Contact, tedy kontaktní styčnou osobu.

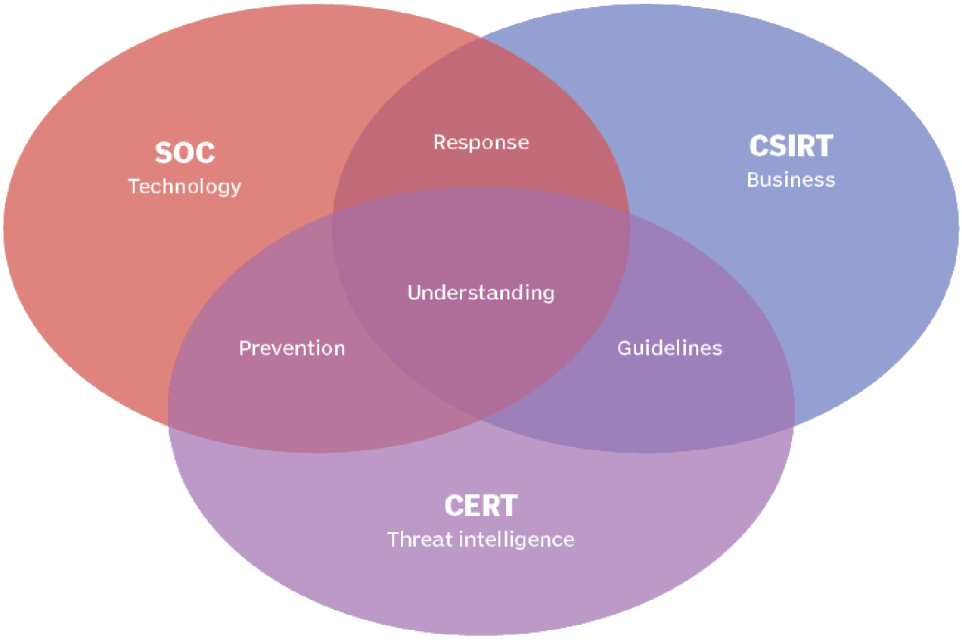
Ransomnote – vzkaz zanechaný útočníky na stroji úspěšně zasaženém ransomwarovým útokem.

SIEM – Security Information and Event Management. Typ bezpečnostního nástroje s bohatou škálou funkcí. Centralizuje logování, kontroluje síťový provoz, vyhodnocuje nasbíraná data nebo i ovládá endpoint detection systémy.

ZKB – Zákon o Kybernetické Bezpečnosti. V současné chvíli pojmem ZKB rozumí 181/2014 Sb. zákonů v jeho platném znění.

2.2 Bezpečnostní týmy

Ve světě kybernetické bezpečnosti narazíte na pojmy CERT, CSIRT a SOC. Jde o týmy, jejichž práce se zdá být z laického pohledu stejná. Existují mezi nimi však výrazné rozdíly, které mají velký vliv při výběru, který tým je vhodné v dané organizaci implementovat. Každý z týmů má během incident response procesu jiné nástroje a sehrává jinou roli. V rámci širšího měřítka je však k dosažení cíle, tedy k zajištění bezpečnosti informační infrastruktury, nutná jejich vzájemná kooperace. Základní charakteristiku těchto týmů je možné znázornit následujícím množinovým grafem:



Obrázek 1: Rozdíly bezpečnostních týmů [2]

Je patrné, že všechny tři typy týmů sdílí stejnou odbornou znalost z oboru. Jejich rozdíly však vysvětlím níže.

2.2.1 CERT

Computer Emergency Response Team (CERT) je registrovanou obchodní značkou Carnegie-Mellon Univerzity. Tým, který chce nést tuto značku ve svém názvu, musí požádat o udělení licence na stránkách univerzity: https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/ Ačkoliv to není podmíněno, CERT týmy jsou typicky financované vládou a mají přímou vazbu na zákonodárnou moc daného státu. Jejich gesce, je zákonem jasně stanovena a mnohonásobně převyšuje působnost jakéhokoliv jiného typu kyberbezpečnostního týmu a označuje se jako konstituence. Typicky se jedná například o prvky kritické informační infrastruktury státu. Díky širokému množství konstituentů pod svým dohledem jsou CERT týmy specifické svou schopností provozovat CTI (Cyber Threat Intelligence) aktivity a dívat se na bezpečnostní situaci se strategickým nadhledem. Může tedy například řešit i geopolitický kontext kybernetických incidentů, sdružovat incidenty do kampaní a mnoho dalšího. Více o CTI si však povíme v bodě 2.6. této práce. Vzhledem ke svému postavení v kyberbezpečnostní komunitě však CERT tým běžně nemá přímý přístup k technologiím dané infrastruktury, a tudíž nemůže přímo a pohotově reagovat na aktuální incident. Jeho reakce spočívá převážně v úpravě zákonů, či využívání jiných zákonných nástrojů. Národní CERT týmy tedy fungují jako hlavní koordinační jednotka, operující na národní i nadnárodní úrovni. V rámci incidentů ovšem, v případě potřeby, poskytují subjektům jak metodickou asistenci, tak tzv. pomoc on-premise. Tedy fyzicky na místě.

Nám nejznámějším příkladem takového týmu je český GovCERT CZ, spadající pod Národní úřad kybernetické a informační bezpečnosti (NÚKIB) sekci NCKB (Národní Centrum pro Kybernetickou Bezpečnost), jehož mám tu čest býti součástí. Jako další příklady mohu uvést Taiwanský TWNCERT, Lucemburský CERT-LU nebo Izraelský ILAN-CERT. [1] [2]

2.2.2 CSIRT

Computer Security Incident Response Team neboli CSIRT je svým charakterem velice podobný k CERT. Tento tým je však většinou nasazován v soukromém sektoru. Stejně jako CERT má na starosti koordinaci a řešení kybernetických bezpečnostních incidentů a událostí, ale včetně jejich právní stránky, případně jejich řešení ve vztahu s veřejností nebo lidskými zdroji. Součástí jeho agendy je i informační bezpečnost. CSIRT je hlavním kontaktním místem pro nahlašování incidentů či sdílení IoCs, dotýkajících se dané organizace. Vzhledem ke svému užšímu zaměření na svou oblast není CSIRT schopný provozovat CTI, nebo jiné geopolitické či strategické analýzy. Má však své místo po boku jiných partnerů v závislosti na tom, čím se organizace, kterou zastřešuje, zabývá. Implementace CSIRT týmu je vhodná spíše do větších decentralizovaných organizací.

Ukázkovými příklady jsou třeba CSIRT týmy všech známých poskytovatelů internetového připojení, největších bank, nebo poskytovatelů web hostingu. Důležitými týmy v komunitě jsou nepochybně také CSIRT týmy známých antivirových nebo jiných odborných výzkumných společností, které jsou čistě technicky založenými týmy, s širokým polem působnosti. Jsou velkým přínosem komunitě díky jejich malware analýzám na vysoké úrovni.

V neposlední řadě uvedu národní CSIRT.CZ, jež je provozován sdružením CZ.NIC, správcem české domény. Stává se tedy hlavním kontaktním bodem v ČR, jedná-li se o řešení incidentů mimo kritickou informační infrastrukturu a mimo významné informační systémy dle zákona o kybernetické bezpečnosti. Vzhledem k tomu, že na rozdíl od národního CERTu nedisponuje žádnými zákonnými nástroji k vymáhání určité úrovně kyberbezpečnosti, má mnohem bližší vztahy s CSIRT týmy jednotlivých ISP. Je charakteristický svou pravomocí sundávat závadné stránky vedené pod nejvyšší národní doménou **.cz**.[1] [2]

2.2.3 SOC

Security Operations Center (SOC) má mnohem širší odborný záběr v oblasti kyberbezpečnosti. Nespecializuje se vůbec na koordinaci řešení incidentů širšího měřítka, ale disponuje přístupem ke konkrétním technologiím, používaným při obraně kyberprostoru organizace, jako jsou například SIEM systémy, nastavení firewallu, IPS a IDS systémy nebo centrální správa endpoint detection systémů, též známých jako „antivirů“, které by jinak v menších organizacích byly pod správou běžného IT oddělení. SOC tým je technicky zaměřený a jeho incident response spočívá převážně ve fyzické obraně před konkrétní hrozbou. Členové SOC týmů jsou většinou pověřeni vytvářet výstupy a podklady buď pro vedení organizace nebo pro CSIRT, které poslouží k bezpečnostním auditům. Implementace SOC týmu má větší význam spíše v centralizovaných organizacích v soukromém sektoru. [1] [2]

2.3 Bezpečnostní organizace / komunity

Úspěšnost bezpečnostních týmů v obraně proti kybernetickým hrozbám je z části závislá na národní i nadnárodní spolupráci s ostatními týmy.

2.3.1 ENISA, CISA

European Union Agency for Cybersecurity (ENISA), jak již název napovídá, je agentura zřízená Evropskou unií a zastřešuje koordinaci a kooperaci bezpečnostních týmů na evropské úrovni. Podílí se na na tvorbě národních kyberbezpečnostních strategických plánů, zastřešuje platformu pro sdílení informací, buduje partnerské vztahy se soukromým sektorem a vyvíjí mnoho dalších činností.

Její americký ekvivalent Cybersecurity & infrastructure Security Agency (CISA) plní podobnou roli v USA. Tato agentura má také zákonodárnou moc a zákonnou povinnost dohledu nad kritickou informační infrastrukturou USA. Funguje tedy i jako protipól

českého NÚKIB. Komunikace s touto agenturou a dalšími důležitými agenturami nesouvisejícími s Evropskou unií, je realizována pomocí vyslaných cyber attaché. Tedy diplomatů podílející se na výměně informací se zahraničními partnery, týkajících se národní kybernetické bezpečnosti.[3] [4]

2.3.2 CSIRT Network

Podle evropských směrnic NIS vydaných agenturou ENISA v roce 2016 byl zřízen CSIRT network. Jde o síť složenou ze jmenovaných vládních týmů členských zemí EU. V současné chvíli má 39 členů, z čehož dva členové jsou český GovcCERT a CSIRT.CZ

CSIRT Network zajišťuje sekretariát této sítě a poskytuje fórum ke kooperaci členských týmů, jejich vzájemnému sdílení informací a budování důvěry. Komunikace napříč CSIRT Network je velice rychlá a v porovnání s komunitami uvedenými níže se jedná o nejlepší, nejpřínosnější a nejfunkčnější komunikační kanál.[5]

2.3.3 Trusted Introducer

Provoz této platformy má historii v týmu Task Force for Computer Security Incident Response Teams (TF-CSIRT) na jejímž základě v roce 2001 vznikl. Provoz Trusted Introducer platformy je pod záštitou neziskové organizace GÉANT a má za cíl poskytnout páteřní síť bezpečnostních týmů z celého světa. Stala se však světoznámou certifikační a akreditační platformou pro týmy nejen v Evropě. Kromě koordinace sdílení informací též organizuje odborné školení TRANSIT. Záběr této platformy je velice široký a obsahuje týmy i ze soukromého sektoru. V současné chvíli má komunita stovky členů. Členství v komunitě je děleno na následující úrovně:

- **Listed** – tým byl podpořen dvěma akreditovanými týmy a byl uveden na seznam
- **Accredited** – tým byl ověřen a prošel akreditačním procesem
- **Certified** – tým splnil veškeré náležitosti pro získání TI certifikace

V rámci České republiky je součástí Trusted Introducer platformy dohromady 55 týmů, z čehož jsou 4 týmy certifikované, 13 týmů prošlo akreditačním procesem a 31 je uvedeno pouze jako „listed“. Zbylých 7 týmů si v současné chvíli prochází re-listing procesem. K povšimnutí hodný tým je kupříkladu certifikovaný CSIRT-MU. Tedy vysoce kvalitní bezpečnostní tým Masarykovy Univerzity. [6] [7]

2.3.4 FIRST

Forum of Incident Response and Security Teams (FIRST) byl založen v roce 1990 jako celosvětová síť jednotlivých CSIRT týmů, které zde dobrovolně spolupracují na zvládání kyberbezpečnostních problémů. FIRST má v současnosti 615 členů, které rozlišuje na dvě skupiny. [6] [8]

- **Full members** – organizace zastřešující kybernetickou bezpečnost nad svou definovanou konstituencí
- **Liaison members** – jednotlivci nebo zástupci organizací, kteří mají legitimní zájem o FIRST program.

2.3.5 ISAC

Information Sharing and Analysis Center (ISAC) je model neziskových organizací definovaný podle ENISA ve směrnici NIS, které poskytují centrální řízení sdílení informací o kybernetických hrozbách. Nejčastější nasazení bývá sektorově orientováno. Kupříkladu na zdravotnictví, bankovnictví nebo energetiku. Jednotlivé subjekty si v rámci ISAC skupiny sdílí intel, specifický k jejich oboru. Může se jednat třeba o zranitelnosti zdravotnických informačních systémů a jejich známé mitigace nebo třeba informace o praktikách aktivní kyberzločinecké skupiny se specializací na SCADA systémy v sektoru vodohospodářství.

Nám nejbližším příkladem ISAC je česká iniciativa hSOC. Jedná se o sdružení 57 největších českých nemocnic, medicínských fakult a různých zdravotnických zařízení plus několika zřizovatelů (NAKIT, NÚKIB, CESNET, MV ČR). Existují však v ČR i další organizace podobného charakteru. Například sdružení energetických gigantů ČSRES. [9] [10]

2.3.6 Další důležité týmy

Pro udržení kroku s trendy odehrávajícími se na poli kyberbezpečnosti je třeba neustále míti v hledáčku celou řadu odborných týmů, projektů a aktivit. Kromě již zmíněných národních a nadnárodních organizací uvedu příklady soukromých organizací a týmů, jejichž veřejné výstupy je záhodno aktivně sledovat. V některých případech existují i možnosti navázání bližší spolupráce. Většinou však pro vládní týmy.

- **CESNET, Cisco** – oblast infrastruktury
- **Check Point, Palo Alto Networks** – širší oblast vývoje a výzkumu
- **Avast, ESET, McAfee, BitDefender** – oblast malware výzkumu
- **CrowdStrike, Mandiant** – oblast CTI
- **Microsoft (MSRC tým), ShadowServer** – intel různého charakteru
- **The Hacker News, Bleeping Computer** – specializované oborové zpravodajství

2.3.7 Projekt CRP-Kyber22

25 českých veřejných vysokých škol (včetně VUT) je zapojeno do projektu Kyber22 v rámci centralizovaných rozvojových programů (CRP) Ministerstva školství, mládeže a tělovýchovy. Hlavním koordinátorem tohoto projektu je CSIRT-MU, který se ve spolupráci s CESNET a NÚKIB snaží pozvednout úroveň kybernetické bezpečnosti na vysokých školách v mnoha ohledech.

V rámci letošního ročníku tohoto projektu se stanovilo pět pracovních skupin včetně jejich leaderů:

1. Procesní aspekty ISMS (ČVUT)
2. Bezpečnostní politiky (UPCE)
3. Osvěta a vzdělávání (MUNI)
4. Integrace technicko-personálních opatření KB (VŠE)
5. Právní aspekty kybernetické a informační bezpečnosti v prostředí VVŠ (MUNI)

Přestože je oblast, které se projekt věnuje sektorově orientovaná na vzdělávací instituce, spektrum působnosti je velice široké. Kombinuje jak sdílení novinek ze světa kybernetické bezpečnosti, sdílení informací o incidentech (IoCs, vektory útoku a jejich mitigace), tak právní aspekty nasazování technických řešení, právní aspekty identifikování významných informačních systémů a plnění náležitostí zákona o kybernetické bezpečnosti, školení zaměstnanců, osvětu a mnohé organizační vylepšení.

Výstupy projektu jsou též velice přínosné a navazují na výstupy z loňského úspěšného projektu CRP-Kyber21:

Tabulka 1: Výstupy projektu CRP-Kyber-22 [12]

1	Zmapování funkčních procesů ISMS
2	Doporučení pro nástroje a technologie na podporu zavedení ISMS a KB v organizaci
3	Nasazení vybraných nástrojů a technologií dle vyspělosti jednotlivých VŠ
4	Koncepce, vytvoření a průběžné plnění Společné znalostní báze pro KB
5	Návrh bezpečnostních politik (BP) pro klíčové oblasti VŠ
6	Implementace BP na jednotlivých VŠ
7	Tři specializované moduly KB vzdělávání pro vybrané cílové skupiny
8	Přizpůsobení generických modulů z V7 specifickým podmínkám/potřebám škol a jejich nasazení
9	Model sdíleného SOC pracoviště pro VŠ z pohledu požadavků odběratele služby SOC
10	Ustanovení Fóra manažerů kyberbezpečnosti VŠ
11	Provedení penetračních testů vybraných VIS
12	Identifikace dobré praxe v oblasti KB v prostředí VŠ s ohledem na požadavky legislativy
13	Workshopy pro vybrané klíčové oblasti řešení
14	Závěrečná zpráva projektu

[11] [12]

2.4 Komunikace

Jako jednou z nejúčinnějších zbraní v boji proti kybernetické kriminalitě se jeví komunikace mezi bezpečnostními týmy. Nepřetržitý tok informací mezi jednotlivými organizacemi drasticky zvyšuje jejich schopnosti reagovat na aktuální hrozby nebo detekovat incidenty. Role koordinační autority je proto klíčová pro plošné zlepšení úrovně kybernetické bezpečnosti.

2.4.1 TLP

Traffic Light Protocol (TLP) je mezinárodně uznávaný systém určený pro klasifikaci citlivosti informací. Jeho účelem je určení, do jaké míry původce chce, aby byly informace šířeny mimo bezprostředního příjemce. Přestože TLP protokol nemá nic společného se zákonem o ochraně utajovaných informací a jeho porušení není nijak právně stíháno, jedná se o konvenci a přísně dodržovaný a respektovaný standard v rámci celé komunity. Jeho název je odvozen od barev na semaforu, které zde znázorňují míru citlivosti informací.

TLP:RED - Určeno pouze pro jmenované příjemce. Není možno sdílet.
TLP:AMBER - Sdílení omezeno pouze na dotčené organizace.
TLP:GREEN - Sdílení omezeno na zájmovou komunitu.
TLP:WHITE - Sdílení neomezeno.

Správné užití je definováno používáním těchto příznaků velkým písmem v předmětech e-mailů a definovanými barvami (podle RGB nebo CMYK), v záhlaví a zápatí dokumentů.

V praxi bývá tento protokol využíván i k získání jakéhosi „náskoku“. Kupříkladu citlivé informace o zranitelnostech některých nástrojů bývají přednostně sdíleny dotčenými organizacím s příznakem TLP:AMBER. Teprve po uplynutí předem stanované lhůty bývá tatáž informace sdílena široké veřejnosti s příznakem TLP:WHITE. [13]

2.4.2 Sdílení IoCs

Tok informací, který většinou proudí přirozenou cestou CERT → CSIRT → SOC je různého charakteru. V nejvíce případech se však jedná o sdílení indikátorů kompromitace (IoC). Typů indikátorů kompromitace je mnoho. Může jím být například být IP adresa, hash, anomálie v log záznamech, podezřelá síťová komunikace, soubor, přijatý e-mail a mnoho dalších. Záleží případ od případu. Tyto indikátory je však nutné

sdílet se zainteresovanými organizacemi pro případnou detekci a reakci. Například pro zkontrolování komunikace se zmíněnou IP adresou.

Pro některé případy sdílení informací (například ENISA ↔ CERTs) je však e-mailová komunikace naprosto nedostačujícím komunikačním kanálem a využívají se proto speciální platformy. Nejznámější platformou, k tomuto účelu určenou, je Lucemburská opensource platforma financovaná Evropskou unií a spravovaná lucemburským CERT týmem: MISP (Malware Information Sharing Platform). Existuje mnoho komunit využívajících MISP. Nejznámějšími komunitami s vlastní MISP platformou jsou například X-ISAC, NATO nebo FIRST. Je k nim připojeno obrovské množství státních i civilních bezpečnostních týmů na evropské úrovni. Vzhledem k opensource distribuci je však možné si nasadit vlastní MISP instanci i pro vlastní účely. [16]

2.4.3 End-to-end šifrování

V rámci emailové komunikace se doporučuje využívat en-to-end šifrování. Tedy šifrování zajištěné na koncových stanicích a tím pádem odolné proti útoku **man-in-the-middle** na pozici správce komunikačního kanálu a na pozici správce mailového serveru. V oblasti kybernetické bezpečnosti toto doporučení nabývá o to větší důležitosti. V praxi se nejvíce využívají dva způsoby:

PGP: Pretty Good Privacy je globálně používaný protokol pro koncové šifrování zpráv. Je založen na algoritmu RSA pro asymetrickou kryptografii. Umožňuje tedy jak šifrování, (zajištění integrity) tak podepisování (zajištění důvěrnosti).

V rámci asymetrické kryptografie každý subjekt disponuje párem klíčů. Jeden klíč z tohoto páru je veřejný a jeho majitel jej může jakkoliv sdílet svým protistranám. Třeba za využití svých www stránek, nebo publikováním klíče na veřejný PGP server. Druhý klíč z páru je soukromý a za žádných okolností nesmí být ohrožena jeho důvěrnost. V případě, že chceme dotyčnému poslat šifrovanou zprávu, zašifrujeme ji jeho veřejným klíčem a můžeme si být jisti, že zprávu nedešifruje nikdo kromě vlastníka druhého klíče z páru. Chceme-li ale zprávu i podepsat, aby měl adresát jistotu o jeho

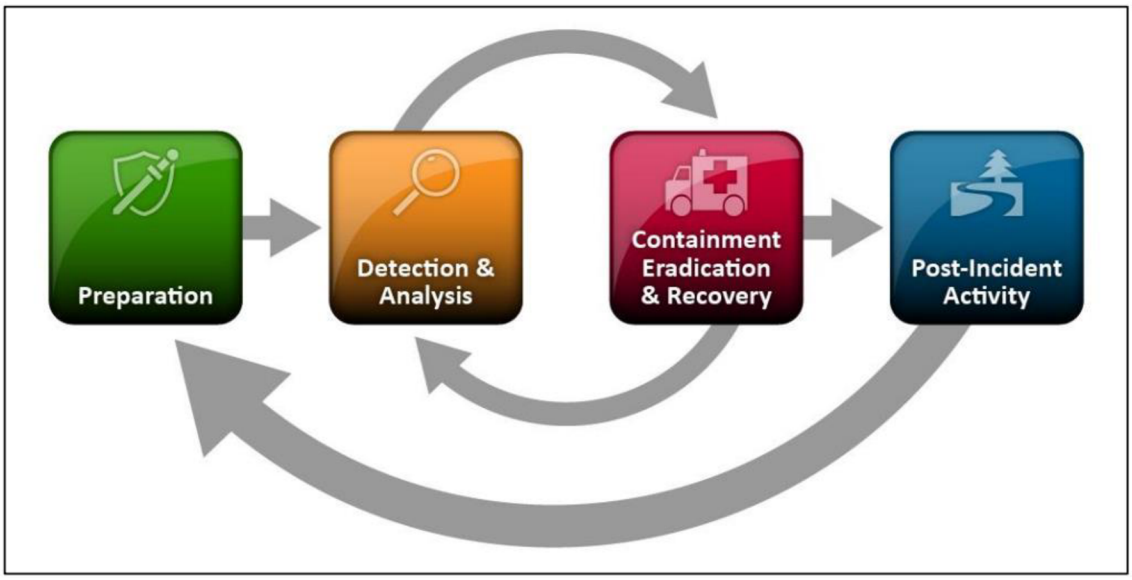
původu, připojíme ke zprávě podpis (obsahující kontrolní součet zprávy), zašifrovaný naším soukromým klíčem. Adresát tedy pomocí našeho veřejného klíče podpis dešifruje a ověří si tím, že zpráva nemohla být podepsána nikým jiným, než vlastníkem našeho soukromého klíče. Vytvoří si kontrolní součet zprávy, porovná jej s kontrolním součtem v našem podpisu a tím dokončí ověřování, že podpis byl se zprávou sloučen už od začátku její cesty. [17]

S/MIME: Secure/Multipurpose Internet Mail Extension je dalším běžně využívaným způsobem koncového šifrování. Jedná se o standardizovaný protokol k šifrování zpráv, jež je charakterizován nutností svůj certifikát podepsat za registrační poplatek u místní certifikační autority. Důvěrnost přenášených zpráv je tedy centrálně zajišťována v rámci hierarchické struktury certifikačních autorit a není třeba distribuovat klíče svépomocí. [17]

2.5 Incident handling

Incident response a incident handling jsou prozatím ne zcela ukotvené pojmy, které jsou v rámci celé komunity vnímány různě. Existuje mnoho různých definic, kde se tyto pojmy překrývají, nebo je jejich sémantická podstata různě seskupována pod pojem Incident Management. Pro zjednodušení však budu ve své práci interpretovat tyto pojmy jako synonyma. Jde o hlavní náplň práce všech CERT, CSIRT, SOC a jiných kyberbezpečnostních týmů.

Přestože každý z nich má v rámci incident handlingu přístup k jiným nástrojům, nebo má ve svém repertoáru odlišné metody a postupy, uvedu zde hlavní jádro celé problematiky, na kterém všechny týmy staví. Samotný incident response se sestává ze tří fází, které na sebe navazují v rámci řešení jednotlivých incidentů. V kontextu celého fungování týmu jde však o fáze a aktivity zcela souběžné, konstantně běžící a neustále se doplňující. Po těchto fázích nastává fáze zvaná „lessons learned“, která je důležitá z manažerského hlediska pro kontinuální zlepšování úrovně kybernetické bezpečnosti v organizaci. V následujícím schématu je znázorněna bodem „Post-incident Activity“. [15]



Obrázek 2: Fáze incident handlingu [15]

2.5.1 První fáze – Příprava

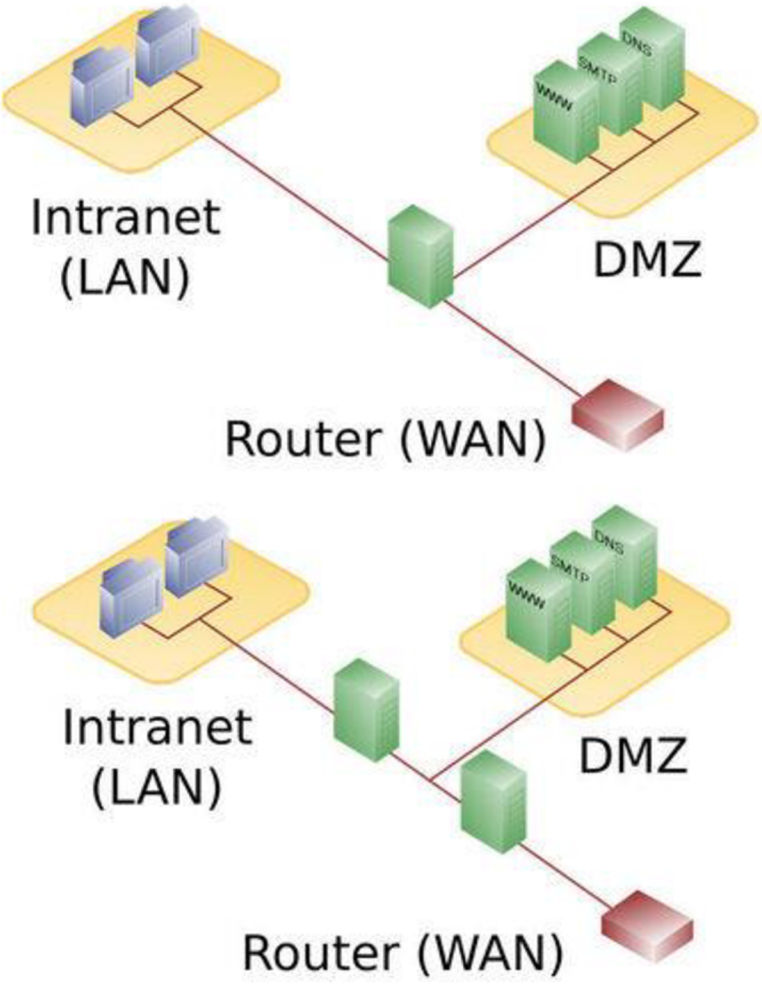
Všem opatřením předchází analýza rizik v rámci ISMS, která identifikuje systémy a aktiva, jež jsou kritické pro fungování organizace či jejich hlavních procesů. Na ochranu těchto aktiv je třeba soustředit více prostředků a v případě dvou souběžných incidentů je třeba ochranu těchto aktiv prioritizovat. Až jsou identifikována rizika na těchto aktivech (jako například systém otevřený do internetu, neaktualizovaný zranitelný systém nebo nezálohované databázové servery) měla by být přijata vhodná opatření k řádné obraně aktiva, ale pouze do výše rizika. Nemá význam vynakládat velké finanční prostředky na zabezpečení nedůležitého systému, který ani není viditelný z internetu. V rámci řízení rizik existují následující čtyři způsoby, jak se s nimi vyrovnat:

1. **Transfer rizika** – neboli přenesení břemene, které sebou riziko nese. Kupříkladu pořízením pojištění.
2. **Přijmutí rizika** – jde o rozhodnutí neinvestovat žádné dodatečné prostředky k vyřešení rizika. Třeba když je cena příliš vysoká, ale dopad incidentu by byl příliš nízký.
3. **Mitigace rizika** – aplikace bezpečnostních opatření, které sníží míru pravděpodobnosti nebo míru dopadu incidentu (nebo obojího).
4. **Vyhnutí se riziku** – aktiva vystavená příliš vysokému riziku mohou být například vyřazena mimo provoz za účelem vyhnutí se riziku. [1]

Analýza rizik by se měla vypracovávat na pravidelné (roční) bázi a pro subjekty spadající do KII nebo VIS je tato činnost povinná dle Zákona o kybernetické bezpečnosti.

Mimo ZKB existují normy a celá řada takzvaných best practices, jež shrnují nejlepší možné způsoby přípravy proti kybernetickým hrozbám. Uvedu pár nejzákladnějších technik:

DMZ – demilitarizovaná zóna je fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od lokální sítě organizace. Do DMZ se standartně umisťují stroje, které ze své podstaty musí být viditelné z internetu. Například webové servery, mailové servery nebo FTP servery. Běžně se pro toto nasazení využívá jeden firewall. Bezpečnější architekturou však je nasazení dvojitého firewallu viz obrázek níže. [14]



Obrázek 3: Umístění FW v DMZ [20]

CLM – Logy jsou velice užitečnými zdroji informací o chodu operačního systému, aplikaci nebo o provozu v síti. Poskytují velice silnou transparentnost a jejich monitoringem lze odhalit mnoho typů útoků. Jejich bližší analýzou pak lze zpětně vypátrat scénář již proběhlého incidentu. Centralized Log management (CLM) je pokročilé řešení sběru těchto logů ze všech dostupných míst pro potřeby analýzy a jejich vzájemné provázání / obohacení (tzv. log enrichment). [1]

FW – Firewall je v dnešní době už naprosto klíčovou a nepostradatelnou komponentou při ochraně perimetru sítě. Jde o bránu mezi lokální a veřejnou síťí, která omezuje

provoz dovnitř i vně na základě vlastní konfigurace a blacklistů. Nedoporučuje se použití defaultních konfigurací, protože útočník pak může předvídat který packet přes firewall projde a který ne. FW chrání systémy před obrovskou škálou hrozeb a slouží jako nástroj detekční i mitigační. V rámci prevence je třeba míti nasazené FW řešení neustále aktualizované. [1]

Group policies – jedná se o centrálně kontrolované bezpečnostní politiky pro všechny uživatele v doméně dané organizace. Tuto funkci mohou využívat organizace na Windows infrastruktuře a diktovat tak všem účtům v doméně pravidla, týkající se například politiky hesel nebo pravidel instalování neověřených aplikací. Správně nastavené group policy může předejít mnohým incidentům. [1]

SPF, DKIM, DMARC – jde o bezpečnostní a reportovací nástroje pro obranu před hrozbama zneužívající e-mailovou komunikaci jako prvotní vektor útoku. E-mailové útoky jsou prvotním vektorem většiny úspěšných útoků vedených jak plošně, tak cíleně a nasazení *Sender Policy Framework* (SPF), *DomainKeys Identified Mail* (DKIM) a *Domain-based Message Authentication, reporting and conformance* (DMARC) je součástí bezpečnostních best practices. Nejdůležitějšími principy jsou mechaniky proti spoofingu adres, kontrola integrity zpráv a vyhodnocování událostí a zasílání hlášení o chování příjemců správci domény. [1]

Školení uživatelů – jedna z nejdůležitějších praktik preventivního opatření. Jelikož velká část úspěšných kybernetických útoků vyžadovala interakci uživatele, je nutné je pravidelně vzdělávat v oblasti kybernetické bezpečnosti. Udržování obezřetnosti a bdělosti při práci s internetem může předejít mnohým incidentům. [1]

Fyzická ochrana – podceňovat by se neměla ani fyzická ochrana. Ani ty nejpokročilejší ochranné mechanismy nám totiž nepomohou, pokud se bude moci útočník volně pohybovat po objektu. Zkušený útočník má při fyzickém přístupu ke stroji prakticky neomezené možnosti. Od nahrávání rootkitů nebo jiného malware, eskalování kořenových oprávnění přes odposlouchávání či DoS až po samotné zašifrování nebo kompletní zlikvidování dat či systému. V mnohých případech nám

nepomůže ani šifrovaný disk nebo zamčený počítač. Pro tyto případy je fyzická obrana klíčová. K nejznámějším mechanikám fyzické obrany patří následující. [1]

- Instalace turniketů
- Přísné omezení fyzického přístupu do server room a switch room
- Dodatečné zabezpečení serveroven (bezpečnostní klece, ochrana RJ45 konektorů, požární řešení, záložní servery atd.)
- Použití repelentů (ploty, cedule, psi)
- Instalace bezpečnostních kamer
- Využití tzv. man traps (typ autorizační místnosti)

2.5.2 Druhá fáze – Detekce

Druhá fáze incident handlingu zahrnuje detekci a do předem stanovené míry i analýzu kyberbezpečnostních incidentů a událostí. Znaky o incidentu se dají zařadit do dvou kategorií: **prekurzory a indikátory.** Prekurzor značí výskyt události. Poukazuje, že incident v budoucnu může nastat (například aktivní phishingová kampaň) a indikátor je náznak, že už incident dávno nastal, nebo zrovna probíhá, (například zanechaný ransomnote od útočníka). Oba tyto typy je nutné aktivně detekovat a následně řešit. Možných vektorů útoků je celá řada a je třeba jistým způsobem pokrýt každý z nich. S ohledem na charakter organizace se však některým musí věnovat větší pozornost a některým menší. Je třeba danému problému porozumět, aby byly podniknuty nejvhodnější mitigační kroky. V této fázi se též začíná celý případ pečlivě dokumentovat pro budoucí účely. V rámci této fáze je také nejpřínosnější komunikace s ostatními týmy. Sdílení PoC od partnerů bývá velice častým impulzem na detekci konkrétního incidentu. Uvedu několik nejefektivnějších metod pro detekci:

YARA – jde o nástroj primárně používaný k detekci malware na základě takzvaných signatur. Tedy klíčových částí textového řetězce, kterým je daný malware charakteristický. Jelikož je každý malware unikátní, stejně tak se pro každý z nich většinou musí napsat unikátní YARA pravidlo. To se musí vždy spustit nad konkrétní oblastí disku či nad celým strojem pro

případnou detekci onoho řetězce. V rámci group policy lze tato pravidla spouštět hromadně. YARA pravidla bývají běžně distribuována v rámci komunity spolu s IoCs. [1]

CMD, PowerShell, Bash – obratné zacházení s Windows command line a s PowerShell (v případě Linuxů pak v Bash)je nedocenitelnou schopností v rámci incident handlingu. Poskytuje obrovskou škálu možností, včetně kontroly běžících procesů, navázaných internetových spojení atd. Zkušený incident handler příkazovou řádku běžně využívá i k analýze zanechaných artefaktů, k získávání a porovnávání otisků, ke kontrolování souborů, nebo k používání mnohých dalších nástrojů, jako je GPG pro šifrování nebo YARA pro skenování. [1]

IDS, IPS – Intrusion Detection System a Intrusion Prevention System jsou označení pro systémy, které poskytují organizaci při ochraně jejich kyberprostoru detekční a kontrolní nástroje. Oba typy pozorují síťový provoz a porovnávají obsah s databází již známých hrozeb. Liší se však v tom, že IDS nevykoná na základě svých pozorování žádnou akci k mitigaci problému. K zásahu je vždy potřeba lidské interakce, zatímco IPS umí zasahovat a omezovat provoz v síti podle vlastních pravidel. Tyto nástroje jsou kritické pro zajištění vysoké úrovně kyberbezpečnosti díky svým schopnostem automatizace procesů, bohatým možnostem konfigurace a mnohým dalším přednostem. [1]

Endpoint detection – Systémy detekce hrozeb na koncových zařízeních, mezi uživateli též známé pod označením antiviry, jsou další nepostradatelnou komponentou v oblasti kyberbezpečnosti. Detekují a mitigují hrozby na jednotlivých koncových bodech. V rámci organizace jsou tyto nástroje běžně centrálně spravovány. Mluvíme pak o integrovaném systému pro sběr, korelace a analýzy dat z koncových stanic v organizaci, za účelem koordinovaných kroků k mitigaci hrozeb. [1]

2.5.3 Třetí fáze – Stabilizace & eradikace

Třetí fáze běžně označována jako **Containment & Eradication** (udržení / stabilizace & vymýcení) zahrnuje samotné kroky v rámci nápravy incidentu a zmírnění jeho dopadu. V rámci této fáze je nejdůležitější pohotově reagovat a udržet samotný předmět incidentu pod kontrolou a zamezit jeho šíření. Následně pak jeho úplné odstranění. V závislosti na typu incidentu se dá tato fáze rozdělit na následující tři typy:

Containment na perimetru – tyto techniky aplikujeme, dojde-li k incidentu na perimetru (neboli v DMZ). Typicky se jedná o DDoS útoky, o skenování zranitelností nebo o bruteforce útoky.

- geofencing, ASN filtering
- IDS/IPS filtrování
- nastavení WAF pravidel
- nastavení null-route-DNS neboli přesměrování do černé díry

Containment v síti – pokud útočník působí vevnitř v síti, je nutné reagovat zcela odlišným způsobem. Může se jednat o odposlech, falešný redirecting nebo třeba o útok typu Man-in-the-middle. Síťový containment je praktikován například pomocí:

- VLAN izolace na přepínačích
- segmentování sítě na směrovači
- blokování portů
- blokování na základě IP nebo MAC
- užití ACLs (access control lists)

Containment na koncových bodech – v případě infikování jakékoli koncové stanice malwarem se používají následující praktiky:

- fyzické odpojení infikovaného systému ze všech sítí
- vypnutí infikovaného systému
- blokační pravidla v systémovém firewallu
- užití HIPS (host intrusion prevention systém)

Jakmile jsme úspěšně zamezili šíření a zakonzervovali hrozbu, můžeme začít s jejím odstraňováním a s obnovou do původního stavu. Opět jde o velice individuální

záležitost a každý případ vyžaduje vlastní postup. Obecně však řešení nejčastěji vyžaduje provedení těchto kroků:

- změna hesel dotčených uživatelů
- odstranění malware artefaktů pomocí antivirových programů
- identifikace původního vektoru útoku, posílení slabého místa
- re-imaging systému, obnovení dat ze záloh [1]

2.5.4 Lessons learned

Nedílnou součástí celého životního cyklu incidentu je fáze zvaná lessons learned. Jedná se o debrief akci, v jejímž rámci si pracovníci kyberbezpečnostního týmu zhodnotí průběh celého incidentu a zamyslí se nad těmito otázkami:

- Co jsme udělali dobře?
- Co jsme udělali špatně?
- Co jsme mohli udělat lépe?

Odpovědi na tyto otázky je nutné promítnout v případných úpravách interních procesů a metodik. Výstupy z tohoto debriefu můžou mít pozitivní vliv na jakoukoliv ze tří zmíněných fází během řešení budoucích incidentů. [1]

2.6 Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) je zpracovaný a zanalyzovaný souhrn všech dat z incidentů, událostí či jiných relevantních zdrojů informací o útočníkovi. CTI pomáhá pochopit útočníkovy cíle, motivy a jeho chování a tím nám umožňuje lépe se připravit na potencionální kybernetické útoky. Existují však tři typy intelu, přičemž každý má naprosto jiné použití na naprosto jiných úrovních obrany.

Strategické CTI

Jedná se o nejvyšší možný záběr, sledující trendy v oblasti kyberbezpečnosti. Výstupy ze strategických analýz jsou netechnického charakteru a jsou srozumitelné širšímu publiku. Šířeny jsou pomocí reportů a poslouží především při rozhodovacích procesech v nejvyšším managementu organizací či dokonce států. Tento intel je svázán jak s geopolitickým tak sociálním i ekonomickým kontextem a poskytuje vysoký nadhled nad vývojem kyberbezpečnostní situace. [25]

Taktické CTI

V rámci taktického CTI jsou zkoumány TTPs (Tactics, Techniques and Procedures) jednotlivých kyberzločineckých aktérů. Jedná se o intel techničtějšího charakteru, který pomáhá obráncům při mitigaci mnohých hrozeb. Reporty taktických CTI analýz jsou určeny především systémovým architektům, správcům aktiv, administrátorům a hlavně kyberbezpečnostnímu personálu. Taktické CTI by mělo výrazně usnadnit všechny fáze incident handlingu.[25]

Operativní CTI

Operativní CTI je představováno vědomostmi o kybernetických útocích, událostech a kampaních. Poskytuje specializovaný vhled do problematiky na vysoce technické úrovni, soustředíce se na velmi specifické případy útoků. Operativní intel může být například výstup z forenzní analýzy disku, malware analýzy či analýzy síťového provozu. Nález konkrétních artefaktů v systému, či jakýchkoliv IOCs. [25]

Kombinace všech tří typů CTI tedy dává dohromady ucelený přehled o hrozbách. Jako příklad mohu uvést zkrácenou verzi nedávného veřejného CTI výstupu:

- Několik ruských, státem sponzorovaných kyberkriminálních skupin, rozšířilo nový destruktivní malware typu wiper, zvaný HermeticWiper, který se šíří v souvislosti s Rusko-Ukrajinským konfliktem a cílí převážně na administrativu

státních finančních organizací na Ukrajině a v některých případech i v Litvě a v Lotyšsku. [19]

Díky informacím, poskytnutým v rámci tohoto výstupu, byly všechny evropské státy schopny řešit tuto kampaň na strategické, taktické i operativní úrovni. Bylo umožněno distribuování IoCs včetně hashů a YARA pravidel do všech organizací i pro širokou veřejnost a pohotově tak reagovat na nově vzniklou hrozbu. V ČR se o koordinaci staral NÚKIB.

Níže uvedu tři nejčastěji využívané modely a metodiky v oblasti Cyber Threat Intelligence.

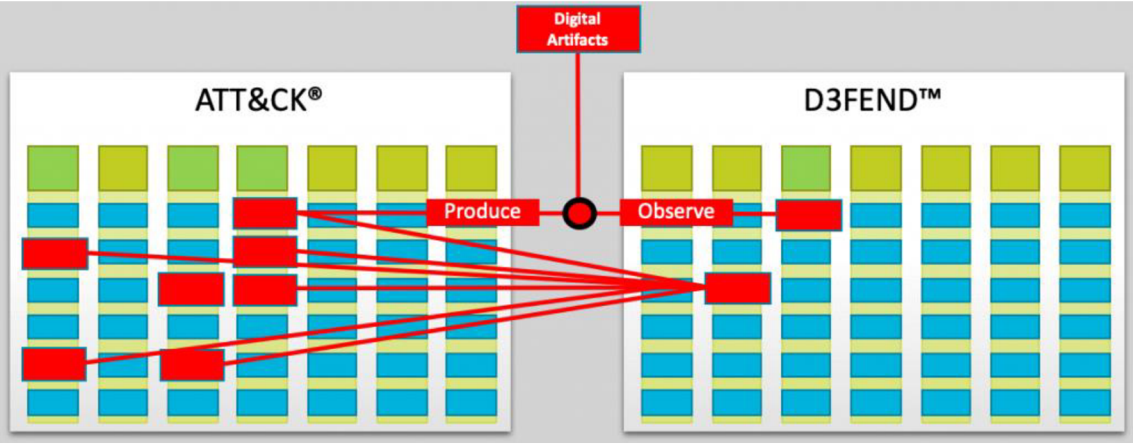
2.6.1 MITRE ATT&CK® MATRIX

Nezisková organizace MITRE vyvinula matici Tactics, Techniques and Common Knowledge (ATT&CK). Jde o globálně dostupnou a rozsáhlou bázi znalostí všech TTPs ve formátu matice, kde taktiky jsou představovány jednotlivými sloupci a techniky a subtechniky jsou v nich obsáhlé na úrovni řádků. Taktiky můžeme interpretovat jako „proč“ a techniky zase označujeme „jak“. V současnosti má matice 14 sloupců, seřazených od těch počátečních útočných taktik, jako je například průzkum prostředí nebo prvotní přístup, přes taktiky jako persistence nebo únik před detekcí až po závěrečné taktiky, jako je například C&C, exfiltrace nebo samotný dopad útoku. Každá z nich obsahuje vyšší jednotky až nižší desítky technik, které se pak dále tříští na jednotlivé sub-techniky.

Účelem není popsat celý životní cyklus útoku, jako je tomu u Kill Chainu (viz 2.6.3), nýbrž setřídit všechny dostupné známé TTPs. Čili útočník v rámci kybernetického útoku nemusí vždy využít všech 14 taktik, ale v případě zpětné důkladné analýzy incidentu lze každou nalezenou taktiku náležitě zařadit do matice a prostudovat doporučené mitigace a prostřednictvím dříve zpracovaných návrhů rychle a správně reagovat.

Jako příklad mohu uvést techniku označenou jako *T1491 – Defacement*. Spadá pod poslední taktiku „*Impact*“ a má dvě sub-techniky. Jedná se o techniku běžně využívanou hacktivistickými skupinami k zastrašení a k propagandě. V Evropě velice zřídka využívanou, ale například v Izraeli nebo v Pákistánu se jedná o jednu z nejčastěji využívaných technik v rámci kybernetických útoků na veřejnou správu. [24]

Udržování této znalostní báze je extrémně důležité pro udržení přehledu o průběhu úspěšných útoků a tedy k identifikování vlastních slabých míst. Výhradně pro tyto účely byla v roce 2021 navíc vytvořena inverzní matice s názvem D3FEND, jež poskytuje ucelený rámec všech obranných technik, které systémoví administrátoři mohou aplikovat, aby pokryli možné útočné techniky popsané v matici ATTA&CK. Obrázek poslouží k lepšímu pochopení vztahu těchto dvou matic. [21]



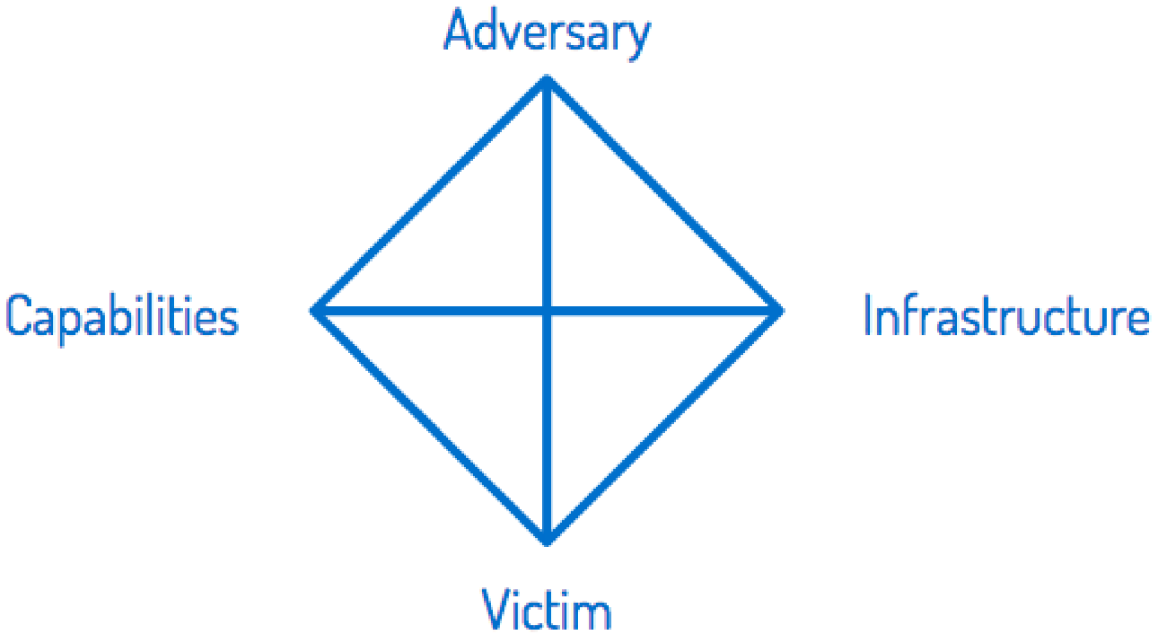
Obrázek 4: Vztah matic ATT&CK® a D3FEND™ [21]

Organizace MITRE je však, kromě těchto matic, známá i svou veřejně dostupnou databází zranitelností, které označuje pod identifikátory CVE.

2.6.2 Diamond model

Tento model prezentuje vztahy mezi mezi čtyřmi pilíři kybernetického bezpečnostního incidentu. Těmi jsou: útočník, schopnosti, infrastruktura a oběť. Axiomem spojujícím

tyto body je, že za každým vniknutím stojí útočník, který za použití svých dovedností, přes dostupnou infrastrukturu, zasáhne oběť.



Obrázek 5: Diamond model [22]

Použití tohoto modelu výzkumníkům ulehčuje soustředit se na propojení důležitých bodů v rámci strategické, taktické i operativní CTI analýzy. Je vhodné zjistit především kdo za incidentem stojí, zda se útočník nevydává za jiného, jaké jsou jeho motivy, jaký je jeho *modus operandi,* jaké použil nástroje a TTPs, případně jaké využil zranitelnosti. Je třeba také shrnout konečné dopady na organizaci a zmapovat stav infrastruktury předcházející incidentu. [22]

2.6.3 The Cyber Kill Chain®

The Cyber Kill Chain®, vyvinut společností Lockheed Martin je celosvětově využívaný rámcový model životního cyklu kybernetického útoku. Popisuje 7 fází, kterými musí každý útočník projít, aby dosáhl svého cíle.

Obrázek 6: The Cyber Kill Chain® [23]

1. Útok začíná krokem zvaným reckon. Jde o zmapování prostředí, sběr užitečných informací a dat potřebných k útoku atd.

2. Následuje fáze weaponization, tedy ozbrojení. Typicky jde o vytvoření malwaru, škodlivého packetu nebo jeho zakoupení.

3. Třetí krok, delivery, reprezentuje dopravení útoku k cíli. Jde o první krok v rámci Cyber Kill Chain, kterému se může obránce bránit. Může jít například o poslání payloadu skrze e-mail, nebo zaslání speciálního packetu na server.

4. Exploitation, neboli zneužití, je krokem, kdy útočník zneužije některé slabiny, aby útok spustil. Slabinou může být například zranitelnost v aplikaci, nebo neproškolený uživatel, který sám otevře a spustí script.

5. Spuštěný skript pak následně nainstaluje samotný malware na stroj. Jedná se o fázi Installation.

6. V šestém kroku je již stroj pod kontrolou útočníka a může jej vzdáleně ovládat.

7. Posledním krokem je vykonání samotného cíle útoku.

Porozumění těmto sedmi na sebe navazujícím fázím je považováno za naprostý základ znalostí v rámci kybernetické bezpečnosti a je důležitým aspektem při provozování CTI aktivit na všech úrovních. Správné zacházení s informacemi v rámci tohoto modelu může pomoci překlopit chování obranných týmů z řešení nastalých incidentů na proaktivní řízení kybernetické obrany a předcházet incidentům.

Stejně, jak tomu bylo u matice od MITRE, i Lockheed Martin na základě svého modelu vytvořil model inverzní, jenž se soustředí na protiopatření. Jedná se o pětifázový model zvaný Intelligence Driven Defense®.[23]

2.7 Nástroje

Bezpečnostní týmy obvykle využívají obrovskou škálu nástrojů a pomůcek k efektivnímu zvládání incident handlingu. Jde jak o nástroje placené, tak zdarma přístupné a mnohdy využívají i vícero nástrojů se stejným zaměřením, což je potřeba k verifikaci. Celá sada používaných nástrojů se však liší tým od týmu, v závislosti na

potřebách, na finančních možnostech, personálních kapacitách a na zaměření organizace, kterou tým zaštiťuje. Níže uvedu nejběžněji používané typy nástrojů v oboru.

Reputační nástroje – tyto nástroje fungují na komunitní bázi. Týmy si v nich ověřují reputaci jednotlivých IP adres, domén, URL, hashů, emailových adres, zjišťují nahlášené škodlivé chování a získané informace dále využívají ve svých aktivitách. Současně na těchto platformách své poznatky sami sdílí.

WHOIS služby – zjišťování původu adres a domén a hledání kontaktů na zodpovědnou osobu je velice častou náplní incident handlera, jelikož během své práce mnohdy narazí na kybernetický bezpečnostní incident, jehož řešení však není v jeho gesci. WHOIS servery udržují databázi mnoha užitečných informací, jako například informace o všech registrovaných doménách, ASN číslech, IP adresách, jejich geologaci, jejich registranty a kontaktní @abuse adresy na zodpovědné osoby, případně na správce webhostingu, na kterém je služba provozována.

Scanovací nástroje – přestože je scanování (portů, zranitelností atd.) bez souhlasu provozovatele systému legislativně zakázáno, skenovací nástroje jsou velice užitečnými nástroji i v rukou obránců. Je běžnou praktikou periodicky skenovat vlastní infrastrukturu a hledat slabá místa k posílení.

Detekční nástroje – tyto nástroje představují samotné jádro práce incident handlingu ve chvílích, kdy se zrovna neřeší žádný aktuální incident. V rámci druhé fáze detekce (viz 2.5.2) se tým plně soustředí na rozpoznání podezřelého chování. Ať už v síti, na koncových stanicích nebo kdekoliv jinde. Pod detekční nástroje můžeme zahrnout jednotlivé IDS a IPS nástroje, antivirové nástroje, SIEM nebo třeba firewall řešení či nástroje obsluhující síťové sondy.

Phishingové nástroje – phishing, jako nejúspěšnější a nejčastěji využívaná technika hned v několika taktikách ATT&CK matice, si zaslouží speciální pozornost. Většina organizací se musí vybavit nástroji, umožňujícími analyzovat phishingové maily, musí

bezpečně zacházet se soubory či odkazy v rámci phishingových útoků nebo testovat a školit vlastní organizaci rozesíláním falešných phishingových útoků.

Analytika – ačkoliv bývá u menších firem v rámci třetí fáze (Containment, Eradication viz 2.5.3) většinou prioritou co nejdříve všechen malware zlikvidovat nebo rovnou celý systém postavit od základu, z širšího hlediska je velice přínosné všechny dostupná data analyzovat a přijít na kloub jádru celého problému. Zajistit díky tomu, aby se problém už neopakoval. Ve větších organizacích je forenzní, síťová a malware analýza nedílnou součástí incident handling týmu. Tato práce vyžaduje obrovské množství specializovaných nástrojů pro analýzu, které se mění s každým případem.

Ransomware nástroje– úspěšně a kvalitně provedený ransomware útok už obráncům ve většině případů nepomůže žádný nástroj zvrátit. Přesto však existuje sada nástrojů a postupů, které obránci mohou zkusit během třetí fáze použít. Jedná se o zveřejněné dekryptory, repozitáře uniklých klíčů, rozpoznávače ransomnotes nebo veřejné rozcestníky takzvaných **leak sites** provozovaných operátory jednotlivých ransomware skupin.

CTI nástroje – pro práci v oblasti CTI jsou to převážně kvalitní zdroje informací. Je doporučováno udržovat zdravý balanc mezi neplacenými zdroji informací a placenými threat-intel platformami, protože obě varianty sebou nesou výhody i nevýhody.

Další podpůrné nástroje – může se jednat například o šifrovací nástroje, komunikační platformy, vlastní interní systémy nebo menší, podpůrné skripty pro automatizaci a workflow. [1]

2.8 Typy hrozeb

V této podkapitole představím nejznámější typy hrozeb, se kterými se společnosti potýkají.

2.8.1 Phishing

Phishing je jedna z nejčastěji využívaných metod sociálního inženýrství, běžně používaná jako útočný vektor velkého množství kybernetických útoků. Zakládá si na omylnosti uživatele, nikoliv techniky. Phishing je využíván na několika úrovních, přičemž běžní uživatelé jsou nejvíce obeznámeni s tou na nejnižší úrovni – s plošně rozesílaným spamem skrz e-mail. Zde se útočník snaží oběť přesvědčit o nutnosti kliknout na odkaz, vyplnit přihlašovací údaje nebo platební údaje, nebo stáhnout například .xls soubor s podporou maker a spustit VBA script. Existují však i mnohem sofistikovanější formy phishingu. Ty jsou velice specializované a velice zaměřené. Například **spear phishing**. Zde je útok mířený většinou na pracovníka na účetním oddělení s požadavkem na uhrazení faktury. **Whaling**, mířící na členy nejvyššího vedení a na ředitele, kteří bývají typicky nejméně vzdělaní v oblasti kybernetické bezpečnosti, přičemž mají současně největší autoritu a rozhodovací moc v organizaci. Phishingový útok může navíc využívat **spoofing**, tedy podvrhávání adres odesílatele. Také se běžně využívá **typo squatting**, kde je v přiložené URL nebo v e-mailové adrese odesílatele snadno přehlédnutelný překlep. Nejčastěji „0“ za „o“, „I“ za „l“. V případě homografického typo squatting útoku lze vyměnit například „e“ z latinky za cyrillické nebo nebo řecké „e“. Unicode znaky v rámci ASCII tabulky tyto techniky umožňují a pro běžného uživatele je identifikace útoku prakticky nemožná. Dotyčný se pak nachází na jiné stránce, než si sám myslí, nebo dostává zprávu od jiného odesílatele, než si sám myslí. [1]

2.8.2 DoS a DDoS

Denial of Service a Distributed Denial of Service jsou typy kybernetického útoku, ve kterém se aktér snaží zastavit provozování služeb daného aktiva. Rozdíl mezi nimi

spočívá v počtu strojů, které se na útoku podílejí. V případě DDoS jsou zdrojem útoku typicky obrovské počty nakažených strojů, které jsou součástí botnetu. Vektorem útoku je zpravidla síť. Nejpoužívanějšími typy DDoS útokú jsou:

SYN flood – útočící stroje hromadně navazují TCP spojení s cílovým serverem a v rámci probíhajícího handshake pošlou pouze první SYN packet. Obdrží od serveru SYN-ACK packet a už mu dále neodpoví ACK packetem. Stroj na druhé straně tedy po určitou dobu čeká na odpoveď, kterou nikdy nedostane a má po tuto dobu otevřenou relaci a pro ni zbytečně alokovanou výpočetní sílu, kterou nevyužije.

DNS aplification – stroje v rámci útoku posílají požadavek na cizí DNS servery, přičemž v rámci svého požadavku spoofují **return-to** adresu na adresu své oběti. DNS stroje pak celou svou obsáhlou odpověď vrací přímo oběti. Tyto zprávy jsou pro oběť mnohem náročnější vyřídit po stránce výpočetního výkonu. DNS servery tedy fungují jako zesilovače.

HTTP flood – jedná se o posílání obrovského množství naprosto legitimních HTTP GET requestů z co nejvíce zdrojů. Ale tak, aby se útočníci vlezli pod limit požadavků, který by spustil případnou Anti-DDoS ochranu u poskytovatele internetu na straně oběti. V rámci tohoto útoku je extrémně obtížné rozeznat legitimní provoz od toho falešného. Mitigace tedy často obnáší i dočasné odříznutí legitimního provozu, tedy samotné omezení služeb.

Útok typu Denial of Service ovšem nemusí být vždy veden distribuovaně přes síť. Existuje mnoho zranitelností, jejichž periodickým a frekventováním zneužíváním může útočník shazovat servery zevnitř. [26]

2.8.3 Odposlech a exfiltrace

Jedná se o kybernetické zločiny jejichž dopad přesahuje do oblasti informační bezpečnosti. Způsobů provedení je však obrovské množství. Může se jednat o kybernetický útok například typu **man-in-the-middle** nebo v případě kompromitace

stanice lze nasadit softwarový **keylogger**. Velká část těchto útoků ovšem probíhá na fyzické, personální rovině. Nespokojení zaměstnanci organizace mohou představovat bezpečnostní riziko. [1]

2.8.4 Bruteforce, password cracking, password spraying

Tyto techniky se snaží prolomit authentizační mechanismy. **Bruteforce** útok k tomu využívá hrubou výpočetní sílu a snaží se heslo uhodnout. Nejběžněji se setkáváme s bruteforcováním otevřených FTP portů, SSL portů nebo jiných přihlašovacích rozhraní. Tento proces značně urychluje využívání takzvaných slovníků, které obsahují statisíce statisticky nejpoužívanějších hesel. V případě, že je však omezen počet pokusů na zadání hesla, se používá **password spraying**, během kterého se pošle jen pár hesel, ale na co největší počet účtů. Čím více účtů, tím statisticky větší šance ke vniknutí. Poslední zmíněnou metodou je tzv. **password cracking.** Jedná se o offline lámání hesel. Tedy o lámání hesel hrubou silou v případě, kdy máme lokálně k dispozici například jejich hashe. Například koupené z nedávného úniku databáze. Využitím velkého výpočetního výkonu pak generujeme hesla, hashujeme je stejným algoritmem a výsledek porovnáváme s ukradnutým hashem. V případě, že jsou oba stejné, znaměná to, že jsme heslo prolomili. Proces může opět značně urychlit využití kvalitního slovníku. [1]

2.8.5 Ransomware

Ransomware se v posledních letech stal jednou z největších kybernetických hrozeb, které se obávají všechny menší, střední i větší organizace. Je to typ malware, jehož úkolem je zašifrovat všechna data na discích oběti (kromě oblastí disku s nainstalovaným operačním systémem). Útočníci pak na strojích zanechají takzvaný **ransomnote**, ve kterém informují o nedostupnosti dat a vymáhají výkupné za jejich dešifrování. Tento model kyberzločinecké aktivity se stal extrémně výdělečným a začal se v posledních letech rozvíjet velmi rychlým tempem. Operátoři ransomwarových skupin se v posledních třech letech neuvěřitelně zlepšili, jak v technickém pozadí tohoto útoku, tak i ve vyjednávání a v sociálním inženýrství s tím spojeným. Vybírají si

nejvhodnější čas k zašifrování dat, dokáží precizně stanovit cenu výkupného podle OSINT analýz dané společnosti tak, aby byla dostatečně vysoká, ale stále snesitelná a využívají mnohé nátlakové nástroje, aby managementu firmy znemožnili jednat s chladnou hlavou a zvýšili si tak šance na zaplacení výkupného. Například odpočtem času, během kterého se každou hodinu smaže náhodných 100 souborů, nebo detekcí pokusů o dešifrování dat obránci. Ransomware se nově člení na další typy:

- **Double extortion ransomware:** operátoři ransomware skupin si zvyšují šanci na zaplacení výkupného ještě pohrůžkou, že v případě nezaplacení pak data zveřejní na svých **leak sites**, nebo prodají zájemci s nejvyšší nabídkou.
- **Tripple extortion ransomware:** V tomto modelu figuruje navíc ještě výhružka poškozování dobrého jména společnosti. Od předem stanoveného času útočníci začnou o úspěšném ransomwarovém útoku informovat i kritické dodavatele a odběratele dané organizace. Zvýší tak nátlak i šance na zaplacení výkupného.

Díky své úspěšnosti se ransomware začal mezi kyberkriminálními skupinami distribuovat i v rámci obchodního modelu RaaS (ransomware as a service). Umožňuje aktérům s nižšími technickými schopnostmi zakoupit si vysoce pokročilý ransomware pro vlastní užívání. Model zahrnuje mnohdy i technickou podporu 24/7, uživatelské recenze a mnohé příplatkové služby navíc. Platba výkupného pak probíhá skrz kanál poskytovatele RaaS, kterému připadne část výdělku. Jako příklad nejznámějších ransomwarových skupin mohu uvést REvil, DarkSide, LockBit nebo Conti. [1]

2.8.6 Zero-day útoky

Zneužívání zranitelností pro vykonání efektu útoku je běžnou praxí kyberzločinců. Předejít se jim však dá jednoduše opravením dané zranitelnosti. Problém nastává, když je zranitelnost známá přesně 0 dní a žádná oprava (patch) ještě neexistuje. Organizace, které zjistí, že jsou touto zero-day zranitelností postihnuty se nachází v komplikované situaci. Dokud není dostupná oprava, mohou však riziko útoku mitigovat vyhnutím se riziku viz bod 2.5.1 nebo mohou zkusit aplikovat takzvané workaround řešení, doporučené vývojářem postihnutého programu / systému. [27]

ANALÝZA SOUČASNÉ SITUACE

V této části analyzuji organizaci, jejíž řešením kybernetické bezpečnosti se budu zabývat v návrhové části. Jedná se o Fakultu Podnikatelskou Vysokého Učení technického v Brně. Výstupy mých analýz jsou jak technického charakteru, tak poskytují i kontextuální vhled do procesů řízení kybernetické bezpečnosti na fakultě.

2.9 Gesce CVIS – CSIRT

V současné situaci je, dle veřejně dostupných zdrojů, řízení kybernetické bezpečnosti na celém VUT v gesci Centra výpočetních a informačních služeb (CVIS). Tato součást VUT je podpůrného technického charakteru a má na starosti také mnoho jiných agend. Zejména provoz následujících služeb:

- Informační systém VUT
- Serverová infrastruktura
- Telefonní síť
- Emaily a Cloudové služby
- Počítačová síť a wifi
- Ekonomický systém
- Podpora uživatelů
- Mobilní aplikace
- E-learning

V minulosti již však vzešel požadavek na utvoření samostatně dedikovaného kyberbezpečnostního týmu pod záštitou CVIS, jehož cílem by byl pouze incident response na VUT. Tak vznikl VUT CSIRT. Tento incident response tým, jak sám deklaruje na vlastních stránkách https://www.vut.cz/cvis/csirt má nastavené tohle pole působnosti:

Domény:

- *.vut.cz, *.vutbr.cz, *.vutbr.net (hvězdička značí „cokoliv“)

IP rozsahy:

- 2001:67c:1220::/46 – IPv6 rozsah. Pro účely této práce nezajímavý.
- 147.229.0.0/16 – IPv4 rozsah o velikosti 256 C sítí, tedy celkově 65 534 IP adres.

Z veřejně dostupných WHOIS záznamů lze potvrdit, že se jedná o IP rozsahy registrované pod ASN 197451 pro registrovanou organizaci VUT-MNT, ovšem kontaktní adresy jsou většinou odlišné. Například lookup.icann.org uvádí kontaktní adresu tpoder@cis.vutbr.cz (Tomáš Podermanski), kdežto RIPE NCC, evropská registrační autorita podřízená celosvětové organizaci IANA zase uvádí abuse@vutbr.cz. („abuse“ je v bezpečnostní komunitě standartně využívaný název pro mailbox, jež slouží pro nahlašování incidentů. Jde ovšem jen o nepsanou konvenci)

Na stránkách CVIS CSIRT je kromě zveřejněného PGP klíče (bez data expirace) též uveden další pár kontaktních emailů. Opět odlišných: cert@vut.cz a noc@vut.cz. Odkaz, uvedený na stránkách https://www.trusted-introducer.org/directory/teams/csirt-vut.html nás zavede na profil týmu uvedeného jako „Listed“ v rámci Trusted Introducer Platform. Údaje uvedené zde v některých částech také lehce odlišné:

- Kromě nám známého ASN jsou zde dvě další: AS60143 a AS201263.
- Mezi IP rozsahy se objevil též rozsahy: 185.1.25.0/24 a 2001:7f8:87::/48
- Mezi doménami zde přibývá br-ix.cz

Pomocí této zběžné OSINT analýzy si lze všimnout jisté nekonzistence uvedených údajů. V případě kybernetického bezpečnostního incidentu, zjištěného externě, může jeho nahlašování zodpovědnému týmu působit dané organizaci potíže. Tuto domněnku mohu potvrdit vlastní zkušeností. Za posledních 7 let nedostal GovCERT jedinou zpětnou vazbu od VUT CSIRTu na zaslané hlášení, upozornění nebo poskytnutý threat intel či IoCs. Pravděpodobně z důvodu uvedené špatné kontaktní adresy. Dále nutno

poznamenat, že telefonní číslo uvedené na TF-CSIRT portálu patří sekretariátu CVIS, po jehož zavolání mi bylo řečeno, že o existenci žádného CSIRT týmu neví.

2.10 Gesce FP

Z registrovaného IP rozsahu 147.229.0.0/16 je fakultě podnikatelské přiřazeno **8 C sítí** počínajíc od 147.229.120.0. V současné době nejsou všechny využívané, ale všechny **jsou v plné odpovědnosti fakulty**. Fakulta tedy dle, interních směrnic, musí řešit kybernetickou bezpečnost v souvislosti s těmito rozsahy. V tabulce níže uvidíte přehled důležitých adresních rozsahů na fakultě a jejich využití.

Tabulka 2: Základní rozdělení sítí na FP

Síť	Minimální host	Maximální host	Maximum hostů	Využití sítě
147.229.120.0/23	147.229.120.1	147.229.121.254	510	adresní prostor pro zaměstnanecké počítače
147.229.122.0/24	147.229.122.1	147.229.122.254	254	dále rozdrobeno na menší účelové, většinou spojovací sítě
147.229.123.0/24	147.229.123.1	147.229.123.254	254	adresní prostor pro servery
147.229.124.0/23	147.229.124.1	147.229.125.254	510	adresní prostor pro studentské a laboratorní počítače

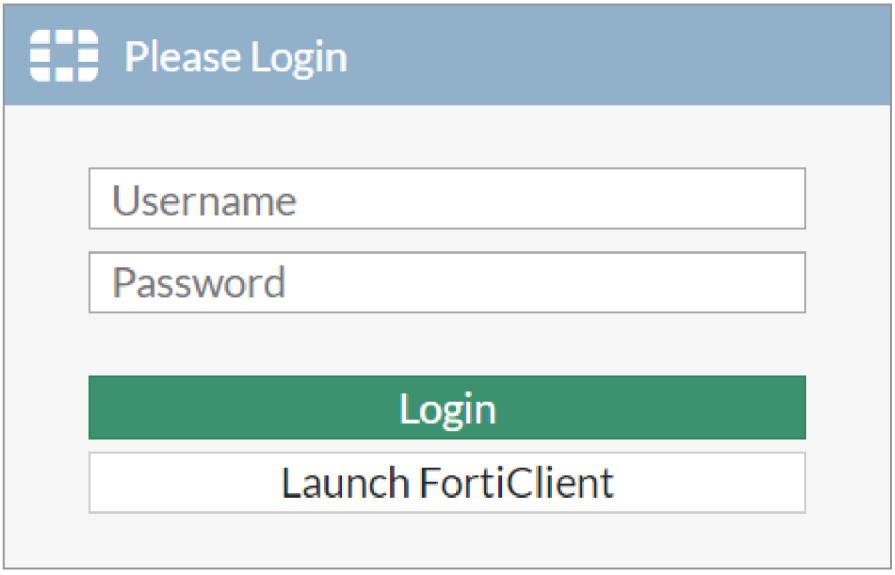
Role přidělená CSIRT týmu na CVISu zdá se být pouze koordinační. Dohled nad kyberprostorem na fakultě neprovozuje. Pouze má reagovat na oznámení externích organizací a distribuovat je mezi fakulty, dle jejich polí působnosti. V našem případě jde převážně o přeposlané zprávy z CESNETu. Tato koordinační aktivita je ovšem velice sporadicky pojata. Zprávy chodí řádově v nižších jednotkách ročně.

2.11 Technická analýza

Ze zjištěných informací, uvedených výše, provedu bližší analýzu kybernetické bezpečnosti na fakultě. Analýza je technického charakteru a nejsou během ní použity žádné invazivní skenovací metody.

2.11.1 Zranitelnosti na perimetru

Jako první krok se pokusím odrazit od něčeho, co již znám. Tedy IP rozsahy fakulty. Pomocí jednoduchého filtru v Shodanu *net:147.229.120.0/21* získám výpis všech viditelných strojů z internetu až po max hosta 147.229.127.254. Obdržel jsem **29** výsledků. Větší část z nich je nic neříkajících, ovšem pro potencionálního útočníka by mohly být zajímavé třeba stroje na adresách 147.229.122.18 a 147.229.122.21. Jde o vystrčené Fortigate Firewall login portály. Z mé pozice však nelze ověřit, zda se jedná o přístup do administrace firewallu, nebo jde o přihlášení k VPN. Případně zda je po přihlášení vyžadována 2FA či zda nejde o zapomenutý vystrčený endpoint.



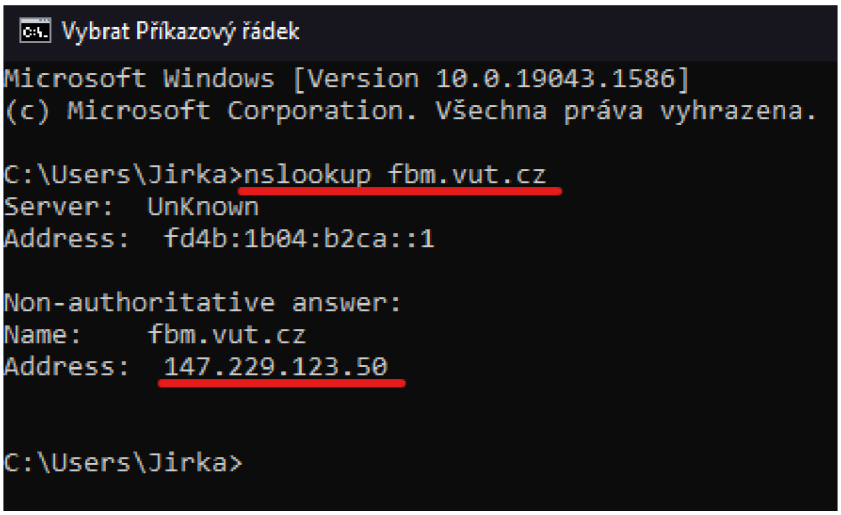
Obrázek 7: Login interface viditelný na 147.229.122.18 a na 147.229.122.21

Dalšími stroji hodnými pozornosti jsou webové servery:

- Esim.fbm.vutbr.cz na 147.229.124.4
- web1.fbm.vutbr.cz na 147.229.123.50
- web2.fbm.vutbr.cz na 147.229.124.25
- web3.fbm.vutbr.cz na 147.229.123.51

První z uvedených webů je ve studentském rozsahu a jedná se o stránky ESIM. Web běží čistě přes port 80 – http, čili stránka nemá platný certifikát a komunikace se serverem je vždy nešifrovaná. To může představovat výraznou bezpečnostní hrozbu, vezmeme-li v potaz, že stránka http://147.229.124.4/Login.aspx?ReturnUrl=%2f slouží jako přihlašovací modul. Heslo během přihlašování jakéhokoliv uživatele tedy vždy putuje internetem v otevřené podobě a vzhledem k běžnému trendu znovu-používání hesel uživateli jsou možnosti útočníků pestré.

Zbylé tři weby všechny souvisí s hlavním webem fakulty. Jednoduchým reverse DNS dotazem v příkazové řádce si potvrdíme, jaká je IP adresa z nich je adresa hlavního fakultního webu.



Obrázek 8: Reverse DNS dotaz na IP fakultního webserveru

Význam vedlejších web2 a weba3 mí není zcela znám. Podle všeho se jedná pravděpodobně o stroje hostující všemožné běžící či hotové projekty a v případě, že uživatel pošle požadavek na nesprávnou URL, přesměruje jej to na hlavní web fakulty, tedy 147.229.123.50. Mají otevřený port 21 pro FTP provoz. Ač je možné, že to má vlastní případ využití, může to představovat bezpečnostní riziko.

Konkrétním dotazem na adresu hlavního webu v Shodanu lze zjistit následující:

Server má do internetu otevřené porty 80, 443 a 8008. (port 8008 je běžně využíván pro odposlech Fortigate) a běží na systému Linux postaveném na Debian architektuře. Konkrétně se jedná o webový server Apache verze 2.4.25. Na základě verze systému byl nástroj Shodan schopný indexovat sadu známých zranitelností, kterými je tento server postihnut. Seznam 18ti adres spolu s odkazy na informace o zranitelnosti uvádím v tabulce níže:

Tabulka 3: Veřejně viditelné zranitelnosti na fakultním webserveru

CVE-2019-0220	https://nvd.nist.gov/vuln/detail/CVE-2019-0220
CVE-2018-1333	https://nvd.nist.gov/vuln/detail/CVE-2018-1333
CVE-2017-7679	https://nvd.nist.gov/vuln/detail/CVE-2017-7679
CVE-2019-0196	https://nvd.nist.gov/vuln/detail/CVE-2019-0196
CVE-2017-7659	https://nvd.nist.gov/vuln/detail/CVE-2017-7659
CVE-2017-9788	https://nvd.nist.gov/vuln/detail/CVE-2017-9788
CVE-2017-9798	https://nvd.nist.gov/vuln/detail/CVE-2017-9798
CVE-2019-0211	https://nvd.nist.gov/vuln/detail/CVE-2019-0211
CVE-2017-15710	https://nvd.nist.gov/vuln/detail/CVE-2017-15710
CVE-2018-11763	https://nvd.nist.gov/vuln/detail/CVE-2018-11763
CVE-2018-1283	https://nvd.nist.gov/vuln/detail/CVE-2018-1283
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167
CVE-2018-1312	https://nvd.nist.gov/vuln/detail/CVE-2018-1312
CVE-2017-7668	https://nvd.nist.gov/vuln/detail/CVE-2017-7668
CVE-2017-3169	https://nvd.nist.gov/vuln/detail/CVE-2017-3169
CVE-2018-17199	https://nvd.nist.gov/vuln/detail/CVE-2018-17199
CVE-2019-0197	https://nvd.nist.gov/vuln/detail/CVE-2019-0197
CVE-2017-15715	https://nvd.nist.gov/vuln/detail/CVE-2017-15715

6 z těchto zranitelností má podle NIST závažnost kritickou. 7 jich má závažnost vysokou a 5 závažnost střední. K posouzení závažnosti zranitelnosti se používá CVSS 3 metrika a je přiděleno skóre od 1 do 10. Mnohé CTI služby tuto hodnotu spolu s dalšími faktory (jako je například zveřejněný PoC, nedávné známé přidružení zranitelnosti k pentest nástrojům nebo vzrůstající trend detekovaných pokusů o zneužití) využívají ke kalkulaci celkové míry hrozby v současné chvíli. Za pomocí nejmenovaného nástroje, který umí tyto hrozby posuzovat mohu uvést 3 nejzávažnější zranitelnosti zkoumaného web serveru:

CVE-2019-0211: Zneužitím této zranitelnosti, které bylo dle CVSS3 přiděleno skóre 7.8/10 – high lze na stanici spustit libovolný kód s nejvyšším oprávněním (většinou oprávnění root) pomocí manipulováním s Apache scoreboard.

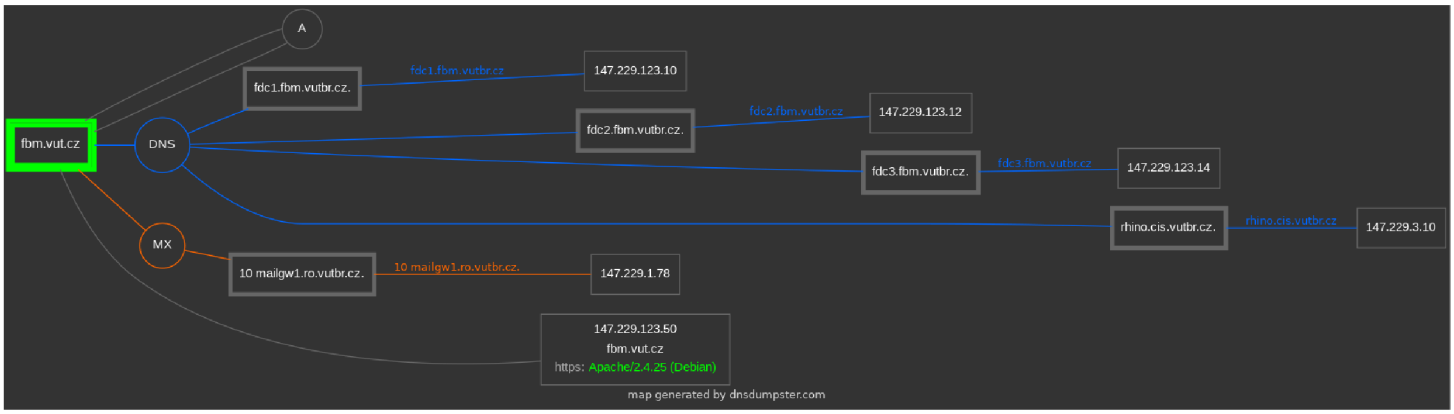
CVE-2017-9788: Tato zranitelnost, postihující zmíněný Apache server má dle CVSS3 přidělenou hodnotu 9.1/10 – critical. Její zneužití může vést k úniku citlivých informací, v jiných případech k DoS.

CVE-2017-3167: Pomocí této zranitelnosti, jež má dle metriky CVSS3 přidělené skóre 9.8/10 – critical může útočník na Apache serveru obejít autentizační bezpečnostní mechaniky.

Shodan ovšem zranitelnosti indexuje čistě podle zjištěných verzí běžících systémů. Je tedy pravděpodobné, že nám známých 18 zranitelností je pouhá podmnožina všech přítomných zranitelností na stroji. Vzhledem k tomu, že některé z nich jsou staré již 5 let, může útočník logicky dedukovat, že správci systému absolutně neřeší patch managment a může se pustit do dalšího (i invazivního) skenování zranitelností. Například je zcela možné, že jak je běžnou praxí, že web server je plně virtualizovaný. Třeba pomocí neaktualizovaného virtualizačního VMware nástroje. Možnou kritickou zranitelností, vhodnou ke zkontrolování útočníkem, je proto například CVE-2021-44228 též nechvalně známá jako **Log4Shell**. Tato zranitelnost s nejvyšším možným CVSS3 skóre 10/10 byla zveřejněna koncem roku 2021 a odhaduje se, že postihuje

miliony strojů po celém světě. Nelze ji skenovat jinak než invazivně, tudíž nelegálně a její zneužití je extrémně snadné a způsobené škody jsou omezené pouze fantazií útočníka.

Využitím volně dostupného skenovacího nástroje DNSdumpster si dotvořím obrázek o struktuře z internetu viditelných strojů na fakultě. Nejprve se dotáži na fbm.vut.cz



Obrázek 9: Schéma viditelných strojů na fbm.vut.cz

Z obrázku vidíme na modré lince 3 DNS servery fdc1, fdc2 a fdc3, které současně slouží jako školní DC (doménové řadiče) pro vícero domén. rhino.cis je mimo fakultní rozsahy. Na oranžové lince sedí Microsoft Exchange server, který slouží pro veškerý SMTP provoz. Tedy e-mailová brána. Není v rozsazích FP, nýbrž VUT. Fakultní mail již přes půl roku údajně neexistuje a veškerá e-mailová komunikace v rámci fakulty je řešena pouze přes VUT MX servery, což vnímám jako správné řešení po technické i bezpečnostní stránce. Na nejnižší lince vidíme již probíraný fbm.vutbr.cz web server, ale pod doménou vut.

Zadám-li však do nástroje DNSdumpster fbm.vutbr.cz, obdržím mnohem rozsáhlejší schéma.

Schéma je dostupné v Příloze 1 a příloze 2 v rámci této diplomové práce, viz seznam příloh.

Konkrétně 105 záznamů. Kromě již zmíněných webserverů a nameserverů lze vidět velké množství strojů ze studentské nebo zaměstnanecké sítě. Všechny tyto stroje mohou být pro útočníky objektem skenování. Vyberu některé příklady, které mě zaujaly již samotným názvem.

Pravděpodobně zapomenuté SMTP endpointy:

- Smtp2.fbm.vutbr.cz
- smtp1.fbm.vutbr.cz
- mail1.fbm.vutbr.cz
- mail2.fbm.vutbr.cz
- mail3.fbm.vutbr.cz

Zaměstnanecké stroje:

- uizam-onrak21.fbm.vutbr.cz
- kukan-13.fbm.vutbr.cz
- ufza-hanusova21.fbm.vutbr.cz
- umzam-skapa.fbm.vutbr.cz
- ntb-navratil-21.fbm.vutbr.cz
- desktop-I2j8gp1.fbm.vutbr.cz
- umzam-jurova21.fbm.vutbr.cz resolved as STEPANKOVA-15.fbm.vutbr.cz
- kriz-2011.fbm.vutbr.cz

Pravděpodobně kamery v místnosti P252:

- kamery-p252.fbm.vutbr.cz

Databázové zdroje pro web fakulty, nebo SQL servery určeny pro výuku:

- sql3.fbm.vutbr.cz
- sql2.fbm.vutbr.cz

2.11.2 Využívaný software

Podle informací poskytnutých od pracovníků fakulty je v organizaci využíváno hardwarové řešení Fortigate FG600E. Potvrzuje to mé odhady vyvozované z otevřených naslouchacích portů a z viditelnosti stroje, sedícího na adrese 147.229.120.21. Jedná se o komplexní a kvalitní firewall řešení zahrnující v sobě systémy IPS a IDS. Více informací nemohu uvést kvůli jejich citlivému charakteru.

2.11.3 Historické události

Na reputační portál AbuseIPDB nebyla nahlášena žádná adresa z rozsahu 147.229.120.0/17.

V rámci hledání historických incidentů a událostí dále pokračuji kontrolou umístění IP adres na známé blacklisty. Zadáme-li do pole ASN „AS197451“ a do pole country code „CZ“ ve veřejné databázi IP blacklistů spravované CESNETem dostupné na https://nerd.cesnet.cz/nerd/ips/ získáme výpis všech IP adres veřejně označených jako škodlivých z našeho VUT IP rozsahu. K datu vypracování téhle práce je momentálně 24 adres umístěno na veřejný blacklist.

Tabulka 4: Blacklisted IPs from VUT ASN

IP adress	Hostname	ASN	Events	Reputation	Comments	Time added	Last event
147.229.165.4	--	AS197451	295422	0.750	1 blacklist, (D)DoS attacks	22.10.2021 9:55	15.04.2022 13:19
147.229.44.158	umt158.fme.vutbr.cz	AS197451	176311	0.238	2 blacklists, Scanner	04.03.2022 7:25	15.04.2022 13:28
147.229.148.100	servman535.utko.feec.vutbr.cz	AS197451	15311	0.062	1 blacklist	06.04.2022 18:15	07.04.2022 7:24
147.229.197.4	b07-1312b.kn.vutbr.cz	AS197451	1011	0.057	1 blacklist, Scanner	05.04.2022 12:25	07.04.2022 12:57
147.229.220.18	a05-0616b.kn.vutbr.cz	AS197451	611	0.052	1 blacklist	11.04.2022 17:35	11.04.2022 18:24
147.229.96.83	pcchromy.ad.ceitec.vutbr.cz	AS197451	311	0.042	1 blacklist	11.04.2022 11:05	11.04.2022 17:16
147.229.133.218	dhcp218.ottp.fme.vutbr.cz	AS197451	4411	0.033	1 blacklist, Scanner	03.04.2022 19:19	04.04.2022 4:54
147.229.198.12	b07-615a.kn.vutbr.cz	AS197451	711	0.033	1 blacklist	07.04.2022 17:05	07.04.2022 22:02
147.229.200.254	c03-616b.kn.vutbr.cz	AS197451	711	0.032	1 blacklist	22.03.2022 7:18	07.04.2022 7:17
147.229.179.126	dhcps126.fit.vutbr.cz	AS197451	111	0.031	1 blacklist	14.04.2022 9:25	14.04.2022 9:18
147.229.183.139	dhcph139.fit.vutbr.cz	AS197451	211	0.029	1 blacklist	06.04.2022 12:48	08.04.2022 13:12
147.229.154.119	pckoktavy6.ufyz.feec.vutbr.cz	AS197451	111	0.029	1 blacklist	12.04.2022 19:25	12.04.2022 19:23
147.229.150.105	VM01.urel.feec.vutbr.cz	AS197451	911	0.029	1 blacklist	06.04.2022 15:53	06.04.2022 16:33
147.229.82.250	qnap-netme.fme.vutbr.cz	AS197451	1211	0.024	1 blacklist, Scanner	06.04.2022 5:14	06.04.2022 6:09
147.229.117.140	nat-kn.net.vutbr.cz	AS197451	211	0.021	2 blacklists, NAT	06.04.2022 19:55	06.04.2022 19:59
147.229.133.176	dhcp176.ottp.fme.vutbr.cz	AS197451	7111	0.019	1 blacklist, Scanner	05.04.2022 5:37	05.04.2022 17:06
147.229.200.80	c01-623a.kn.vutbr.cz	AS197451	211	0.018	1 blacklist	06.04.2022 0:45	06.04.2022 0:46
147.229.25.148	schwarz2015.mat.fce.vutbr.cz	AS197451	111	0.017	1 blacklist	08.04.2022 9:25	08.04.2022 9:21
185.62.108.185	brno.cmi.cz	AS197451	111	0.017	1 blacklist	08.04.2022 11:45	08.04.2022 11:42
147.229.150.119	VM15.urel.feec.vutbr.cz	AS197451	111	0.014	1 blacklist	06.04.2022 15:35	06.04.2022 15:31
147.229.3.54	flamingo.cis.vutbr.cz	AS197451	111	0.002	1 blacklist	02.04.2022 1:52	02.04.2022 1:51
147.229.117.40	nat-kn.net.vutbr.cz	AS197451	1711	0.000	2 blacklists, NAT, Scanner	27.01.2022 17:38	29.03.2022 19:27
147.229.194.5	b04-307a.kn.vutbr.cz	AS197451	211	0.000	1 blacklist	01.04.2022 11:35	01.04.2022 11:36
147.229.147.49	pcmasekp.utko.feec.vutbr.cz	AS197451	0	---	2 blacklists	10.02.2022 23:18	--

Mezi zobrazenými adresami se v současné chvíli nenachází žádná adresa z přidělených rozsahů pro fakultu podnikatelskou. Na seznam však běžně přibývají nové záznamy a je třeba jej kontrolovat na pravidelné bázi. Některé adresy jsou tam však umístěny dlouhodobě a je třeba kontaktovat příslušnou koordinační jednotku k prověření a napravení problému. Kupříkladu je alarmující, že první adresa v seznamu už přes půl roku rozesílá (D)DoS útoky a problému stále nebylo zamezeno.

V rámci bádání po historických událostech jsem současně využil JA3S otisky navazovaného TLS spojení ze serveru. Pomocí Shodanu jsem zjistil, že TLS odpověď serverů z následujících čtyř adres má otisk **e35df3e00ca4ef31d42b34bebaa2f86e**:

- 147.229.123.51
- 147.229.122.18
- 147.229.124.25
- 147.229.122.21

Pomocí pivotování na portálech několika placených reputačních služeb se mi podařilo zjistit, že tento otisk má historickou spojitost s BazarLoader, což je backdoor malware používající se k propašování tzv. payload na infikovanou stanici. V případě našeho otisku jde podle dostupných informací konkrétně o TLS odpověď C&C serveru pro Conti Ransomware dotaz. Nelze tedy vyloučit, že tyto stanice jsou již infikované a fungují jako C&C server pro ransomware aktivity známé kyberkriminální skupiny Conti. Jedna z publikací podporující mé závěry, kterou jsem našel, je dostupná na: https://malware.news/t/bazarloader-to-conti-ransomware-in-32-hours/52638. Existuje však mnoho dalších zmínek rezonujících komunitou. Celkově byl tento otisk zmíněn 70x na 7 různých zdrojích (a z toho 2x jen za měsíc březen) v souvislosti s mnohými dalšími rodinami malware. Kupříkladu Metasploit, Ryuk Ransomware a některé rodiny Trojan malware. Bližší odborná analýza by mohla tento nález objasnit. Podobný nález jsem našel pomocí JA3S otisku **364ff14b04ef93c3b4cfa429d729c0d9** na adrese 147.229.124.4 (tedy server na němž běží mimo jiné i již zmíněný portál ESIM), který má historickou spojitost s backdoor malwarem z rodiny SUNBURST.

2.12 Celkové zhodnocení

Pomocí mých analýz si lze utvořit představu o současném stavu o kybernetické bezpečnosti na fakultě. V rámci přidělených IP rozsahů pro FP se mi podařilo najít sadu zranitelností, jež dlouho nikdo neopravil na fakultním webserveru. Našel jsem mnoho stanic, které jsou z neznámého důvodu viditelné z internetu a některé jsou již pravděpodobně zapomenuté endpointy. Dále se mi podařilo pomocí JA3S otisků chytnout stopy k pivotování kolem historických zmínek o přítomnosti několika typů malware, z čehož lze vyvozovat pravděpodobnou kompromitaci několika fakultních strojů.

Přestože je možné, že závěry mých analýz jsou mylné a jedná se o takzvaný false-positive nález, faktem nadále zůstává, že neexistuje odborník, jenž by to mohl ověřit. VUT-CSIRT je zdá se jen logické spojení několika technických odborníků z různých oddělení CVISu, kde každý má svou roli v tomto týmu jako pouhou boční agendu. Kybernetická bezpečnost je řešena velice sporadicky, o čemž svědčí, že neupozornili FP ani na sadu pět let starých kritických zranitelností serveru veřejně zjistitelných z internetu. Kybernetická bezpečnost fakultní techniky je svěřena do rukou správce sítě, který současně působí jako učitel. Pro incident handling na fakultě v současné době není vybudováno žádné zázemí.

Z toho vyplývá, že neexistuje pověřený pracovník, jenž by:

- se staral o opravování zranitelností serverů
- držel dohled nad síťovým provozem v rámci fakulty
- fungoval jako kontaktní bod pro incident handling / protistrana VUT-CSIRT
- aktivně kontroloval zabezpečení školních stanic

Přestože nejde v ČR o nic neobvyklého, situace na fakultě je kritická. V následující části tedy navrhnu možná řešení pro pozvednutí úrovně kybernetické bezpečnosti na fakultě.

3 VLASTNÍ NÁVRHY

V této kapitole se budu věnovat návrhům možných řešení, jak na fakultě pozvednout úroveň kybernetické bezpečnosti a začít na dostatečné úrovni řešit incident handling. Jádro celé návrhové části představuje nasazení dedikovaného bezpečnostního týmu, jenž by měl tuto oblast na starosti.

3.1 Nasazení bezpečnostního týmu

Fakulta podnikatelská je po personální stránce středně velkou organizací. Zaměstnává sice cca 200 zaměstnanců, ale její činnost se dotýká tisíců dalších uživatelů – studentů. Dopady kybernetických útoků by mohly různými způsoby znesnadňovat či znemožňovat hlavní činnost organizace. Současně se nástroje, metody a postupy útočníků neustále vyvíjejí, a proto je nutné na tento trend reagovat a rozvíjet i obranu. **Navrhuji proto zřízení malého bezpečnostního týmu, jež by měl na starosti dohled nad všemi informačními aktivy spadající do gesce fakulty.** Dosavadní stav je těžce nevyhovující.

Informační infrastruktura VUT je velice decentralizovaná a proto je pozice univerzitního CSIRT týmu na CVIS velice důležitá. Formát onoho týmu je v rámci školy logický a vhodný. Z teoretické části této práce (bod 2.2.2) však vyplývá, že role CSIRT týmu je převážně koordinační. Mnoho systémů, rozmístěných na různých fakultách, nemá pod správou (včetně jejich IP rozsahů) a jeho efektivní funkčnost je těžce závislá na nastavených komunikačních kanálech s fakultami, na nastavených procesech a na jejich vzájemné spolupráci. Z analytické části současně vyplynulo, že komunikace mezi FP a CSIRT je takřka nulová a neexistují pověřené kontaktní osoby, jež by měly ve svém popisu práce se problematice incident handlingu na straně fakulty plně věnovat.

Z výše uvedeného vyplývá, že nejvhodnějším formátem nově nasazeného týmu by byl **SOC – Security Operations Centre**. Vzhledem k velikosti a komplexnosti fakultního prostředí, navrhuji vybudování zázemí pro tento tým o velikosti dvou až tří pracovníků. Tento celek je techničtějšího charakteru a musí fungovat jako protistrana VUT – CSIRT. Jedná se ve světě o běžně využívaný model v rámci silně decentralizovaných organizací a bylo by vhodné jej unifikovat pro každou fakultu a každý větší organizační celek v rámci VUT. To však přesahuje rozsah této práce.

3.2 Agenda bezpečnostního týmu

Nasazený SOC tým musí mít jasně stanovenou agendu. Stejně tak je třeba určit, co už v jeho agendě není.

3.2.1 Nepotřebné úkony

E-mailová komunikace: jak vyplynulo z analýzy, VUT má e-mailovou komunikaci spravovanou a zastřešenou centrálně na CVIS. Fakultní mailové servery byly v nedávné minulosti údajně všechny zrušeny a vše je nyní řešeno skrz Microsoft Exchange server *5mailgw1.ro.vutbr.cz* na adrese 147.229.1.78, což nespadá pod fakultní rozsahy. Odpadává tudíž velká část incident handlingu, a sice kontrola SMTP provozu, implementace SPF, DKIM, DMARC nebo záchyt a analýza phishingu a spamu.

CTI: v organizaci o velikosti FP VUT nemá praktický význam provozovat cyber threat intel v plném rozsahu. Tato aktivita přísluší vyšším koordinačním celkům, tedy národnímu CERT týmu, jež intel sám distribuuje. Je však nutné intel zvenčí přijímat a na podněty reagovat.

Forenzika: z důvodů značně omezených kapacit nebude možné v případě kybernetického bezpečnostního incidentu provádět detailní forenzní analýzu napadených strojů. Přestože to může snížit schopnost přijímat správná bezpečnostní

opatření, fakultní SOC tým musí plně prioritizovat včasné odstranění problému. V případě velké potřeby je možné analytickou činnost řešit outsourcingem.

3.2.2 Potřebné vstupní úkony

Po samotném nasazení SOC týmu na fakultě je třeba provést několik úkonů.

Průzkum infrastruktury – nejprve je potřeba provést „velký jarní úklid“. Jedná se o kompletní detailní průzkum celé infrastruktury spadající do gesce FP a následné provedení všech potřebných ochranných opatření. Konkrétně je potřeba:

1. Provést hloubkový sken na všech strojích. Nevyjímaje webových serverů, SQL serverů, DNS / DC strojů, laboratorních počítačů, počítačů v učebnách a všech zaměstnaneckých počítačů. Tento úkon lze většinou vynutit globálně skrze Group Policy. U strojů, kde to možné není (např. stroje běžící na Linuxech) doporučuji použít Malwarebytes uvedený níže viz 4.3. Důvodem je nutnost zbavit všechny fyzické i virtuální stroje jakýchkoliv případných botnet malwarů, webshellů, coinminerů i jakéhokoliv dalšího malwaru, který se za ty roky s největší pravděpodobností nakumuloval.

2. Aplikovat záplaty na všech systémech, kde neběží aktuální verze. Především stroj na adrese 147.229.123.50, na němž běží pět let starý Apache verze 2.4.25 (Debian). Kromě toho je třeba aktualizovat veškerý firmware na switchích v interní síti. Dále je nutné aktualizovat i verze všech kritických aplikací. Typickým příkladem je VMware nebo VirtualBox, na kterých s největší pravděpodobností běží web servery.

3. Zkontrolovat všechny stroje viditelné z internetu. Zjistit, zda jejich vystrčení ven má nějaký význam a poté co nejvíce minimalizovat jejich počet. Konkrétně se jedná o stroje uvedené v bodě 3.3.1. Současně je nutné zkontrolovat, proč mají

dva webové servery otevřen port SSH. Pokud neexistuje důležitá příčina, porty je nutné zavřít.

4. Zkontrolovat verze používaných protokolů v rámci infrastruktury. V případě systému ESIM na adrese 147.229.124.4 je naprosto nezbytné nastavit provoz skrze vrstvu TLS. Přihlašovací jména a hesla do systému v současné chvíli putují v otevřené podobě protokolem HTTP naprosto čitelné pro každého, kdo stojí v cestě.

5. Zkontrolovat konfiguraci firewallu Fortigate a aktualizovat ji k současným potřebám.

6. Zakázat příchozí i odchozí ICMP provoz v rámci celé sítě vyjma vybraných zařízení SOC týmu pro administrátorské potřeby.

7. Ustanovit komunikační kanál mezi CSIRT-VUT týmem a SOC-FP týmem. Nainstalovat do Gpg4win, vygenerovat dostatečně silné páry klíčů a předat jeho veřejnou část pracovníkům na CSIRT-VUT.

8. Převzít zodpovědnost za kybernetickou bezpečnost i za všechny ostatní informační aktiva provozované mimo IP rozsah přidělený VUT. Jako příklad mohu uvést fp-mba.cz provozovaný na webhostingu WEDOS na adrese 46.28.104.67.

9. Provést další potřebná bezpečnostní opatření, vyplývající z detailního průzkumu prostředí.

3.2.3 Hlavní agenda

Hlavní náplň práce nasazeného SOC týmu je shrnuta následující body:

1. **Incident handling** – hlavním těžištěm celé agendy SOC týmu bude incident handling / incident response, včetně všech jeho fází.

    a. **První fáze**

        i. **Analýza rizik –** v rámci přípravy je analýza rizik důležitou částí při vyhodnocování kritických aktiv a rizik na ně působící. Je potřeba ohodnotit pravděpodobnosti a dopady vzniku incidentu. Ačkoliv se na FP nevztahuje zákon o kybernetické bezpečnosti a tato povinnost tedy není zákonem uložena, jedná se o takzvané „best practices“ a doporučuji tuto analýzu provádět. Jednou při samotném zahájení činnosti SOC týmu a poté periodicky každý rok. Z kvalitně zpracované analýzy rizik vyplývají potřebné bezpečnostní opatření.

        ii. **Patch management –** aktualizace a záplatování **všech systémů, aplikací i aktivních prvků v síti** je nejefektivnější metoda v boji proti zranitelnostem. Patch management je periodický proces. Doporučuji jej provádět pravidelně minimálně každý měsíc a v případě opravy kritické zranitelnosti bezodkladně. Podotýkám, že aktualizovat je nutné naprosto všechny verze softwaru a firmwaru. Nejen kritická aktiva. Dokonce i tiskárna připojena v síti se může stát útočným vektorem kybernetického útoku, nebo přinejmenším součástí botnetu.

        iii. **Zálohování –** SOC tým by měl být zodpovědný za provádění záloh kritických informačních aktiv. Zálohování je nejúčinnější zbraní proti ransomwarovým útokům. Je tedy nutné provádět jak úplné zálohy, tak menší inkrementální (přírůstkové) nebo diferenciální (rozdílové) zálohy. Interval mezi zálohami se liší podle potřeby v rámci každého aktiva zvlášť.

iv. **Logování** – další důležitou aktivitou, uloženou fakultnímu SOC týmu, bude logování na všech důležitých aktivních prvcích a koncových bodech. Důležité jsou logy síťového provozu (netflow), server logy (i web server logy), windows security event logy, authentikační logy v Active Directory a další logy dle potřeby. K logování je možno užívat CLM řešení, nebo je všechny posílat do SIEM systému.

v. **Pentesting** – fakultní SOC tým bude zodpovědný za správné provádění penetračních testů. Ať už ve spolupráci s univerzitním CSIRT týmem, v rámci projektu Kyber22 nebo jinou outsourcovanou službou. Obnáší to organizační záležitosti, technickou přípravu na vykonání testů, dohled nad jejich samotným provedením a následné přijetí bezpečnostních opatření na základě výsledků penetračních testů.

b. **Druhá fáze**

i. **Detekce prekurzorů** – z obráncovy perspektivy je většinou velice obtížné, někdy takřka nemožné detekovat prekurzory možných bezpečnostních incidentů. Přesto je však naprosto nutné tuto aktivitu vyvíjet a zařadit ji do hlavní agendy SOC týmu. Jedná se o aktivitu, v jejímž jádru je převážně monitoring síťového provozu, kontrola access logů nebo threat hunt. Možnými prekurzory může být cokoliv. Detekovaný pokus o skenování portů vystrčených do internetu, zjištěný veřejný PoC zneužívající kritickou zranitelnost týkající se fakultních aktiv, nebo například obdržená výhružka od kyberzločineckých aktérů.

ii. **Detekce indikátorů** – indikátory kompromitace je na rozdíl od prekurzorů mnohem snazší detekovat. Mnohdy se může jednat o false-positive, ale je nezbytné se průběžně prodírat množstvím

alertů vygenerovaných systémem, hledat mezi nimi podezřelou aktivitu a případně upravovat pravidla spouštění alertů a tím tak přispívat k plynulejšímu workflow.

c. **Třetí fáze**

i. **Minimalizace dopadu** – v případě nastalého kybernetického incidentu je role SOC týmu jasná. Minimalizovat funkční dopad na organizaci, její aktiva, reputaci nebo funkci. Metody využívané v rámci této fáze se vždy liší v závislosti na charakteru samotného incidentu.

ii. **Prioritizace** – v případě dvou souběžných incidentů padá rozhodovací proces prioritizace na bedra SOC týmu. Je třeba stanovit prioritu na základě vyhodnocení funkčních dopadů.

iii. **Identifikace vektoru útoku** – tříčlenný tým sice nemá kapacity na provádění podrobných forenzních analýz, ovšem identifikace vektoru útoku je naprosto základním a naprosto stěžejním zjištěním v rámci incident handlingu. Proto bod zařazuji do agendy.

2. **Evidence** – kromě samotného procesu incident handlingu je SOC tým pověřen důkladnou evidencí všech řešených kybernetických bezpečnostních událostí a incidentů. Evidence musí obsahovat všechny data a detaily spojené s incidentem, nevyjímaje historii všech aplikovaných mitigačních postupů, nalezené vzorky malware v zazipované podobě pod heslem „Infected“ nebo všechny nalezené artefakty či zachycené signatury.

3. **Reporting** – další povinností nasazeného SOC týmu je pravidelný reporting vedení fakulty a univerzitnímu CSIRTu. Doporučuji měsíční interval a poté

celoroční shrnutí. Jedná-li se o důležitý a aktuální incident, forma reportingu je povýšena na ad-hoc úroveň a zprávy jsou předávány mimořádně. Pointou je podávání zpráv o aktivitách SOC týmu, týkajících se detekovaných událostí, či řešených incidentů. Současně informace o zprávě týkající se spolupráce s partnery nebo v rámci projektů a koordinačních skupin.

4. **Funkce styčného bodu** – SOC tým funguje jako hlavní POC pro komunikaci s fakultou ohledně věcí, týkajících se kybernetické bezpečnosti.

    a. **Zapojení se do komunit** – jako styčný bod je SOC tým pověřen aktivně komunikovat v rámci otevřené kyberbezpečnostní komunity, podílet se na projektu Kyber-22 (viz bod 2.3.7.) a přijímat i distribuovat veškerá IoCs. Současně bude fungovat jako kontaktní bod pro všechny poskytovatele služeb v oblasti kyberbezpečnosti pro fakultu. Např. Fortinet, WEDOS, apod.

    b. **Threat hunt** – provozování aktivity threat huntingu též spadá do agendy fakultního SOC. Tato činnost velice úzce souvisí s bodem 4.a., protože je třeba sledovat aktuální dění v komunitě a obecně v oblasti kyberbezpečnosti. Ovšem výstupy těchto aktivit drasticky podporují detekci prekurzorů a indikátorů v rámci druhé detekční fáze incident handlingu.

3.3 Doporučení nástrojů

Každý incident handler se v rámci své práce běžně setkává s desítkami různých nástrojů a služeb. V tabulce níže uvádím naprosto elementární, základní sadu nástrojů, kterou si zařadí fakultní SOC tým do svého repertoáru. V průběhu následujících let působení týmu na fakultě se bude sada využívaných nástrojů pochopitelně vyvíjet, rozšiřovat a upravovat.

Tabulka 5: Doporučení nástrojů

Skupina nástrojů	Nástroj	Popis	Odkaz	Distribuce	Poznámka
Reputační nástroje	Virus Total	Ověřování reputace hashů, IP adres, domén a dalších IoCs u desítek antivirových nástrojů současně. Možnost pivotovat kolem jednotlivých nálezů	virustotal.com	Zdarma pouze základní verze	Výrazně nedoporučuji uploadovat do databáze VirusTotal jakýkoliv soubor. Vždy jen jeho hash. Útočník by tak viděl aktivity obránců.
	';--have i been pwned?	Ověřování přítomnosti citlivých dat uživatelů ve velkých veřejných únicích dat na základě e-mailové adresy nebo telefonního čísla.	haveibeenpwned.com	Zdarma	
	AbuseIPDB	Veřejná databáze všech IP adres, jež byly komunitou označeny za škodlivé z různých důvodů.	abuseipdb.com	Zdarma	
WHOIS služby	CZ.NIC	Vyhledávání adres a domén v českém registru s nejvyšší doménou **.cz**	nic.cz/whois	Zdarma	Jen a pouze pro české adresy.
	RIPE.NET	WHOIS nástroj spravovaný evropskou organizací RIPE	ripe.net	Zdarma	
	Icann Lookup	WHOIS nástroj spravovaný americkou vládní organizací ICANN	lookup.icann.org	Zdarma	
	WHOIS lookup	WHOIS služby poskytované společností Domaintools, špičkovou organizací v oblasti cybersecurity.	whois.domaintools.com	Zdarma	
	BGPView	Známá WHOIS služba poskytovaná třetí stranou. Leaderem v oblasti CTI, Recorded Future.	bgpview.io	Zdarma	

Skenovací nástroje	Nessus	Velice komplexní řešení v oblasti pentestu a skenování.	tenable.com/products/nessus	Zdarma pouze základní verze	
	Shodan	Skenovací nástroj, který skenuje na základě výměny headerů mezi klientem a serverem.	shodan.io	Zdarma pouze základní verze	
	DNSdumpster	Skenovací nástroj, který mapuje z internetu dostupnou infrastrukturu pomocí DNS dotazů.	dnsdumpster.com	Zdarma	
	nmap	Invazivní skenovací nástroj, který mapuje infrastrukturu pomocí specielně vytvořených packetů.	nmap.org	Open source	Jde o invazivní sken. Není legální tímto nástrojem skenovat síť bez souhlasu jejího správce.
Detekce	Fortigate	IPS a IDS řešení	-	Placené	
	Snort	IPS a IDS řešení	snort.org	Open source	
	Suricata	IPS a IDS řešení	suricata.io	Open source	
	Zeek	IPS a IDS řešení	zeek.org	Open source	
	Malwarebytes	antivirus	malwarebytes.com	Zdarma	Specializace na hloubkové skeny.
	Splunk	IPS / IDS / SIEM / Analysis nástroj.	splunk.com	Zdarma pouze základní verze	Velice ohebný nástroj, jehož bližší specializace závisí na datech, kterými je krmen.
Phishingové nástroje	urlscan.io	Skenovací nástroj využívající HTTP requesty a threat intel feed.	urlscan.io	Zdarma	
	wannabrowser	Nástroj umožňující přístup na URL z jiného stroje / prohlížeče.	wannabrowser.net	Zdarma	
	URL2PNG	Nástroj umožňující bezpečně prohlédnout škodlivou stránku bez přistupování k ní.	url2png.com	Zdarma	

	PhishTank	Nástroj na bázi komunitní spolupráce pro ověřování a sundávání phishingových stránek.	phishtank.org	Zdarma	
	PhishTool	Nástroj pro analýzu phishingových útoků.	phishtool.com	Zdarma pouze základní verze	
Analytické nástroje	Hybrid analysis	Online analytický nástroj malwaru.	hybrid-analysis.com	Zdarma	
	Cuckoo sandbox	Analytický sandbox pro pasivní analýzu malware	cuckoosandbox.org	Open source	
	Wireshark	Nástroj pro záchyt a analýzu všech příchozích a odchozách packetů.	wireshark.org	Open source	Doporučuji spustit full packet capture v případě jakékoli podezřelé události.
Ransomware	id-ransomware	Nástroj k rozpoznání konkrétního ransomwaru a aktéra podle ransomnote nebo podle zašifrovaného souboru.	id-ransomware.malwarehunterteam.com	Zdarma	"Vědění je půl vítězství"
	nomoreransom	Iniciativa bojující proti ransomware pomocí sběru dešifrovacích nástrojů od profesionálních malware analytiků.	nomoreransom.org	Zdarma	
	TOR Browser	Prohlížeč využívající TOR síť. Nutné pro přístup na darknet.	torproject.org/download	Zdarma	Nutné používat v kombinaci s VPN připojením! Doporučuji využívat linuxový OS Tails, který má TOR provoz vynucený systémem a obsahuje další zabezpečující mechaniky. Užitečný nástroj např. pro kontrolu tzv. **leak sites**.
Threat hunt (OSINT)	twitter	Sociální síť, současně nejaktivnější platforma pro sdílení threat intelu do veřejnosti.	twitter.com	Zdarma	Je potřeba sledovat desítky kvalitních zdrojů threat intelu.

	The Hacker News	Kvalitní odborný zpravodajský portál v oblasti kyberbezpečnosti.	thehackernews.com	Zdarma	
	Bleeping Computer	Kvalitní odborný zpravodajský portál v oblasti kyberbezpečnosti.	bleepingcomputer.com	Zdarma	
Další podpůrné nástroje	Gpg4win	Nástroj pro PGP šifrování e-mailů a souborů.	gpg4win.org	Open source	Pro lepší pohodlí je možno využívat v kombinaci s PGP addony do Outlooku / Mozilly Thunderbird.
	VMware	Virtualizační nástroj	Wmvare.com/products/Workstation-player.html	Zdarma	Spolu s Kali OS nutný nástroj pro sandboxing.
	MITRE ATT&CK	Matice popisovaná v teoretické části v bodě 2.6.1.	attack.mitre.org	Zdarma	
	CyberChef	Nástroj pro kódování a dekódování.	gchq.github.io/cyberchef	Open source	
	abuse.ch	Služby pod neziskovou organizací abuse.ch jsou: Malware bazaar, Feodo tracker, SSL blacklist, URL Haus, a Threat FOX. Poskytujou	abuse.ch	Zdarma	
	GitLab	Verzovací repozitář pro spravování ukládání a spravování vlastních scriptů a vlastní silou vyvinutých nástrojů.	gitlab.com	Zdarma	Lze použít i jako platforma pro evidenci a archivaci incidentů.

V kategorii detekce jsem uvedl nástroje Snort, Suricata a Zeek. Jedná se o přední IDS a IPS systémy. Ovšem preference jednoho z nich je čistě subjektivní a nechávám ji na administrátorech. Jejich použití však záleží na úrovni používání hardwarového řešení Fortigate, které z mé pozice není možné zjistit. Je tedy zbytečné, aby se jejich služby překrývaly.

Současně uvádím mnohé nástroje, vhodné pro řešení phishingových útoků, přestože jsem zmiňoval, že kontrola SMTP provozu nespadá do gesce FP. Zabezpečení koncových stanic ovšem ano. Také je třeba mít na paměti, že e-mail je pouze jedna z mnoha forem distribuování phishingového útoku. Každý incident handling tým by se měl aktivně podílet na sundávání závadných stránek a přispívání k bezpečnosti celého kyberprostoru.

3.4 Procesní nastavení

Úroveň SOC týmu z největší části závisí na kvalitě pracovníků. Nedostatek odborné pracovní síly sužuje obor kyberbezpečnosti už dělší dobu a jeden ze způsobů jak vytěžit nejvíc z toho, co je k dispozici, je nastavit si správně interní procesy.

Nejčastějším modelem, využívaným v bezpečnostních týmech, je rozdělení incident handlerů na tři stupně. Navrhuji tento model zavést ve zmenšené verzi o dvou stupních i zde:

Tier 1 – na první úrovni incident handlingu je nutno provádět triáž. Tedy rutinní třídící práci. Vyhodnocovat množství alertů které nám prezentuje IPS a SIEM a vytřídit z nich false-positives, provádět threat hunt, obstarávat pravidelnou komunikaci s partnery nebo kontrolovat IoCs. Zde je třeba obsadit jednoho až dva juniorní pracovníky.

Tier 2 – práce vhodná pro vedoucí pozici. Seniornějšího, zkušenějšího pracovníka. V rámci tier 2 se řeší samotná třetí fáze incident handlingu a druhá fáze je zde řešena více do hloubky. Na této úrovni se též vyvíjí snaha o automatizaci, nastavování

systémů, jejich deployment nebo propojování. V rámci fakultního SOC by na tier 2 byl jeden pracovník.

Tento model též do jisté míry předchází takzvanému syndromu vyhoření, ke kterému v oblasti incident handlingu běžně dochází velice brzy.

3.4.1 Vzdělávání

Navrhuji také zavést zaměstnancům studijní plán. Oblast kybernetické bezpečnosti se rozvíjí extrémně rychle a je třeba s tímto trendem držet krok. Pro začátek navrhuji absolvování základního kurzu **CompTIA Cybersecurity Analyst (CySA+)**. Tento pětidenní kurz je určený pro členy SOC týmu. Tedy je hlavně pro administrátory a správce sítí a bezpečnostní adminy. Více detailů je dostupných na adrese:

https://www.gopas.cz/comptia-cybersecurity-analyst-(cysa)_ctca

3.5 Finanční zhodnocení

3.5.1 Odhad

Personál – Nejdražší položku v rámci nasazení SOC týmu je personál samotný. Odborníků v oblasti kybernetické bezpečnosti je dlouhodobě nedostatek a neočekává se, že by se to v následujících letech razantně změnilo. Veřejný sektor je tímto nedostatkem zasažen nejvíce, protože je výrazně přeplácen firmami v soukromém sektoru a nemá moc nástrojů, jak jim konkurovat na trhu práce, je-li řeč o odbornících v oblasti kyberbezpečnosti. Navrhuji tedy s ohledem na možnosti fakulty platové ohodnocení kolem **32 000 Kč**. Jedná se zhruba o polovinu platu běžného v soukromém sektoru. Tato částka by byla závislá na zkušenostech a na praxi pracovníka. Dále navrhuji:

- Zaměřit se z počátku na nábor absolventů fakulty informačních technologií, po vzoru CSIRT-MU. Tedy v našem případě inženýrů a doktorů z VUT FIT.
- Nabídnout sestavení individuálního vzdělávacího plánu
- Další možné benefity

HW – Další neodmyslitelnou položkou jsou náklady na hardware. Jedná se však o počáteční jednorázovou investici. Náklady na 3 služební počítače, jejich periferie, projektor, externí disky a USB disky, 2FA tokeny a případně další potřebná zařízení odhaduji na **180 000 Kč.** Tedy **60 000 Kč** na jednoho zaměstnance.

SW – V tabulce doporučených nástrojů jsem vybíral převážně open-source nástroje a nástroje zdarma dostupné. Nepochybně však po uplynutí pár měsíců po vzniku týmu vykrystalizují požadavky na potřebné placené licence některých nástrojů, bez kterých se provoz incident handling týmu neobejde. Proto v ekonomickém zhodnocení zohledňuji i obnos na SW licence. Doporučuji stanovení tohoto rozpočtu na ve výši **150 000 Kč** ročně.

Vzdělávání – Jednotlivá školení, kurzy a přednášky, jako nezbytná část vzdělávání zaměstnanců, se od sebe cenově velice liší. Běžnou praxí je v případě juniorních pracovníků začínat na zdarma dostupných kurzech. Nejznámějšími jsou: **Try Hack Me**, **Over the Wire** nebo **Security Blue Teams**. Po absolvování mnohých kurzů v těchto nabídek je vhodné zakupovat levné placené kurzy od stejných poskytovatelů, které se pohybují většinou pod 20 000 korun. Středně drahé kurzy i se světově uznávanými certifikacemi se pohybují většinou pod 70 000 (např. silně doporučený kurz od CompTIA v bodě 3.4.1.) a v případě růstu seniorních zkušených pracovníků je vhodný kurz **SANS 504: Hacker Tools, techniques, and Incident Handling**, pohybující se zatím ještě pod 200 000 korun.

Tento benefit se však dá zneužívat. Nutným procesem k zavedení se proto stává takzvaný úpis. Aby se předešlo zneužívání finanční rezervy na absolvování školení a certifikací před plánovaným odchodem zaměstnance, zavádí se v rámci kolektivní smlouvy s pracovníky nutnost závazku výkonu práce po určitou dobu po absolvování školení. V případě odchodu zaměstnance před vypršením daného úpisu je zaměstnanec povinen doplatit cenu kurzu. Nárok na jednotlivé úrovně by současně vznikal počtem let. Doporučuji nastavit následující rozsahy:

Tabulka 6: Návrh systému na úpis

Počet let v zaměstnání / úroveň kurzu	Cena od	Částka do	Délka trvání úpisu zaměstnance [roky]
1	0	29 999	0
2	30 000	69 999	0,5
3	70 000	149 999	1
4	150 000	200 000	2

Z tabulky vyplývá, že například novému juniornímu zaměstnanci vznikne až po čtyřech letech nárok na nejvyšší kurz po maximální cenu 200 000, kterým se ale současně upíše na další dva roky v zaměstnání.

3.5.2 Sumarizace

Celkové roční náklady na provoz SOC týmu se odvíjí podle toho, kolik se podaří zaměstnat pracovníků a jaké školení absolvují.

Tabulka 7: Shrnutí nákladů

	Zaměstnanci	HW	SW	Vzdělání
Vstupní náklady	0	60000 * p	0	0
Pravidelné roční náklady	384 000 * p	0	150 000	Max 200 000 * p

Kde **p** znamená počet zaměstnanců. Při použití navrhovaných limitů a v případě úspěšného náboru dvou pracovníků by první rok dosahovaly náklady maximálně výše **1 097 998 Kč**.

3.5.3 ROSI

Pro zasazení částky do kontextu za účelem vytvoření přehledu pro manažerské rozhodování se využívá model ROSI neboli Return on Security Investment. Tento model je postaven na bázi ROI, ovšem s tím rozdílem, že bezpečnostní opatření negenerují žádný zisk. Pouze předchází ztrátám. Základní vzorec pro výpočet ROSI je:

$$ROSI = \frac{\text{Redukce finanční ztráty} - \text{Cena řešení}}{Cena\ řešení}$$

Zohledníme-li, že průměrné výkupné požadované po středně velkých organizacích po kompletním zasažením ransomware útokem činí 4 BTC, tedy zhruba 3 360 000 korun a připočteme-li další odhadované ztráty (ztráta produktivity zaměstnanců, ztráta reputace organizace, únik citlivých dat atd.) Můžeme se dostat až na odhadovanou částku **5 milionů korun**.

$$= \frac{5\,000\,000 - 1\,000\,000}{1\,000\,000} = 4$$

Výsledkem je hodnota vysoce převyšující hranici rovnu jedné. Výsledek potvrzuje potřebu investice do fakultního SOC týmu. Kromě přímých dopadů na fakultu existují i jiné faktory, vyplývající z analytické části této práce. Eliminace možnosti, že fakultní servery mohou být používány jako C&C servery kyberzločinců, že mohou distribuovat malware skrze nahraný webshell, nebo že můžou posílat bruteforce útoky na cizí aktiva atd. výrazně přispěje k celkové bezpečnosti českého kyberprostoru.

3.5.4 Ohodnocení návrhu

Vypracování analýzy a návrhu v této práci trvalo v součtu 70 hodin. Hodinu času stráveného vypracováním návrhu si cením na 250 korun. Tedy celkové ohodnocení návrhu je **15000 Kč.**

ZÁVĚR

Práce byla věnována návrhu řešení kybernetické bezpečnosti ve vybrané organizaci – Fakultě podnikatelské. V teoretické části bylo k danému tématu představeno mnoho funkčních modelů bezpečnostních týmů, důležitost jejich existence a jejich vzájemné kooperace. Byly také stručně představeny nástroje, postupy a metodiky, které tyto týmy využívají a základný typy hrozeb, jejichž mitigace je hlavním předmětem práce všech týmů v rámci kyberbezpečnostní komunity.

Na teoretický základ navázala analýza současného stavu řešení kybernetické bezpečnosti na fakultě. Nejprve z hlediska organizačního, poté z hlediska technického. V analýze byla odhalena řada nedostatků a přímo vedla k řešení, které bylo představeno v části následující.

V poslední části byl vypracován návrh na zřízení menšího fakultního SOC týmu. Stanovení agendy týmu, doporučené nástroje a další části této kapitoly byly navrženy na základě vlastních zkušeností získaných při práci v národním CERT, především s ohledem na velikost nasazovaného SOC týmu, jeho roli v rámci VUT a jeho konstituenci.

Jednotlivé části diplomové práce by měly dohromady poskytnout čtenáři ucelený vhled do problematiky kybernetické bezpečnosti a poskytnout představu o šíři této oblasti a o důležitosti se jí na dostatečné úrovni věnovat jak ve velkých, tak i menších organizačních celcích. Tím byly cíle práce splněny.

SEZNAM POUŽITÉ LITERATURY

[1] SECURITY BLUE TEAM. Blue Team Level 1. [kurz] Dostupné z: https://securityblue.team/why-btl1/

[2] MOYLE, E. CERT vs CSIRT vs. SOC: What's the difference? [online] Dostupné z: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

[3] ENISA. About ENISA – The European Union Agency for Cybersecurity [online] Dostupné z: https://www.enisa.europa.eu/about-enisa

[4] CISA. About CISA [online] Dostupné z: https://www.cisa.gov/about-cisa

[5] ENISA. CSIRTs Network. [online] Dostupné z: https://csirtsnetwork.eu/

[6] ENISA. CERT community: Recognition mechanisms and schemes [online] 2013 ISBN 978-92-9204-083-3. Dostupné z: https://www.enisa.europa.eu/publications/cert-community-recognition-mechanisms-and-schemes.

[7] GÉANT. Services for Security and Incident Response Teams. [online] Dostupné z: https://www.trusted-introducer.org/

[8] FIRST. FIRST is the global Forum of Incident Response and Security Teams. [online] Dostupné z: https://www.first.org/

[9] ENISA. Information Sharing and Analysis Centres (ISACs) Cooperative models. [online] 2018 ISBN: 978-92-9204-239-4 Dostupné z: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

[10] CESNET. Hospital SOC – hSOC. [online] Dostupné z: https://hsoc.cesnet.cz/

[11] MASARYKOVA UNIVERZITA. Projekt CRP-Kyber22 podpořen! [online] 2022 Dostupné z: https://www.crp-kyber.cz/clanky/projekt-crp-kyber22-podporen

[12] PLESNIK, Tomáš. RE: Dotaz na CRP-Kyber22 [e-mailová komunikace] 20.4.2022 10:40

[13] FIRST. TRAFFIC LIGHT PROTOCOL (TLP) [online] Dostupné z: https://www.first.org/tlp/

[14] FORTINET. What is a DMZ Network? [online] Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

[15] NIST. Computer Security Incident Handling Guice [online] Special Publication 800-61 revize druhá. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[16] MISP. MISP Communities and MISP feeds. [online] Dostupné z: https://www.misp-project.org/communities/

[17] TECHDIFFERENCES. Difference Between PGP and S/MIME. [online] Dostupné z: https://techdifferences.com/difference-between-pgp-and-s-mime.html

[18] RECORDED FUTURE. What Is Threat Intelligence? [online] Dostupné z: https://www.recordedfuture.com/threat-intelligence/

[19] NÚKIB. Upozornění na výskyt nového destruktivního malware typu wiper [online] 2022 Dostupné z: https://nukib.cz/cs/infoservis/hrozby/1813-upozorneni-na-vyskyt-noveho-destruktivniho-malware-typu-wiper/

[20] SCHMITZ, P. a LUBER S. Was ist eine DMZ (Demilitarized Zone)? [online] 2018 Dostupné z: https://www.security-insider.de/was-ist-eine-dmz-demilitarized-zone-a-677267/

[21] MITRE. About the D3FEND Knowledge Graph Project. [online] Dostupné z: https://d3fend.mitre.org/about

[22] CARREON, Cris. Applying Threat Intelligence to the Diamond Model of Intrusion Analysis. [online] 2018 Dostupné z: https://www.recordedfuture.com/diamond-model-intrusion-analysis/

[23] LOCKHEED MARTIN. The Cyber Kill Chain ®. [online] Dostupné z: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[24] MITRE. ATT&CK®. [online] Dostupné z: https://attack.mitre.org/

[25] BAKER, Kurt. What is Cyber Threat Intelligence? [online] 2022 Dostupné z: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

[26] CLOUDFLARE. What is a DDoS attack? [online] Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[27] KASPERSKY. What is a Zero-day Attack? – Definition and Explanation. [online] Dostupné z: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH