Scénář řešení kybernetického bezpečnostního incidentu

Bc. Michaela Dubská

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michaela Dubská**
Osobní číslo:	**L19395**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Rizikové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Scénář řešení kybernetického bezpečnostního incidentu**

Zásady pro vypracování

1. Zpracujte literární rešerši vztahující se k dané problematice s důrazem na monografie.
2. Charakterizujte jednotlivé typy kybernetických bezpečnostních incidentů.
3. Vytvořte scénář vybraného kybernetického bezpečnostního incidentu.
4. Implementujte vytvořený scénář do vybraného výcvikového či výukového simulátoru.

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

Seznam doporučené literatury:

1. AWAD, Ali Ismail a Machael FAIRHUST. *Information security : foundations, technologies and applications*. Institution of Engineering & Technology, 2018. ISBN 9781849199742.
2. JOHNSON, Thomas A. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Taylor and Francis, 2015. ISBN 9781482239225.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

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

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 7. 5. 2021

Jméno a příjmení studenta: Bc. Michaela Dubská

…….
podpis studenta

ABSTRAKT

Scénář řešení kybernetického bezpečnostního incidentu je problematika, které se věnuje diplomová práce. Teoretická část vymezuje základní pojmy, právní předpisy, organizace a instituce, které se zabývají kybernetickými bezpečnostními incidenty. Dočteme se zde také, jaké jsou druhy kybernetických bezpečnostních incidentů, jak se rozdělují do jednotlivých kategorií, jaký je rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickou bezpečnostní událostí. V praktické části je na úvod popsán program PractisGo a vymezení základních pojmů. PractisGo je softwarový program, který umožňuje tvorbu scénáře, určení rolí a následné provedení cvičení. Následuje popis postupu vytvoření scénáře, vymezení vlastního scénáře a provedení cvičení. Výstupem práce je vyhodnocení kybernetického zabezpečení a navržení možných opatření, která povedou ke zlepšení zabezpečení a budou předcházet možnosti případného vzniku kybernetického bezpečnostního incidentu.

Klíčová slova: cvičení, kybernetický bezpečnostní incident, scénář, PractisGo, zabezpečení.

ABSTRACT

Cybersecurity Incident Response Scenario is an issue that is addressed in the thesis. The theoretical part defines the basic concepts, legislation, organizations and institutions that deal with cyber security incidents. We will also read here what are the types of cyber security incidents, how they are divided into individual categories and what is the difference between a cyber security incident and a cyber security event. The practical part introduces the PractisGo program and the definition of basic concepts. PractisGo is a software program that allows you to create scenarios, determine roles and then perform exercises. The following is a description of how to create a scenario, define your own scenario, and perform the exercise. The output of the work is the evaluation of cyber security and the proposal of possible measures that will lead to improved security and will prevent the possibility of a potential cyber security incident.

Keywords: Cyber Security Incident, Exercise, Scenario, Security, PractisGo.

Ráda bych poděkovala svému vedoucímu práce Ing. Petr Svoboda Ph.D za cenné rady, připomínky, jeho ochotu a věnovaný čas. Mgr. Monice Vašíčkové za pomoc při překladu do anglického jazyka a Mgr. Janě Tažejové za jazykovou korekturu

Velké dík patří také mé rodině, která mi umožnila studovat, také přátelům a známým, kteří mi byli po celou dobu studia velkou oporou.

"Je jenom jedna cesta za štěstím a to přestat se trápit nad tím, co je mimo naši moc."

Epiktétos

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

OBSAH

ÚVOD

Kybernetická bezpečnost začíná v poslední době být velmi často slýchané a populární téma. Jedná se o bezpečnost, která je spojená se zajištěním bezproblémového fungování informačních technologií, které nás v současné moderní době provází našim každodenním životem, ať už doma nebo na pracovišti. Správné zajištění kybernetické bezpečnosti nebo se jenom bezpečně chovat při používání informačních technologií, není v dnešní době plné nástrah vůbec jednoduché. Stačí se jenom zamyslet nad tím, jaké internetové stránky navštěvujeme, jak dobře máme zabezpečený svůj vlastní počítač, tablet nebo jiné zařízení, které využíváme. Zabezpečení je velmi široký okruh, který začíná už i tím, když na svém zařízení máme heslo, které nikdo nezná a chrání před neoprávněným přístupem do našeho zařízení. Dále můžeme mezi zabezpečení zařadit využívání ochranného softwaru, který nás bude včas, pokud se budeme chystat navštívit nějaké podezřelé internetové stránky informovat, i když nám budou připadat úplně v pořádku. Konkrétně kybernetická bezpečnost je poměrně novým oborem, ale velmi často slýchaným.

V nedávné době jsme měli všichni možnost v médiích zaslechnout kauzu kybernetického útoku na nemocnici v Benešově. Dalším velmi známým útokem byl kybernetický útok na nemocnici v Brně. Tyhle dva případy kybernetického útoku patří mezi lidmi k těm známějším, díky jejich zveřejnění v médiích. Určitě si ale nesmíme myslet, že to byly jediné kybernetické útoky, které se kdy staly. V České republice a ne jenom u nás si troufám říct, že každý den proběhne minimálně jeden pokus o kybernetický útok. Ne vždy je pokus úspěšný a útočníkovi se útok podaří.

V současné době, kdy počítače a veškeré IT vybavení je součástí našeho každodenního života si troufám tvrdit, že každý z nás by měl mít alespoň základní povědomí o tom co to je kybernetický útok, jaké jsou možnosti jeho působení. Taky se nesmí opomenout na předcházení možnosti vzniku, což je prevence. Prevence je jedním z důležitých faktorů, které se nesmí podceňovat.

Důvod, proč jsem si vybrala tohle téma diplomové práce spočívá v tom, že kybernetická bezpečnost je velmi aktuální téma. Dalším důvodem bylo zjištění nových informací a rozšíření si vědomostí s možností vyzkoušet si a zjistit jak kybernetický bezpečnostní incident může fungovat a co všechno je potřebné provést pro jeho správné identifikování, správné a včasné reakce a celkový postup úkolů, které zajistí co nejmenší ztráty pro organizaci.

CÍL A POUŽITÉ METODY

Tato kapitola obsahuje vymezení cíle diplomové práce a popis odborných metod, které byly použity při zpracování diplomové práce

Cíle diplomové práce

Hlavním cílem diplomové práce je vytvořit scénář cvičení pro zvýšení kybernetické bezpečnosti vybraného subjektu. Hlavní cíl je naplněn za pomoci dílčích cílů. Prvním z dílčích cílů práce je seznámení se se současnými hrozbami v kyberprostoru. Další dílčí cíl je identifikace problematiky vhodné pro nácvik za účelem zvýšení kybernetické bezpečnosti osob. Třetím dílčím cílem je pak vlastní návrh a modelování scénáře cvičení vybraného kybernetického incidentu a souvisejících reaktivních opatření. Posledním dílčím cílem je implementace scénáře do vybraného softwarového simulátoru.

Metody použité při zpracování diplomové práce

V diplomové práci je využito mnoho odborných metod. Jednou z nich je literární rešerše. Jejím cílem bylo sesbírat co nejvíce dostupných informací a seznámit se s veškerými odbornými pojmy z oblasti kybernetické bezpečnosti. Dále jsou uvedeny a popsány některé další metody využité při zpracování:

- Analogie – srovnání. Jedná se o metodu, která srovnává dříve získané informace s nově získanými informacemi.
- Analýza – proces myšlenkového rozčlenění celku na části.
- Deskripce – slouží k uspořádání sesbíraných informací a jejich utřídění dle svých potřeb.
- Dotazníkové šetření včetně vyhodnocení dat – slouží k sesbírání informací pro možnost dalšího využití.
- Komparace názorů a hypotéz – slouží k vytváření či zdůvodnění vlastního názoru. Při provádění komparace názorů a hypotéz dochází k porovnávání názorů různých autorů.
- Syntéza – myšlenkové spojení získaných poznatků. Slouží k vzájemnému pochopení souvislostí.

Využila jsem také možnost vzdáleného přístupu k učebně IT na Fakultě logistiky a krizového řízení v Uherském Hradišti, kde jsem implementovala scénář řešení kybernetického bezpečnostního incidentu do programu PractisGo.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

Kybernetická bezpečnost je oblast velmi široká, neustále se rozvíjející a aktuální. Poslední dobou se o ní čím dál více doslechneme v televizi ať už to se jedná o vznik kybernetického útoku nebo souvisí se zavedením nové strategie proti vzniku kybernetického útoku. Kybernetickou bezpečností se v České republice zabývá několik institucí a některé z nich jsou vymezeny v některých zákonech z dané problematiky.

1.1 Právní předpisy

Výchozím dokumentem zajišťujícím kybernetickou bezpečnost v Česku je Národní strategie kybernetické bezpečnosti České republiky pro roky 2021 — 2025. Další klíčový dokument se nazývá je Koncepce rozvoje národního úřadu pro kybernetickou a informační bezpečnost 2020.

Národní strategie kybernetické bezpečnosti určuje strategické cíle, kterých chce v období od roku 2021 do roku 2025 v oblasti kybernetické bezpečnosti dosáhnout. Hlavní vizí je vybudovat v České republice odolnou společnost a infrastrukturu, v kybernetickém prostoru vystupovat sebevědomě a aktivně dokázat čelit různému spektru kybernetických hrozeb za pomoci spolehlivých spojenectví. (Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025, 2020)

Dalšími právními předpisy, které upravují kybernetickou bezpečnost v České republice je zákon č. 181/2014Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon vstoupil v platnost 1. ledna 2015. Zákon vymezuje práva a povinnosti, působnost a pravomoc orgánů veřejné moci a osob v oblasti kybernetické bezpečnosti. Vymezená práva a povinnosti se netýkají informačních a komunikačních systémů, které pracují s utajovanými informacemi. (Česko, 2014) (Smejkal, Sokol a Kodl, 2019)

Hlavním cílem zákona o kybernetické bezpečnosti je:

- Zlepšit detekci kybernetických bezpečnostních incidentů.
- Upravit činnost dohledových pracovišť.
- Zavést systém opatření k reakci na kybernetické bezpečnostní incidenty.
- Stanovit základní úroveň bezpečnostních opatření.
- Zavést hlášení kybernetických bezpečnostních incidentů. (Legislativa KB, b.r.)

Oblasti kybernetické bezpečnosti se také věnuje:

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS).
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti.

Vyhláška č. 317/2014 Sb., zahrnuje významné informační systémy a kritéria pro jejich určení.

Vyhláška č. 437/2017 Sb., zpracovává požadavky směrnice Evropské unie. Upravuje kritéria po určení základní služby a vymezení dopadu narušení služby na zabezpečení činností podle zákona o kybernetické bezpečnosti.

Vyhláška č. 82/2018 Sb., seznamuje s příslušnými předpisy Evropské unie a dohlíží na zajištění bezpečnosti sítí elektronických komunikací a informačních systémů. (Smejkal, Sokol a Kodl, 2019) (Česko, 2014) (Česko, 2017) (Česko, 2018)

1.2 Mezinárodní normy

International Organization for Standardization (ISO) norma ČSN ISO 27000 je skupina norem v oblasti informační bezpečnosti. 27000 určuje pojmy a obsahuje terminologických slovník pro všechny ostatní normy 27000:

- Norma 27000 – přehled a slovník.
- Norma 27001 – požadavky.
- Norma 27002 – soubor postupů.
- Norma 27003 – návod k implementaci.
- Norma 27004 – měření.
- Norma 27005 – řízení rizik.

- Norma 27007 – návod k provádění auditů.
- Norma 27011 – řízení bezpečnosti v telekomunikačních organizacích.
- Norma 27799 – řízení bezpečnosti ve zdravotnictví. (Hrůza, 2012) (Smejkal, Sokol a Kodl, 2019) (Bezpečnostní normy, 2020) (Standardy a definice pojmů bezpečnosti informací, 2011)

ČSN ISO 27000

Mezinárodní norma zajišťující přehled o systému řízení bezpečnosti informací, které tvoří skupinu norem systému řízení bezpečnosti informací (ISMS) a vymezuje související termíny. Termíny a definice uvedené v normě se zabývají termíny běžně používanými v normách ISMS. Skupina norem má pomoci organizacím všech typů a velikostí se zavedením a provozováním systému ISMS.

Organizace mohou využitím norem ISMS vyvinout a zavést rámec pro řízení bezpečnosti svých bezpečnostních aktiv a vytvořit si tak nezávislé ohodnocení svých ISMS týkajících se ochrany informací, např. o zaměstnancích, ale také informace které jim poskytli zákazníci nebo třetí strana.

Skupina norem ISMS obsahuje normy, které definují požadavky na ISMS, normy, které certifikují požadavky, normy poskytující přímou podporu, podrobné pokyny nebo uplatnění pro všechny procesy. (ČSN ISO/IEC 27000, 2021)

ČSN ISO 27001

Norma obsahuje doporučení jak zavést do praxe opatření v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací v organizaci. Norma uplatňuje zavedení procesu k řešení ISMS, využitím modelu PDCA (plánuj-dělej-kontroluj-jednej), který je možné využít pro všechny procesy ISMS tak, jak jsou vymezeny normou. Norma je propojena s normami ISO 90001 pro systémy řízení jakosti a ISO 14001 pro systém řízení ochrany životního prostředí.

Hlavní část normy vymezuje požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde přesně definovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva. (ČSN ISO/IEC 27001, 2021)

Proces řízení bezpečnosti informací

V procesu řízení bezpečnosti informací se nejčastěji využívá Demingův cyklus PDCA.

Demingův cyklus PDCA

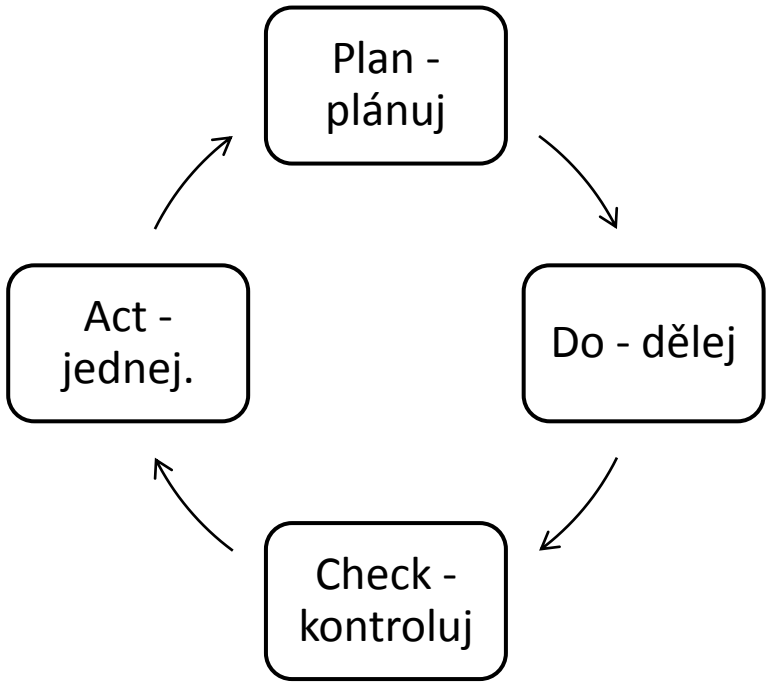
Demingův cyklus PDCA je základní vzor pro tvorbu zákona o kybernetické bezpečnosti, který definuje záměry a cíle, organizační, dokumentační a řídící struktury a procesní ucelení.(Legislativa, 2020)

Plánuj - první část, která popisuje procesy, situace a postup sestavení plánu, který povede ke zlepšení situace.

Dělej - uplatnění/zavedení první části.

Kontroluj - vyhodnocení a kontrola zavedených změn. Zhodnocení jestli změny vedly k úspěchu nebo ne. V případě, že nedojde ke zlepšení je potřeba se vrátit k předchozím dvěma bodům a vymyslet jiná opatření.

Jednej - poslední část procesu, kdy dojde k zavedení opatření a změn do praxe. Po čase dojde k vyhodnocení výsledků a pokračujeme k dalšímu kroku Plan a plánujeme další opatření, která povedou ke zlepšení. (Mlýnek, 2007)



Obrázek 1 - Cyklus PDCA *[Zdroj: vlastní]*

Proces řízení bezpečnosti informací vycházející z modelu PDCA

Plan – příprava a implementace

- Zavedení schématu a pravidla řízení bezpečnostních incidentů.
- Vybudování infrastruktury (procesy - lidé - nástroje).
- Informování manažerů, zaměstnanců a uživatelů.

Do – provoz a monitoringu

- Detekce, sběr informací pro došetření, pravidelné reportování.
- Reakce na incidenty a náprava případných škod.

Check – kontrola přínosů a výstupů

- Vyhodnocení a ponaučení z incidentů.
- Identifikování možností pro vylepšování preventivních opatření.

Act – trvalé zlepšování bezpečnosti

- Promítnutí výsledků do celkového managementu bezpečnosti.
- Vyšší objektivita podkladů pro analýzu a zvládání rizik, optimalizace schématu řízení incidentů.(Bezpečnost standardně a trochu praxe, b.r.)

1.3 Organizace a instituce zabývající se kybernetickou bezpečností v ČR

Kybernetickou bezpečnost zajišťuje mnoho organizací a institucí. Jednou z nejdůležitějších institucí je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který zastřešuje vládní bezpečnostní tým Vládní CERT (Computer Emergency Response Team) České republiky a spolupracuje s CERT a CSIRT týmy.

1.3.1 Národní úřad pro kybernetickou a informační bezpečnost

Ústředním správním orgánem zajišťujícím kybernetickou bezpečnost, ochranu utajovaných informací v oblasti informačních a komunikačních systémů je v České republice Národní úřad pro kybernetickou a informační bezpečnost. Úřad vznikl na základě zákona o kybernetické bezpečnosti dne 1. 8. 2017. NÚKIB je správním úřadem pro kybernetickou bezpečnost, kryptografickou ochranu, ochranu utajovaných informací pro oblasti informačních a komunikačních systémů a problematiku veřejně regulované služby navigačního systému Galileo. Součástí NÚKIB je Národní centrum kybernetické bezpečnosti. (Smejkal, Sokol a Kodl, 2019) (NÚKIB, b.r.)

1.3.2 CERT – Computer Emergency Response Team

Computer Emergency Response Team = Tým pro nouzové reakce na počítači. CERT týmy zajišťují dodržování povinností dle zákona. Dělí se na pracoviště vládního CERTu a pracoviště národního CERTu. Rozdíl mezi vládním a národním CERTem je v tom kdo ho provozuje. Vládní CERT provozuje úřad jako součást Národního centra kybernetické bezpečnosti a národní CERT provozuje právnická osoba, která bude oprávněna k provozování činnosti na základě uzavřené smlouvy s úřadem.(NCKB, b.r.)(Smejkal, Sokol a Kodl, 2019)

Národní CERT

Národní CERT nemá podle zákona žádnou pravomoc, ale funguje jako metodická podpora, pro subjekty, které projeví zájem o pomoc při zajištění kolektivní ochrany před kybernetickým bezpečnostním incidentem.

Vládní CERT

Vládní CERT je součástí úřadu a podle zákona má pravomoc nařizovat a udělovat sankce. Zajišťuje působení státní moci v oblasti kybernetické bezpečnosti. (Hromada et al., 2015)

1.3.3 CSIRT – Computer Security Incident Response Team

Computer Securrity Incident Response Team = Tým reakce na incidenty v oblasti počítačové bezpečnosti. CSIRT je tým plně zodpovědný za řešení bezpečnostních incidentů. Hlavním úkolem CSIRT týmu je včasná a účinná, pokud možno úspěšná reakce na hrozbu a odborná spolupráce při řešení incidentu. CSIRT týmy se dělí na národní a vládní.(Kolouch a Bašta, 2019)(O týmu CSIRT.CZ, b.r.)

Národní CSIRT

Od roku 2010 je provozován sdružením CZ. NIC podle veřejnoprávní smlouvy a Zákona o kybernetické bezpečnosti. Spolupracuje s ostatními CSIRTy, ale jeho role v celém systému je odlišná. Hlavním cílem je zajistit kontakt mezi napadeným a týmem, který může útok řešit. Národní CSIRT zajišťuje vzdělávání a spolupráci spolu s veřejností v rámci internetové infrastruktury. Cílem je pomoci při zavedení dalších týmů v zemi, jejich zavedení na mezinárodní scénu a pomoc při praktikování standardních postupů.(Peterka, 2011)

Vládní CSIRT

Vládní CSIRT se na rozdíl od národního, který se zabývá národní spoluprácí a zajištěním bezpečnosti na národní úrovni zaměřuje na oblast státní správy, samosprávy a řeší incidenty, které ohrožují bezpečnost státu. Většinou se jedná o státní instituce, pro které jsou vytvořeny konkrétní zákony, a je možnost přímého zásahu v případě problému. (Peterka, 2011)

1.3.4 Národní bezpečnostní úřad

Národní bezpečnostní úřad (NBÚ) je výkonný orgán zřízený zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Zajišťuje ochranu utajovaných informací a bezpečnostní způsobilost. NBÚ vydává osvědčení nebo doklad o bezpečnostní způsobilosti a tím garantuje, že u jeho držitele nebyly nalezeny žádné skutečnosti, které by mohly bránit přístupu k utajovaným informacím nebo k výkonu citlivých činností. NBÚ spolupracuje se zpravodajskými službami ČR, Policií ČR, Ministerstvem vnitra a na národní úrovni s bezpečnostními organizacemi zejména členských států NATO a EU. (O nás, b.r.)

1.4 Základní pojmy z oblasti kybernetické bezpečnosti

Oblast kybernetické bezpečnosti má obrovské množství odborný pojmů a názvů, kde jsou všechny uvedeny ve Výkladovém slovníku kybernetické bezpečnosti.

Bezpečnostní incident – "*Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie."*

Bezpečnostní událost – "*Událost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně."*

Informační a komunikační technologie – "*Informační a komunikační technologií se rozumí veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení."*

Kybernetická bezpečnost – "*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru."*

Kybernetický bezpečnostní incident – "*Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity elektronických komunikací v důsledku kybernetické bezpečnostní události."*

Kybernetická bezpečnostní událost – *"Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti*
a integrity sítí elektronických komunikací."

Kybernetický prostor – *"Digitální prostředí tvořené informačními a komunikačními technologiemi, ve kterých informace vznikají, jsou zpracovávány a dochází k jejich výměně."*

Kybernetický prostor si lze představit jako virtuální prostředí vytvořené propojením počítačů v jedné síti. Probíhá zde vzájemné působení a ovlivňování mezi jednotlivými subjekty.

Stav kybernetického nebezpečí – *"Stav kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací."*

(Jirásek, Novák a Požár, 2015)(Česko, 2014)(Hrůza, 2012)(Hromada et al., 2015)

1.5 Vývoj kybernetické bezpečnosti

Tato kapitola popisuje vývoj kybernetické bezpečnosti. Zaměřuje se na jednotlivé vývojové cykly, se kterými se můžeme v oblasti kybernetické bezpečnosti setkat.

1.5.1 Kybernetická bezpečnost

První zmínky pojmu kybernetická bezpečnost můžeme najít v Computer Science and Telecommunications Board´s Report z roku 1991. Definice bezpečnosti je definována jako: "*Ochrana proti nechtěnému zpřístupnění, modifikaci nebo zničení dat v systému, a také zabezpečení systémů samotných… obsahuje důležité procedurální, administrativní, fyzické a lidské prvky."* Od vzniku této definice se objevilo mnoho dalších definicí kybernetické bezpečnosti, kde každá pod pojmem kybernetická bezpečnost vymezuje něco jiného. Obecně je možné uvést bezpečnost jako stav připravenosti na potenciální útok, jeho následky a postup pro obnovení funkčnosti. Můžeme zde uvést tři základní principy, které vymezují kybernetickou bezpečnost:

- Životní cyklus kybernetické bezpečnosti (prevence, detekce a reakce).
- Prvky kybernetické bezpečnosti (lidé, procesy a technologie).
- CIA - Confidentiality (důvěrnost), Integrity (celistvost), Availability (dostupnost).

1.5.2 Životní cyklus kybernetické bezpečnosti

První trojice má za cíl předcházet a působit preventivně, aby nedošlo k nějakému útoku nebo narušení funkčnosti. Ovšem je důležité si uvědomit, že není nejdůležitější prevence, ale mnohem důležitější je detekce a reakce. Je totiž velmi důležité soustředit se na efektivní detekci a plánovat co nejúčinnější reakci. Reakce musí také obsahovat plán obnovy a prostředky pro opětovné vzniknutí.

Obrázek 2 - Životní cyklus kybernetické bezpečnosti *[Zdroj:* (Základní pojmy, 2020)*]*

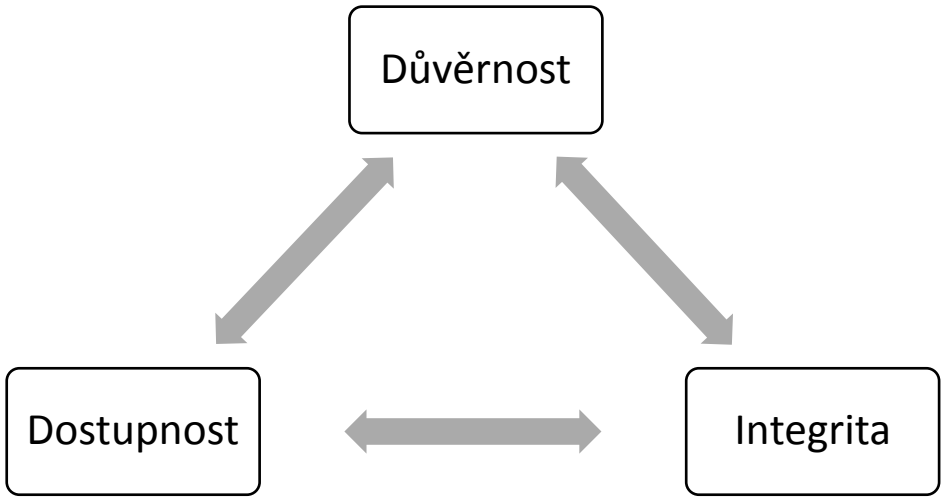
Prvky kybernetické bezpečnosti

Druhá trojice ukazuje propojitelnost a spolupráci mezi jednotlivými složkami. Je důležité si uvědomit, že systémy potřebují lidský faktor k tomu, aby dokázaly správně, efektivně a bez nějakých chyb a omylů fungovat. Závěr je jednoduchý tyto tři složky nemůžou fungovat každá zvlášť, tj. bez ostatních dvou.

CIA triáda

Třetí trojice je nejznámější. Důvěrnost je založená na povolení přístupu k informacím pouze autorizovaným osobám, nesmí se k nim dostat neoprávněné osoby. Integrita definuje

nemožnost zásahu do informací, dat, počítačových systémů a nezměnitelnost nastavení jinou než oprávněnou osobou. Dostupnost vyjadřuje přístup k informacím jenom oprávněným osobám. (Kolouch a Bašta, 2019)(Pačka, 2019)



Obrázek 3 - CIA triáda *[Zdroj: vlastní]*

1.5.3 Vývoj názvosloví v oblasti kybernetické bezpečnosti

Kyberbezpečnost

Kyberbezpečnost navazuje na svého předchůdce – informační bezpečnost. Kyberbezpečnost je velmi spjatá a propojená s informační bezpečnostní, ale liší se hlavně v tom, že obsahuje nové hrozby a rizika, které vznikly s pokrokem, rozvojem a vylepšováním v oblasti informačních a komunikačních technologií. Docházelo postupně ke zlepšování, rozvoji a rozšíření oblasti informační bezpečnosti. Proto bylo nutné informační bezpečnost rozšířit o další odvětví a to kybernetickou bezpečnost. Kybernetická bezpečnost má širší pole působnosti a to díky tomu že obsahuje nejen informace, ale i jejich zpracování a virtuální realitu v kyberprostoru, kdy vrcholem hrozby je umělá inteligence. Vzhledem k tomu že docházelo a dochází k různým druhům hrozeb, bylo nutné, aby vznik úřad, který se bude bezpečnostní zabývat, a proto vznikl NÚKIB. Vzhledem k tomu jak se společnost vyvíjí a digitalizuje, dochází ke zvýšení počtu hrozeb a rizik kybernetického charakteru a snižuje se množství hrozeb přirozeného charakteru. Jako příklad můžeme uvést banky a jejich poměr o jaké množství peněz přijdou při loupeži ale i o jaké množství informací a důležitých dat při kybernetickém útoku. S vývojem a větším množství kyberútoků a větším zajišťování kyberbezpečnosti došlo k rozčlenění kybernetických útoků na více skupin a kategorií, kdy každý název jasně identifikuje, o jaký druh útoku se jedná. (Sak, 2018)

Kybernetická kriminalita - jedná se o trestnou činnost spáchanou za pomocí informačních technologií.

Kyberšikana - jedná se o druh šikany, která je většinou propojena s reálnou šikanou. Oběť v mnoha případech na začátku poskytne informace, které jsou následně zneužity.

Kyberstalking - velmi úzce spojen s kyberšikanou. Útočník získá informace o oběti v reálném světě a neustále ji obtěžuje elektronickými sdělením s nepříjemným až obtěžujícím obsahem. S kybestalkingem se setkávají veřejné osoby, herci, zpěváci, ale můžou se s ní setkat i běžní lidé (např. dojde k rozchodu u párů a jeden z aktérů neunese ztrátu).

Kybergrooming - útočník se snaží získat důvěru dítěte, kde následně dojde ke zneužití dětí nebo informací o nich získaných.

Sexting - jedná se o aktivitu spojenou s rozesíláním a sdělování fotografií s erotickou tematikou.

Hoax - velmi často užívaný pojem v kyberprostoru. Jedná se o nevyžádanou, často smyšlenou a nepravdivou zprávu, která má za úkol mystifikovat.

Fake news - pojem, který je úzce spojen s hoax. Také se jedná o zprávu, která má za cíl ovlivnit názor, postoj nebo chování v reálném světě.

Kyberterorismus - trestná činnost páchána pomocí informačních technologií, která vede k neadekvátní reakci nebo minimálně vyvolá strach. Většinou se využívá při akcích politicky, extremisticky nebo nacionalisticky motivovanými.

Kybernetický útok a kyberválka - jedná se o druh hybridní války, která velmi často přesahuje do reálného světa. Je velmi obtížné získat informace o útočníkovi a také o tom kdy přijde k útoku. Útoky mohou být realizovány státy, podniky, ale i jednotlivci. (Jirásek, Novák a Požár, 2015) (Sak, 2018)

2 MALWARE

Každému kybernetickému bezpečnostnímu incidentu předchází kybernetický útok, kterého je mnoho druhů, možností a způsobů jejich provedení. Následující kapitola nás seznámí s nejznámějšími a nejpoužívanějšími útoky podle několika studií.

Malware

Malware je anglický název pro označení škodlivého softwaru. Jde vždy o software, který je použit k narušení standardní činnosti počítačového systému, k získání informací nebo k získání přístupu k počítačovému systému. Jeden malware může poškodit i více počítačů naráz, např.: pokud se šíří pomocí e-mailu (obsažen v příloze). V minulosti byly jako malware označovány všechny druhy škodlivých softwarů. Postupem času došlo k rozdělení do jednotlivých skupin podle činnosti, kterou daný program vykonává. Jedná se o skupiny:

- Adware – software podporující reklamu.
- Spyware – software získává statistická data o provozu počítače a bez souhlasu a vědomí uživatele je odesílá útočníkovi. Keylogger je druh spywaru. Jedná se o software, který zaznamenává stisknutí jednotlivých kláves na napadeném zařízení a tato data zasílá útočníkovi.
- Ransomware – druh malware, konkrétně vyděračský kdy dojde k ukradnutí dat, která budou vrácena pouze při zaplacení výkupného.

Další skupinou malware, který se rozděluje do skupin podle toho, jakým způsobem dochází k přenosu jsou:

- Viry – součást jiného souboru, kdy při jeho spuštění dojde k nakažení PC.
- Červi – jde o druh viru, který si liší tím, že nemusí být součástí souboru, aby došlo k přenosu do PC.
- Trojské koně – jde o programy v počítači obsahující skryté funkce, které buď uživatel neschválí, nebo o nich neví.
- Backdoor – jedná se o druh trojského koně, který napadá komunikační porty počítače a umožňuje ovládání poškozeného počítače na dálku.
- Rootkity – technologie nebo počítačové programy sloužící k neprozrazení a co nejlepšímu ukrytí malware v napadeném systému. (Kolouch, 2016) (Jirásek, Novák a Požár, 2015)

2.1 Phishing (rybaření)

Phishing je forma útoku s pomocí technik sociálního inženýrství, kdy se útočník vydává za důvěryhodnou autoritu s cílem získat citlivá data oběti. Nejčastějším phishingem je pokus o získání citlivých informací o kreditní kartě nebo internetovém bankovnictví oběti s pomocí podvodného e-mailu. Ten obvykle obsahuje formulář na zadání čísla kreditní karty a CVV kód nebo odkazu na externí webové stránky se stejným obsahem. Existuje několik bodů na rozpoznání phishingu. Podvodný e-mail obvykle obsahuje obecné nebo formální oslovení, požadavek na citlivé informace, špatnou gramatiku, nebo podezřele výhodnou nabídku. Bývá to často neočekávaný e-mail z podezřelé domény a je příliš naléhavý. Chránit se můžeme především svou opatrností, pozorností a samozřejmě kvalitním bezpečnostním řešením, které je základním kamenem zabezpečení počítače a dokáže si poradit s velkým množstvím phishingu. (Phishing, b.r.)

2.2 Spear-phishing

Spear phishing je počítačová kriminalita, která využívá e-maily k cíleným útokům na jednotlivce a firmy. Zločinci používají důvtipnou taktiku ke shromažďování osobních údajů o svých cílech a k posílání známých a důvěryhodných e-mailů.

Tyto e-maily často obsahují přílohy, které obsahují škodlivé odkazy na malware, ransomware nebo spyware. E-mail navíc bezostyšně požádá příjemce, aby naléhavě odpověděl, například přenesl konkrétní částku peněz nebo poslal osobní údaje, jako je bankovní heslo.

Protože e-maily jsou psány velmi známým tónem a odkazují na osobní údaje o příjemci, oběti se mylně domnívají, že vědí a důvěřují odesílateli a odpovídají na žádost. (What Is Spear Phishing?, 2021)

2.3 Pharming (farmaření)

Pharming je druh kybernetického útoku zahrnující přesměrování webového provozu zlegitimního webu na falešný web za účelem krádeže uživatelských jmen, hesel, finančních údajů a dalších osobních údajů. Pharming je sofistikovaný druh phishigového útoku a může ovlivnit kohokoli na jakémkoliv webu.

Typický phispingový web je falešný nebo upravený aby vypadal stejně jako web, který oběť navštěvuje. Cílem phishingového webu je "sklízet" nebo "farmařit" uživatelská jména a hesla, když se nic netušící oběť pokusí přihlásit ke svému účtu. (Pharming, 2020)

2.4 SQL Injection a Cross-sitte scripting (XSS)

Hlavní rozdíl mezi útokem injekcí SQL a XSS spočívá v tom, že útoky injekcí SQL se používají ke krádeži informací z databází, zatímco útoky XSS se používají k přesměrování uživatelů na webové stránky, kde z nich mohou účastníci ukrást data. Injekce SQL je zaměřena na databázi, zatímco XSS je zaměřena na útoky na koncové uživatele.

K útoku vložení SQL dojde, když je kód strukturovaného dotazovacího jazyka (SQL) vložen do formulářů, souborů cookie nebo hlaviček http, které nepoužívají metody dezinfekce nebo ověření dat k ověření, takže informace zapadají do předepsaných parametrů GET nebo POST. Tato chyba umožňuje filtrování dat, změny nebo mazání z databází připojených webů.

Naproti tomu útok XSS používá škodlivý kód k přesměrování uživatelů na škodlivé webové stránky, ke krádeži souborů cookie nebo pověření nebo zneužití webových stránek. To obvykle provádí pomocí škodlivých skriptů, které se spouští v klientských prohlížečích v důsledku vstupu uživatele, funkčních příkazů, požadavků klientů nebo jiných výrazů. Útočníci mohou například útočit na škodlivě vytvořené adresy URL pomocí pokusů o phishing e-mailů, e-mailových příloh s vloženými odkazy. (SQL vs. XXS Injection Attacks Explained, 2018)

2.5 Botnet

Botnety - skupina počítačových systémů řízených hackery. Botnet, zkratka pro robotickou síť, je agregace napadených počítačů, které jsou připojeny k centrálnímu "vedoucímu". Ohrožené počítače jsou často označovány jako "zombie". Tato hrozba se bude i nadále šířit, jak se bude vyvíjet technika útoku a budou dostupné širšímu publiku, s méně technickými znalostmi potřebnými k zahájení úspěšného útoku. Botnety určené ke krádeži dat zlepšují jejich šifrovací schopnosti, a proto je jejich detekce stále obtížnější. (Awad a Fairhust, 2018)

2.6 DoS a DDoS

Útok DoS si klade za cíl, aby cílová služba byla zahlcena zprávami, takže ji již nebude možné uspokojivě provádět a tím uživatelům odepřít přístup ke službě. Toho je dosaženo bombardováním služby požadavky obvykle generovanými automaticky. Útok DoS v dnešní době je obvykle distribuovaný útok, který se nazývá útok DDoS (distributed denial of service), kdy jsou požadavky odesílány z mnoha webů, často v důsledku ohrožení zúčastněných útočných webů, poté, co byly infikovány škodlivým softwarem.

Zúčastněné weby jednají škodlivě bez vědomí vlastníka. Dalším typem útoku DoS je infikování cíle virem, který již není schopen fungovat. Počítačový virus je malware program, který se šíří po síti a může být nastaven tak, aby záměrně poškodil nebo odstranil data. Virus se obvykle šíří prostřednictvím příloh v e-mailech nebo prostřednictvím stahování. Když uživatel soubor otevře, virus se aktivuje. Poté může pokračovat s šíření svého kódu do dalších programů a souborů uložených v počítači oběti. Počítačový červ funguje podobně jako virus, ale nenese užitečné zatížení, aby způsobil poškození systému oběti. (Awad a Fairhust, 2018)

2.7 Zero-Day Vulnerabilities

Zranitelnost nulového dne je definována jako chyba zabezpečení, která dosud nebyla oznámena prodejci ani vývojáři. Když útočníci vyvinou úspěšné zneužití pro zranitelnost nulového dne, říká se tomu zneužití nulového dne. Pro vývojáře a bezpečnostní techniky je velmi těžké najít všechny bezpečnostní chyby, takže útočníci očekávají, že existují a vynaloží značné úsilí na odhalení chyb zabezpečení. Výsledkem jsou "závody ve zbrojení" mezi útočníky a bezpečnostním průmyslem.

Zneužívání v nulový den poskytuje útočníkovi obrovskou výhodu, protože bezpečnostní ochrana je postavena na známém zneužití, takže cílové útoky založené na zneužití nulového dne mohou zůstat po dlouho dobu bez povšimnutí. Úspěch útoku zneužití v nulový den závisí na okně zranitelnosti - době mezi objevem zneužití a jeho opravou. I známá chyba zabezpečení může mít dlouhé okno zranitelnosti, pokud je obtížné její opravu vytvořit. Čím větší je okno zranitelnosti, tím větší je šance, že útok bude bez povšimnutí - čímž se zvýší jeho účinnost. I když je k opravě zranitelnosti vyvinuta oprava, mnoho systémů zůstává zranitelných, často po celá léta. Oprava může často narušit stávajíc systémy a způsobit vedlejší účinky a nestabilitu se škodlivými následky. (Zero-Day Vulnerability, 2014)

Zero Day Attack poškozuje více než 20 % systémů společností. (Andress a Winterfeld, 2011)

2.8 Man-in-the-Middle (MIMT)

Útok typu Man-in-the-Middle je útok, kdy útočník zachytí konverzaci mezi dvěma stranami a předá zprávy mezi stranami, které se vydávají za každou z nich. Útočník tak získá přístup k informacím, které si obě strany vyměňovaly a může také měnit zprávy nebo posílat falešné zprávy. Útok MITM může být používán k odeslání trojského koně. (Awad a Fairhust, 2018)

2.9 Cryptojacking malware

Cryptojacking je objevujíc se online hrozba, která se skrývá v počítači nebo mobilním zařízení a využívá zdroje stroje k "těžbě" forem online peněz známých jako kryptoměny. Je to narůstající hrozba, která dokáže ovládnout webové prohlížeče a kompromitovat všechny druhy zařízení, od stolních počítačů a notebooků, až po chytré telefony, dokonce i síťové servery.

Stejně jako většina ostatních škodlivých útoků na počítačovou veřejnost je motivem zisk, ale na rozdíl od mnoha hrozeb je navržen tak, aby zůstal před uživatelem zcela skrytý.

Pokud jste obětí kryptojackingu možná si toho ani nevšimnete. Většina softwaru pro kryptojacking je navržena tak, aby zůstala skryta před uživatelem, ale to neznamená, že si nevybírá svou daň. Tato krádež vašich výpočetních zařízení zpomaluje jiné procesy, zvyšuje účty za elektřinu a zkracuje životnost vašeho zařízení. Pokud váš PC, notebook nebo Mac zpomalí nebo používá svůj chladící ventilátor více než obvykle, můžete mít důvodné podezření na kryptojacking. Motivace kryptojackingu je jednoduchá – peníze. (Cryptojacking – What is it?, 2021)

3 BEZPEČNOSTNÍ SYSTÉMY

Mezi jedny z nejpoužívanějších bezpečnostních systémů pro zajištění kybernetické bezpečnosti se využívají systémy – IDS a IPS systém a SIEM.

3.1 IDS systém

IDS (Intrusion Detection System) – systém detekce narušení. Jedná se o softwarový nebo hardwarový nástroj nebo i jejich kombinace, který je schopen monitorovat síťový provoz a snaží se odhalovat podezřelé aktivity. Mezi hlavní činnosti IDA systému patří detekce neobvyklých aktivit, které můžou způsobit narušení bezpečnosti operačního systému nebo počítačové sítě. IDS se nevěnuje jenom konečnými pokusy o prolomení bezpečnosti, ale zabývá se také detekcí akcí, které jim předcházejí. Mezi nejčastější akce, které jim předcházejí a následně vedou k prolomení bezpečnosti patří skenování portů, sbírání informací potřebných k útoku a další. Hlavním prvkem IDS systému je senzor, ve kterém je zabudovaný mechanismus pro detekci škodlivých a nebezpečných kódů a jeho hlavní a nejdůležitější činností je odhalování těchto nebezpečí.

Systém IDS patří mezi pasivní systémy, které při odhalení podezřelé aktivity nijak nezasahují do síťového provozu. Pasivní systém IDS v případě odhalení nebezpečí vygeneruje pouze varování, případně jej zaznamená do systémového logu. (IDS/IPS, 2014) (IDS: základní informace, 2007)

3.2 IPS systém

Na rozdíl od pasivního systému IDS existuje i aktivní systém IPS (Intrusion Prevetntion Systems) – systém prevence proniknutí, který zareaguje na podezřelou aktivitu resetováním spojení nebo nastavením systému, tak aby zablokoval provoz v sítí ze zdroje, který je podezřelý ze škodlivého působení.

Systém IPS je velmi často označován jak vyšší stupeň ochrany, který je aktivní. Pokročilé IPS systémy dokážou poskytnout ochranu na všech úrovních a to od zajištění bezpečnosti operačního systému aplikace až po síťový provoz. Na základě toho IDS potom dokáže vyhodnotit jak velká je míra rizika a podle toho jednat. Systém je schopný upozornit administrátora, zablokovat přístup uživatelů v aplikaci až po odpojení serveru ze sítě, pokud to bude třeba.

Moderní IPS systémy dokonce umí zabránit novým druhům útoků. Potřebují k tomu pouze databázi obsahující určité vzory chování sítových provozů. Dále dokážou sledovat dění na síti, např. zvýšenou aktivitu na nějakém portu, přenos dat nebo připojená zařízení.

V současné době jsou systémy IPS na velmi vysoké úrovni. Dovedou poskytnout velmi kvalitní ochranu a také velmi pomohou při zajištění prevence. Systém je schopen si poradit nejen s běžným DoS útokem, ale i s robotem, který hledá slabá místa v online aplikacích. (IDS/IPS, 2014) (IPS/IDS ochrana, 2015)

IDSP (Intrusion Detection and Prevention Systems) – systém odhalení a prevence proniknutí. Jedná se o systém, který se využívá v oblasti, kde se toto může provádět automaticky nebo na příkaz operátora. Jde o systém, který jak detekuje útoky, tak se jim snaží i předcházet. (IDS/IPS, 2014)

3.3 SIEM

SIEM (Security Information and Event Management) – nástroj pro správu bezpečnostních informací a událostí organizace. SIEM poskytuje monitorování, ukládání, spojování, souvztažnost bezpečnostních informací a z nich vyplývajících incidentů a jejich zobrazování, podávání hlášení a vydávání varování. Technologie SIEM shromažďuje v reálném čase informace ze síťových počítačových systémů, aplikací, systémových logů, jejichž vyhodnocení umožňuje identifikovat potenciální bezpečnostní hrozby.

Systém může data sbírat z routerů, webových serverů, firewallů nebo databázových serverů a tyto informace mohou být dále rozšířeny o informace, které je doplňují, jako jsou informace o výsledcích bezpečnostních skenů, informace o uživatelích, informace z externích zdrojů a informace o běžných zvycích uživatelů. Získané informace jsou následně sloučeny a je nad nimi provedena analýza, která dokáže odhalit možné bezpečnostní problémy.

SIEM systém patří mezi jeden ze složitějších a vyžaduje každodenní údržbu a není vhodný pro každou situaci na rozdíl od firewall. (Kolouch a Bašta, 2019)

4 KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT

Kybernetický bezpečnostní incident a kybernetická bezpečnostní událost se může zdát mít pro mnoho lidí velmi podobný nebo dokonce stejný význam. Opak je ovšem pravdou a proto je důležité najít a vymezit rozdíly mezi těmito výrazy.

Pro zopakování definice:

Kybernetický bezpečnostní incident – "*Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity elektronických komunikací v důsledku kybernetické bezpečnostní události."*

Kybernetická bezpečnostní událost – "*Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity sítí elektronických komunikací."* (Kolouch a Bašta, 2019)

4.1 Rozdíl mezi kybernetickou bezpečnostní událostí a kybernetickým bezpečnostním incidentem

Porovnání definic kybernetického bezpečnostního incidentu (KBI) a kybernetické bezpečnostní události (KBU) můžeme najít v příručce pro řešení incidentů vydané Národním institutem norem a technologií.

4.1.1 Kybernetická bezpečnostní událost

Příručka uvádí, že událostí je jakýkoliv pozorovatelný výskyt v systému nebo síti. Jedná se o případy, kdy se uživatel připojí k síti za účelem sdílení, když server přijme požadavek přístupu k webové stránce, blokování brány firewall a pokus o připojení. Nepříznivé události jsou události s negativním dopadem, jako jsou havárie systému, neoprávněné použití systémových oprávnění, neoprávněný přístup k citlivým datům. (Cichonski et al., 2011)

4.1.2 Kybernetický bezpečnostní incident

Kybernetický bezpečnostní incident příručka vymezuje jako narušení nebo bezprostřední hrozba porušení zásad zabezpečení počítače, zásad přijatelného použití nebo standardních postupů zabezpečení. Příklady incidentů:

- Uživatelé jsou navedeni k otevření "čtvrtletního přehledu" zaslaného e-mailem, který je ve skutečnosti malwarem. Spuštěním nástroje dojde k infikování jejich počítače a navázání připojení s externím hostitelem.

- Uživatel poskytuje nebo vystavuje citlivé informace ostatním prostřednictvím služby souborů peer-to-peer.(Cichonski et al., 2011)

4.2 Typy kybernetických bezpečnostních incidentů

Typy kybernetických bezpečnostních incidentů jsou definovány ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti.

Kybernetické bezpečnostní incidenty podle dopadu:

- *"Kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv".*
- *"Kybernetický bezpečnostní incident způsobující narušení integrity aktiv".*
- *"Kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv".*
- *"Kybernetický bezpečnostní incident způsobující kombinaci výše uvedených".* (Česko, 2018)

Kybernetické bezpečnostní incidenty podle závažnosti:

- *"Kategorie I – méně významný KBI, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření KBI včetně minimalizace vzniklých škod".*
- *"Kategorie II – významný KBI, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření KBI včetně minimalizace vzniklých škod".*
- *"Kategorie III – velmi významný KBI, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření KBI včetně minimalizace vzniklých i potenciálních škod".*(Česko, 2018)

Kybernetické bezpečnostní incidenty nemusí mít dopad a poškodit jenom jednotlivce, firmu nebo společnost. KBI můžou mít i negativní vliv na chod celého státu. V následující tabulce můžeme najít různé druhy KBI,co nám hrozí, jak nás můžou poškodit a jaká jsou potřebná opatření v případě ochromení chodu státu nebo některých jeho částí.

Tabulka 1 – Příklady hrozeb, újmy a opatření KBI *[Zdroj:* (Lukáš, 2017)*]*

	Hrozba	Újma	Opatření
Příklady hrozeb, újmy a opatření kybernetické bezpečnosti	KBI způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb.	Vliv na život a poškození zdraví osob v důsledku způsobení krizového stavu.	Realizace podrobné analýzy rizik ve vztahu ke struktuře provozních sítí.
	KBI způsobený škodlivým kódem.	Omezení možností použití elektronických komunikačních a technických prostředků pro situační monitorování stavu.	Zřízení orgánu zodpovědných za krizové řízení u společností se státní působností.
	KBI způsobený překonáním technických opatření.	Výpadek nebo poškození komunikačních systému používaných pro záchranu majetku.	Zpracování plánu krizové připravenosti, plánů bezpečnostní kontinuity činnosti a plánu obnovy.
	KBI způsobený porušením organizačních opatření.	Dysfunkce systému tísňového volání.	Zabezpečení součinnosti s IZS.
	KBI způsobený projevem trvale působící hrozby.	Dysfunkce monitorovacích systémů dopravní informační služby.	Periodický a cílený nácvik činností řešení a likvidace variant havarijních nebo krizových situací.
	KBI způsobené narušení důvěrnosti aktiv.	Dysfunkce řídících, informačních a komunikačních systémů.	Udržování záložních zdrojů elektrické energie v pohotovostním režimu.

	KBI způsobené narušením dostupnosti.	Omezení nebo znemožnění plnění mezinárodních hospodářských politických a vojenských závazků.	Vykonávání pravidelného testování aktivnosti a funkčnosti záložních systémů.
	Narušení dodávky elektrické energie včetně dodávky ze záložního zdroje.	Omezení nebo ochromení řídících a komunikačních procesů.	Zabezpečení ochrany objektů a obsluhy technologických zařízení.
	Výpadky v důsledku prudkého zvýšení provozu v síti.	Omezení nebo znemožnění zásobování obyvatelstva v důsledku výpadku výroby a distribuce závislé na ICT	Systém řízení bezpečnosti informací.

4.3 Opatření předcházející vzniku kybernetického bezpečnostního incidentu

Opatření vedoucí k zabránění nebo snížení narušení bezproblémového fungování se můžou dělit do několika kategorií.

Podle způsobu implementace:

- Organizační (administrativní) – zavedení směrnic, nařízení, standardů, které jasně definují pravidla a postupy, také školení a přednášky v oblasti informační bezpečnosti.
- Technická (fyzická či logická) – zabránění vstupu neoprávněných osob, kontrola pohybu osob.

Technická opatření můžeme dále rozlišovat, na komunikační, systémová, aplikační, databázová a kryptografická.

Další možnost rozdělení je na:

- Preventivní – předchází nežádoucím aktivitám a brání útočníkovi ke vniknutí do systému.
- Detekční – odhalují nežádoucí působení, např. senzor, záznam z kamery.
- Reaktivní – po odhalení, kdy je nutno na akci nějak reagovat.

Také se velmi často využívá kategorizace:

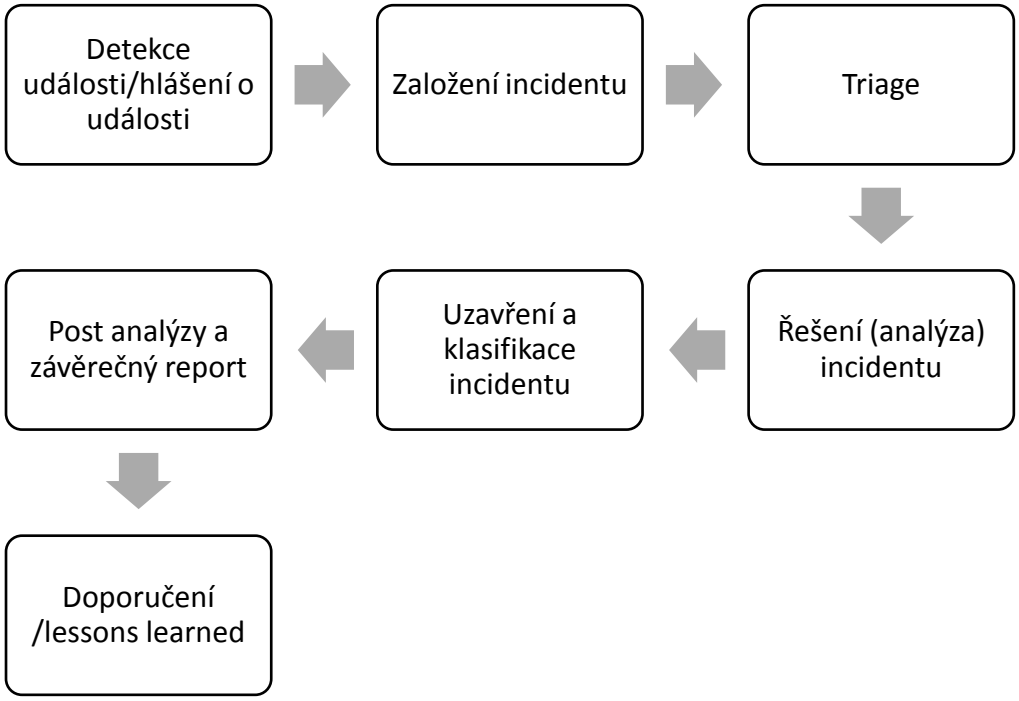
- Odstrašující – viditelná opatření, která by měla útočníka odradit od nežádoucího jednání.
- Zdržující – vede k zpomalení postupu účastníka při útoku.
- Obnova – vede k obnovení funkčnosti systému.

Při kombinaci výše uvedených opatření je možnost získat velmi účinná a efektivní opatření, která vedou k přecházení nežádoucího působení. Kromě výše uvedených lze opatření ještě rozdělit na:

- Kompenzační – nahradí některé běžně využívané opatření.
- Direktivní – u některých opatření je nutnost provádět kontrolu a je potřeba aby existoval postup jak provádět kontrolu.
- Nápravná – vedou k možnosti opakovaného vzniku události. (Šulc, 2018) (Singer a Friedman, 2014) (Požár, 2005)

4.4 Proces řešení kybernetického bezpečnostního incidentu

Proces řešení kybernetického bezpečnostního incidentu je jedním z úkolů CSIRT pracovišť.



Obrázek 4 - Proces řešení KBI *[Zdroj:* (Pačka, 2019)*]*

Řízení informační bezpečnosti je jeden z dalších důležitých kroků zajištění bezpečnosti. Provádíme ji několika způsoby. Jako první krok je důležité určit osobu, která bude zodpovědná za řízení informační bezpečnosti. Dále je potřeba zavést základní bezpečnostní pravidla organizace. Tato pravidla by měla zavést každá firma, podnik nebo organizace. Nezáleží na tom, jestli se řadí mezi malé, střední nebo velké svou velikostí, ani v jakém oboru nebo odvětví působí.

Dalším důležitým krokem je provedení analýzy rizik a podle zjištěných rizik navrhnout vhodný způsob jak je zvládnout. Většinou to vede k zavedení nových bezpečnostních organizačních a technických opatření. Navrhnutá a zavedená opatření by se měla pravidelně kontrolovat a vyhodnocovat. V případě zjištění neshody s požadavky je potřeba včas a efektivně zareagovat. Lze zde využít Demingův cyklus PDCA - metodu postupného zlepšování založenou na opakování čtyř základních kroků. (Šulc, 2018) V oblasti informační bezpečnosti můžeme postupovat podle normy ISO/IEC 27001 – Management bezpečnosti informací.

Norma ISO 27001 je mezinárodně platná norma, která vymezuje požadavky na systém managementu bezpečnosti informací. Norma přesně určuje požadavky na řízení bezpečnosti informací. Určuje firmám pravidla, jakým způsobem mají zacházet s veškerými interními ale i externími informacemi, aby nemohlo dojít k jejich ztrátě, zneužití nebo narušení důvěry. (ISO 27001, b.r.)

ISO norma obsahuje 11 důležitých oblastí a firma nesmí ani na jednu z nich zapomenout aby její uplatnění a zavedení bylo co nejefektivnější. Manažer bezpečnosti by měl v souladu s ISO normou postupovat následovně:

- Stanovit rozsah a hranice ISMS
- Definovat metodiku hodnocení rizik.
- Provést analýzu rizik.
- Zvolit vhodný způsob zvládání rizik.
- Získat souhlas vedení organizace.
- Formulovat plán zvládání analýzy rizik.
- Zavést bezpečnostní opatření.
- Zpracovat bezpečností politiku, standardy a směrnice.
- Zvyšovat bezpečnostní povědomí.
- Monitorovat a vyhodnocovat funkčnost zavedených opatření.
- V pravidelných intervalech opakovat analýzu rizik.
- Provádět interní audity.
- Zavádět nová a účinnější opatření.
- Aktualizovat a optimalizovat. (Požár, 2005) (Šulc, 2018)

5 DÍLČÍ ZÁVĚR

Cílem teoretické části je seznámit čtenáře s informacemi, které se týkají oblasti kybernetické bezpečnosti. Tato oblast je velmi široká, v poslední době se stává čím dál více populární a medializovaná. Tak jako každý oblast i kybernetická bezpečnost je vymezena v České republice zákony, vyhlášky a normami, které určují a vymezují kybernetickou bezpečnost. Kybernetická bezpečnost je zajišťována institucemi a organizacemi. V České republice je k tomuto účelu zřízen Národní úřad pro kybernetickou a informační bezpečnost, známý pod zkratkou NÚKIB, dále CERT, CSIRT a Národní bezpečnostní úřad. Jedná se o organizace zřizované státem, které zajišťují kybernetickou bezpečnost, provádí jednotlivá cvičení a snaží se pomáhat i poskytovat rady při řešení kybernetických útoků.

Mezi další důležitou oblast patří malware. Malware má mnoho druhů a podob, ve kterých se s ním můžeme setkat. S několika základními druhy jsme se v práci seznámili a popsali si jejich funkci.

V souvislosti s kybernetickou bezpečností nesmíme zapomenout zmínit bezpečnostní systémy. Jedná se o systémy, které mohou být nápomocné při zabránění vzniku kybernetického bezpečnostního incidentu. Na závěr je také vhodné si ujasnit a vymezit rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickou bezpečnostní událostí. Mnoha lidem se mohou zdát tyhle pojmy stejné nebo podobné. Ve skutečnosti je mezi nimi ale rozdíl. Také nesmíme zapomenout na opatření, která vedou ke snížení pravděpodobnosti vzniku incidentu a postupem jak probíhá řešení, v případě vzniku incidentu.

II. PRAKTICKÁ ČÁST

6 ANALÝZA FUNKCIONALITY ZVOLENÉHO SIMULÁTORU

Tato kapitola se zabývá analýzou a seznámením se s programem PractisGo, ve kterém je následně vytvořen scénář a provedeno cvičení.

6.1 Practis Go

Aplikace PRACTIS GO je nástroj nové generace pro přípravu, simulaci a vyhodnocení cvičení. Jedná se o nástroj, který slouží pro tvorbu jakéhokoliv scénáře za pomoci audiovizuálních vstupů, jeho simulaci, díky níž jsou hráči vtaženi do hry a vyhodnocení cvičení po jeho ukončení. Aplikace je určena těm, kteří cvičení vytvářejí a moderují, i těm, kteří jsou na druhé straně pomyslné barikády a mají za úkol jednotlivé simulované situace řešit. Navíc je zde přítomen interaktivní prvek umožňující hráčům komunikovat na chatu či plnit různé úkoly.

Tato verze je obohacena o vizualizační aplikace SITUNET a SITUBOARD, které slouží pro přehledné zobrazení složité situace pomocí mapového podkladu a dashboardu. Vybrané vstupy (injecty) jsou zobrazovány na mapě a hráči mohou naopak některé úkoly do mapy zakreslovat. Souhrnné údaje o celém cvičení jsou zobrazeny na přehledném dashboardu, jehož podobu lze nakonfigurovat pomocí několika různých widgetů.

Tato komplexní sada nástrojů pro podporu cvičení umožňuje prožít kritickou událost, najít způsob jejího řešení a připravit se tak na složité krizové situace, které v reálném životě mohou nastat.

6.2 Terminologie

Cvičení – jedná se o způsob výuky hrou a prožitkem pomocí scénáře, který simuluje krizovou situaci. Může se jedna to table-top cvičení, operační či plně funkční cvičení.

Operátor/moderátor a jeho role – osoba sestavující scénář a dále pak zodpovědná osoba za průběh celého cvičení. Vyžaduje se od něj, aby moderoval a korigoval cvičení, pokud mají hráči tendence odbočit od scénáře, zpochybňovat jej, používat k řešení nereálné zdroje a prostředky. Může tak učinit verbálně, či do scénáře zasáhnout dalším, dalo by se říci, "bočním" injectem. Dále sleduje počínání hráčů, které vyhodnocuje pomocí nastaveného bodového systému. Během cvičení může s hráči komunikovat výhradně prostřednictvím injectů, chatu, či zpráva v aplikaci SITUBOARD, případně může mezi hráči procházet, mluvit s nimi a do hry se částečně zapojovat.

Operátor si také volí, zda cvičení poběží automaticky, tedy jestli se scénář odvíjí sám dle nastavených časů, či jej bude řídit manuálně spíše intuitivně dle průběhu a schopností hráčů. V neposlední řadě určuje, jaký zvolí typ cvičení, a to v závislosti na obtížnosti scénáře a cílech cvičení. V některých případech hráči danou problematiku znají a jsou tedy schopni určit, jaké kroky by v jednotlivých rolích měli konat. V tomto případě operátor nechává kroky hráčů zakryté, maximálně zobrazí nápovědu. V jiném případě může být problematika příliš složitá a hráči daný postup nejsou schopni určit, případně se postup teprve učí, či jej hledají. V tomto případě nechá kroky hráčům odkryté a hru stimuluje pomocí doplňkových úkolů v podobě Take the action.

Hráč – účastník cvičení v určité přiřazené roli dle daného sestaveného scénáře. Očekává se od něj plná participace na cvičení ve smyslu snahy nacházet postupy a řešení na daný inject, plnit pokyny moderátora cvičení, pracovat s poskytnutými podklady a používat vymezené zdroje a prostředky.

Hráči v aplikaci sledují jednotlivé promítané injecty a určují, jaké kroky je třeba podniknout pro úspěšné řešení prezentovaného problému. Komunikují s operátorem pomocí funkcionality chatu a přes funkcionalitu Take the action plní úkoly. Ty mívají nejčastěji textovou podobu, nebo zákres do mapy.

Scénář – série vnějších vstupů (injectů) vytvářející příběh, který simuluje danou událost. Na každý inject jsou vázány kroky plněné jednotlivými rolemi, které jsou v rámci scénáře vydefinovány. Tyto kroky vždy shrnuje milník.

Inject – jedná se o vnější vstup, který hráči nejsou schopni ovlivnit, a naopak na něj musí reagovat. Tato reakce sestává z kroků, které se poskládají do milníku. Inject může nabývat textové, obrázkové či audiovizuální podoby a během cvičení se hráčům promítají na jejich dashboardu.

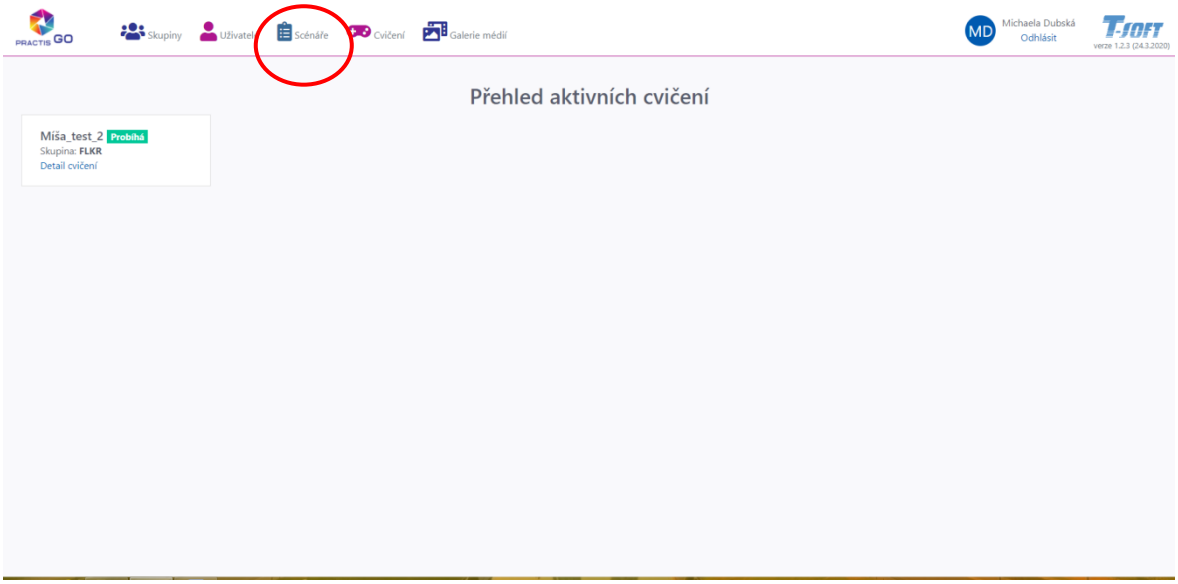
Doplňující inject – inject "bokem" – umožňuje scénář dále rozvíjet mimo jeho hlavní linii, případně jej korigovat. Tyto injecty lze naplánovat předem a je na operátorovi, zda je využije. Inject bokem lze použít i během samostatného cvičení spontánně v závislosti na průběhu hry.

Take the action – jedná se o doplňující úkoly, jejichž účelem je zpestření hry pomocí interakce a rozšíření znalostí týkající se daného kroku. Nejčastější způsob plnění úkolu je v textové podobě. Další možností je zákres specifických údajů do mapy.

Hotwash, After Action Report – provádí se po cvičení, kdy operátor a hráči spolu proberou průběh celého cvičení za účelem identifikace slabých stránek a ponaučení.(Klemensová, b.r.)

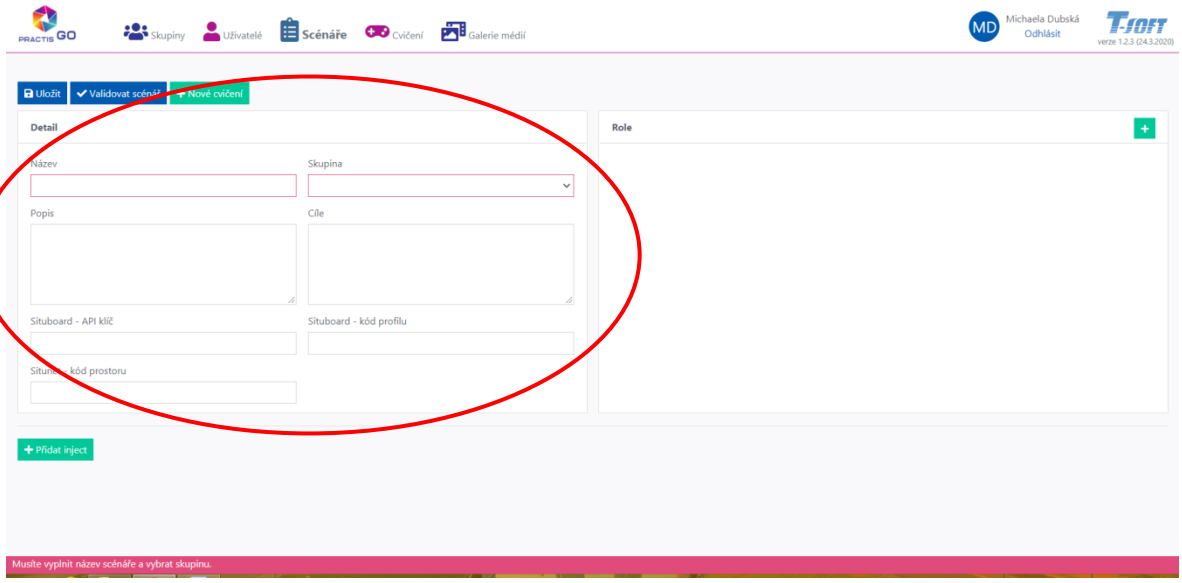
6.3 Tvorba scénáře

Po přihlášení se do programu, se nám zobrazí úvodní stránka PractisGo, na které vidíme aktivní cvičení viz obrázek č. 5



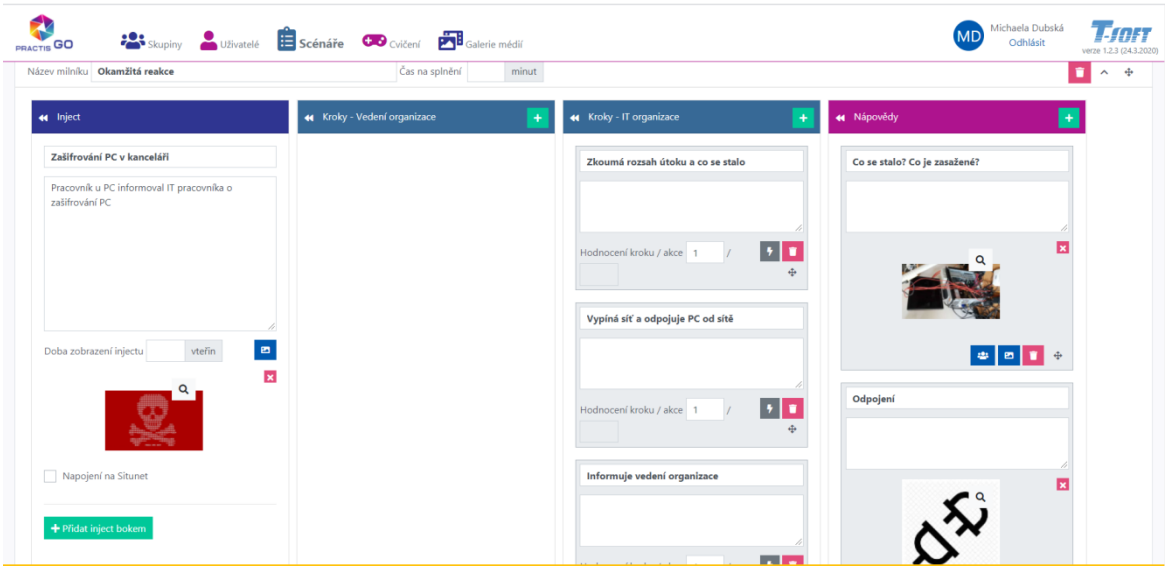
Obrázek 5 – Přehled aktivních cvičení *[Zdroj: vlastní]*

Následuje kliknutí na ikonu scénáře a nový – začíná tvorba nového scénáře. Viz obrázek č. 6. Postup vytvoření scénáře kybernetického bezpečnostního incidentu obsahuje mnoho kroků. Prvních z nich je název, popis cvičení, určení skupiny, stručný popis a vymezení cíle cvičení. Následuje určení jednotlivých rolí v cvičení.



Obrázek 6 – Tvorba nového scénáře *[Zdroj: vlastní]*

Dalším krokem je vytvoření jednotlivých injectů, které nejsou schopni hráči ovlivnit a určují, jak se bude dále scénář vyvíjet. Co se stane za události a jak na ně budou jednotlivé role reagovat. Viz. obrázek č. 7.

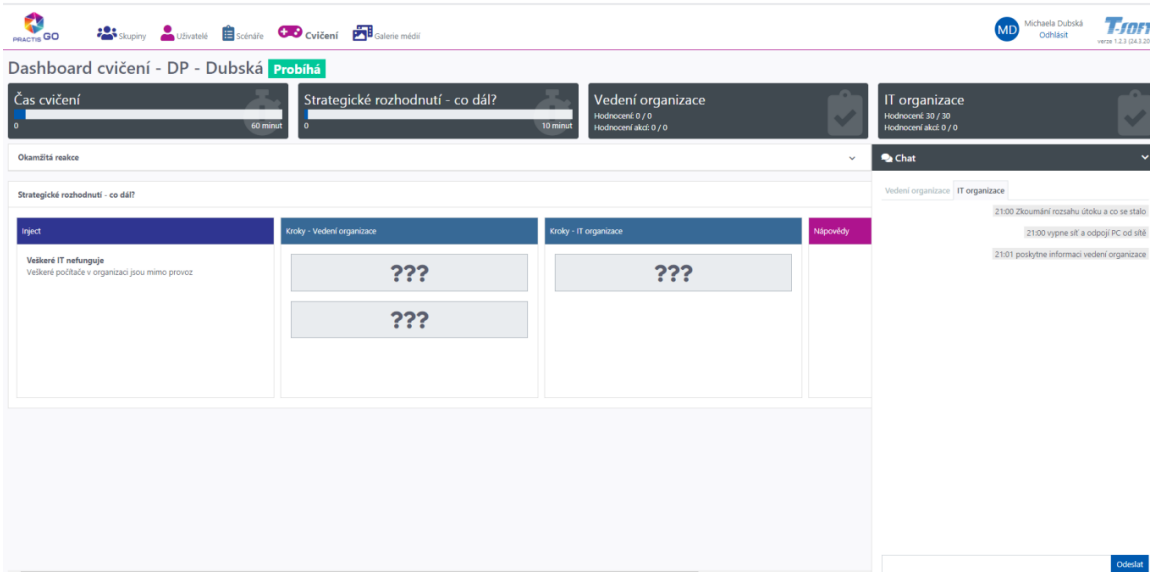


Obrázek 7 – Tvorba injectů ve scénáři *[Zdroj: vlastní]*

Po vytvoření všech injectů, kterých může být neomezený počet – čím více, tím delší scénář, dochází k uložení scénáře. Scénář se může následně využít ke cvičení, kde se vyzkouší jeho funkčnost a případná schopnost aplikovatelnosti do praxe.

6.4 Scénář z pohledu hráče

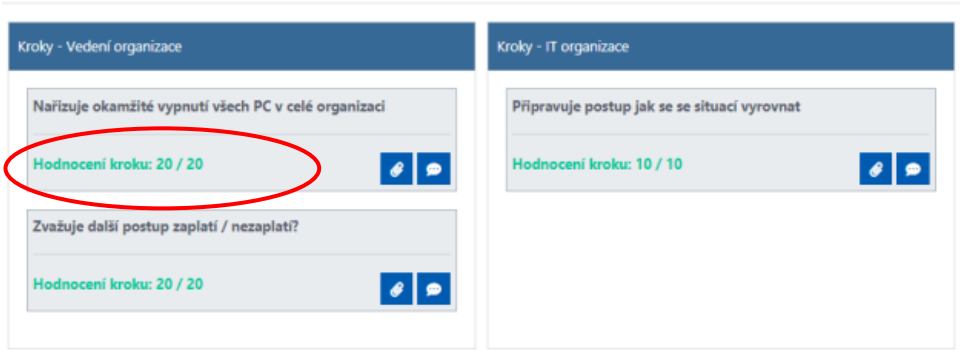
Na obrázku č. 8 vidíme názornou ukázku z prostředí programu PractisGO z pohledu hráče. V tomto konkrétním případě hráč zastává roli, jak managementu organizace, tak i IT specialisty. Na obrázku můžeme vidět inject, na který musí hráči (management + IT specialisté) reagovat. Reakce se provádí pomocí chatu, ve kterém se přepínají okna, podle toho za koho reagujeme. Na obrázku také můžete vidět, kolik reakcí se od každého hráče očekává (zobrazeno obdélníky s otazníky)



Obrázek 8 – Ukázka z průběhu cvičení *[Zdroj: vlastní]*

6.5 Hodnocení cvičení

Hodnocení cvičení (viz. obrázek č.9) probíhá v průběhu cvičení po zadání jednotlivých reakcí hráče do programu. Zadavatel ihned vidí odpověď a může hráči ohodnotit, na kolik bodů byla jeho odpověď správná. V případě, že nebyla odpověď úplně správná, vidí bodové ohodnocení, kolik získal bodů z maximálního možného počtu. Hodnocení si zadavatel nastavuje sám, dle svého uvážení a posouzení náročnosti odpovědi na inject.



Obrázek 9 – Ukázka hodnocení cvičení *[Zdroj: vlastní]*

6.6 Vyhodnocení cvičení

Po ukončení cvičení je možné provést jeho výsledné vyhodnocení a konzultaci s jednotlivými účastníky nad jejich reakcemi, případně návrhy na zlepšení. Na obrázku č. 10 vidíme protokol ze cvičení. Můžeme zde vidět název cvičení, jeho popis, datum provedení. Také vidíme, jaká role byla přidělena kterému uživateli a jak si uživatel vedl v průběhu cvičení – bodové hodnocení.

Protokol ze cvičení				
Název cvičení	DP - Dubská			
Popis cvičení a jeho cíle	Simulace ransomwaru v organizaci XY. Totální výpadek organizace. Řešení ze strany organizace a IT organizace Ransomware, příklad, jak se do sítě dostane. Spear-phishing – detekce podezřelého emailu, prevence. Reakce na ransomware v organizaci po technické a procesní stránce			
Datum cvičení	08.04.2021 20:59 - 08.04.2021 21:09			
	Přidělení uživatelé	Bodování	Diskutabilní místa ?	Slabá místa ×
Vedení organizace	Dubská	Počet bodů: 60 z 60 100% Hodnocení akcí: 0 z 0 NaN%	Návrh na zlepšení, aby se situace neopakovala Kroky vedoucí k návratu provozu do stavu před útokem	Návrh na zlepšení, aby se situace neopakovala Kroky vedoucí k návratu provozu do stavu před útokem
IT organizace	Dubská	Počet bodů: 60 z 60 100% Hodnocení akcí: 0 z 0 NaN%		
Komentář ke cvičení				

Obrázek 10 – Protokol ze cvičení *[Zdroj: vlastní]*

7 IDENTIFIKACE PROBLEMATIKY

Tato kapitola je věnována návrhu na možnost dalšího využití softwarového programu PractisGo a laboratoře kybernetické bezpečnosti na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně.

7.1 Dotazníkové šetření

Na základě vytvořeného dotazníku jsem provedla šetření týkající se kybernetické bezpečnosti. Dotazník obsahuje otázky, které zjišťují základní informace o organizaci – velikost a odvětví, ve kterém organizace působí. O tom jak se organizace ke kybernetickému zabezpečení staví, jestli jej považují za důležité, jestli se v organizaci provádí pravidelné školení a pokud ano tak jak často. Další otázka je zaměřena na to, jestli by organizace měla zájem o školení týkajícího se kybernetického bezpečnostního incidentu, které by probíhalo s využitím programového softwaru PractisGo.

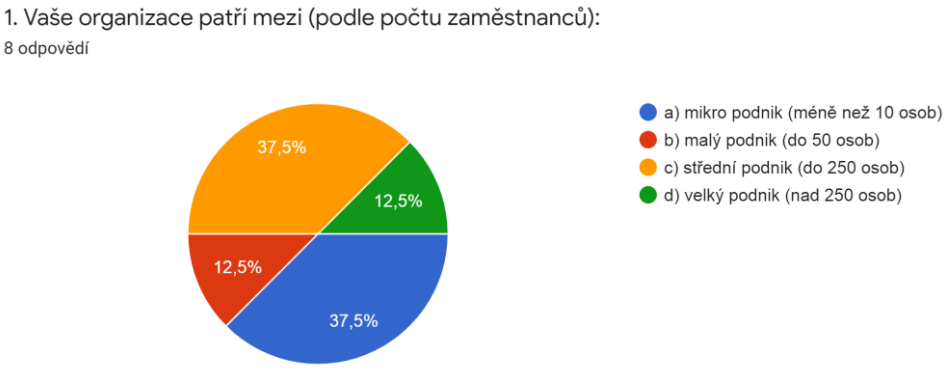
7.2 Vyhodnocení dotazníkového šetření

Dotazníkové šetření bylo prováděno pomocí online dotazníku, který byl rozeslán několika respondentům. Celkově jsem si vytipovala 10 organizací ve svém okolí, které jsou z různých oblastí a jsou různě velké.

Dotazník prozatím vyplnilo 8 organizací. Výsledky ze šetření jsou promítnuty ve formě grafů se slovním a procentuálním popiskem odpovědí respondentů. Analýza zpracovaných odpovědí se nachází níže a je interpretována po jednotlivých otázkách.

Otázka č. 1. – Vaše organizace patří mezi (podle počtu zaměstnanců):

První otázka v dotazníku byla uzavřená. Respondent odpovídal pouze z výběru, zda mikro podnik, malý podnik, střední podnik nebo velký podnik. Otázka sloužila k rozdělení organizací do kategorií – viz graf 1.

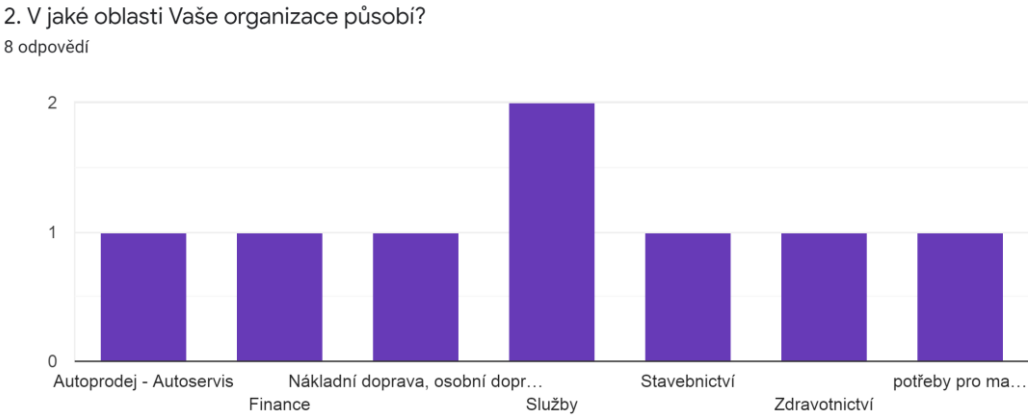


Graf 1 – Velikost podniku *[Zdroj: vlastní]*

Podle výsledků dotazníkového šetření se průzkumu zúčastnilo celkově 8 firem. Stejný byl počet mikro podniků a středních podniků 37,5 %. Malé a velké podniky byly v menším zastoupení 12,5 %.

Otázka č. 2. – V jaké oblasti Vaše organizace působí?

Otázka druhá se zabývá odvětvím, ve kterém dotazovaná organizace působí. Jedná se o otevřenou otázku, kdy každý respondent uvedl odvětví, ve kterém působí – viz graf 2.



Graf 2 – Oblast působení organizace *[Zdroj: vlastní]*

Otázku číslo 2 zodpovědělo 8 organizací. Každá organizace byla úplně z jiného odvětví. Největší zastoupení je z odvětví poskytování služeb, další jsou autoprodej – autoservis, finance, nákladní doprava, osobní doprava, stavebnictví, zdravotnictví a potřeby pro mazlíčky.

Otázka č. 3 – Považujete zajištění kybernetické bezpečnosti ve vaší organizaci za důležité?

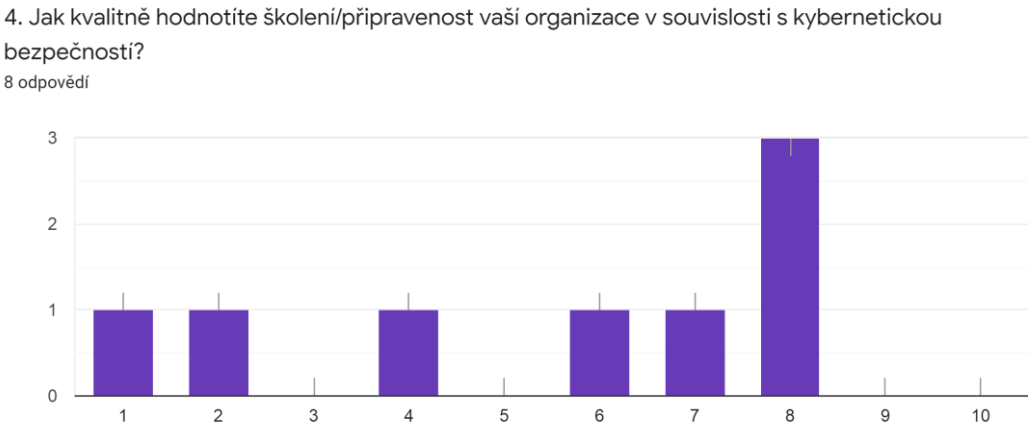
Cílem otázky č. 3 bylo zjistit, za jak moc důležité je považovaná kybernetická bezpečnost v organizacích. Jednalo se o otázku, kde respondenti odpovídali na stupnici od 1 – 10. Hodnota 1 = nejméně důležité, hodnota 10 = velmi důležité. Výsledek viz graf 3.

Graf 3 – Důležitost zajištění KB *[Zdroj: vlastní]*

Graf č. 3 ukazuje výsledky důležitosti kybernetické bezpečnosti v organizacích. Hodnota 8 z 10 je nejčastější odpověď. Z toho vyplývá, že kybernetická bezpečnost v organizacích je považovaná za hodně důležitou.

Otázka č. 4 – Jak kvalitně hodnotíte školení/připravenost vaší organizace v souvislosti s kybernetickou bezpečností?

V otázce č. 4 měli respondenti zvážit a vybrat odpověď na jaké úrovni je školení/připravenost organizace ve spojitosti s kybernetickou bezpečností. Odpovědi respondenti zapisovali na stupnici od 1 – 10. Hodnota 1 = žádna kvalita, hodnota 10 = hodně vysoká úroveň. Výsledek viz graf 4.

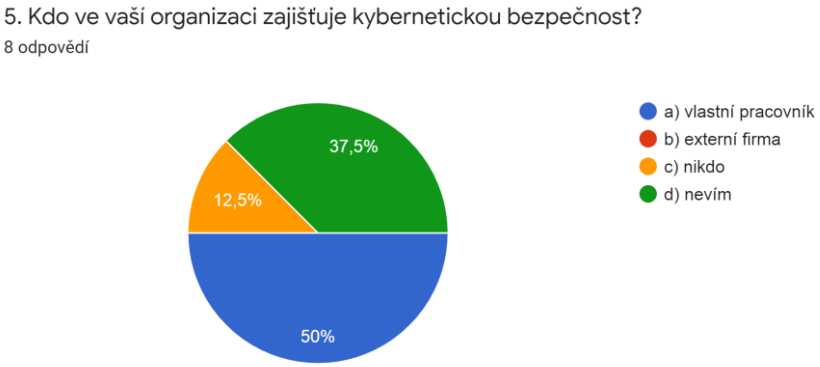


Graf 4 – Kvalita školení/připravenosti *[Zdroj: vlastní]*

Z grafu o kvalitě nebo připravenosti organizace vyplývá, že 3 organizace z 8 dotazovaných považují připravenost/kvalitu kybernetické bezpečnosti za hodně důležitou. Byla ohodnocena 8 body z 10 možných.

Otázka č. 5 – Kdo ve vaší organizaci zajišťuje kybernetickou bezpečnost?

Otázka č. 5 byla zaměřena na to, kdo v organizaci zajišťuje kybernetickou bezpečnost. Respondenti měli na výběr ze čtyř variant – viz graf 5.

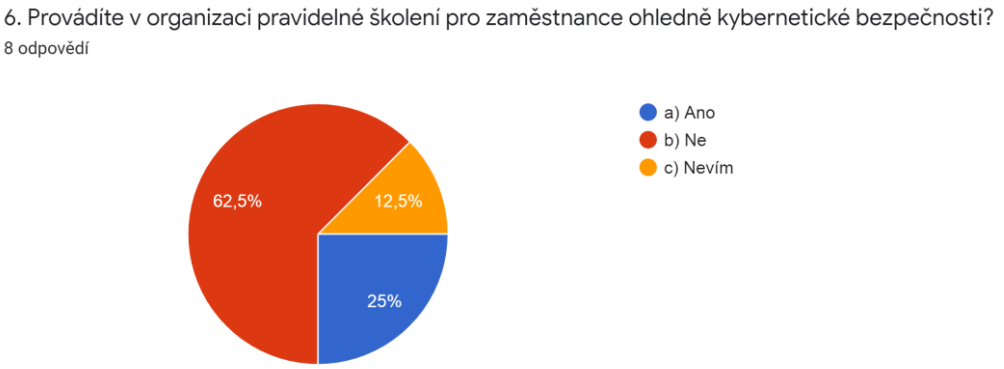


Graf 5 – Poskytovatel KB *[Zdroj: vlastní]*

Na tuto možnost zajišťování kybernetické bezpečnosti odpověděla polovina dotazovaných 50 % – vlastní pracovník. 37,5 % dotazovaných zvolilo odpověď nevím, dalších 12,5 % nikdo.

Otázka č. 6 – Provádíte v organizaci pravidelné školení pro zaměstnance ohledně kybernetické bezpečnosti?

Další otázka v pořadí se respondentů dotazuje na pravidelné školení pro zaměstnance. Respondenti vybírali odpovědi ze tří možností – viz graf 6.



Graf 6 – Pravidelnost školení *[Zdroj: vlastní]*

62,5 % dotazovaných odpovědělo, že se v organizaci neprovádí pravidelné školení zaměstnanců ohledně kybernetické bezpečnosti. 25 % odpovědělo ano a 12,5 % nevím.

Z výše uvedených odpovědí vyplývá, že organizace sice považují kybernetickou bezpečnost za důležitou, ale bohužel neprovádí žádná školení pro zaměstnance. Neznalost zaměstnanců může vést ke vzniku kybernetického útoku v organizaci.

Otázka č. 7 – S jakou periodou je ve vaší organizaci běžný zaměstnanec školen v oblasti kybernetické bezpečnosti?

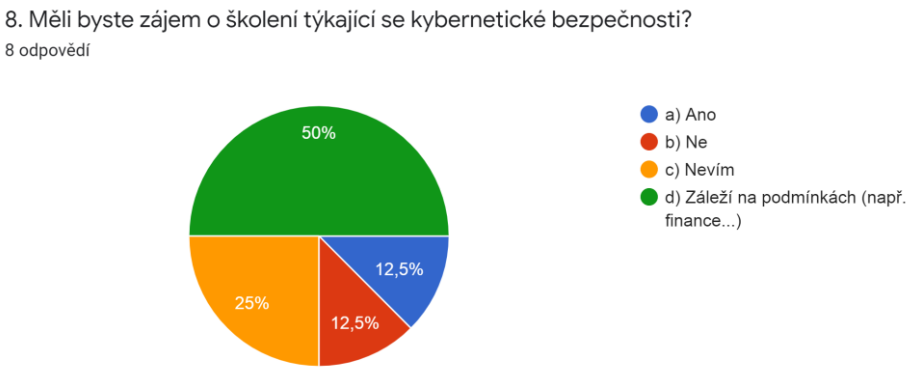
Následující otázka v pořadí, na kterou respondenti odpovídali, byla zaměřena na pravidelnost provádění školení o kybernetické bezpečnosti zaměstnanců v organizaci – viz graf 7. Otázka byla otevřená, respondenti měli za úkol číslem vyjádřit pravidelnost školení v měsících 0 = vůbec.

Graf 7 – Perioda pravidelného školení *[Zdroj: vlastní]*

Již z výše uvedené otázky je jasné, že perioda opakovaného školení je 0, protože se žádné školení zaměstnanců v organizacích nekoná. V 1 organizaci se provádí každý druhý měsíc a v další jednou za půl roku.

Otázka č. 8 – Měli byste zájem o školení týkající se kybernetické bezpečnosti?

Otázka osmá se zabývá zájmem o školení v oblasti kybernetické bezpečnosti. Otázka byla uzavřená a respondenti vybírali ze čtyř možných odpovědí – viz graf 8

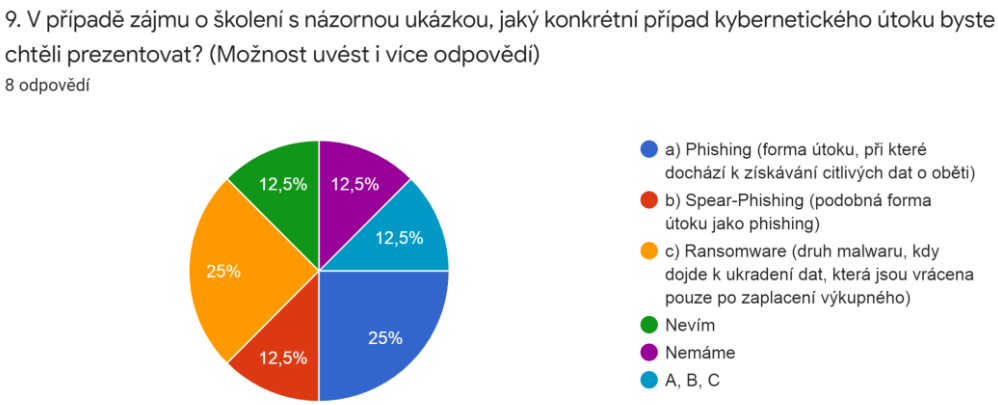


Graf 8 – Zájem o školení *[Zdroj: vlastní]*

Na otázku týkající se zájmu o školení kybernetické bezpečnosti 50 % respondentů odpovědělo, záleží na podmínkách. 25 % zvolilo odpověď nevím a 12,5 % ano a ne.

Otázka č. 9 – V případě zájmu o školení, jaký konkrétní případ kybernetického útoku byste chtěli prezentovat?

Tato otázka navazuje na otázku předchozí. Jedná se o uzavřenou otázku se čtyřmi odpověďmi, kdy jedna z nich je možnost napsání vlastního návrhu odpovědi – viz graf 9.

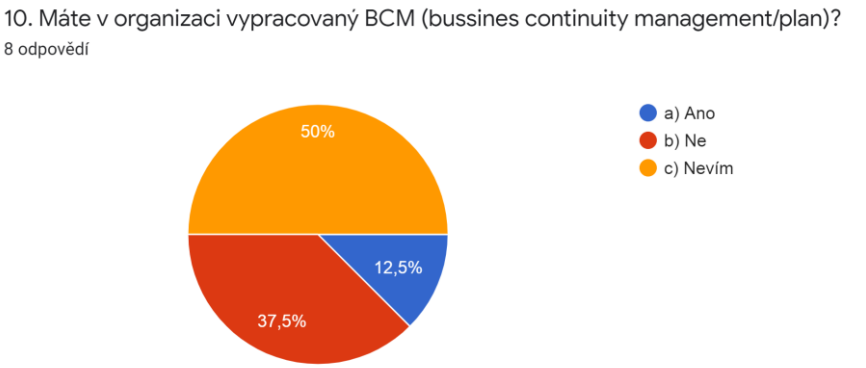


Graf 9 – Druh školení *[Zdroj: vlastní]*

Z grafu č. 9 vyplývá, že největší zájem by byl o školení zaměřené na phishing a ransomware, odpověď zvolilo 25 % respondentů. Odpověď Spear-Phishing zvolilo 12,5 % respondentů. Ostatní respondenti využili možnosti jiné odpovědi. 12,5 % napsalo nevím, dalších 12,5 % napsalo, nemáme. A posledních 12,5 % napsalo možnost A, B, C, takže by mělo zájem o všechny tři typy.

Otázka č. 10 – Máte v organizaci vypracovaný BCM (bussines continuity management/plan)?

Předposlední otázka č 10 zjišťuje, jestli organizace má nebo nemá vypracovaný BCM. Otázka byla uzavřená s možností výběru tří odpovědí – viz graf 10.



Graf 10 – BCM plán *[Zdroj: vlastní]*

Desátá otázka byla věnována tématu BCM. Cílem BCM je tedy předejít negativním jevům nebo alespoň zmírnit jejich následky a co nejrychlejší zajištění obnovy běžného provozu. 50 % respondentů o tomto plánu neví, 37,5 % zvolilo odpověď Ne a pouze 12,5 % zvolilo možnost Ano

Otázka č. 11 – Vlastní sdělení

Poslední otázka v dotazníku, dávala respondentům prostor vyjádřit vlastní názor, připomínku nebo komentář, ať už k dotazníku samotnému, konkrétní otázce nebo ke kybernetické bezpečnosti. Tuto možnost nevyužil nikdo z dotazovaných.

7.3 Návrh cvičení na školení

Z dosavadních výsledků zodpovězených dotazníků vyplývá, že některé dotazované organizace by měly zájem o možnost využití případného školení v laboratoři kybernetické bezpečnosti. Největší zájem se jeví o kybernetický útok pomocí ransomwaru. K tomuto účelu byl vytvořen v programu PractiGo scénář "Ransomware v podniku". Jde

o jednoduchý scénář, který na základě pár kroků vystihuje a dokáže vytvořit účastníkovi představu o tom, jak útok probíhá, kdo všechno a jak musí na incident reagovat.

Ransomware v podniku

Ransomware v podniku je situace, která se může stát jakémukoliv podniku v jakémkoliv odvětví. Scénář, který je vytvořen a následně je na něj provedeno cvičení, vede k ověření návaznosti a správné posloupnosti jednotlivých kroků za sebou. Vybrala jsem si podnik, který má vlastní IT specialisty.

Tabulka 2 – Ransomware v podniku *[Zdroj: vlastní]*

<table>
<tr><th colspan="5">Ransomware v podniku</th></tr>
<tr><td colspan="2">Popis:
Simulace ransomwaru v organizaci. Totální výpadek v organizaci. Řešení ze strany organizace, IT specialisty a uživatele.</td><td colspan="3">Cíl:
• Ransomware (spear-phishing) – detekce podezřelého emailu, prevence.
• Reakce na ransomware v organizaci po technické a procesní stránce.</td></tr>
<tr><td colspan="5">Role ve scénáři:
• Management
• IT specialista
• Uživatel</td></tr>
<tr><th>Inject</th><th>Reakce managementu</th><th>Reakce IT specialistů</th><th>Uživatel</th><th>Nápovědy</th></tr>
<tr><td rowspan="2">Zjištění problému</td><td rowspan="2"></td><td rowspan="2"></td><td>Zjištění zpomalení zařízení</td><td rowspan="2"></td></tr>
<tr><td>Hlášení výskytu problému IT specialistovi</td></tr>
<tr><td rowspan="3">Zašifrování PC pracovníka</td><td rowspan="3"></td><td>Zkoumání rozsahu útoku a co se stalo</td><td></td><td>Co se stalo? Co je zasažené?</td></tr>
<tr><td>Vypnutí sítě a odpojení PC od sítě</td><td></td><td>Odpojení</td></tr>
<tr><td>Informování vedení organizace</td><td></td><td>Tok informací</td></tr>
<tr><td rowspan="2">Veškeré IT v organizaci nefunguje</td><td>Zvažuje další postup zaplatit/nezaplatit</td><td rowspan="2">Pokus o obnovení systému ze zálohy</td><td></td><td>Co se musí bezprostředně po takovém zjištění udělat?</td></tr>
<tr><td>Hledání dalšího</td><td></td><td>Jak vyřešit</td></tr>
</table>

	postupu řešení – vyžádání pomoci třetí strany			vydírání?
IT organizace si není schopna sama zajistit obnovení provozu	Nalezení pomoci třetí strany	Obnovení systému pomocí šifrovacího hesla		Kdo může pomoci?
		Tvorba nového IT systému		
Organizace připravuje ICT infrastrukturu a zaměstnance na vrácení do provozu	Implementace nových bezpečnostních patření	Návrh nových bezpečnostních opatření	Přijetí nových bezpečnostních opatření	Opatření pro posílení kybernetické bezpečnosti
		Obnovení provozu všech IT zařízení		Návrat do normálu

V tabulce č. 2 vidíme rozepsané jednotlivé části scénáře, které byly vloženy do programu PractisGo. V tabulce máme rozepsané jednotlivé injecty – podněty, které ovlivňují vývoj scénáře:

- Zjištění problému.
- Zašifrování PC v kanceláři pracovníka.
- Veškeré IT v organizaci nefunguje.
- IT organizace si není schopné samo zajistit obnovení provozu.
- Organizace připravuje ICT infrastrukturu a zaměstnance na vrácení do provozu.

Následují jednotlivé reakce, ať už ze strany IT specialistů tak samotného managementu organizace nebo uživatele. Scénář také může a nemusí obsahovat nápovědu. Nápověda slouží jako pomůcka pro hráče pokud neví, jak reagovat.

8 NÁVRH CVIČENÍ

Tato kapitola je věnována popisu průběhu cvičení scénáře kybernetického bezpečnostního incidentu. Konkrétně na téma ransomware v organizaci.

8.1 Popis průběhu cvičení

Každý proces musí mít jeden začátek a jeden konec (viz obrázek č. 4) V případě kybernetického útoku je začátek u útočníka, který vytvoří ransomware a zašle ho uživateli, aby získal citlivá data, která následně může zneužít, nebo využít pro vydírání organizace.

Útočník nejčastěji využívá možnost šíření ransomwaru pomocí e-mailové přílohy. Je tu ale i mnoho jiných možností např. nalezení neznámého flash disku s ransomwarem, kdy ho uživatel ze zvědavosti vloží do svého PC a aniž by měl tušení, dochází k šíření ransomwaru.

V případě zaslání ransomwaru e-mailovou přílohou, dochází u uživatele k otevření přílohy a začne probíhat šifrování PC. V tenhle okamžik je důležité a rozhodující, jestli uživatel šifrování a následné zpomalení zaznamená, nahlásí problém IT specialistovi a ten problém začne řešit. Pokud uživatel zpomalení nezaznamená a nenahlásí, dochází k rozšíření na dalších zařízení v síti. U těchto dalších zařízení dochází také ke šifrování a následnému zpomalení PC. A vracíme se zpět k tomu, jestli některý z dalších uživatelů si zpomalení všimne a nahlásí problém nebo ne.

Pokud IT specialista obdrží informaci o problému zpomalení PC, začne hledat příčinu. Dojde k objevení ransomwaru. Informuje management o výskytu ransomwaru. Nařídí vypnutí celé sítě a analyzuje rozsah dotčených zařízení. Po provedené analýze dotčených zařízení dochází k hledání řešení problému.

Mezitím management organizace analyzuje u útočníka požadavky, za jakých podmínek, je ochotný vrátit získaná data. Ve většině případů management dostane od útočníka požadavek na určité výkupné. Zde nastává důležitá otázka pro management, jestli se vyplatí přistoupit na podmínky a zaplatit požadované výkupné nebo hledat jinou možnost řešení a riskovat zveřejnění získaných dat a jejich ztrátu.

Ani v případě, že management přistoupí na podmínky a požadované výkupné útočníkovi zaplatí, není jistota získání dat zpět. V tomhle případě tu máme pořád riziko, zveřejnění dat, nebo poskytnutí dat, která budou poškozená, nebude možné je zpět obnovit a dojde ke ztrátě dat.

IT specialisté po zjištění rozsahu dotčených zařízení, hledají řešení problému. Zde nastává důležitá otázka, jestli organizace provádí pravidelné zálohy a je možnost obnovit data ze zálohy nebo ne.

V případě provádění zálohy, je možnost využití zálohovaných dat. Dalším bodem je to, jestli je IT specialista natolik schopný aby provedl obnovení sám.

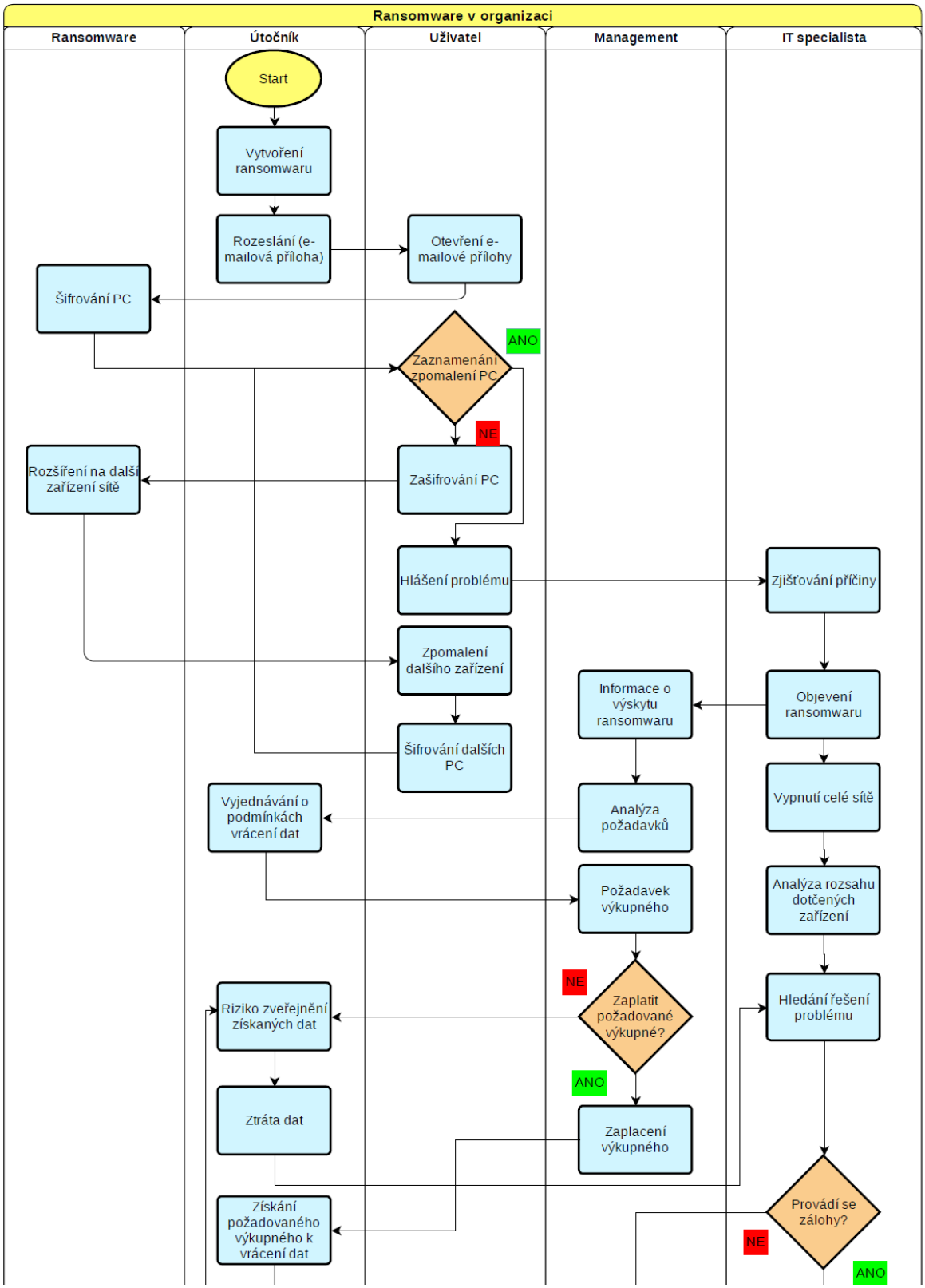
Pokud zálohy neprovádíme, ani IT specialista není schopen provést obnovení ze zálohy sám. Nastává situace vyhledání specializované organizace pro poskytnutí pomoci. Organizace se snaží identifikovat druh ransomwaru. Pokud už nějaký takový druh ransomwaru byl použit, většinou jsou i přístupná hesla pomocí, kterých je možnost ransomwar rozklíčovat a získat data zpět.

Bohužel může nastat i situace, kdy ani organizace se s takovým druhem ransomwaru nesetkala, není schopna poskytnout pomoc a dochází ke ztrátě dat. Jestliže, dojde ke ztrátě dat, organizace nemá jinou možnost, než vytvořit nový IT systém, obnovit provoz a začít vše úplně od začátku.

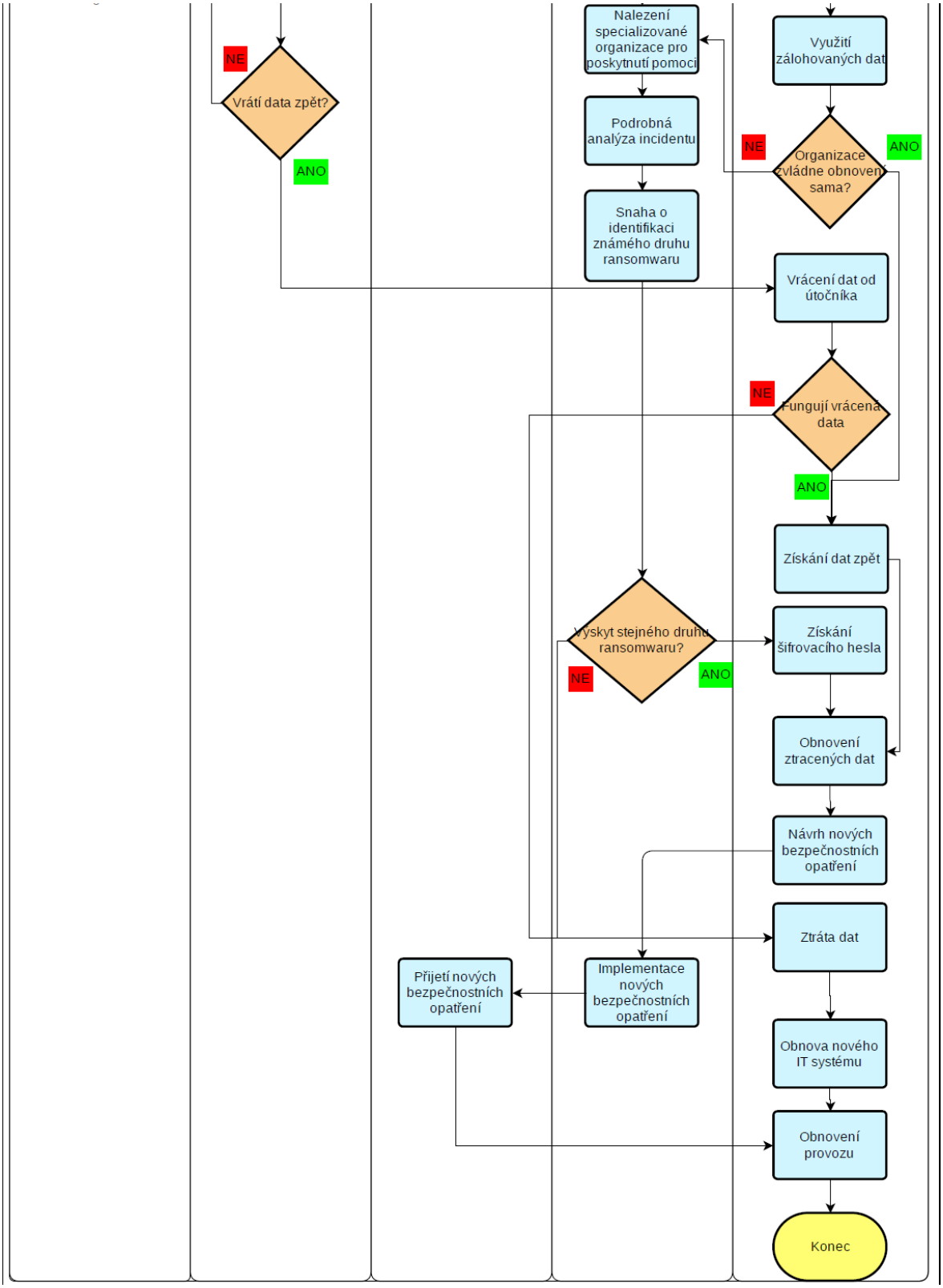
V případě, že specializovaná organizace už s tímto druhem ransomwaru měla zkušenost, poskytne IT specialistovi přístupové heslo, dojde k rozšifrování a obnovení dat ze zálohy. IT specialista po této zkušenosti navrhne nová bezpečnostní opatření. Management organizace provede implementaci nových bezpečnostních opatření a zaměstnanci musí nová bezpečnostní opatření přijmout. Následně dochází k obnovení provozu.

8.2 Algoritmus

Tato kapitola znázorňuje popis průběhu ransomwaru v organizaci. Popis průběhu je vyobrazen pomocí algoritmu, který znázorňuje jednotlivé kroky a reakce jednotlivých účastníků.



Obrázek 11 – Postup průběhu cvičení 1/2 *[Zdroj: vlastní]*



Obrázek 12 – Postup průběhu cvičení 2/2 *[Zdroj: vlastní]*

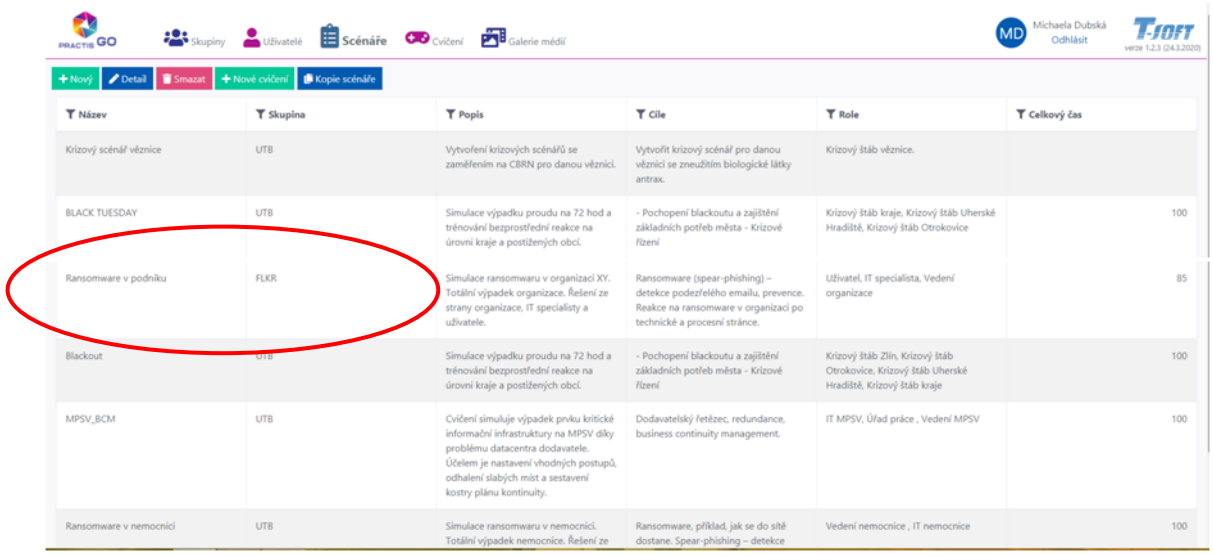
Ne každý kybernetický útok má takto jednoduchý a bezproblémový průběh. Ne všechny organizace, považují za důležité a podstatné zajištění kybernetické bezpečnosti. Důležité je také při tvorbě scénáře brát ohled na to o jak velkou organizaci se jedná. Jestli si kybernetickou bezpečnost a celkové zabezpečení zajišťují samy, nebo na to mají nějakou externí firmu, se kterou spolupracují. Ovlivňuje to také školení zaměstnanců a poučení o tom, že něco takového v organizaci může nastat, jak velké to může mít následky. O co všechno může organizace přijít.

Nikdy není možné vytvořit úplně přesný vývojový diagram, který bude popisovat průběh útoku. Je tu možnost působení dalších externích, ale i interních faktorů, které mohou negativně působit a narušit proces, který směřuje k obnovení provozu, ať už ze zálohy nebo jiným způsobem. Může se jednat např. o výpadek elektrického proudu, při obnovování dat ze zálohy, který přeruší tento proces.

Dále je tu možnost, že uživatel nenahlásí výskyt ihned, ale až po uplynutí nějaké doby, kdy mezitím útočník získá dostatek citlivých informací a může je zneužít ve svůj prospěch většinou pro vydírání managementu při vyjednávání o jejich navrácení.

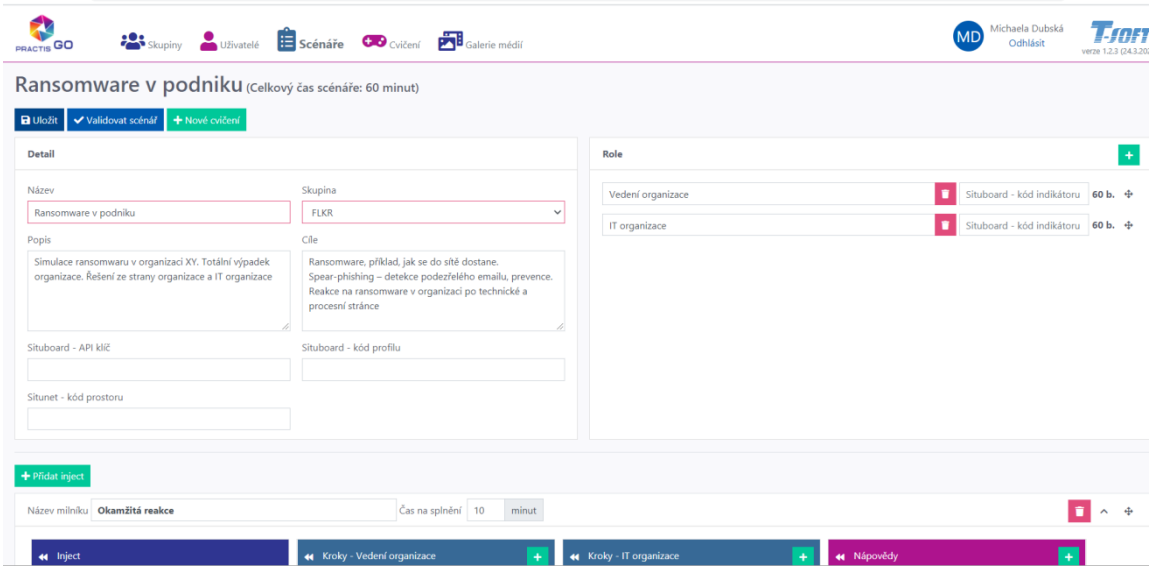
8.3 Ověření vytvořeného cvičení

Obrázek č. 13 ukazuje vytvoření scénář na téma "Ransomware v podniku" v softwarovém programu PractisGo.



Obrázek 13 – Vytvořený scénář v programu *[Zdroj: vlastní]*

Na obrázku č. 14 vidíme ukázku z programu PractisGo. Jedná se o úvodní stránku, která je klíčová pro tvorbu scénáře. Zde se uvádí základní informace k identifikaci scénáře – název, stručný popis, cíl scénáře a vymezení jednotlivých rolí.



Obrázek 14 – Tvorba cvičení *[Zdroj: vlastní]*

SHRNUTÍ

Praktická část diplomové práce se věnuje tvorbě a implementaci scénáře kybernetického bezpečnostního incidentu. K tvorbě scénáře cvičení jsem si vybrala softwarový program PractisGo, který máme v laboratoři kybernetické bezpečnosti na Fakultě logistiky a krizového řízení. Tento program je v laboratoři nový a ne mnoho studentů se s ním mělo možnost setkat. I pro mě to byla novinka. Jsem ráda, že jsem tuhle možnost měla a mohla si vyzkoušet, jak se scénář tvoří a probíhají jednotlivé jeho etapy vývoje.

Abych získala informace pro tvorbu scénáře, vytvořila jsem si dotazník na základě, kterého jsem získala od dotazovaných organizací informace. Informace byly zaměřené na vztah organizace ke kybernetické bezpečnosti. Z dotazníků vyplývá, že ne všechny organizace považují kybernetickou bezpečnost za důležitou. Ani pravidelnost školení, které se řadí mezi velmi důležité, není v organizacích prováděno v nějakých pravidelných cyklech. Zájem organizací o možnost využití případného školení z oblasti kybernetické bezpečnosti o konkrétní druh útoku je závislí na podmínkách, za kterých by školení bylo prováděno.

Z výsledků dotazníkového šetření vyšel ransomware a některé další druhy útoků, jako jeden z nejžádanějších, v případě školení. Já osobně jsem si vybrala ransomware. Pro tvorbu scénáře jsem si vytvořila algoritmus průběhu cvičení. Algoritmus se skládá z 5 účastníků – ransomwar, útočník, uživatel, management organizace a IT specialista. Na základě vytvořeného algoritmu průběhu útoku, jsem vytvořila v softwarovém programu PractisGo cvičení. Cvičení s názvem "Ransomware v organizaci" je k dispozici pro případné zájemce o školení nebo i studenty v laboratoři kybernetické bezpečnosti na Fakultě logistiky a krizového řízení.

ZÁVĚR

Diplomová práce na téma "Scénář řešení kybernetického bezpečnostního incidentu" pro mě byla velmi přínosnou a aktuální. Práce má za cíl rozšířit mé a čtenářovi informace a povědomí o oblasti kybernetické bezpečnosti. V úvodu práce jsem se zaměřila na právní předpisy na území České republiky, které vymezují kybernetickou bezpečnost. Následně jsem se seznámila se mezinárodní normou ISO 27000, která zajišťuje přehled o systému řízení bezpečnosti informací, které tvoří skupinu norem systému řízení bezpečnosti informací (ISMS) a vymezuje související termíny. Po vymezení právních předpisů a mezinárodních norem jsem se zaměřila na organizace a instituce, které působí na území České republiky a pracují na zajištění kybernetické bezpečnosti. Jedná se o 4 instituce – Národní úřad pro kybernetickou a informační bezpečnosti, CERT a CSIRT a Národní bezpečnostní úřad. Všechny tyto organizace se ať už z větší nebo menší části věnují kybernetické bezpečnosti. Dále jsem se musela seznámit se základními pojmy kybernetické bezpečnosti. Oblast kybernetické bezpečnosti je velmi bohatá na specifické pojmy ze své oblasti. Všechny pojmy z oblasti kybernetické bezpečnosti můžeme najít ve výkladovém slovníku kybernetické bezpečnosti, ze kterého jsem čerpala a vybrala si dle svého názoru ty nejdůležitější pojmy.

Oblast kybernetické bezpečnosti obsahuje velké množství hrozeb. Jednou z nich je malware. Malware má mnoho druhů a podob, se kterými se můžeme setkat. Pro lepší orientaci a přehled v této oblasti jsem se seznámila s jednotlivými druhy, které jsem si dle různých analýz. Analýzy se týkaly malware a popisovaly ty nejznámější a nejčastěji používané druhy. V souvislosti s malware je důležité se také zaměřit na bezpečnostní systémy. Bezpečnostní systémy se využívají pro předcházení vzniku kybernetického bezpečnostního incidentu.

Pro lepší orientaci v problematice kybernetické bezpečnosti je vhodné si ujasnit a vymezit rozdíl mezi dvěma na první pohled pro někoho stejnými pojmy – kybernetický bezpečnostní incident a kybernetickou bezpečnostní událostí. Také je dobré znát druhy kybernetických bezpečnostních incidentů, popis možných opatření a jak jim předcházet. V poslední řadě, také nesmí chybět popis průběhu kybernetického bezpečnostního incidentu.

Diplomová práce se zaměřovala na scénář kybernetického bezpečnostního incidentu a provedení následné implementace pomocí vybraného simulátoru. Pro vytvoření scénáře

jsem si vybrala softwarový program PractisGo, který vlastní laboratoř kybernetické bezpečnosti na Fakultě logistiky a krizového řízení. Abych se lépe orientovala v programu a rozuměla jednotlivým postupů a názvům musela jsem se seznámit se základními pojmy, které se při práci se softwarovým programem využívají. Před tvorbou cvičení jsem si navrhla a vytvořila jednoduchý dotazník. Dotazník byl zaměřen na analýzu problematiky kybernetické bezpečnosti v organizacích. Cílem dotazníku bylo zjistit jak moc je pro jednotlivé organizace kybernetická bezpečnosti důležitá, jestli provádí v této oblasti nějaké pravidelné školení. Dále mě také zajímal zájem organizací o případnou možnost využití školení v laboratoři kybernetické bezpečnosti s názornou ukázkou. Výsledky dotazníku mě vedli k tvorbě scénáře. Tvorba scénáře probíhala podle předem vlastního vytvořeného algoritmu. Algoritmus obsahuje několik možností, jak lze útok řešit. Scénář jsem vytvořila ve vybraném programu PractisGo. Softwarový program je součástí laboratoře kybernetické bezpečnosti na Fakultě logistiky a krizového řízení. Mnou vytvořený scénář může dál sloužit buď k využití případného školení, ale také pro další studenty při výuce předmětu Aplikovaná kybernetická bezpečnost v rámci navazujícího magisterského studia na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Na základě výše uvedeného považují cíle diplomové práce za splněné.

SEZNAM POUŽITÉ LITERATURY

ANDRESS, Jason a Steve WINTERFELD, 2011. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* [online]. United States of America: Elsevier [cit. 2020-11-22]. ISBN 978-1-59749-637-7. Dostupné z: http://index-of.es/Hack/Cyber%20Warfare.pdf

AWAD, Ali Ismail a Machael FAIRHUST, 2018. *Information security : foundations, technologies and applications* [online]. London: Institution of Engineering & Technology [cit. 2020-11-22]. ISBN 978-1-84919-976-6.

Bezpečnost standardně a trochu praxe [online], b.r. In: . [cit. 2021-01-20]. Dostupné z: https://is.muni.cz/el/1433/podzim2007/PA168/um/LNovak_MU_Bezpecnost.pdf

Bezpečnostní normy, 2020. *Bezpečnostní normy* [online]. Kybez, Platforma kybernetické bezpečnosti [cit. 2020-11-08]. Dostupné z: https://www.kybez.cz/bezpecnost/normy

CICHONSKI, Paul et al., 2011. Computer Security Incident Handling Guide. In: *National Institute of Standards and Technology* [online]. [cit. 2020-11-13]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cryptojacking – What is it?, 2021. *Alwarebytes* [online]. [cit. 2021-04-09]. Dostupné z: https://www.malwarebytes.com/cryptojacking/

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

ČESKO, 2014. Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů České republiky*. Zákony pro lidi. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

ČESKO, 2017. Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby. In: *Sbírka zákonů České republiky*. Zákony pro lidi. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-437

ČESKO, 2018. Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Zákony pro lidi. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

ČSN ISO/IEC 27000, 2021. *KYBEZ: Platforma kybernetické bezpečnosti* [online]. GORDIC [cit. 2021-01-23]. Dostupné z: https://www.kybez.cz/bezpecnost/iso-2700-2

ČSN ISO/IEC 27001, 2021. *Kybez: Platforma kybernetické bezpečnosti* [online]. GORDIC [cit. 2021-01-23]. Dostupné z: https://www.kybez.cz/bezpecnost/iso-2700-2

HROMADA, Martin et al., 2015. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint. ISBN 978-80-87994-72-6.

HRŮZA, Petr, 2012. *Kybernetická bezpečnost*. Brno: Univerzita obrany. ISBN 978-80-7231-914-5.

IDS/IPS, 2014. *DataCom* [online]. [cit. 2021-02-23]. Dostupné z: https://www.datacom.cz/piktogramy/ids-idp/

IDS: základní informace, 2007. *Computerworld* [online]. [cit. 2021-02-23]. Dostupné z: https://computerworld.cz/securityworld/ids-zakladni-informace-46154

IPS/IDS ochrana, 2015. *Jak na webové stránky* [online]. [cit. 2021-02-23]. Dostupné z: http://timehosting.cz/ipsids-ochrana/

ISO 27001: Management bezpečnosti informací, b.r. *ISO.CZ* [online]. [cit. 2020-11-29]. Dostupné z: http://www.iso.cz/iso-27001

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

KLEMENSOVÁ, Ing. Anežka, b.r. *PractisGo: Uživatelský a metodický manuál*.

KOLOUCH, Jan, 2016. *CyberCrime*. Praha: CZ.NIC. ISBN 978-80-88168-18-8.

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

Legislativa KB, b.r. *Legislativa* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-11-07]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

Legislativa: Legislativa kybernetické bezpečnosti CR, 2020. *ACS office* [online]. [cit. 2020-11-29]. Dostupné z: https://acsoffice.cz/kyberneticka-bezpecnost/legislativa/

LUKÁŠ, Luděk, 2017. *Teorie bezpečnosti I.* [online]. Zlín: Radim Bačuvčík - VeRBuM [cit. 2020-11-17]. ISBN 978-80-87500-89-7. Dostupné z:

https://ndk.cz/view/uuid:0f27a380-fbe5-11ea-9c2e-005056827e51?page=uuid:1d095d3c-41f2-4673-b566-74d73cd15769

MLÝNEK, Jaroslav, 2007. *Zabezpečení obchodních informací*. Brno: Computer Press. ISBN 978-80-251-1511-4.

Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025, 2020. In: *Strategie/Akční plán* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-11-07]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

NCKB, b.r. *Kybernetická bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-11-08]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/

NÚKIB, b.r. *O NÚKIB* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-11-08]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

O nás, b.r. *O NBÚ* [online]. Národní bezpečnostní úřad [cit. 2020-11-08]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

O týmu CSIRT.CZ, b.r. *O nás* [online]. CSIRT.CZ [cit. 2020-11-08]. Dostupné z: https://www.csirt.cz/cs/o-nas/

PAČKA, Roman, 2019. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Brno: Centrum pro studium demokracie a kultury. Politologická řada. ISBN 978-80-7325-473-5.

PETERKA, Martin, 2011. Role a počet bezpečnostních týmů rostou. Co o nich ale víme?. *Články* [online]. Lupa.cz [cit. 2020-11-08]. Dostupné z: https://www.lupa.cz/clanky/role-a-pocet-bezpecnostnich-tymu-rostou-co-o-nich-ale-vime/

Pharming, 2020. *Malwarebytes* [online]. [cit. 2020-11-17]. Dostupné z: https://www.malwarebytes.com/pharming/

Phishing, b.r. *ESET* [online]. [cit. 2020-11-17]. Dostupné z: https://www.eset.com/cz/phishing/

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

SAK, Petr, 2018. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. [Praha]: Petrklíč. ISBN 978-80-7229-652-1.

SINGER, P. W. a Allan FRIEDMAN, 2014. *Cybersecurity and cyberwar: What everyone needs to know* [online]. New York: Oxford University Press [cit. 2020-11-11]. ISBN 978-019-9918-096. Dostupné z: https://is.muni.cz/el/1423/podzim2018/BSS469/um/P.W._Singer__Allan_Friedman_-_Cybersecurity_and_Cyberwar__What_Everyone_Needs_to_Know___2014__Oxford_University_Press_.pdf

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

SQL vs. XXS Injection Attacks Explained, 2018. *Keirstenbrager* [online]. [cit. 2020-11-22]. Dostupné z: https://www.keirstenbrager.tech/sql-vs-xxs-injection-attacks-explained/

Standardy a definice pojmů bezpečnosti informací, 2011. In: *Příspěvky a publikace* [online]. Cybersecurity.cz [cit. 2020-11-07]. ISBN 978-80-7251-356-7. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

What Is Spear Phishing?, 2021. *TERRANOVA SECURITY* [online]. Terranova Worldwide Corporation [cit. 2021-04-15]. Dostupné z: https://terranovasecurity.com/what-is-spear-phishing/

Základní pojmy, 2020. In: *KYBEZ* [online]. [cit. 2020-11-30]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

Zero-Day Vulnerability, 2014. K SOOD, Aditya a Richard ENBODY. *Targeted Cyber Attacks* [online]. Syngress [cit. 2020-11-22]. ISBN 978-0-12-800604-7. Dostupné z: https://www.sciencedirect.com/topics/computer-science/zero-day-vulnerability

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BCM	Bussines Continuity Management – Řízení kontinuity činností organizace
CERT	Computer Emergency Response Team – Tým pro nouzové reakce na počítači
CIA	Confidentiality (důvěrnost)
	Integrity (celistvost)
	Availability (dostupnost)
CSIRT	Computer Security Incedent Response Team – Tým reakce na incidenty v oblasti počítačové bezpečnosti
ČR	Česká republika
ČSN	Česká technická norma
DDOS	Distributed Denial of Service
EU	Evropská unie
ICT	Informační a komunikační technologie
IDS	Intrusion Detection System – systém detekce narušení.
IDSP	Intrusion Detection and Prevention Systems – systém odhalení a prevence proniknutí.
IPS	Intrusion Prevention Systems – systém prevence proniknutí
ISMS	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
IT	Informační technologie
KB	Kybernetická bezpečnost
KBI	Kybernetický bezpečnostní incident
NATO	North Atlantic Treaty Organization – Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Počítač

PDCA Plan – plánuj,

Do – dělej,

Check – kontoluj,

Act – jednej

SIEM Security Information and Event Management – nástroj pro správu bezpečnostních informací a událostí organizace

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Dobrý den,

jmenuji se Bc. Michaela Dubská a jsem studentka Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně. Studuji obor Bezpečnost společnosti. Píši diplomovou práci na téma Scénář řešení kybernetického bezpečnostního incidentu.

Tento dotazník má za cíl analyzovat vztah organizací ke kybernetické bezpečnosti. Poslouží ke zjištění zájmu o případná školení prostřednictvím Laboratoře kybernetické bezpečnosti na Fakultě logistiky a krizového řízení.

Výsledky tohoto dotazníku mi pomohou k vyhodnocení situace v organizacích. Také bude sloužit jako podklad pro případnou možnost vzniku školení v oblasti kybernetické bezpečnosti.

Předem Vám moc děkuji za váš čas věnovaný vyplňování dotazníku

Bc. Michaela Dubská

1. Vaše organizace patří mezi (podle počtu zaměstnanců):
   a) Mikro podnik (méně než 10 osob)
   b) Malý podnik (do 50 osob)
   c) Střední podnik (do 250 osob)
   d) Velký podnik (nad 250 osob)
2. V jaké oblasti Vaše organizace působí?

   volná odpověď

3. Považujete zajištění kybernetické bezpečnosti ve vaší organizaci za důležité?

   Hodnocení 1-10,

   1 – nejméně důležité, 10 – hodně důležité

4. Jak kvalitně hodnotíte školení/připravenost vaší organizace v souvislosti s kybernetickou bezpečností?

   Hodnocení 1-10,

   1 – žádná kvalita, 10 – hodně vysoká úroveň

5. Kdo ve vaší organizaci zajišťuje kybernetickou bezpečnost?
   a) Vlastní pracovník
   b) Externí firma
   c) Nikdo
   d) Nevím
6. Provádíte v organizaci pravidelné školení pro zaměstnance ohledně kybernetické bezpečnosti?
   a) Ano
   b) Ne
   c) Nevím

7. S jakou periodou je ve Vaší organizaci běžný zaměstnanec školen v oblasti kybernetické bezpečnosti (v měsících, 0= vůbec)

vlastní odpověď

8. Měli byste zájem o školení týkající se kybernetické bezpečnosti?

a) Ano
b) Ne
c) Nevím
d) Záleží na podmínkách (finance...)

9. V případě zájmu o školení, jaký konkrétní případ kybernetického útoku byste chtěli prezentovat? (Možnost uvést i více odpovědí)

a) Phishing (forma útoku, při které dochází k získávání citlivých dat o oběti)
b) Spear-Phishing (podobná forma útoku jako phishing)
c) Ransomware (druh malwaru, kdy dojde k ukradení dat, která jsou vrácena pouze po zaplacení výkupného)
d) jiná možnost (vlastní návrh)

10. Máte v organizaci vypracovaný BCM (bussines continuity management/plan)?

a) Ano
b) Ne
c) Nevím

11. Vlastní sdělení

možnost vlastních připomínek, komentářů….