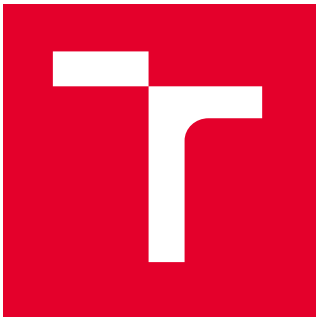


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE TABLE TOP CVIČENÍ DO UNIVERZITNÍHO PROSTŘEDÍ

IMPLEMENTATION OF TABLE TOP EXERCISES IN A UNIVERSITY ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Sára Juricová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Sára Juricová**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2023/24
Studijní program:	Informační management

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

Implementace Table Top cvičení do univerzitního prostředí

Charakteristika problematiky úkolu:

Úvod
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je navrhnout a implementovat Table Top cvičení do univerzitního prostředí.

Základní literární prameny:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně dne 4.2.2024

L. S.

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

Abstrakt

Táto diplomová práca sa zaoberá tvorbou simulačných cvičení na základe poskytnutého kybernetického incidentu s využitím techniky využívanej v hernom prostredí pre vrcholový manažment za účelom otestovania ich reakčných a kolaboračných schopností. V práci sú predstavené ciele, stratégia a tvorba simulačného cvičenia. Analyzuje sa prostredie univerzity, riziká, konkrétny incident a vyhodnocuje finančný plán projektu.

Kľúčové slová

table top cvičenie, simulačné cvičenia, kybernetická bezpečnosť, kybernetický incident, riziko, vrcholový manažment

Abstract

This thesis deals with the creation of simulation exercises based on a provided cyber incident, using techniques employed in the gaming environment for top management in order to test their response and collaboration skills. The work presents the objectives, strategy, and creation of the simulation exercise. It analyzes the university environment, risks, a specific incident, and evaluates the financial plan of the project.

Keywords

table top exercise, simulation exercises, cyber security, cyber incident, risk, top management

Bibliografická citace

JURICOVÁ, Sára. *Implementace Table Top cvičení do univerzitního prostředí* [online]. Brno, 2024 [cit. 2024-05-11]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/158747. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácie použitých prameňov sú úplné, že som vo svojej práci vedome neporušila autorské práva (v zmysle zákona č. 121/2000 Zb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 13. 5. 2024

Bc. Sára Juricová

autor

Poďakovanie

Ďakujem vedúcemu svojej diplomovej práce, pánovi Ing. Petrovi Sedlákovi, za odborné vedenie, zhovievavosť a užitočné rady pri spracovaní tejto práce. Ďalej by som rada poďakovala Matejovi Zápotočnému a Vojtechovi Sommerovi za spoluprácu a rady pri tvorení cvičenia a v neposlednom rade, svojej rodine za veľkú podporu po celý čas môjho štúdia.

OBSAH

ÚVOD

Aktuálne sa začína klásť vysoký dôraz na bezpečnosť vo firmách. Pravda je častokrát taká, že firmy zaplatia externým spoločnostiam, vytvoria si smernice a politiky, avšak aktívne neaplikujú tieto vedomosti do fungovania firmy. Stále sa vyvíjajúce nároky na efektívne vzdelávanie a rozvoj zručností v modernom svete zdôrazňujú potrebu inovatívnych a interaktívnych metód vzdelávania. Jedným z týchto prístupov, ktorý naberá na popularite, je použitie table top cvičení. Tieto cvičenia predstavujú simulované scény alebo situácie, ktoré umožňujú účastníkom prakticky riešiť problémy, spolupracovať a zlepšovať svoje zručnosti a rozhodovacie procesy. Sú to často realistické, významné a dynamické situácie, ktoré poskytujú účastníkom príležitosť využiť svoje schopnosti a znalosti na riešenie komplexných úloh.

Cieľom tejto diplomovej práce je ukázať, ako môže byť table top cvičenie účinným nástrojom v rôznych oblastiach vzdelávania a profesionálneho rozvoja. Zameriame sa na návrh, vytváranie a aplikáciu takýchto cvičení s dôrazom na ich prínosy pre účastníkov. Okrem toho bude analyzovať, aký vplyv majú table top cvičenia na zlepšenie rozhodovacích procesov, tímovej spolupráce a riešenia problémov.

1 METÓDY SPRACOVANIA A CIEĽ

1.1 Cieľ práce

Cieľom tejto práce je na základe analýzy predošlých incidentov a analýzy rizík navrhnúť, vytvoriť a aplikovať simulačné cvičenia „table top“, ktoré budú slúžiť ako efektívny nástroj na vzdelávanie a profesionálny rozvoj vrcholového manažmentu organizácie. Konkrétne sa budeme snažiť dosiahnuť nasledujúce ciele:

1. **Vytvorenie univerzálneho cvičenia** - Cvičenie by malo byť možné použiť na viacero škôl s menšími úpravami. Cvičenie bude interaktívne, ale stále relevantné pre konkrétnu záujmovú skupinu.
2. **Návrh riešenia –** Návrh riešenia sa prispôsobí incidentu, ktorý sa na univerzite odohrával v minulosti, aby účastníci pochopili relevantnosť cvičení.
3. **Otestovanie riešenia v praxi** - Vytvorenie reálnej situácie so zámerom otestovať funkčnosť cvičenia.
4. **Vyhodnotenie riešenia –** Ako efektívni sme s cvičením boli, či prinieslo pridanú hodnotu a akým spôsobom univerzita reagovala na cvičenie.

1.2 Diplomová práca nezahŕňa

Táto diplomová práca sa nezameriava na vytváranie komplexných softvérových simulácií, či na technické aspekty vytvárania hardvérových modelov. Taktiež nebudeme podrobne riešiť psychologické alebo pedagogické aspekty vzdelávania, ako napríklad vývoj výučbových osnov či osobnostný rozvoj účastníkov. Nezaoberá sa doslovným znením politík ani materiálov použitých pri tvorbe školenia. Práca je zároveň metodologickou príručkou pre budúcu tvorbu iných table top cvičení. Nezahŕňa taktiež celkovú analýzu rizík univerzity - venuje sa čiastočnej analýze relevantnej pre vytvorenie table top cvičenia.

1.3 Metódy spracovania

Pri spracovaní diplomovej práce bola využitá literatúra a jej rešerš. Analýza existujúcich štúdii, článkov, zdrojov na tému table top cvičení. Následne dotazníky

a ankety, kvalitatívne rozhovory vo firemnom prostredí, analýza výsledkov a využitie výpočtových metód a prípadové štúdie na tému table top cvičení.

2 TEORETICKÉ VÝCHODISKA PRÁCE

V časti „Teoretické východiska práce“ budú uvedené pojmy, ktoré budú boli využívané počas analýzy a praktickej časti tejto práce. Pomocou tejto kapitoly začleníme riešenú problematiku do teoretickej sféry.

2.1 Aktívum

Termín "aktívum" sa v kontexte seminárnej práce používa na označenie všetkých hodnôt, majetkov alebo prostriedkov, ktoré organizácia, osoba alebo univerzita vlastní, má hodnotu alebo ktoré majú potenciál vytvoriť hodnotu alebo príjem v budúcnosti. Aktíva môžu zahŕňať rôzne položky, ako sú nehnuteľnosti, inventár, patenty, licencie, ale aj informácie alebo procesy využívané na chod univerzity. Sú to v podstate zdroje, ktoré majú hodnotu a môžu byť využité na generovanie hodnoty. (1)

Aktíva delíme na hmotné a nehmotné. Každé aktívum je ohodnotené z hľadiska dôvernosti, dostupnosti a integrity. (1)

2.1.1 Dôvernosť

Dôvernosť sa zameriava na zabezpečenie toho, že informácie sú dostupné iba pre oprávnené osoby alebo entity. Tento koncept zahrňuje ochranu citlivých informácií pred neoprávneným prístupom, aby sa zabránilo úniku dôležitých dát alebo porušeniu dôvernosti. Dôvernosť sa týka nielen elektronických dát, ale aj fyzických dokumentov a komunikácie. (2)

Implementácia dôvernosti zahŕňa bezpečnostné opatrenia, ako sú autentizácia, autorizácia, šifrovanie a správa prístupových práv. Je to nevyhnutné pre ochranu citlivých osobných údajov, obchodných tajomstiev a iných dôležitých informácií, ktoré by nemali byť dostupné pre neoprávnené subjekty. (2)

2.1.2 Dostupnosť

Dostupnosť je kritickým aspektom informačnej bezpečnosti. Zameriava sa na to, aby informačné systémy, dáta a služby boli k dispozícii pre autorizovaných užívateľov v

požadovanom čase a bez výpadkov. Tento koncept je nevyhnutný nielen pre podniky a subjekty, ale aj pre verejný sektor a kritickú infraštruktúru, pretože výpadky alebo nedostupnosť dôležitých systémov môžu mať závažné následky.

Dostupnosť je jedným zo základných princípov informačnej bezpečnosti, ktorý zabezpečuje, že systémy sú odolné voči rôznym typom hrozieb, vrátane kybernetických útokov, prírodných katastrof alebo ľudských chýb. Dôležité je tiež zabezpečiť pravidelné zálohovanie dát, vytváranie plánov obnovy po havárii a implementáciu opatrení na udržanie dostupnosti systémov. (2)

2.1.3 Integrita

Zachovanie integrity znamená, že dáta a informácie zostávajú nedotknuté, nedostupné pre neautorizovaných ľudí a nepodliehajú neoprávneným zmenám či znehodnoteniu. Táto ochrana je nevyhnutná pre správne fungovanie informačných systémov a dôvernosť dát.

Integrita zahŕňa viacero opatrení, ako je zabezpečenie, že dáta nie sú poškodené alebo zmenené v dôsledku chýb, útokov alebo iných nežiaducich udalostí. Okrem toho je dôležité mať aj mechanizmy na overovanie autentickosti a celistvosti dát, napríklad digitálne podpisy a hashovacie funkcie. Zabezpečenie integrity je nevyhnutnou súčasťou celkovej bezpečnostnej stratégie organizácií a zaručuje, že informácie zostanú dôveryhodné a spoľahlivé. (2)

2.1.4 Vlastník aktíva

Vlastník, alebo garant aktíva, je zodpovedný za monitorovanie, hodnotenie a riadenie bezpečnostných aspektov týchto aktív s cieľom zabezpečiť ich ochranu a dôvernosť.

Garant aktíva môže v organizácii zabezpečiť, že aktíva sú správne identifikované, klasifikované a chránené na základe ich dôležitosti a hodnoty pre organizáciu. To zahŕňa implementáciu bezpečnostných politík, postupov a technických opatrení, ako aj sledovanie, auditovanie a reagovanie na potenciálne riziká. (3)

2.2 Traffic Light Protocol

Traffic Light Protocol (TLP) je systém klasifikácie informácií, ktorý sa používa v oblasti kybernetickej bezpečnosti a spravovania informácií. Bol vydaný americkou inštitúciou CISA. TLP kategorizuje informácie podľa ich dôvernosti a dostupnosti a pomáha pri riadení a zdieľaní citlivých informácií v bezpečnostných a spravovacích procesoch. (4)(5)

Klasifikácia je rozdelená na štyri stupne podľa striktnosti používania informácii (4)(5):

1. **Red (Červená)** - Informácie s touto klasifikáciou sú najdôvernejšie. Tieto informácie by mali byť zdieľané len so subjektami, ktoré majú oprávnený dôvod na ich získanie. Zvyčajne ide o informácie, ktoré by mohli ohroziť národnú bezpečnosť alebo súvisia s veľmi citlivým obsahom firmy.
2. **Amber (Oranžová)** - Informácie s touto klasifikáciou sú dostupné obmedzene, ale môžu byť zdieľané s istou skupinou subjektov, ktorí majú oprávnenie k ich prístupu. Ide o informácie, ktoré majú významnú hodnotu, ale nie sú tak kritické ako informácie označené červenou farbou.
3. **Green (Zelená)** - Informácie s touto klasifikáciou sú dostupné pre širokú skupinu subjektov a nemajú obvykle žiadne obmedzenia na ich zdieľanie. Ide o informácie, ktoré sú verejného charakteru alebo nemajú významné bezpečnostné následky v prípade ich uniknutia.
4. **White (Biela)** - White je špeciálna klasifikácia, ktorá sa používa v kontexte TLP na informácie, ktoré nemajú žiadne obmedzenia. Tieto informácie môžu byť zdieľané voľne a nevyžadujú dodatočnú kontrolu.

2.3 Hrozba

Hrozba označuje potenciálny nebezpečný faktor alebo udalosť, ktorá môže ohroziť informačné systémy, dáta alebo aktíva univerzity, ktorá môže mať následok poškodenia organizácie a jej aktív. Hrozby môžu byť rôznorodé, či už ide o kybernetické útoky, prirodzené katastrofy, alebo iné nebezpečenstvá. Identifikácia a klasifikácia

hrozieb je dôležitá pre riadenie rizík a umožňuje organizáciám na základe ich závažnosti vysporiadať sa s rizikom. (5)

Norma ISO 27005(6) opisuje pôvod hrozby nasledovne:

- (D) úmyselné
- (A) náhodné
- (E) environmentálne

2.4 Zraniteľnosť

Zraniteľnosť je nedostatok alebo slabé miesto, ktorá môže byť zneužitá hrozbami na spôsobenie útokov. Zraniteľnosti môžu mať rôzne podoby, vrátane softvérových chýb, nedostatočnej konfigurácie systémov, zlých bezpečnostných postupov alebo fyzických slabín. Identifikácia a správa zraniteľností sú dôležité pre predchádzanie bezpečnostným incidentom. (2)

V Európe je tento kybernetický problém riešený pomocou dvoch noriem ISO/IEC.

ISO/IEC 29184:2020 *Norma poskytuje dodávateľom požiadavky a odporúčania týkajúce sa odhalenia zraniteľných miest. Zverejnenie chýb pomáha užívateľom optimalizovať ochranu a lepšie hodnotiť ochranu ich systémov a údajov (podľa špecifikácie normy ISO/IEC 27002). Cieľom odhalenia zraniteľnosti je znížiť riziko spojené s využívaním zraniteľnosti. Koordinované odhalenie zraniteľnosti je obzvlášť dôležité v dodávateľskom reťazci.* (7)

ISO/IEC 30111:2020 *Táto medzinárodná norma obsahuje smernice, ako postupovať pri zverejňovaní informácií o potenciálnych zraniteľnostiach v produktoch alebo online službách. Je vhodná pre predajcov (dodávateľov). Táto norma je určená tiež pre spotrebiteľov, vývojárov, predajcov (dodávateľov) a hodnotiteľov bezpečných ICT produktov.* (7)

2.5 Riziko

Riziko opisuje možnosti, kde sa môže vyskytnúť nejaký nepriaznivý alebo nežiadúci jav, ktorý ovplyvní činnosť alebo výsledok udalosti. V kontexte informačnej

bezpečnosti zahrňuje riziko možné hrozby, zraniteľnosti a potenciálne následky pre všetky aktíva. Riziko vzniká pôsobením aktíva a hrozby navzájom. **Úroveň rizika** je možné získať hodnotou aktíva. Jej úroveň sa dá znižovať protiopatreniami. (1)

Identifikácia, hodnotenie a riadenie rizík sú kľúčovými procesmi a pomáhajú subjektom identifikovať potenciálne hrozby a následky ich realizácie. Na základe tejto analýzy môžu prijať opatrenia na minimalizáciu rizika, napríklad implementovaním bezpečnostných opatrení alebo vypracovaním plánov obnovy po havárii. (2)

2.6 Analýza rizík

Analytický proces identifikácie a hodnotenia rizík sa začína určením, ktoré aktíva sú zásadné pre organizáciu a jej fungovanie. Hlavným cieľom je rozpoznať hrozby a riziká spojené s týmito aktívami a posúdiť ich potenciálny dopad. Je dôležité zvážiť všetky možné negatívne vplyvy, ktoré by mohli tieto kľúčové prvky ohroziť. Tento proces sa nezameriava len na fyzické aktíva, ale tiež zahŕňa všetky relevantné informácie a systémy. Po identifikácii možných rizík sa hodnotí ich pravdepodobnosť a možný dopad. Na základe tohto hodnotenia je potom možné vypracovať stratégie pre zvládanie a minimalizáciu rizík. (1)

Správne pochopenie vzťahov pri analýze rizík je zásadné pre úspešnú analýzu. Tieto vzťahy môžeme definovať niekoľkými kľúčovými bodmi spomenutými vyššie (1):

- Riziko je často vyjadrené ako hrozba, ktorá využíva slabiny aktíva a prekonáva ochranné mechanizmy, čím môže spôsobiť škodu.
- Aktíva sú motiváciou pre útočníka, keďže majú hodnotu, a sú teda zároveň zraniteľné aj chránené.
- Mechanizmy na ochranu aktív sú navrhnuté tak, aby detegovali hrozby a buď ich zmierňovali, alebo úplne eliminovali. Ich úlohou je teda chrániť aktíva.
- Hrozba pôsobí priamo na aktívum alebo na ochranné mechanizmy, aby sa dostala k hodnotám, ktoré aktívum predstavuje.

Analýza rizík zahrňuje(1):

1. Identifikáciu aktív
2. Stanovenie hodnoty aktív

3. Identifikácia hrozieb/zraniteľností
4. Stanovenie ich závažnosti a miery

2.7 Incident

Podľa platnej kybernetickej vyhlášky NIST, Incident v kontexte informačnej bezpečnosti označuje nežiaduci udalosť alebo situáciu, ktorá ohrozuje bezpečnosť, dostupnosť alebo integritu informačných systémov a dát organizácie. Tieto incidenty môžu zahŕňať kybernetické útoky, zlyhanie systémov, stratu dát alebo iné udalosti, ktoré vyžadujú okamžitú pozornosť a reakciu na obnovenie normálneho stavu a minimalizáciu škôd. (9)

Skupina pre reakciu na incidenty (CSIRT)

Computer Security Incident Response Team je organizácia alebo skupina odborníkov, ktorá sa špecializuje na reagovanie na bezpečnostné incidenty v IT prostredí. Hlavnou úlohou CSIRT je detekcia, analýza a reakcia na kybernetické hrozby a incidenty, ktoré môžu ovplyvniť organizáciu. Tento tím zohráva kritickú úlohu pri ochrane citlivých informácií a systémov spoločnosti pred kybernetickými útokmi a zabezpečuje rýchlu a účinnú reakciu v prípade bezpečnostných incidentov. (7)

Computer Emergency Response Team (CERT)

Computer Emergency Response Team (CERT) je organizácia alebo tím, ktorý je špecializovaný na reagovanie na bezpečnostné incidenty týkajúce sa počítačových systémov a sietí. Hlavnou úlohou CERT je rýchle identifikovanie, vyšetrovanie a riešenie bezpečnostných hrozieb a incidentov, aby sa minimalizovali škody a obnovila normálna činnosť. Tieto tímy často poskytujú aj preventívne služby, ako je vzdelávanie a šírenie informácií o hrozbách a najlepších postupoch v oblasti kybernetickej bezpečnosti. (7)

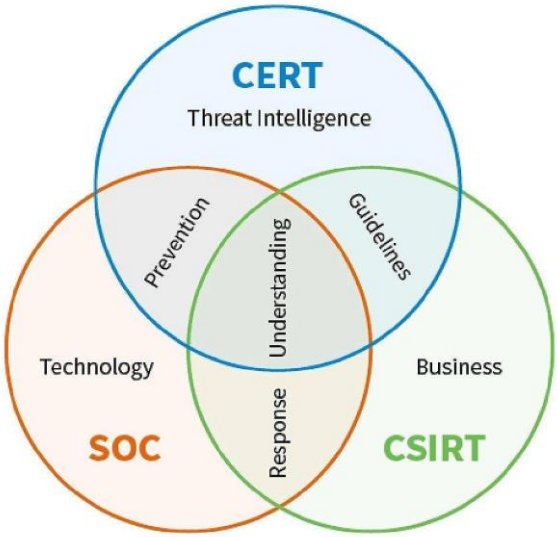
Bezpečnostné operačné centrum (SOC)

Security Operational Center (SOC) je kľúčovou súčasťou stratégie kybernetickej bezpečnosti organizácie. Funguje ako centrálny bod, z ktorého sa monitorujú, analyzujú a riadia bezpečnostné hrozby a incidenty. SOC je vybavený špecializovaným softvérom

a hardvérom a skúsenými bezpečnostnými analytikmi, ktorí pracujú nepretržite na ochrane proti vnútorným a vonkajším hrozbám. (7)

CSIRT, CERT a SOC predstavujú kľúčové prvky v procese efektívneho riadenia kybernetických incidentov a celkového zabezpečenia informačných systémov. Ich vzájomné pôsobenie a úlohy sú vizualizované v diagramoch, ktoré ukazujú ich prepojenie a spoluprácu. Ich základnou misiou je poskytovanie odbornej podpory a zdrojov v oblasti IT bezpečnosti pre štátne inštitúcie, súkromné organizácie aj jednotlivcov. SOC špeciálne zabezpečuje ústredné riadenie bezpečnostných opatrení a rýchlu reakciu na incidenty, s cieľom znižovať dobu reakcie a minimalizovať vznikajúce škody. (7)

Tieto organizácie sú tiež zodpovedné za detekciu a hlásenie kybernetických bezpečnostných udalostí vo svojich sieťach a systémoch, ako aj za rýchlu reakciu na tieto incidenty, s cieľom chrániť kritickú infraštruktúru a služby. Je dôležité, aby tieto orgány mohli kategorizovať incidenty podľa ich dôležitosti a dopadu, čím zabezpečia primeranú reakciu a obnovu systémov. (10)



Obrázok 1 Prelínanie SOC,CERT a CSIRT [Zdroj: 10]

Kategórie kybernetických bezpečnostných incidentov:

Kategória III: Veľmi významný kybernetický bezpečnostný incident, pri ktorom je priamo a významne narušená bezpečnosť poskytovaných služieb alebo aktív. Jeho

riešenie vyžaduje okamžité zásahy obsluhy s tým, že musí byť všetkými dostupnými prostriedkami zabránené ďalšiemu šíreniu kybernetického bezpečnostného incidentu vrátane minimalizácie vzniknutých a potenciálnych škôd. (7)

Kategória II: Významný kybernetický bezpečnostný incident, pri ktorom je narušená bezpečnosť poskytovaných služieb alebo aktív. Jeho riešenie tiež vyžaduje okamžité zásahy obsluhy a je nevyhnutné použiť vhodné prostriedky na zabránenie ďalšiemu šíreniu kybernetického bezpečnostného incidentu, vrátane minimalizácie vzniknutých škôd. (7)

Kategória I: menej významný kybernetický incident, pri ktorom dochádza k obmedzeniu bezpečnosti poskytovaných služieb alebo aktív. Jeho riešenie vyžaduje zásahy obsluhy, a to tak, aby boli čo najefektívnejšie a minimalizovali vzniknuté škody. (7)

S kategorizáciou súvisia aj typy kybernetických incidentov (7):

- Kybernetický bezpečnostný incident, ktorý narušuje dôvernosť aktív.
- Kybernetický bezpečnostný incident, ktorý narušuje integritu aktív.
- Kybernetický bezpečnostný incident, ktorý narušuje dostupnosť aktív.
- Kybernetický bezpečnostný incident, ktorý kombinuje dopady uvedené v predchádzajúcich troch prípadoch.

Proces riešenia kybernetického incidentu je pevne stanovený a prebieha na nasledujúcich úrovniach (7):

- Vládna CERT (počítačový tím pre riešenie núdzových situácií) - pre systémy spadajúce pod kybernetický zákon v kategóriách KII, VIS, PZS.
- Národná CERT - pre systémy, ktoré nespadajú pod kybernetický zákon a ostatné systémy.

Rizikový incident sa tiež rieši v súlade s normou rady 27 000 a podobne vo formáte NIST (7):

- NIST SP 800-61 - Príručka pre riešenie kybernetických bezpečnostných incidentov z roku 2012.
- ISO/IEC 27035:2016 - Norma o bezpečnosti informačných technológií obsahuje tri časti: riadenie bezpečnostného incidentu, princípy, plánovanie a prevádzka.

2.8 Identita

Identita je kľúčovým konceptom v oblasti informačnej bezpečnosti a označuje jednoznačný spôsob identifikácie a overenia totožnosti jednotlivca alebo entity, ktorá sa pokúša získať prístup k informačným systémom alebo dátam. Identita je často založená na kombinácii používateľského mena a hesla, biometrických údajov alebo digitálnych certifikátov. Správna identifikácia a overenie identity je kľúčovým prvkom zabezpečenia prístupu a minimalizácie rizika neoprávneného prístupu k citlivým informáciám. (11)

2.9 Autentifikácia

Autentifikácia je proces overovania totožnosti jednotlivca alebo entity, ktorá sa snaží získať prístup k informačným systémom alebo dátam. Cieľom autentifikácie je zabezpečiť, že osoba alebo systém, ktorý sa pokúša získať prístup, je skutočne ten, za koho sa vydáva. Autentifikácia sa často vykonáva prostredníctvom kombinácie faktorov, ako sú niektoré z týchto: používateľské meno/heslo, biometrické údaje (napr. odtlačky prstov), fyzické karty alebo digitálne certifikáty. (11)

2.10 Autorizácia

Autorizácia je proces, v rámci ktorého sa kontroluje oprávnenie jednotlivca alebo entity na vykonávanie určitých akcií alebo prístup k špecifickým zdrojom alebo informáciám v informačných systémoch. Ide o druhý krok po autentifikácii, kde sa určuje, čo oprávnená osoba alebo systém môže robiť po úspešnom overení identity. Autorizácia zabezpečuje, že prístup je pridelený iba tým, ktorí majú legitímne právo na konkrétnu činnosť alebo zdroje. (11)

2.11 PDCA cyklus

PDCA cyklus (Plan-Do-Check-Act) je manažérska metóda, ktorá sa často používa na neustále zlepšovanie a riadenie procesov v organizáciách. Tento cyklus sa skladá z štyroch hlavných krokov: (7)

1. **Plan (Plánovanie)**: V tomto kroku organizácia identifikuje ciele a cesty, ako ich dosiahnuť. Plán obsahuje definovanie cieľov, stanovenie stratégií a vytvorenie plánov na ich dosiahnutie.
2. **Do (Vykonávanie)**: V tomto kroku organizácia implementuje plán a vykonáva potrebné činnosti na dosiahnutie stanovených cieľov.
3. **Check (Kontrola)**: Po vykonaní sa kontroluje, či boli ciele dosiahnuté, a porovnávajú sa výsledky s plánom. Analyzuje sa efektívnosť opatrení.
4. **Act (Akcia)**: Na základe analýzy výsledkov sa prijímajú opatrenia na zlepšenie procesov alebo plánu na budúcnosť. (7)

Súčasťou je aj dokumentácia každého kroku procesu. Procesy je potrebne identifikovať, popísať a zdokumentovať, riadiť na základe tejto dokumentácie a následne ich priebeh optimalizovať. (7)

2.12 Service Level agreement

SLA, alebo Service Level Agreement (Dohoda o úrovni poskytovaných služieb), je formálny dokument, ktorý definuje úroveň služieb poskytovaných medzi poskytovateľom služby a jeho zákazníkom. SLA obsahuje konkrétne kritériá služieb, na základe ktorých sa posudzuje plnenie poskytovateľa služby. Tieto kritériá môžu zahŕňať aspekty ako dostupnosť služby, výkonnosť, doby reakcie na podporu, a postupy pri porušení dohodnutých úrovní služieb. Hlavným cieľom SLA je zabezpečiť, aby boli očakávania klienta týkajúce sa poskytovaných služieb jasne definované, merateľné a právne záväzné. To umožňuje obom stranám mať jasne vytýčené povinnosti, práva a očakávania, čo prispieva k efektívnejšej a transparentnejšej spolupráci. (12)(33)

SLA typicky obsahuje(12):

- Podrobný opis služieb, ktoré majú byť poskytnuté.
- Špecifikácie úrovne služieb, ako sú rýchlosť, dostupnosť a kvalita.
- Postupy pri nedodržaní SLA
- Mechanizmy na sledovanie výkonnosti služieb a periodicita reportovania.
- Časové rámce, v ktorých musí poskytovateľ reagovať na žiadosti o službu alebo problémy a akcie potrebné na nápravu.

SLA je kľúčová súčasť mnohých obchodných dohôd, najmä v oblasti IT služieb, cloudových služieb, telekomunikácií a profesionálnych služieb, kde je potrebné zabezpečiť spoľahlivosť a kvalitu poskytovaných služieb. (12)(33)

2.13 Kybernetické útoky

Základné delenie typov útokov bolo prebraté z dokumentu európskej bezpečnostnej agentúry „ENISA Threat Landscape 2023“. Sú radené podľa pravdepodobnosti výskytu.

Ransomware

Podľa správy ENISA sa ransomware definuje ako typ útoku, pri ktorom útočníci ovládajú aktíva cieľa a požadujú výkupné výmenou za navrátenie dostupnosti aktíva. (13)

Hrozby voči dostupnosti: Distributed Denial of Service (DDOS)

Dostupnosť je cieľom množstva hrozieb a útokov, medzi ktorými výrazne vyniká DDoS. DDoS cieli na dostupnosť systému a dát a hoci nie je novou hrozbou, zohráva významnú úlohu. Útok ma za cieľ zahltiť násobnými inputmi systém tak, aby používateľ nemohol k danému systému pristupovať. To môže byť dosiahnuté preťažením komponentov sieťovej infraštruktúry. (13)

Hrozby voči dátam (DATA)

Porušenie dát je v GDPR definované ako akékoľvek porušenie bezpečnosti vedúce k náhodnému alebo nezákonnému zničeniu, strate, zmenení alebo neoprávnenému

zverejneniu alebo prístupu k osobným údajom prenášaným, ukladaným alebo inak spracovávaným (článok 4.12 GDPR). (13)

Malvér (Malware)

Je bežný typ kybernetického útoku vo forme škodlivého softvéru. Jeho spoločnými cieľmi sú informácie alebo krádež identity, špionáž a narušenie služieb. Rodina malvéru je dosť rozsiahla – od vírusov cez červy, ransomware až po najrozšírenejší malvér cryptominers (cryptojacking). (13)

Sociálne inžinierstvo (Social Engineering)

Sociálne inžinierstvo zahŕňa širokú škálu aktivít, ktoré sa snažia využiť ľudskú chybu s cieľom získať prístup k informáciám alebo službám. Využíva rôzne formy manipulácie, aby obete presvedčili k chybám alebo odovzdaniu citlivých a tajných informácií. Používatelia môžu byť zlákaní otvoriť dokumenty, súbory alebo e-maily, navštíviť webové stránky alebo udeliť prístup k systémom alebo službám. Aj keď môžu byť nástrahy a triky technologicky jednoduché, spoliehajú sa najmä na ľudský prvok. Táto hrozba zahŕňa nasledujúce vektory útokov(13):

- **Phishing cez e-mail (Email Phishing)** - Útočníci posielajú falošné e-maily, ktoré sa tvária, že sú od dôveryhodných zdrojov, ako sú banky, vládne agentúry alebo známe spoločnosti, s cieľom získať prihlasovacie údaje alebo iné citlivé informácie. (7)
- **Phishing cez webové stránky (Phishing Websites)** - Útočníci vytvárajú falošné webové stránky, ktoré sa zdajú byť dôveryhodné, aby podviedli ľudí na zadanie svojich citlivých údajov, napríklad na prihlasovacích stránkach. (7)
- **Spear Phishing** - Tento typ phishingu je cielený na konkrétne osoby alebo organizácie. Útočníci získavajú informácie o obetiach a vytvárajú personalizované útoky, čo ich robí ťažšie odhaliteľnými. (7)
- **Vishing (Voice Phishing)** - Útočníci kontaktujú obete prostredníctvom hovorov alebo zanechávajú hlasové správy, vydávajúc sa za dôveryhodné osoby alebo inštitúcie s cieľom získať informácie. (7)

- **SMS phishing (Smishing)** - Útočníci posielajú falošné textové správy, ktoré obsahujú odkazy na podvodné webové stránky alebo požiadavky na získanie citlivých údajov.(7)

Aj keď sú techniky sociálneho inžinierstva často používané na získanie počiatočného prístupu, môžu byť použité aj v neskorších fázach incidentu. (13)

Hrozby voči dostupnosti: Internetové hrozby (Internet threats)

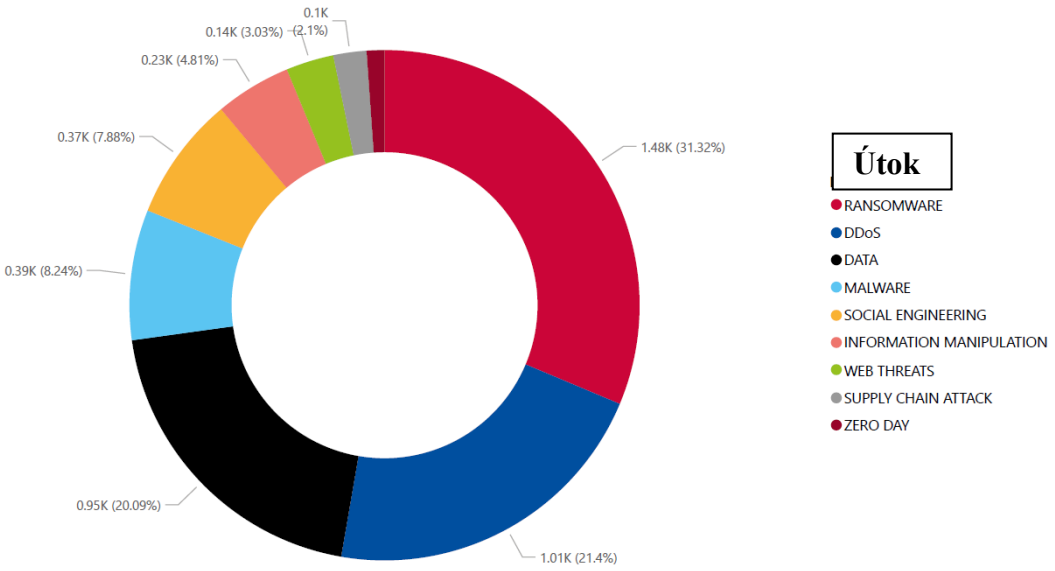
Hrozby pre dostupnosť Internetu sa vzťahujú na úmyselné alebo neúmyselné prerušenia Internetu alebo elektronických komunikácií, ktoré majú za následok výpadky Internetu, blackouts, shutdowns alebo cenzúru. Prerušenia Internetu môžu byť spôsobené vládou riadenými výpadkami Internetu, cyklónmi, masívnymi zemetraseniami, výpadkami elektriny, poškodením káblov, kybernetickými útokmi, technickými problémami a vojenskými akciami. Tieto hrozby sú čoraz rozmanitejšie a rastú, dosiahli nový rekord v tomto spravodajskom období a spôsobili obrovské finančné straty národným ekonomikám.(13)

Manipulácia s informáciami (Information Manipulation)

Manipulácia s informáciami a zasahovanie (FIMI) opisuje väčšinou nelegálny vzor správania, ktorý ohrozuje alebo má potenciál negatívne ovplyvniť hodnoty, postupy a politické procesy. Takáto aktivita je manipulatívna, vykonávaná úmyselne a koordinovane. FIMI môže byť vykonávané štátnymi alebo neštátnymi aktérmi, vrátane ich zástupcov vo vnútri a mimo ich vlastného územia. (13)

Útoky na dodávateľský reťazec (Supply Chain Attacks)

Útok na dodávateľský reťazec cieli na vzťah medzi organizáciami a ich dodávateľmi. Tento útok sa považuje za súčasť dodávateľského reťazca, keď obsahuje kombináciu aspoň dvoch útokov. Aby bol útok klasifikovaný ako útok na dodávateľský reťazec, musia byť cieľom útoku tak dodávateľ, ako aj zákazník. Plocha útoku na zákazníka sa teda rozširuje o plochu útoku dodávateľa. (13)



Obrázok 2 Enisa trendy za rok 2023 [Zdroj: 13]

2.13.1 Zero-day

Existujú tri pojmy - zraniteľnosť, exploit a útok, ktoré často vidíme v spojitosti so "zero-day".

Zero-day zraniteľnosť predstavuje nedávno identifikovanú bezpečnostnú slabinu, o ktorej dotknutá strana zatiaľ nemá poznatky a neexistuje pre ňu žiadna bezpečnostná oprava. Keď sa dodávateľ dozvie o existencii zero-day zraniteľnosti, je kľúčové čo najskôr zabezpečiť distribúciu opravného patchu vzhľadom na potenciálne riziko exploitov tejto zraniteľnosti. Avšak, v momente keď sa informácie o zero-day zraniteľnosti dostanú na verejnosť, stupňuje sa riziko jej zneužitia, nakoľko útočníci majú tendenciu takúto slabiny rýchlo využívať proti zraniteľným systémom. Inými slovami, každé zdržanie vo vydávaní bezpečnostných patchov pre zero-day zraniteľnosti implikuje zvýšené riziko jej zneužitia. (14)

Aby mohol útočník využiť túto zraniteľnosť na získanie prístupu k systému alebo jeho dátam, musí vytvoriť zero-day exploit — penetračnú techniku alebo kus malware, ktorý využíva slabosť. Zatiaľ čo niektorí útočníci navrhujú tieto exploity pre vlastné použitie, iní ich predávajú. (14)

Keď je vyzbrojený exploitom, hacker môže vykonať zero-day útok. Inými slovami, zraniteľnosť predstavuje iba potenciálnu cestu útoku, a exploit je nástrojom na vykonanie tohto útoku; je to samotný útok, ktorý je skutočne nebezpečný. To môže byť bodom sporu v komunite bezpečnostných výskumníkov, kde sú zraniteľnosti často odhalené — a občas zverejnené — s cieľom zvýšiť povedomie a dosiahnuť ich rýchlejšie opravenie. Avšak, výrobcovia, ktorých zraniteľnosti sú vystavené, niekedy považujú toto vystavenie za rovnocenné s útokom samotným. (14)

2.14 Penetračné testovanie

Cieľom penetračného testu je nájdenie slabých miest v organizácii, systéme alebo aplikácii, ktoré by mohol zneužiť potenciálny útočník. Penetračný test je simulácia útoku, kde jednotlivé kroky postupu testovania sa menia podľa aktuálnych zistení. Overujú nielen mieru zraniteľnosti systémov proti neoprávnenému prieniku, ale tiež ochránia pred existujúcimi hrozbami. Za použitia mnohých nástrojov sú vykonávané pokusy preniknúť do rôznych častí informačného systému zvnútra aj zvonka. Výsledkom týchto testov je odhalenie slabých miest v ochrane informácií. (7)

Štandardy (7):

- OWASP (The Open Web Application Security Project),
- OSSTMM (The Open Source Security Testing Methodology Manual),
- PTES (Penetration Testing Execution Standard),
- ISA (Information Systems Audit and Control Association),
- NIST (National Institute of Standards and Technology).

Norma NIST pre túto problematiku je vydaná vo forme manuálu a odporúčaní pre penetračné testovanie: NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

Kategorizácia penetračného testovania je nasledujúca (7):

- manuálne testy,
- automatizované testy,
- semi-automatizované testy,

- black-box testy (testovanie s užívateľským pohľadom bez bližších informácií – čierna skrinka, určené iba cieľu testu),
- white-box testy (znalosť testovaného napríklad zdrojového kódu u webových aplikácií),
- grey-box testy (testovanie s užívateľské a čiastočnou znalosťou vnútorných procesov).

Penetračné testy majú 4 fázy (7):

- plánovanie (cieľ a rozsah penetračného testu),
- vyhľadávanie (zbierka dát),
- útok (skenovanie a exploitácia),
- reportovanie.

Cieľom a rozsahom penetračného testu je otestovanie pomocou detailnej analýzy. Cieľom zbierky dát je získať o konkrétnych systémoch čo najviac informácií, ktoré sú potom vstupom do ďalšej fázy penetračného testu. (7)

Cieľom skenovania a exploitácie je testovať už konkrétne ciele (napríklad získanie prístupu do systému bez platných prihlasovacích údajov). Celá táto fáza je postavená na využívaní zistených testovacích techník pre penetračné testovanie - sú buď rozdelené na jednotlivé testovacie utility, alebo sú združené do takzvaného Toolkitu. Neoddeliteľnou súčasťou penetračného testovania je záverečná správa penetračného testovania. Obsahuje (7):

- Prehľad slabých miest informačných aktív.
- Definície stupňa závažnosti slabých miest.
- Návrh bezpečnostných opatrení k odstráneniu slabých miest.
- Manažérsky výstup.

Reportovanie je popis toho, čo bolo penetračným testom nájdené a odporúčanie na odstránenie v nasledujúcom obsahu (7):

- označenie testovaného systému,
- termín testu,

- použitá metodológia,
- manažérske zhrnutie,
- závažnosť zistení,
- opatrenia.

2.15 Útočníci

V oblasti kybernetickej bezpečnosti sa používajú termíny "white hat," "grey hat" a "black hat" pre označenie rôznych typov hackerov na základe ich motivácií a etiky. (15)

- **White Hat Hacker**: White hat hackeri sú etickí hackeri, ktorí pracujú v rámci zákona a v súlade s etickými normami. Ich cieľom je identifikovať a odstraňovať zraniteľnosti a zlepšovať bezpečnosť systémov a sietí. Títo hackeri často pracujú ako bezpečnostní konzultanti alebo penetrační testeri. (15)
- **Grey Hat Hacker**: Grey hat hackeri sú kombináciou white hat a black hat hackerov. Môžu vykonávať hackerstvo bez povolenia, ale s dobrými úmyslami. To znamená, že môžu objavovať zraniteľnosti, ale nevyužívajú ich na škodu. Napriek tomu ich činnosť môže byť stále nelegálna. (15)
- **Black Hat Hacker**: Black hat hackeri sú hackeri, ktorí konajú nezákonne a neeticky s cieľom spôsobiť škodu, krádež, podvod alebo iný neoprávnený zisk. Ich cieľom môže byť krádež citlivých údajov, poškodenie systémov alebo šírenie malwaru. (15)

2.15.1 Útočné skupiny

Medusa

Medusa je známa svojou činnosťou od roku 2021. Špecializujú sa na ransomvérové útoky. Ich „modus operandi“ spočíva v šifrovaní súborov obetí a vyžadovaní výkupného za dešifrovací kľúč. Používajú variant ransomvéru známeho ako MedusaLocker a fungujú na modeli Ransomware-as-a-Service (RaaS), pričom spolupracujú s globálnymi aktérmi na vykonávanie rozsiahlych útokov. Oznámenia o ich obetiach zverejňujú na špeciálnom blogu a na komunikáciu ohľadom výkupného a potenciálneho úniku dát obetí, ktoré odmietnu platiť, používajú rôzne kanály vrátane e-

mailu a Telegramu (aplikácia pre komunikáciu). Medusa je známa tým, že cielene vyberá svoje obete v rôznych krajinách a odvetviach s cieľom maximalizovať dopad. Jedným z ich významných útokov bol útok na školský okres Minneapolis v marci 2023, kde požadovali výkupné vo výške milión dolárov a nakoniec zverejnili ukradnuté dáta po nezaplatení. (17) (16)

Skupina Monti

Skupina Monti je známa svojou činnosťou v oblasti ransomvéru, ktorá bola prvýkrát identifikovaná v júni 2022. Táto skupina sa zameriava hlavne na právne a vládne subjekty a používa varianty ransomvéru pre systémy Linux a Windows. Monti často využíva zdrojový kód a taktiky skupiny Conti, ktorá ukončila svoju činnosť krátko pred vznikom Monti. Skupina Monti občas označuje svoje útoky za etické hackovanie a tvrdí, že ich softvér poukazuje na bezpečnostné problémy v sieťach firiem. Ak firmy nezaplatia výkupné, Monti umiestňuje ich mená na "Stenu hanby" na svojom webe s únikmi dát.

V minulosti bola skupina zodpovedná za útoky na viaceré inštitúcie, vrátane Auckland University of Technology, pričom využila to, čo považovala za nedostatočné bezpečnostné opatrenia tejto inštitúcie. (18) (19)

2.16 Audit kybernetickej bezpečnosti

Audit kybernetickej bezpečnosti podľa noriem ISO/IEC, najmä ISO/IEC 27001, je štruktúrovaný proces, ktorý umožňuje organizácii systematicky hodnotiť svoje informačné bezpečnostné riziká, zahŕňajúc hrozby, zraniteľnosti a dosahy. Norma ISO/IEC 27001 je medzinárodný štandard, ktorý poskytuje požiadavky na zavedenie, implementáciu, udržiavanie a neustále zlepšovanie systému riadenia informačnej bezpečnosti (ISMS). (3)

Kľúčové aspekty auditu kybernetickej bezpečnosti podľa ISO/IEC 27001:

Plánovanie a príprava -Stanovenie, ktoré oblasti, procesy, systémy budú zahrnuté. Audit by mal byť vykonávaný kompetentnými audítormi, ktorí majú príslušné vedomosti a skúsenosti v oblasti informačnej bezpečnosti. Odporúča sa zapojenie externých audítorov pre objektívnosť. (3)

Vykonávanie auditu (3)

- Kontrola existujúcich bezpečnostných politík a postupov v súlade s požiadavkami normy.
- Preskúmanie procesu hodnotenia rizík, ktorý organizácia používa, a spôsobu, akým sú riziká riadené.
- Kontrola implementácie bezpečnostných kontrol, ktoré sú súčasťou ISMS a zabezpečujú ochranu pred identifikovanými rizikami.
- Zhodnotenie procesov pre nápravné a preventívne akcie a ich efektívnosť pri riešení zistených bezpečnostných slabín.

Spracovanie a dokumentácia výsledkov - Zhrnutie zistení, vrátane identifikovaných slabín a odporúčaní na ich nápravu. Diskusia o výsledkoch auditu s vedením organizácie a plánovanie ďalších krokov. (3)

Po-auditové aktivity - Vytvorenie a implementácia plánu zlepšenia na adresovanie zistených nedostatkov. Pravidelné sledovanie a revízia implementovaných zlepšení na zabezpečenie trvalého dodržiavania štandardov ISO/IEC. (3)

Výhody auditu podľa ISO/IEC 27001 (3):

- Audit pomáha identifikovať a opraviť slabiny, čím zvyšuje celkovú úroveň bezpečnosti.
- Certifikácia a dodržiavanie medzinárodných štandardov zvyšuje dôveru vo vaše bezpečnostné praktiky.
- Dodržiavanie predpisov: Pomáha v súlade s regulačnými a zákonnými požiadavkami na ochranu dát a informácií.
- Norma ISO/IEC 27001 poskytuje osvedčené postupy a metodiky, ktoré môže organizácia využiť pre efektívne riadenie svojich informačných bezpečnostných rizík.

2.17 General Data Protection Regulation

Zákon o ochrane osobných údajov zo dňa 29. novembra 2017 je slovenský právny predpis, ktorý reguluje spracovanie a ochranu osobných údajov občanov. Tento zákon bol prijatý v súlade s európskym právnym rámcom GDPR (Všeobecné nariadenie o ochrane

osobných údajov) a mal za cieľ zabezpečiť ochranu osobných údajov občanov na Slovensku. (20)

Medzi hlavné ciele tohto zákona patrí (20):

1. Zabezpečiť práva jednotlivcov týkajúce sa ich osobných údajov, vrátane práva na informácie o tom, ako sa ich údaje spracovávajú.
2. Upraviť povinnosti organizácií, ktoré spracovávajú osobné údaje, vrátane povinnosti získavať súhlas jednotlivcov na spracovanie ich údajov a zabezpečiť ich bezpečnosť.
3. Udeliť práva jednotlivcom, ako je právo na prístup k svojim údajom, opravu, vymazanie a prenosnosť.
4. Upraviť postupy pre porušenie bezpečnosti údajov a nahlásenie takýchto porušení dozornému orgánu a dotknutým osobám.
5. Stanoviť sankcie za nesprávne spracovanie osobných údajov a porušenia ustanovení tohto zákona.

2.18 Kontinuita podnikania

Kontinuita podnikania (Business continuity) je proces a súbor opatrení, ktoré organizácie prijímajú na zabezpečenie svojej schopnosti pokračovať v podnikaní a minimalizovať vplyv prírodných katastrof, nečakaných udalostí, výpadkov alebo iných krízových situácií. Cieľom business continuity je udržať kľúčové operácie, služby a funkcie organizácie, aby sa minimalizovali straty a obnovil normálny chod podnikania čo najrýchlejšie v prípade uskutočnenia jednej zo spomínaných hrozieb. (21)

2.19 Game based learning (Učenie sa pomocou hier)

Game-Based Learning (GBL) je výučbová metóda, ktorá využíva herné prvky na zlepšenie učebného prostredia a zvýšenie zapojenia účastníkov. Tento prístup kombinuje edukačné obsahy s hernými mechanizmami, aby motivoval a zlepšil proces učenia. GBL môže byť aplikovaný vo viacerých formách, od jednoduchých kvízových hier až po komplexné simulácie a virtuálne svety.

Hlavným cieľom GBL je využiť motivujúce aspekty hier na podporu učenia. Hry poskytujú okamžitú spätnú väzbu, umožňujú účastníkom experimentovať v bezpečnom prostredí, zvyšujú angažovanosť a pomáhajú rozvíjať dôležité zručnosti, ako sú kritické myslenie, riešenie problémov a spolupráca. Výskumy ukazujú, že GBL môže zlepšiť učebné výsledky a zvýšiť záujem študentov o učivo. (22)

2.20 Table top cvičenie

Table top cvičenie (TTX) je druh simulácie používanej hlavne v organizáciách na testovanie a zlepšovanie ich núdzových reakcií, riadenia rizík a prevádzkových postupov. Ide o interaktívnu diskusiu, pri ktorej sa zúčastnené osoby s konkrétnymi úlohami a zodpovednosťami stretnú, často v učebnom prostredí, aby prediskutovali simulovanú núdzovú situáciu. Hlavnými cieľmi týchto cvičení sú (22) (23) (24):

- **Testovanie a hodnotenie** - Umožňujú organizáciám hodnotiť ich núdzové reakčné plány, politiky a postupy v bezrizikovom prostredí. To pomáha identifikovať silné a slabé stránky existujúcich plánov.
- **Tréning a príprava** - Table top cvičenia poskytujú kľúčovému personálu tréning pre rôzne núdzové scenáre, pomáhajúcim porozumieť a efektívne vykonávať ich úlohy.
- **Zlepšenie reakcie na obnovy** - Cvičením vypracovaných reakčných plánov môžu organizácie zlepšiť svoje schopnosti reagovať na skutočné núdzové situácie a zotaviť sa z nich.
- **Overenie vybavenia a úloh** - Tieto cvičenia tiež zabezpečujú, že všetko potrebné vybavenie a nástroje sú funkčné a že každý zúčastnený má povedomie o svojich úlohách počas núdzovej situácie.
- **Plánovanie špecifické pre scenár** - Table top cvičenia môžu byť prispôsobené konkrétnym situáciám, ako sú kybernetické hrozby alebo prírodné katastrofy, čo umožňuje zameranejšie a efektívnejšie plánovanie (22) (23) (24):.

História table top cvičení:

Počiatky table top cvičení siahajú do obdobia studenej vojny, keď sa používali na tréning vojenských veliteľov a štábnych dôstojníkov na riešenie situácií v rámci jadrovej vojny a strategických operácií. Neskôr sa tento typ cvičení rozšíril do iných oblastí, ako sú zdravotníctvo, verejná bezpečnosť, a civilný sektor, ako nástroj na prípravu na rôzne katastrofy a krízy. Dnes sú table top cvičenia široko používané v rôznych odvetviach, vrátane vládnych inštitúcií, zdravotnej starostlivosti, podnikov, a mimovládnych organizácií na zvýšenie schopnosti rýchlo a efektívne reagovať na núdzové situácie. (22) (23) (24)

2.21 Metódy zberu údajov

Zber údajov spoločnosti zahŕňa systematický proces zhromažďovania a hodnotenia informácií o činnostiach a financiách spoločnosti. Tento proces zvyčajne zahŕňa (25):

[1] **Revízia finančných záznamov -** Skúmanie bilancií, výkazov ziskov a strát, daňových priznaní a ďalších finančných dokumentov.
[2] **Kontrola interných kontrol -** Hodnotenie efektívnosti vnútorných kontrol a procesov rizikového manažmentu.
[3] **Rozhovory s manažmentom a zamestnancami -** Získavanie informácií o interných postupoch a politikách.
[4] **Fyzická inventarizácia -** Overenie hmotného majetku spoločnosti.
[5] **Analýza vnútorných a externých dokumentov -** Skúmanie zmlúv, smerníc, poriadkov a iných dôverných materiálov.

2.21.1 Dotazník

Dotazník je výskumná metóda, ktorá umožňuje efektívne a rýchle zhromažďovanie údajov od rozsiahlej skupiny respondentov. Hoci jeho použitie je relatívne jednoduché, dôkladná príprava a vytvorenie dotazníka je kľúčové. Dotazníky sú vhodné aj pre menšie výskumné skupiny alebo ako nástroj na zaznamenávanie dát v experimentoch. Informácie získané pomocou dotazníkov zahŕňajú vedomosti, postoje, správanie a osobné vlastnosti respondentov. (25)

2.21.2 Pozorovanie

Pozorovanie je dôležitá výskumná metóda pozostávajúca zo systematického sledovania a zaznamenávania ľudského správania, nasledovaného jeho analýzou a vyhodnotením. Táto metóda sa často využíva v pedagogickom výskume, obzvlášť v situáciách, kde etické dôvody neumožňujú vykonávanie experimentov. Na rozdiel od bežného pozorovania, ktoré je nesystematické a subjektívne, vedecké pozorovanie vyžaduje presne definované podmienky, systematický prístup a objektívnosť. Pozorovanie môže prebiehať v laboratóriách alebo v prirodzených podmienkach, pričom v laboratórnych podmienkach môže byť súčasťou experimentu. (25)

3 ANALÝZA PROSTREDIA A DOPADY NEDÁVNYCH INCIDENTOV

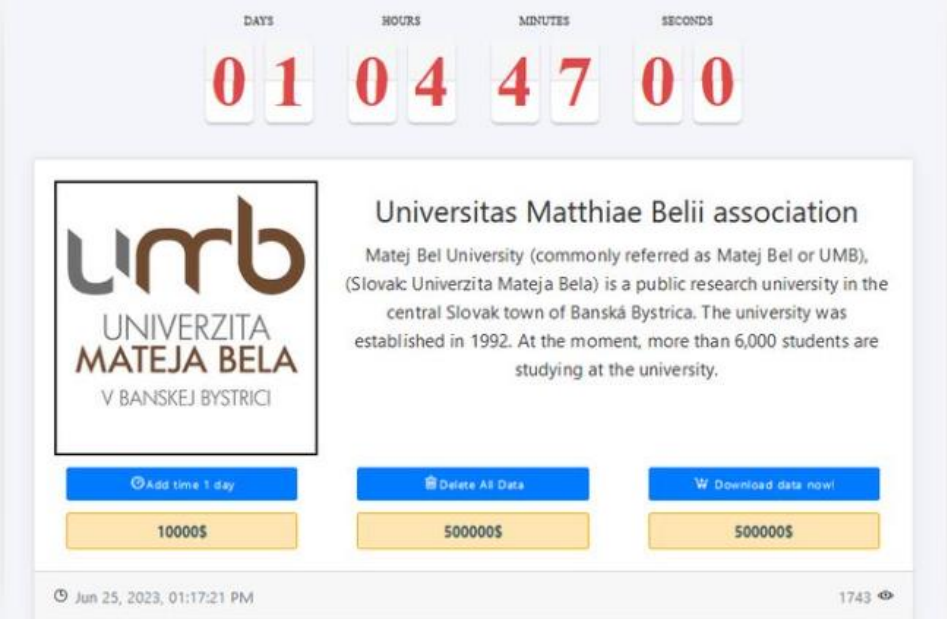
V tejto kapitole sa budeme zaoberať aktuálne nedávnymi incidentami, ktoré sa odohrali na území Slovenskej republiky a susednej krajiny. V aktuálnom období 2023 a 2024 sa odohrali ako v Českej republike, tak na Slovensku kritické incidenty, ktoré by mohli znamenať hrozbu pre iné univerzity na tomto území.

3.1 Predošlé incidenty v školskom prostredí

V tejto kapitole sa budeme venovať incidentom, ktoré sú úzko späté s prostredím, alebo incidentami spájané s školským prostredím.

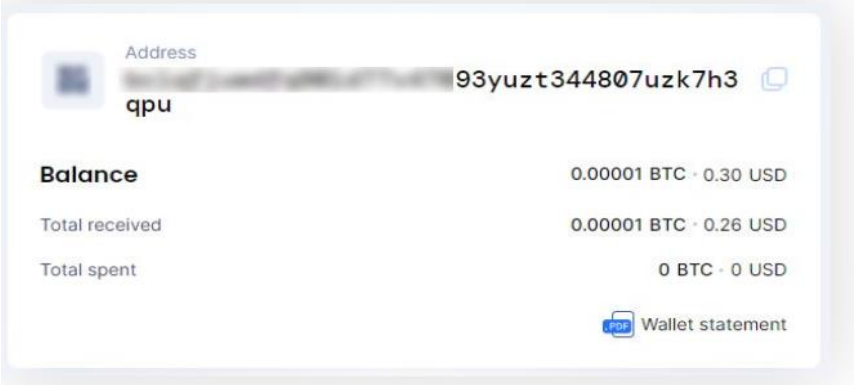
3.1.1 Univerzita Mateja Bela v Banskej Bystrici

Na konci júna a začiatku júla 2023 sa Univerzita Mateja Bela v Banskej Bystrici stala cieľom útokov kybernetickej skupiny *Medusa*. V dôsledku toho prestali fungovať jej informačné systémy, internetová stránka a došlo aj k úniku veľkého množstva dát z jej serverov. Počas toho, ako sa IT špecialisti s pomocou Národného centra kybernetickej bezpečnosti SK-CERT snažili o obnovu týchto systémov, blížil sa termín na zaplatenie požadovaného výkupného. Tento termín uplynul v pondelok 3. júla o 15:15 miestneho času. (26)



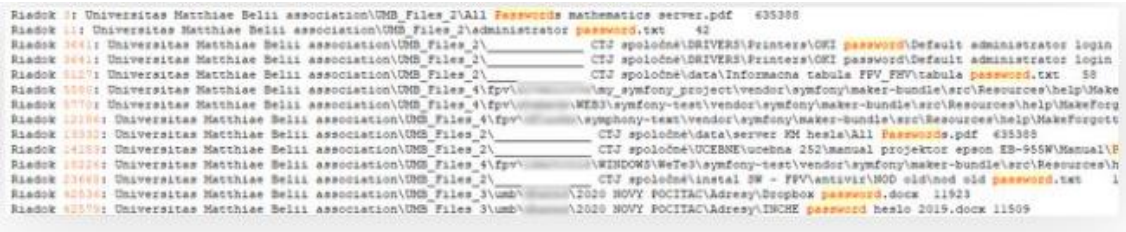
Obrázok 3 Medusa útok [Zdroj: 26]

Na blogu skupiny Medusa, dostupnom na darkwebe, existovala možnosť posunúť deadline pre zaplatenie výkupného o 24 hodín za sumu 10 000 amerických dolárov (9 275 eur). Aby boli všetky odcudzené údaje vymazané, bolo by to za cenu 500 000 dolárov (približne 463 760 eur), a za tú istú sumu si mohol ktokoľvek stiahnuť skopírované dáta. V extrémnom prípade by univerzita mohla čeliť nákladom až do výšky jedného milióna dolárov: pol milióna za obnovu zašifrovaných súborov, ak by nebolo možné obnoviť kritické dáta zo záloh, a pol milióna za ich definitívne vymazanie, vychádzajúc z predpokladu, že univerzita nezískala od útočníkov lepšiu ponuku. Vladimír Hiadlovský, rektor UMB, uviedol, že už od prvého momentu počas incidentu bolo rozhodnuté nezaplatiť požadované výkupné. Toto rozhodnutie je podložené aktuálnym snímkom bitcoinovej peňaženky útočníkov, ktorá bola prázdna. (26)



Obrázok 4 Medusa útok peňaženka [Zdroj: 29]

Na svojom blogu hackeri zverejnili 25 obrázkov, ktoré ilustrujú, čo obsahoval únik dát. Medzi týmito obrázkami sa nachádzajú aj verejne dostupné dáta, ktoré nemajú veľkú hodnotu, ako napríklad informácie o termínoch prihlášok, popisy študijných programov a informačné listy predmetov. Medzi ukradnutými dátami sú však aj citlivejšie informácie, vrátane rozhodnutí o prijatí študentov, interné emailové komunikácie a osobné údaje študentov. Na blogu je tiež zoznam všetkých odcudzených súborov, čo naznačuje, že útočníci pravdepodobne získali prístup k súborovému serveru určenému pre zamestnancov UMB. (26)



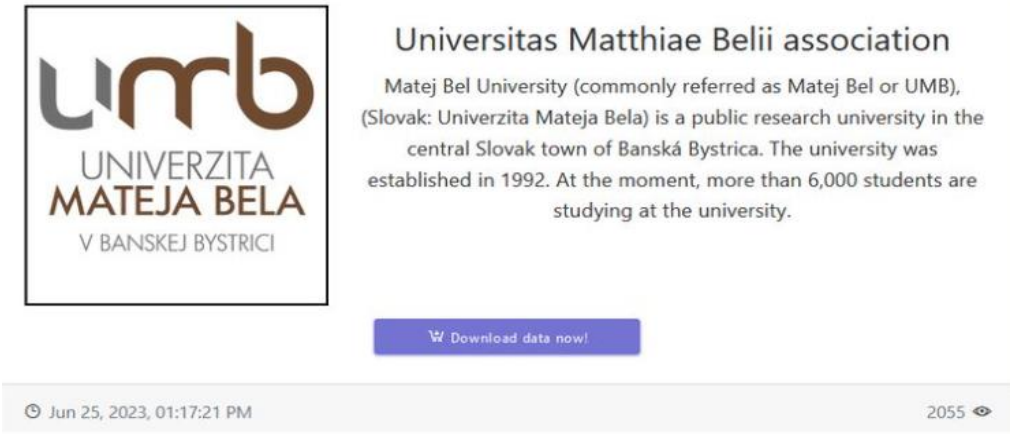
Obrázok 5 Medusa útok detail [Zdroj: 26]

Zoznam obsahoval vyše 400-tisíc položiek, medzi ktorými sa nachádzali fotografie, interné dokumenty, testy, študijné materiály, uložené e-maily, zoznamy IP adries a pravdepodobne aj heslá uložené ako obyčajný text. (26)

Priebeh

Prvé varovné signály o narušení bezpečnosti sa prejavili 20. júna 2023, keď bola školská komunita - študenti a zamestnanci - naliehavo požiadaná, aby prestali používať počítače a vyhýbali sa prístupu k svojim emailovým účtom. Nasledujúci deň univerzita

vyjadrila oficiálne vyhlásenie, v ktorom potvrdila, že sa stala terčom kybernetického útoku. Tento útok zasiahol zásadné časti infraštruktúry školy, čo viedlo k výpadkom hlavných systémov, vrátane webovej stránky školy, Akademického informačného systému (AIS), platformy Moodle určenej pre e-learning a ďalších dôležitých služieb. (26)



Obrázok 6 Medusa útok, dáta na stiahnutie [Zdroj: 26]

Univerzita spresnila, aké typy osobných údajov súbory obsahovali (26):

- *meno a priezvisko,*
- *titul,*
- *rodné číslo,*
- *dátum narodenia,*
- *miesto narodenia,*
- *rodinný stav,*
- *osobné číslo,*
- *adresa,*
- *e-mail,*
- *telefón,*
- *fotografie,*
- *videozáznamy,*
- *údaje obsiahnuté vo fotokópiách a skenoch dokladov ako preukaz poistenca, cestovný pas, občiansky preukaz, osvedčenie o evidencii II, technický preukaz osvedčenie o evidencii I a podobne,*

- *údaje týkajúce sa mzdy a zrážok zo mzdy zamestnancov, finančných príspevkov a stravovania zamestnancov,*
- *údaje týkajúce sa ubytovania, štúdia a sociálnej podpory študentov UMB,*
- *ID osoby,*
- *skratka zdravotného znevýhodnenia študentov UMB,*
- *IBAN bežného účtu a prípadne iné údaje.*

Hrozba, ktorou sa Medusa vyhrážala sa napokon naplnila a univerzita utrpela reputačné škody a citlivé údaje žiakom a zamestnancov sa zverejnili verejnosti.

3.1.2 Univerzita obrany v Brne

Vojenská akadémia čelila útoku v kybernetickom priestore, pričom útočníci odcudzili dáta z administratívnej časti univerzity. Redaktorom portálu „Radiožurnál“ sa podarilo získať informácie o dátach, ktoré hackeri mali k dispozícii. Predstaviteľ univerzity Vladimír Šidla potvrdil, že škola situáciu aktívne rieši, pričom útočníci požadujú za vrátenie dát výkupné. (27)

Zverejnený zoznam obsahuje 150 000 súborov, ktoré skupina označená ako Monti ransomware ukradla a uverejnila. Zoznam zahŕňa súbory z e-mailových účtov, ktoré sú identifikovateľné podľa mien zamestnancov a pedagógov univerzity, vrátane dôležitých e-mailových správ, ktoré môžu obsahovať informácie o významných akademických osobnostiach. (27)

Medzi údajmi sa nachádzajú aj záznamy z porád, operatívne dokumenty, finančné správy, faktúry a varovania o bezpečnostných incidentoch v sieti univerzity. Tieto informácie by mohli obsahovať citlivé údaje, ako sú informácie o platbách alebo prepúšťaní na akadémii, čo vyvolalo obavy. (27)

Zverejnené dokumenty pochádzajú z rôznych častí univerzity, vrátane rektorátu a Fakulty vojenských technológií, a zahŕňajú údaje z oddelení zaoberajúcich sa zbraňami, muníciou a bojovými vozidlami. Zoznam zahŕňa informácie staré až desať rokov, čo môže znamenať, že medzi uniknutými údajmi sú mená bývalých študentov, ktorí môžu byť teraz v aktívnej službe. (27)

Podľa vyjadrení odborníka na kybernetickú bezpečnosť, hoci množstvo ukradnutých dokumentov samo o sebe nemusí predstavovať problém, stačí jeden kritický dokument, aby situácia bola vážna. Útočníci navyše vyhlasujú, že ak nedôjde k dohode s univerzitou o výkupnom, plánujú v októbri zverejniť ďalších 750 gigabajtov dát. (27)

Presne to sa stalo v prípade brnianskej univerzity, ktorá predtým odmietla zaplatiť požadované výkupné. Hackeri zverejnili prvú várku údajov. Sú medzi nimi osobné údaje prednášajúcich, ktorí sú v mnohých prípadoch vysokými vojenskými dôstojníkmi. Sú v nej uvedené ich adresy, dátumy narodenia a osobné telefónne čísla. Týka sa to oddelení logistiky a krízového riadenia. Podľa hackerov sa očakáva, že ich budú nasledovať aj ďalšie fakulty. Podľa plukovníka Otakara Foltýna z Vojenskej kancelárie prezidenta republiky, ktorý je bývalým náčelníkom Vojenskej polície, je závažnosť úniku informácií vysoká. *"Z vysokoškolákov sa stanú dôstojníci, o 20 rokov budú na vrchole velenia. Nepriateľské spravodajské služby bude prirodzene zaujímať, ako vyzerá príprava budúcich veliteľov*.“ (27)

3.2 Kybernetický zákon

Zákon 181/2014 Sb. o kybernetické bezpečnosti a o zmenách súvisiacich zákonov, ktorý bol prijatý dňa 23. júla 2014 a platný dňa 1. januára 2015, sa priamo nezameriava na univerzity, ale stanovuje všeobecné povinnosti pre rôzne subjekty v oblasti kybernetickej bezpečnosti. V zákone sú špecifikované povinnosti pre orgány verejnej moci, správcov a prevádzkovateľov kritických informačných systémov a infraštruktúry, poskytovateľov základných a digitálnych služieb a ďalších. (28)

K tomuto zákonu patria aj ďalšie podporné zákony, nariadenia a vyhlášky *(32)*:

- *Smernica Európskeho parlamentu a Rady (EU) 2016/1148 zo 6. júla 2016 o opatreniach k zaisteni vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernice NIST)*
- *Vyhláška o kybernetickej bezpečnosti*
- *Vyhláška č. 317/2014 Sb., o významných informačných systémoch a ich určujúcich kritériách*
- *Nariadenie vlády č. 432/2010 Sb., o kritériách pre určenie prvkov kritickej infraštruktúry*

- *Vyhláška č. 437/2017 Sb., o kritériách pre určenie prevádzkovateľa základnej služby*

Ak univerzity spadajú do niektorej z týchto kategórií, napríklad ako prevádzkovatelia významných informačných systémov alebo ako súčasť kritickej infraštruktúry, môžu byť povinnosti stanovené v tomto zákone pre ne relevantné (32).

Tabuľka 1 Povinnosti z hľadiska kybernetického zákona [Zdroj: 32]

Povinnosť	***EK***	***VS***	***IS/KS KII, VIS, IS ZS***	***PZS***	***PDS***
Písmeno § 3 KBZ	*a*	*b*	*c, d, e, f*	*g*	*h*
Hlásiť kontaktné údaje národnému CERT	✓	✓	x	x	✓
Hlásiť kontaktné údaje vládnemu CERT	x	x	✓	✓	x
Detekovať kybernetické bezpečnostné udalosti	x	✓	✓	x	x
Hlásiť kybernetické bezpečnostné incidenty[1]	x	✓	✓	x	✓2
Zavádzať bezpečnostné opatrenia a viesť o nich dokumentáciu	x	x	✓	x	✓3
Zohľadňovať požiadavky vyplývajúce z bezpečnostných opatrení pri výbere dodávateľov pre ich IS alebo KS systém	x	x	✓	x	x
Zavádzať reaktívne opatrenia vydané Úradom	✓4	✓4	✓	x	x
Zavádzať ochranné opatrenia vydané Úradom	x	x	✓	x	x
Ohlasovať Úradu zavedenie reaktívneho opatrenia a jeho výsledok	✓	✓	✓	x	x

1 = subjekt hlási incident tam, kde je evidovaný (národný alebo vládny CERT) s výnimkou viď 2.

2 = pokiaľ má významný dopad na poskytovanie jeho služieb, hlási to národnému CERT, pokiaľ má významný dopad na kontinuitu poskytovania základnej služby, tak hlási vládnemu CERT.
3 = nie sú dané žiadne konkrétne opatrenia zo strany štátu, PDS prijíma opatrenia, ktoré on považuje za vhodné.
4 = len za stavu kybernetického nebezpečia alebo za núdzového stavu vyhláseného na základe žiadosti podľa § 21 odstavec 6.(32)

3.3 Opis prostredia

Fakulta podnikateľská Vysokého učení technického (VUT) v Brne je jednou z popredných inštitúcií vo vzdelávaní v oblasti podnikania a manažmentu nielen v Českej republike, ale aj v strednej Európe. Bola založená v roku 1991. (29) (30)

Po páde komunizmu a otvorení nových možností v ekonomike začal rásť záujem o podnikanie a manažérske zručnosti. V tomto kontexte bola zriadená Fakulta podnikateľská VUT v Brne. Jej cieľom bolo pripraviť študentov na podnikateľské prostredie a poskytnúť im znalosti a nástroje potrebné pre úspešnú kariéru v oblasti manažmentu, podnikania a ekonomiky. Od svojho založenia fakulta prešla významným vývojom a rozšírením svojich študijných programov. Ponuka odborov sa postupne rozšírila o rôzne špecializácie v oblastiach ako je podnikové hospodárstvo, manažment, medzinárodné podnikanie, ekonomika a manažérska informatika. (29) (30)

Fakulta podnikateľská VUT v Brne sa stala centrom výskumu a vzdelávania v oblasti podnikania a manažmentu. Spolupracuje s radom firiem a inštitúcií ako v Českej republike, tak aj v zahraničí. Študenti tu majú možnosť získať praktické skúsenosti prostredníctvom stáží a projektov v reálnom podnikateľskom prostredí. (29) (30)

V priebehu rokov sa fakulta stala obľúbenou destináciou pre študentov ako z Českej republiky, tak aj zo zahraničia. Jej absolventi sa presadzujú v rôznych odvetviach a zastávajú vedúce pozície v renomovaných spoločnostiach po celom svete. (29) (30)

3.4 Analytická časť

Táto časť práce predstavuje kritickú analýzu spoločnosti. Najprv bude vykonaná analýza vonkajšieho (mikro a makro) prostredia prostredníctvom metódy SLEPTE, ďalej bude analyzované prostredie pomocou Porterovho modelu piatich konkurenčných síl. S využitím metódy McKinsey 7S budú analyzované faktory ovplyvňujúce vnútorné prostredie. Všetky výstupy z týchto analýz budú na záver zhrnuté do SWOT analýzy.

3.4.1 Vonkajšie faktory

V časti vonkajšie faktory rozoberieme faktory pomocou SLEPTE a Porterovho modelu piatich síl.

SLEPTE analýza

Sociálne faktory

Medzi hlavné faktory ovplyvňujúce univerzitu patrí počet ľudí so záujmom o štúdium. Fakulta prepája záujem o podnikateľské vzdelanie v súvislosti s rastúcou podnikateľskou kultúrou a snahou jednotlivcov dosiahnuť podnikateľský úspech, s neustále stúpajúcim záujmom o informačné technológie. Súčasne je univerzita čoraz viac multikultúrna, čo prináša na fakultu rôznorodé pohľady a kultúrne skúsenosti študentov.

Legislatívne faktory

Vzhľadom k štatútu vysokej školy je univerzita ovplyvňovaná viacero zákonmi nie len základných správnych orgánov - napríklad zákony týkajúce sa vysokých škôl, zákon o ochrane osobných údajov, o autorských právach, pracovné právo, verejné obstarávanie, finančné a daňové zákony a v neposlednom rade o zdraví a bezpečnosti - ale aj z hľadiska bezpečnosti a kybernetickej bezpečnosti – Zákon o kybernetickej bezpečnosti, nariadenie o internetovej neutralite, zákon o kybernetickej bezpečnosti. Zákon o elektronických komunikáciách. Pre vysoké školy je dôležité, aby boli informované o všetkých relevantných zákonoch a reguláciách a aby zaviedli vhodné

postupy na zabezpečenie súladu s nimi, najmä pri používaní aj cloudových technológií. To zahŕňa zabezpečenie zmlúv s poskytovateľmi cloudových služieb, ktoré zohľadňujú požiadavky na ochranu a bezpečnosť dát.

Ekonomické faktory

O tom, ako sa bude univerzite dariť rozhoduje viacero ekonomických faktorov. Napríklad v časoch ekonomickej neistoty môže byť záujem o vzdelanie a výdavkov na vzdelanie menší- čo by mohlo viesť k poklesu zápisov do univerzity. Veľká zamestnanosť, resp. nezamestnanosť absolventov ovplyvňuje reputáciu univerzity a záujem. V prípade poklesu štátneho financovania univerzity môže dôjsť k zníženiu kvality vzdelávania.

Politické faktory

Mimo vojny , ktorá sa aktuálne odohráva na Ukraine, nenachádza sa Česká ani Slovenská republika v žiadnom stave, ktorý by mal ovplyvňovať fakultné / univerzitné prostredie. Politické udalosti a vzťahy medzi krajinami môžu ovplyvniť medzinárodnú spoluprácu a mobilitu študentov a pracovníkov na fakulte.

Technologické faktory

Technologické faktory hrajú kľúčovú úlohu v transformácii a rozvoji vysokých škôl, pričom ich vplyv sa prejavuje vo viacerých aspektoch akademickej a administratívnej činnosti. Digitalizácia vzdelávacích a správnych procesov otvára nové možnosti pre efektívnejšie spravovanie škôl a prístup študentov k vzdelávaniu, napríklad prostredníctvom online kurzov a digitálnych knižníc. Rozvoj vzdialeného vzdelávania, posilnený technológiami ako video konferencie a virtuálne triedy, zabezpečuje kontinuitu vzdelávania aj v náročných obdobiach a umožňuje študentom flexibilnejšie sa zapájať do študijného procesu z rôznych geografických lokácií. Kybernetická bezpečnosť sa stáva prioritou v ochrane dát študentov a výskumných informácií pred kybernetickými hrozbami. Vysoké univerzity tiež čelia potrebe modernizovať svoje výskumné infraštruktúry pomocou najnovších technológií, čím zvyšujú svoju výskumnú kapacitu a lákavosť pre študentov. Okrem toho „green way“ a udržateľné postupy začínajú byť

integrálnou súčasťou univerzitného prostredia, čím sa zvyšuje environmentálna zodpovednosť a poskytuje vzor pre budúce generácie. Technologické inovácie, ako sú aplikácie virtuálnej a rozšírenej reality v pedagogike, navyše transformujú tradičné vzdelávacie metódy a zvyšujú zapojenie a motiváciu študentov. Vysoké školy, ktoré sú schopné pružne reagovať na technologický pokrok a integrovať nové technológie do svojho fungovania, si tak môžu udržať konkurencieschopnosť a lepšie pripraviť svojich študentov na výzvy budúcnosti.

Porterov model piatich konkurenčných síl

V tejto kapitole sa budeme venovať aplikácii Porterovho modelu na Fakultu podnikateľskú VUT v Brne:

1. Hrozba nových vstupov na trh: - Vysoká -

Vstup do odvetvia vzdelávania nie je nijakým spôsobom obmedzený. Nové online vzdelávacie platformy, ako aj nové vysokoškolské inštitúcie, môžu vstúpiť na trh s relatívne nízkymi vstupnými bariérami.

2. Dodávatelia: - Nízka až stredná -

Fakulta má obvykle viac možností výberu dodávateľov, napríklad dodávateľov technologických zariadení alebo vzdelávacích materiálov. Avšak, v niektorých prípadoch môže závisieť od istých kľúčových prvkov, napríklad kníh alebo špecializovaných laboratórnych zariadení.

3. Hrozba substitúcií: - Nízka až stredná -

Napriek existencii online vzdelávania je vysokoškolské vzdelanie stále cenovo efektívnym a významným spôsobom získavania kvalifikácie. Avšak, vzhľadom na rastúcu popularitu online kurzov a alternatívnych foriem vzdelávania, je potrebné sledovať konkurenčné substitúcie.

4. Odoberatelia: - Vysoká -

Študenti a ich rodičia majú často veľký vplyv na výber vysokoškolského vzdelania. Ich rozhodnutia sú ovplyvnené nielen kvalitou výučby, ale aj cenou, renomé univerzity a dostupnosťou štipendií a iných finančných pomôcok.

5. Iné konkurencie v odvetví: - Vysoká -

Konkurencia medzi vysokoškolskými inštitúciami je obvykle veľmi silná, pričom univerzity sú aktívne v konkurenčných snahách o získanie študentov, fondy a akademických pracovníkov.

3.4.2 Vnútorné faktory

V tejto časti budeme využívať vnútornú analýzu pre kritické faktory úspechu – konkrétne pôjde o model McKinseyho 7S.

McKinsey 7S

Na základe poskytnutých informácií, využijeme rámec McKinsey 7S na analýzu vnútorného prostredia Fakulty podnikateľskej VUT v Brne. Rámec 7S zahŕňa sedem kľúčových prvkov: stratégiu, štruktúru, systémy, spoločné hodnoty (zdieľané hodnoty), štýl, zamestnancov a zručnosti, ktoré by mali byť vzájomne v harmónii, aby univerzita dosiahla úspech.

1. Stratégia

Fakulta sa zameriava na prípravu študentov na podnikateľské prostredie, ponúkaním širokého spektra študijných programov, ktoré pokrývajú podnikové hospodárstvo, manažment, medzinárodné podnikanie, ekonomiku a podnikovú informatiku. Stratégia fakulty je adaptívna voči meniacim sa požiadavkám trhu práce a technologickému pokroku, čo umožňuje študentom získať relevantné znalosti a zručnosti.

2. Štruktúra

VUT má decentralizovanú štruktúru, čo podporuje flexibilitu a inovácie v rámci rôznych fakúlt, katedier a odborov. Táto štruktúra umožňuje efektívnu spoluprácu s firmami a inštitúciami a podporuje medzinárodnú mobilitu študentov a akademických pracovníkov.

3. Systémy

Fakulta implementuje rôzne administratívne a vzdelávacie systémy, ktoré podporujú digitalizáciu vzdelávania. Využívanie cloudových technológií, digitalizovaných knižničných služieb a online hodín, kurzov umožňuje efektívne spravovanie univerzity a zabezpečuje prístup študentov k vzdelávaciemu materiálu.

4. Spoločné hodnoty

Zdieľané hodnoty fakulty odrážajú dôraz na podnikateľskú kultúru, inovácie a medzinárodnú spoluprácu. Multikultúrne prostredie a spolupráca s priemyselnými partnermi podporujú tieto hodnoty a posilňujú reputáciu fakulty ako vedúcej inštitúcie v oblasti podnikania a manažmentu.

5. Štýl vedenia

Vedenie fakulty podporuje otvorenú komunikáciu, inovácie a osobný rozvoj študentov a zamestnancov. Dôraz na praktické skúsenosti prostredníctvom stáží a projektov v reálnom podnikateľskom prostredí naznačuje participatívny prístup k vedeniu. V rámci štúdia majú žiaci dokonca povinnú prax.

6. Zamestnanci

Fakulta zamestnáva kvalifikovaných akademických a administratívnych pracovníkov, ktorí sú schopní poskytovať vysokokvalitné vzdelávanie a podporu študentom. Dôraz na kontinuálne vzdelávanie a profesionálny rozvoj zamestnancov prispieva k udržiavaniu vysokého štandardu vzdelávania. Nielenže kladú dôraz na tituly, taktiež sú profesori povinní vydávať v rôznych intervaloch články a knihy.

7. Zručnosti

Študenti a absolventi fakulty majú získavať široké spektrum zručností, od odborných znalostí v oblasti podnikania a manažmentu po medzikultúrnu kompetentnosť a schopnosť inovácii.

3.4.3 SWOT analýza

Silné stránky (Strengths)

- Prestížna pozícia v oblasti podnikateľského vzdelávania a výskumu
- Široká ponuka študijných programov a špecializácií
- Silná spolupráca s podnikmi a inštitúciami – poskytnutie praktických skúseností
- Významné investície do technologického vybavenia a modernizácie výučby
- Aktívna účasť na medzinárodných výskumných projektoch a výmenných programoch

Slabé stránky (Weaknesses)

- Závislosť od verejných financií a príjmov z univerzitných poplatkov
- Nedostatok flexibility vo výučbe a administratíve kvôli byrokratickým procesom
- Nedostatok jasnej stratégie na riadenie rastúcej konkurencie zo strany online vzdelávacích platforiem a zahraničných univerzít

Príležitosti (Opportunities)

- Rastúci dopyt po podnikateľskom vzdelaní v súvislosti so zvýšeným záujmom o podnikanie a inovácie
- Možnosť rozšírenia ponuky online kurzov a dištančného vzdelávania pre medzinárodných študentov
- Získavanie finančnej podpory od súkromných firiem a nadácií na rozvoj výskumu a inovácií
- Posilnenie medzinárodnej spolupráce a zvýšenie mobility študentov a pracovníkov
- Využitie moderných technológií a digitálnych nástrojov na zlepšenie výučby a komunikácie

Hrozby (Threats)

- Konkurencia zo strany nových vstupov, ako sú online vzdelávacie platformy a zahraničné univerzity
- Zmeny v legislatíve týkajúcej sa financovania vzdelávania a výskumu

- Rastúca náročnosť študentov a ich očakávania voči kvalite a flexibilite vzdelávacieho procesu
- Možné obmedzenia mobility študentov a pracovníkov v dôsledku geopolitických udalostí alebo zdravotných kríz
- Technologické výzvy spojené so udržiavaním krokov s rýchlym technologickým vývojom a zabezpečením prístupnosti moderných technologických nástrojov
- Aktuálna klesajúca potreba vysokoškolských titulov v súkromnom sektore

Výsledkom je, že negatívne vlastnosti prevažujú nad pozitívnymi.

3.4.4 Súhrn analýz

Zmena ktorej sa budeme venovať bola vybraná na základe predošlých analýz.

Na základe SWOT analýzy pre Fakultu podnikateľskú Vysokého učení technického (VUT) v Brne, ktorú sme práve vykonali, by som odporučila nasledujúce kroky pre riadenú zmenu:

Zmiernenie slabých stránok:

Zlepšenie flexibility vo výučbe a administratíve fakulty môže vyžadovať revíziu interných procesov a štruktúry riadenia s cieľom zefektívniť rozhodovacie mechanizmy a zvýšiť agilitu v riešení problémov.

3.5 Riziková politika

V tejto časti sa budeme zaoberať efektívnou metódou redukcie rizika. Jej výhody sú, že je efektívna prijateľná, účinná a včasná.

3.5.1 Analýza rizík

Najprv budú identifikované riziká, ktoré vstupujú do zavedenia zmeny, tie budú pomocou skórovanej metódy ohodnotené. Následne bude aplikovaná metóda zníženia rizík, ktorá zahŕňa aj konkrétne opatrenia, ktoré by mohli viesť k zníženiu ich pravdepodobnosti alebo zmierňovaniu dopadu.

Ohodnotenie rizík pomocou skórovanej metódy

Tabuľka 2 Ohodnotenie pravdepodobnosti výskytu [Zdroj: vlastné spracovanie]

PRAVDEPODOBNOSŤ HROZBY		**DOPAD HROZBY**				
		Zanedbateľný	**Minimálny**	**Stredný**	**Závažný**	**Katastrofický**
		5	20	50	70	100
Vysoká	1	5	20	50	70	100
Stredná	0.8	4	16	40	56	80
Nízka	0.5	2.5	10	25	35	50
Veľmi nízka	0.1	0.5	2	5	7	10

Tabuľka 3 Ohodnotenie dopadu [Zdroj: Vlastné spracovanie]

DOPAD HROZBY	
HODNOTA	**OPIS DOPADU**
5	**Zanedbateľný**
20	**Minimálny**
50	**Stredný**
70	**Závažný**
100	**Katastrofický**

Tabuľka 4 Analýza rizík [Zdroj: Vlastné spracovanie]

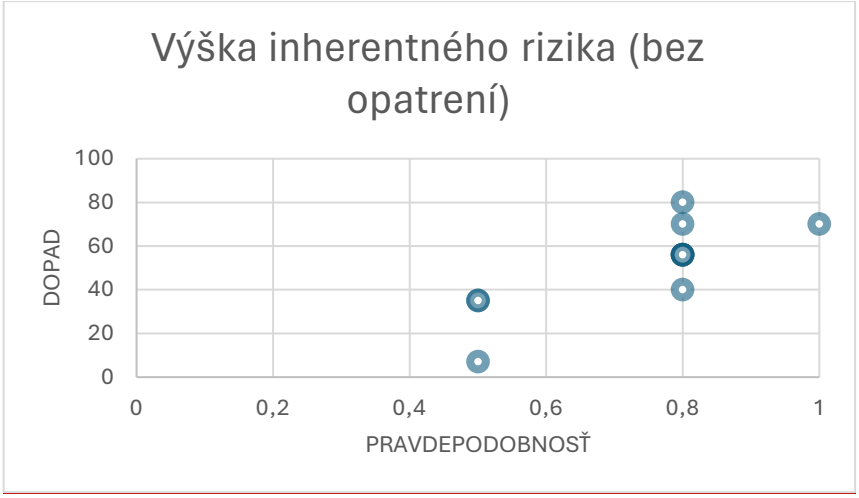
Hrozby	Popis hrozby	Pravdepodobnosť (slovne)	Pravdepodobnosť (hodnota)	Dopad (slovne)	Dopad (hodnota)	Výška inherentného rizika Hodnota	Slovné hodnotenie
Únik informácií	Náhodné alebo cielené získanie údajov neautorizovanými alebo autorizovanými osobami a ich využitie nepovoleným spôsobom, nelegálne zhromažďovanie údajov.	**Stredná**	**0.8**	**Stredný**	**50**	**40**	***NÍZKE***
Infiltrácia	Plánovaná aktivita za účelom získania informácií napríklad pre získanie výhod v konkurenčnom prostredí.	**Stredná**	**0.8**	**Katastrofický**	**100**	**80**	***MIMORIADNE VYSOKÉ***
Krádež	Aktivita, ktorej cieľom je neoprávnené získanie / nadobudnutie aktív vo vlastníctve spoločnosti.	**Stredná**	**0.8**	**Závažný**	**70**	**56**	***VYSOKÉ***

Neautorizovaná činnosť	Výkon činností, ktoré sú v rozpore so zásadami používania prostriedkov v prostredí IS/ICT Výkon činností, ktoré sú v rozpore s právami a povinnosťami a platnými zmluvami	**Stredná**	**0.8**	**Závažný**	**70**	**56**	***VYSOKÉ***
Nedostatočné riadenie informačnej bezpečnosti	Nejasná stratégia a koncepcia, organizačné problémy (zdieľanie funkcií, nedostatočné kompetencie)	**Vysoká**	**1**	**Závažný**	**70**	**70**	***VYSOKÉ***
Nejasne, alebo zle interpretovaná legislatíva	Nedodržanie požiadaviek stanovených legislatívou, prevádzkovanie IS/ICT v rozpore s požiadavkami legislatívy.	**Stredná**	**0.8**	**Závažný**	**70**	**56**	***VYSOKÉ***
Porušenie legislatívy	Úmyselné porušenie legislatívy personálom.	**Stredná**	**0.8**	**Závažný**	**70**	**56**	***VYSOKÉ***

Podvod	Cieľavedomá činnosť osôb (interných zamestnancov, externých spolupracovníkov), ktorej cieľom je nelegálne obohatenie.	**Stredná**	**0.8**	**Závažný**	**70**	**56**	***VYSOKÉ***
Škodlivý softvér	Softvér vykonávajúci / umožňujúci vykonanie nežiaducich aktivít v prostredí IS/ICT (vírusy, červy, trójske kone a pod).	**Nízka**	**0.5**	**Závažný**	**70**	**35**	***NÍZKE***
Sociálne inžinierstvo, prinútenie k spolupráci	Plánovaná aktivita za účelom získania informácií a/alebo získania prístupu k nim zneužitím dôvery personálu spoločnosti alebo prinútením zamestnanca vydieraním, zastrašovaním a pod..	**Stredná**	**0.8**	**Závažný**	**70**	**70**	***VYSOKÉ***

Terorizmus	Plánovaná aktivita v okolí objektu alebo v objekte s cieľom spôsobiť škody. Teroristický útok je realizovaný osobami, ktoré nie sú v pracovno-právnom (alebo inom obdobnom) vzťahu so spoločnosťou.	**Nízka**	**0.5**	**Závažný**	**70**	**7**	***ZANEDBATEĽNÉ***
Únik informácií	Náhodné alebo cielené získanie údajov neautorizovanými alebo autorizovanými osobami a ich využitie nepovoleným spôsobom, nelegálne zhromažďovanie údajov.	**Nízka**	**0.5**	**Závažný**	**70**	**35**	***NÍZKE***

V tabuľke sú ohodnotené jednotlivé riziká podľa bodovacieho systému uvedeného vyššie



Graf 1 Mapa rizík [Zdroj: vlastné spracovanie]

3.6 Analýza incidentu v prostredí VUT

V období od 4. septembra 2021 prebiehal na univerzite incident, z ktorého sme obdržali výslednú správu. Na základe výslednej správy sme boli schopní vytýčiť niekoľko bodov, ktoré mohli incidentu pomôcť predísť alebo potencionálne úplne zamedziť.

Pre analýzu incidentu bola dodaná kópia súborového systému kompromitovanej webovej aplikácie (súbor fp-mba-zavirovana.zip). V čase analýzy bežala webová aplikácia na CMS WordPress 5.8, čo je najnovšia hlavná verzia tohto CMS. Webová aplikácia bežala však na staršej verzii WordPressu, čo viedlo ku kompromitácii, a táto aktualizácia prebehla až v rámci riešenia incidentu. Analýza preukázala prítomnosť niekoľkých škodlivých súborov.

Dodaný súbor MSedge_cache.7z obsahoval nacachované súbory pri prístupe k webovým aplikáciám, avšak neobsahuje žiadne škodlivé súbory. Súbor quarantine.7z obsahuje súbory v karanténe umiestnené nástrojom Fortinet. Ďalej boli dodané prístupové logy z webového servera, počiatok dostupných logov siaha k 4. septembru 2021. V danom časovom období bola analýzou logov preukázaná škodlivá komunikácia, avšak vzhľadom na to, že nie je dostupné dlhšie časové obdobie, nie je možné dokázať, kedy a akým spôsobom došlo k kompromitácii. Záujem bol zameraný predovšetkým na komunikáciu medzi NÚKIB (185.48.22.35) a kompromitovanou webovou aplikáciou. Komplexná analýza bola iniciovaná po kompromitovaní webovej aplikácie bežiacej na WordPress 5.8, ktorý bol potenciálne aktualizovaný počas alebo po incidente. Dodané údaje zahŕňali

kópiu kompromitovaného súborového systému, nacachované súbory webovej aplikácie, karanténované škodlivé súbory a prístupové logy webového servera.

Po tom , čo Webový portál MBA začal nečakane rozosielať spam, NÚKIB portál umiestnil na čiernu listinu. Incident nastal v čase, keď na oddelení incident handlingu pracoval študent 5. ročníka, ktorý sa rozhodol aktívne zasiahnuť.

Študent univerzity sa pokúsil kontaktovať CSIRT tím servisnej organizácie CVIS, no neúspešne, keďže na CVIS o incidente nikto nevedel. Po neúspešnom pokuse komunikovať so zodpovednou osobou na CVIS, študent kontaktoval hostingovú spoločnosť, ktorá portál MBA hostovala. Tento kontakt bol úspešný a problém bol následne odstránený.

Tento incident poukázal na významné bezpečnostné nedostatky a zraniteľnosti v konfigurácii a monitoringu webového servera.

Kľúčové zistenia a analýza

1. **Malware Analýza**:

    - JavaScriptové súbory **f_001aff a f_001b05** boli napadnuté malwareom typu JS/Agent.NDSW!, ktorý ukladá informácie. Malware inicioval komunikáciu so skriptom blue.php na serveri, ktorý zberá údaje o používateľoch (IP adresa, user agent, referrer) a mohol pôsobiť ako backdoor pri zaslaní špecifických GET parametrov.
    - Modifikácia súboru **wp-load.php** zahŕňala vloženie Webshell Droppera, čo umožnilo ďalšie škodlivé činnosti, vrátane úniku údajov na externé škodlivé domény.

2. **Identifikované technické zraniteľnosti**:

    - Server pravdepodobne nebol chránený firewallom (z analýzy incidentu nie je možné vyčítať, že by server chránený firewallom bol), čo mohlo umožniť neobmedzený prístup z internetu a zvýšilo riziko napadnutia.

- Monitoring nie je dostačujúci**.** Logy zachytili podozrivú aktivitu a vidíme ju retrospektívne. Systém pravdepodobne nebol schopný identifikovať škodlivé aktivity v reálnom čase, čo umožnilo dlhodobé zneužívanie zraniteľností bez zásahu.
- Software, ktorý sa používal, bol neaktualizovaný. Nedostatky v správe aktualizácií (neaktualizovaný Wordpress) mohli ponechať neopravené zraniteľnosti, ktoré boli zneužité na infiltráciu malware.
- Zvykom v „security operation centre“, skrátene SOC, je mať dva tímy – thread intelligence a thread hunters. Prvý tím dodáva informácie, ako sú „novinky“ v kybernetických hrozbách a zraniteľnostiach. Druhý tím proaktívne hľadá takéto zraniteľnosti a hrozby v infraštruktúre. Ani jeden z tímov neoperuje na pôde univezrity. Ak by tieto dva tímy na univerzite fungovali, mohli by popredne vedieť rozpoznať a zamedziť alebo blokovať tuto komunikáciu.
- Univerzita používa FortiClient. FortiClient má databázu signatúr, ktoré fungujú ako odtlačky prstov pre vírusy, avšak ak je vírus nový a nie veľmi známy, nemusí ho vedieť detegovať.
- Útočník pravdepodobne musel vykonať formu skenu prostredia, aby zistil, že server má zraniteľnú aplikáciu – táto aktivita nebola zaznamenaná v logovacom systéme.
- V prípade, že sa ukradli citlivé dáta, po incidente nebola vykonaná forenzná analýza, aby sa zistilo, k čomu ešte útočník pristúpil a či neboli ukradnuté aj iné informácie.

3. Identifikované procesné zraniteľnosti

- Nedostatočný faktor je komunikácia. Absencia komunikácie a povedomia v rámci CSIRT tímu CVIS o incidente naznačuje potrebu lepšej internej koordinácie, komunikácie a informovanosti.
- Fakt, že hosťovaný portál MBA nebol podložený SLA (Service Level Agreement), poukazuje na nedostatočné formálne zabezpečenie služieb. ktoré by zahrňovalo aj rýchle a efektívne riešenie takýchto incidentov.

- Priebeh udalostí ukazuje, že prvá reakcia na incident neprebiehala cez oficiálne kanály, ale až na základe iniciatívy študenta, čo môže znamenať nedostatočnú pripravenosť alebo nedostatočné zdroje na riešenie incidentov zo strany CVIS.
- Nie je vedená evidencia o revízii procesov v súvislosti s detekciou, reakciou a komunikáciou v prípade bezpečnostných incidentov. Je potrebné revidovať procesy. Incident odhalil potrebu prehodnotiť a zlepšiť procesy detekcie, reakcie a komunikácie v prípade bezpečnostných incidentov.

3.7 Směrnice č. 1/2024 řízení kybernetické a informační bezpečnosti VUT

Smernica č. 1/2024 o riadení kybernetickej a informačnej bezpečnosti na Vysokom učení technickom v Brne (VUT) stanovuje komplexný rámec pre zabezpečenie kybernetickej a informačnej bezpečnosti na univerzite. Smernica, ktorá nadobúda účinnosť 1. februára 2024, definuje zodpovednosti a role zainteresovaných strán a zavádza opatrenia pre zabezpečenie bezpečnosti a odolnosti voči kybernetickým hrozbám (31).

- **Účel -** Smernica definuje osoby zodpovedné za riadenie kybernetickej a informačnej bezpečnosti na VUT a stanovuje ich práva a povinnosti s cieľom zabezpečiť kybernetickú bezpečnosť a odolnosť v súlade s právnymi predpismi.
- **Role -** Ustanovuje role Manažéra kybernetickej bezpečnosti, Architekta kybernetickej bezpečnosti a Auditora kybernetickej bezpečnosti, pričom každá z týchto rolí má svoje špecifické úlohy a zodpovednosti. Zvláštnou normou je tiež zriadený Výbor pre riadenie kybernetickej bezpečnosti (Výbor KB), ktorý schvaľuje stratégiu kybernetickej bezpečnosti a vyhodnocuje stav kybernetickej bezpečnosti na univerzite.
- **Manažér kybernetickej bezpečnosti -** Zodpovedá za komunikáciu s Národným úradom pre kybernetickú a informačnú bezpečnosť (NÚKIB), evidenciu aktív, koordináciu riešenia kybernetických bezpečnostných udalostí a incidentov, ako aj za plánovanie a riadenie projektov kybernetickej bezpečnosti.

- **Architekt kybernetickej bezpečnosti -** Navrhuje vhodné postupy a opatrenia pre kybernetickú bezpečnosť, udržuje dokumentáciu v aktuálnej podobe, identifikuje riziká a navrhuje opatrenia na ich zníženie.
- **Audítor kybernetickej bezpečnosti** -Vykonáva dohľad nad implementáciou modelov a opatrení, vypracováva záverečné a priebežné správy o implementácii opatrení a plnení stratégie kybernetickej bezpečnosti, a informuje Výbor KB o výsledkoch auditu.
- **Garant aktíva -** Zodpovedá za konkrétne aktívum a vykonáva všetky rozhodnutia s ním spojené, zabezpečuje poskytovanie informácií potrebných pre hodnotenie rizík a aplikáciu opatrení vyplývajúcich zo schválených dokumentov.
- **Kybernetické bezpečnostné udalosti a incidenty -** Smernica stanovuje postupy pre riešenie a hlásenie kybernetických bezpečnostných udalostí a incidentov, kde každý zamestnanec je povinný pri zistení udalosti alebo incidentu podniknúť kroky na elimináciu prípadnej ujmy a informovať o tom Manažéra kybernetickej bezpečnosti.

Záverečné ustanovenia uvádzajú, že Rektor do 30 dní od nadobudnutia účinnosti smernice vymenuje Manažéra KB, Architekta KB, Audítora KB a členov (31).

3.8 Vyhodnotenie analýzy prostredia incidentu

Na základe uvedenia analýzy konkrétneho incidentu na VUT sme z technického hľadiska detegovali niekoľko hrozieb, ktoré vyústili do incidentu.

Po vyhodnotení súborových dotazníkov, ktoré sme distribuovali medzi zamestnancov a študentov Vysokého Učení Technického v Brne, spolu s pozorovaniami prístupov k digitálnym zdrojom a analýzou existujúcich bezpečnostných postupov, sme zistili, že na univerzite prevláda značná absencia školení a aktivít na zvyšovanie povedomia o kybernetickej bezpečnosti. Napriek tomu, že smernica č. 1/2024 o riadení kybernetickej a informačnej bezpečnosti stanovuje jasné rámce a zodpovednosti, v praxi sme identifikovali významné nedostatky v implementácii a šírení týchto zásad medzi koncovými používateľmi.

Pozorovania naznačujú, že mnohí zamestnanci a študenti nie sú plne informovaní o základných princípoch kybernetickej bezpečnosti, potenciálnych hrozbách a najlepších praktikách na ich predchádzanie, chýba efektívna komunikácia v rámci univerzitného prostredia a v prípade potencionálneho incidentu , ako napríklad incident spomínaný vyššie, je veľké riziko reputačného, informačného aj finančného rizika. Na základe analýzy súčasného stavu, analýzy rizík a analýzy posledného incidentu na Vysokom Učení Technickom v Brne sme sa rozhodli vytvoriť cvičenie table top na základe podobného incidentu pre preukázanie dôležitosti bodov vytýčených z analýzy.

4 NÁVRH VLASTNÉHO RIEŠENIA

4.1. Simulácia Table Top cvičenia

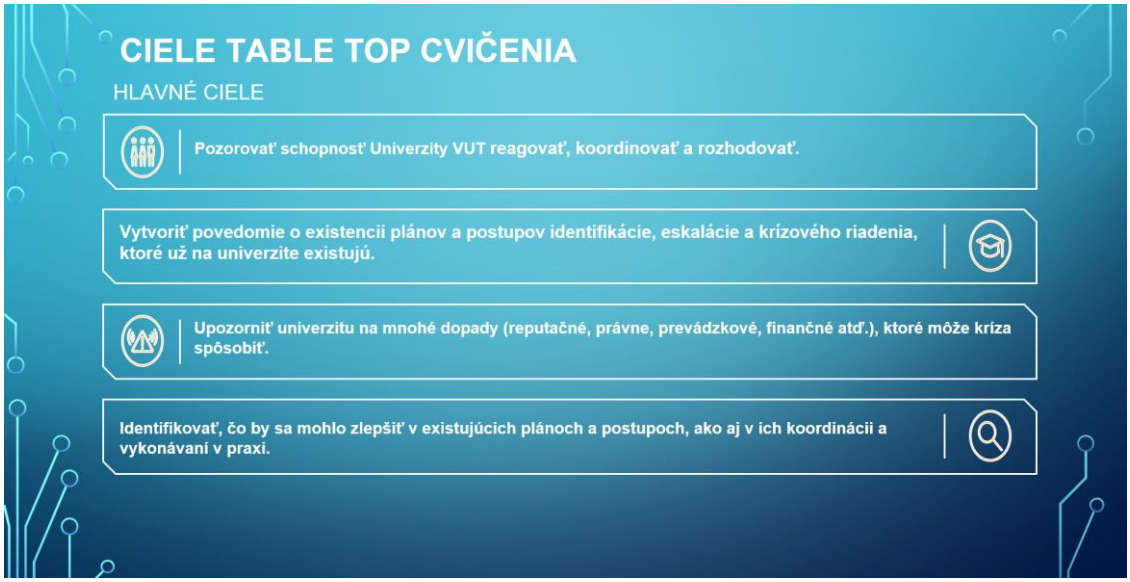
Riešenie je tvorené viacerými „power point“ prezentáciami. Prezentácia je prezentovaná účastníkom v reálnom čase. Pre diplomovú prácu však bude využívaný opis týchto stránok prezentácie a opis procesov prebiehajúcich v pozadí týchto stránok. Prezentácie sa skladajú z týchto častí:

1. Ciele table top cvičenia
2. Prečo je cvičenie dôležité?
3. Príklady z iných incidentov
4. Pravidlá a štruktúra
5. Dynamika cvičenia
6. Rozdelenie účastníkov
7. Úvodný kontext cvičenia
8. Simulácia
9. „Hot debrief“ simulácie
10. Spracovanie Feedbacku
11. Komplexnejšie vyhodnotenie
12. Prezentácia a diskusia výsledkov

[1] Ciele cvičenia

Prvé úvodne strany sa venujú zoznámeniu účastníka s typom table top cvičenia. Vysvetľujú, prečo je takéto cvičenie potrebné, čo ním , či univerzita, alebo samotný účastník, môže získať. Na ďalších stranách prezentácie je prehľad programu cvičenia. Obsahuje harmonogram aktivít a časový plán pre celý deň, vrátane uvítania účastníkov, prípadových štúdií a praktických cvičení. Tento slide je určený na to, aby účastníkom poskytol jasnú predstavu o tom, čo môžu očakávať počas dňa a ako bude cvičenie štruktúrované. Obsahujú pozorovanie schopnosti univerzity reagovať, koordinovať a rozhodovať, vytvorenie povedomia o existujúcich plánoch a postupoch identifikácie, eskalácie a krízového riadenia, upozornenie na mnohé dopady - reputačné, právne,

prevádzkové, finančné - ktoré môže incident spôsobiť, identifikáciu oblastí na zlepšenie v existujúcich plánoch a postupoch, ako aj ich koordinácii a vykonávaní v praxi, a hodnotenie výkonu a rozhodnutí prijatých univerzitou.



Obrázok 7 Ciele table top cvičení [Zdroj: Vlastné spracovanie]

[2] Útočníci a motivácie

Vysvetľuje dôvody, prečo by útočníci mohli potenciálne zaútočiť na univerzitu - získanie kontroly nad činnosťou konkrétneho oddelenia, dosiahnutie zisku, poškodenie dobrého mena univerzity, získanie uznania a slávy, negatívneho ovplyvňovania príjmov a činností spoločnosti, finančné podvody, a získavanie citlivých informácii.

Obrázok 8 Útočníci [Zdroj: Vlastné spracovanie]

[3] **Príklady z iných incidentov na univerzitách**

V slide „incidenty na iných univerzitách“ sa spomínajú incidenty, ktoré sme v práci spomenuli v kapitole 3.1 – predošlé incidenty v školskom prostredí.

Cieľom je poukázať, na základe príkladov z iných univerzít, na zvýšenú potrebu prevencie a pripravenosti voči daným útokom, z dôvodu ich zvyšujúcej sa frekvencie za obdobie posledných dvoch rokov.

[4] **Table top pravidlá a štruktúra**

Obsahuje zásady a organizáciu cvičenia, ktoré účastníci musia dodržiavať, aby bolo cvičenie efektívne a bezpečné. Hlavné pravidlá zahŕňajú:

- **Zákaz používania osobných zariadení** - Účastníkom sa oznámi, že počas cvičenia nesmú používať svoje osobné zariadenia. Všetky potrebné materiály a vybavenie im budú poskytnuté organizátormi.
- **Dôvernosť materiálov** - Materiály použité počas cvičenia sú považované za prísne dôverné. Účastníci sú vyzvaní, aby všetky materiály po skončení cvičenia nechali v miestnosti a nezdieľali informácie získané počas cvičenia mimo neho.
- **Rozdiel medzi reálnym a virtuálnym časom** - Cvičenie môže zahrňovať urýchlenie času na simuláciu dlhších období, aby bolo možné prejsť viacerými fázami incidentu alebo krízy v krátkom čase.
- **Nespochybňovanie scenára** - Účastníkom sa odporúča, aby nespochybňovali predpoklady alebo udalosti zadané v scenári, aj keď by sa mohli odlišovať od skutočnosti. Toto pravidlo je zavedené na zabezpečenie plynulého priebehu cvičenia a jeho dynamiky.
- **Dynamika cvičenia** - Slide zdôrazňuje, že udalosti počas cvičenia môžu byť dynamické a môžu sa líšiť od skutočných situácií. Tento prístup pomáha účastníkom cvičenia pripraviť sa na nečakané situácie a podporuje ich schopnosť adaptácie a rýchleho rozhodovania v krízových situáciách.

Obrázok 9 Pravidlá cvičenia [Zdroj: Vlastné spracovanie]

Tieto pravidlá a štruktúra cvičenia sú navrhnuté cielene, aby podporili účinné učenie a rozvoj zručností potrebných pre manažment kybernetických incidentov a krízové riadenie v kontrolovanom a bezpečnom prostredí. Bez obmedzení by sa ťažko simuloval kybernetický incident.

Obrázok 10 Pravidlá a štruktúra [Zdroj: Vlastné spracovanie]

[5] Table Top Účastníci

Na slide sa nachádza zoznam rôznych úloh alebo rolí, ktoré sú priradené účastníkom cvičenia. Presné role nie sú explicitne uvedené, zahŕňali by širokú škálu pozícií relevantných pre kybernetickú bezpečnosť a riadenie krízových situácií. Okrem toho sú tu aj lektori a asistenti table top cvičenia.

- **Rečník / Direktor -** Poskytuje zadanie cvičenia a vedie diskusiu. Podľa potreby tiež poskytuje ďalšie informácie alebo rieši otázky. Členovia tímu pre plánovanie cvičení môžu tiež pomáhať s facilitáciou počas cvičenia.
- **Zapisovateľ / Facilitátor -** Zapisovatelia sú pridelení k pozorovaniam a dokumentačným úlohám. Ich primárnou úlohou je dokumentovať diskusie účastníkov, vrátane toho, ako a či sa tieto diskusie zhodujú s plánmi, politikami a postupmi, čas reakcie a schopnosti kolaborovať v rámci skupiny.
- **Riadiaci tím** - Zodpovedá za strategické rozhodnutia a celkové vedenie počas cvičenia.
- **Bezpečnostný analytik** - Skúma bezpečnostné hrozby a poskytuje analýzy rizík.
- **IT tím** - Zodpovedný za správu a ochranu IT infraštruktúry.
- **Manažér incidentu -** Koordinuje reakciu na incidenty a zabezpečuje efektívnu komunikáciu medzi tímami.
- **Právne oddelenie** - Poradí s právnymi aspektmi incidentov, vrátane otázok súvisiacich s ochranou údajov.
- **Média a PR -** Zodpovedný za komunikáciu s médiami a verejnosťou.
- **Tím na obnovu po incidentoch** - Plánuje a koordinuje obnovu systémov a služieb po incidente.
- **Predstaviteľ regulačného orgánu -** Poskytuje usmernenia a podporu z externého hľadiska, môže zahŕňať zástupcov z NÚKIB alebo iných relevantných organizácií.

Obrázok 11 Účastníci [Zdroj: Vlastné spracovanie]

[6] Samotná simulácia

Následne začína samostatná simulácia s uvedením účastníkov do centra diania. Určí sa konkrétny dátum čas pre efektívne vtiahnutie do simulácie. Séria stránok postupne vytýči situáciu, v ktorej sa vrcholový manažment nachádza. Dôležitým prvotným bodom je rozpísanie si incidentu pomocou fázy, ktoré chceme simulovať. V predošlej analýze sme si rozobrali na základe akých chýb incident vznikol a teraz na nich budeme stavať a dotvárať autenticitu cvičenia.

Fáza 1 - Úvodný kontext

Scenár: Opísanie niekoľkých udalostí, ktoré ešte priamo neústia do incidentu

Ciele: Detekcia reakcie účastníkov

Úlohy: Evidovať hrozby, ktoré môže na VUT pôsobiť z daných udalostí

Fáza 2 - Spomalené webové stránky

Scenár: Študentská komora oznamuje spomalenie webových stránok

Ciele: Rýchlo identifikovať zdroj

Úlohy:

- Spraviť počiatočnú analýzu problému
- Informovať vedenie univerzity o probléme

Fáza 3 - Útok

Scenár: Oddelenie IT na univerzite zaznamená neobvyklú sieťovú aktivitu, ktorá naznačuje možný bezpečnostný incident

Ciele:

- Okamžite vyhodnotiť vplyv incidentu
- Nájsť efektívne spôsoby a osoby zodpovedné za odstránenie incidentu

Úlohy:

- Kontaktovať poskytovateľa hostingu portálu a vyžiadať si spoluprácu pri riešení incidentu
- Informovať vedenie fakulty o probléme a zistených komplikáciách

Fáza 4 - Spamy a NÚKIB

Scenár: Oddelenie IT zistí, že webový portál Univerzity MBA, ktorý beží na platforme WordPress, začal odosielať spamy. Portál je zaradený na čiernu listinu NÚKIBom. Študent 5. ročníka pracujúceho na oddelení incidentov sa pokúsi nadviazať kontakt s tímom CVIS ale neúspešne.

Ciele:

- Pozrieť sa na interné a externé komunikačné protokoly
- Určiť efektívne spôsoby komunikácie s externými organizáciami v prípade incidentov

Úlohy:

- Spolupracovať s NÚKIB na čistení a obnovení služieb portálu
- Preskúmať a posilniť bezpečnostné politiky a postupy univerzity

Fáza 5 - Útočník a výkupné

Scenár: Univerzita dostane žiadosť o výkupné od útočníka, ktorý hrozí šifrovaním servera a odstránením všetkých údajov, pokiaľ sa nevyplatí značná suma v kryptomene

Ciele:

- Vyhodnotiť požiadavky výkupného týkajúce sa právnych, finančných a etických dôsledkov. Rozhodnúť sa, či konať, platiť alebo odmietnuť a pripraviť sa na následky
- Informovať verejnosť áno/nie?

Úlohy:

- Spolupracovať s NÚKIB v rámci právneho prostredia
- Informovať políciu a potrebné úrady

Fáza 6 - Obnova

Scenár: IT tím reaguje na kontakt a pomáha eliminovať problém. Medzitým sa zistilo, že portál MBA nemá SLA.

Ciele:

- Implementovať nápravné opatrenia na odstránenie zraniteľnosti a spamu
- Skontrolovať a aktualizovať zmluvy a SLA s poskytovateľmi externých služieb

Úlohy:

- Preskúmať a posilniť bezpečnostné politiky a postupy univerzity
- Obnoviť tím CVIS na univerzite

Prezentácie a celé table top cvičenie bude pripojené k práci ako príloha. Fázy implementujeme do modulov, ktoré účastníci majú vo forme časového harmonogramu spomenutého vyššie. V module sa odohrá niekoľko udalostí a následne vyústi do diskusie. Modul predstavuje jednu časť cvičenia časovo obmedzenú 15 minútami a následne 10 minútami je sprevádzaná diskusia. Diskusia je tvorená niekoľkými otázkami. Sú cielene otvorené a navrhnuté tak, aby vyvolali diskusiu v skúšanej skupine.

Moduly sme podľa rozloženia fázy navrhli nasledovne:

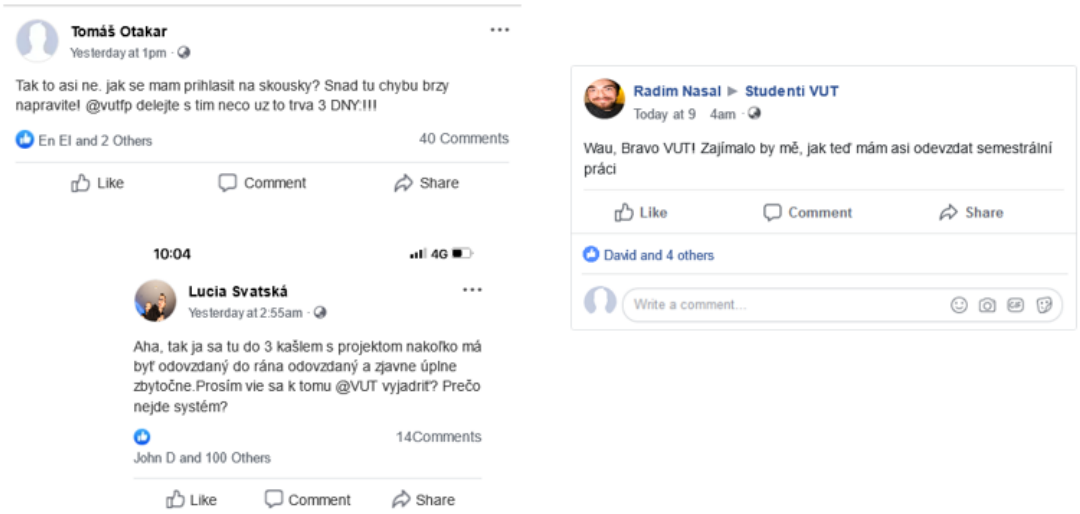
MODUL 1:

11.12.2023

NÚKIB vydáva upozornenie o novej zákernej Zero-day zraniteľnosti aplikácie Wordpress CVE-2023-XXXX

Deň 1

Študenti sa ozývajú na sociálnych sieťach. Na univerzitu mieri formou príspevkov vlna kritiky.



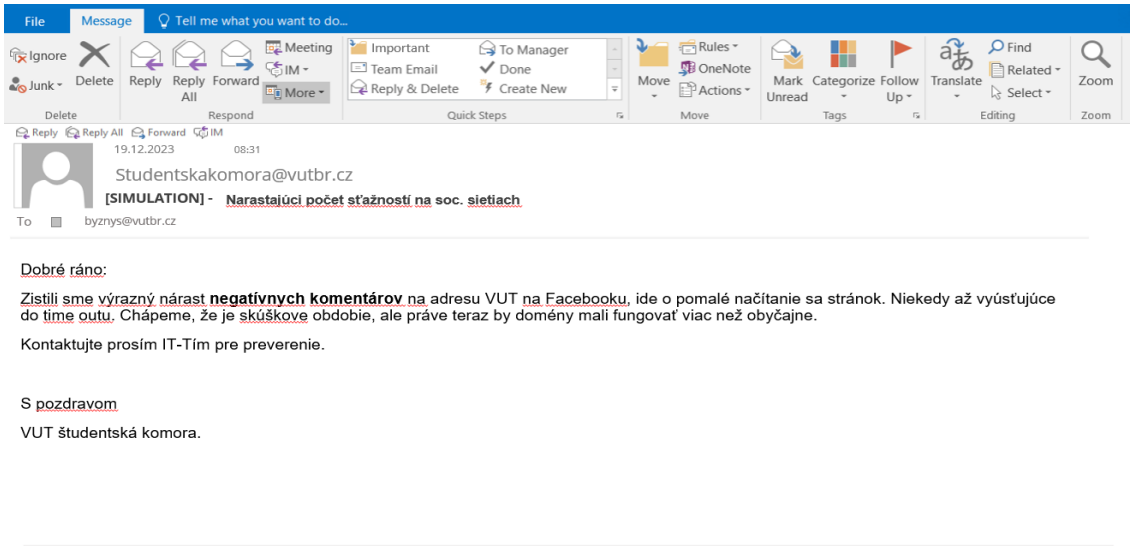
Obrázok 12 Príspevky na sociálnych sieťach [Zdroj: Vlastné spracovanie]

Deň 4

Je skúškové obdobie. Študenti sa snažia odovzdávať semestrálne práce. Nezdržiavajú sa na univerzite. Často využívajú práve informačný systém školy pre komunikáciu. Prihlasovanie na skúšky je komplikované.

Deň 5

Študentská komora si problém všimne a upozorňuje naň IT tím.



Obrázok 13 Email zo študentskej komory [Zdroj: Vlastné spracovanie]

Diskusia 1:

- **Otázka 1:** Tento scenár sa zaoberá upozornením na kybernetickú bezpečnosť. Zaznamenali ste tieto upozornenie?
- **Otázka 2:** Poskytuje VUT školenie zamestnancov o kybernetickej bezpečnosti alebo bezpečnosti informačných technológii?
- **Otázka 3:** Má VUT zavedený plán/program obnovy?
- **Otázka 4:** Bola niektorá z udalostí popísaných v tomto module identifikovaná ako kybernetický incident alebo udalosť? Ak áno, ako by sa s nimi zaobchádzalo?

MODUL 2:

Deň 10

Študenti sa vyjadrujú na sociálnych sieťach o neprístupnosti VUT stránky. Nemôžu sa prihlasovať na skúšky. Komunikácia začína prebiehať emailmi.

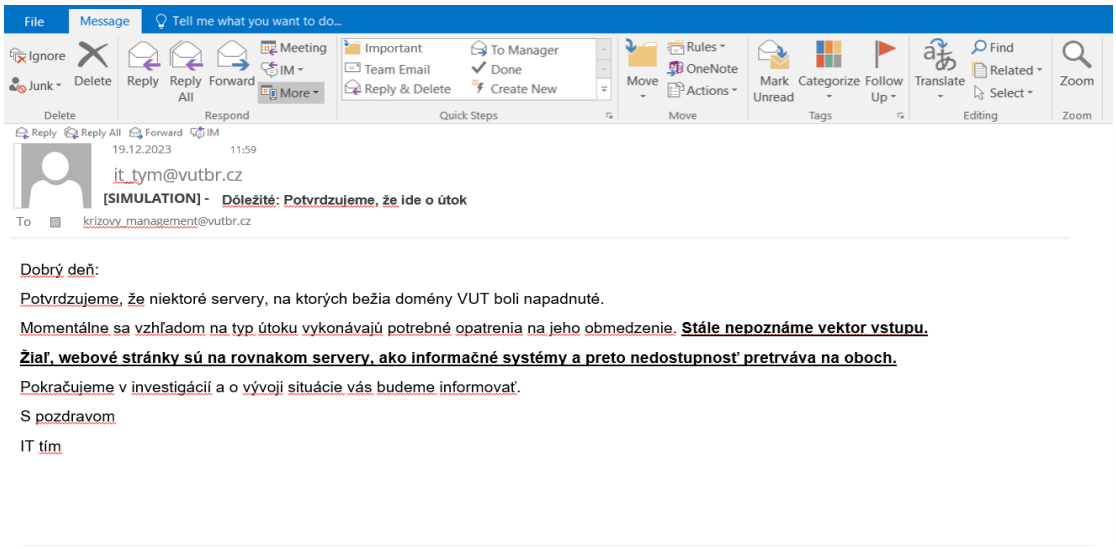
Deň 13

IT oddelenie VUT si všimne sériu neobvyklých špičiek aktivity v jednom z ich systémov. Tieto špičky boli pôvodne odmietnuté ako rutinné fluktuácie.

Krízový manažment dostáva predbežnú správu o situácii od IT tímu, v ktorej sa uvádza že evidujú spomalené webové stránky a situáciu riešia.

Deň 14

IT oddelenie potvrdzuje útok.



Obrázok 14 Email od IT tímu [Zdroj: Vlastné spracovanie]

Deň 18

Na rektorát sa valí vlna telefonátov. Niektoré od študentov, niektoré od médií. (Nefunkčnosť prihlasovania, rozhorčenie študentov. Nemožnosť odovzdávať semestrálne práce.)

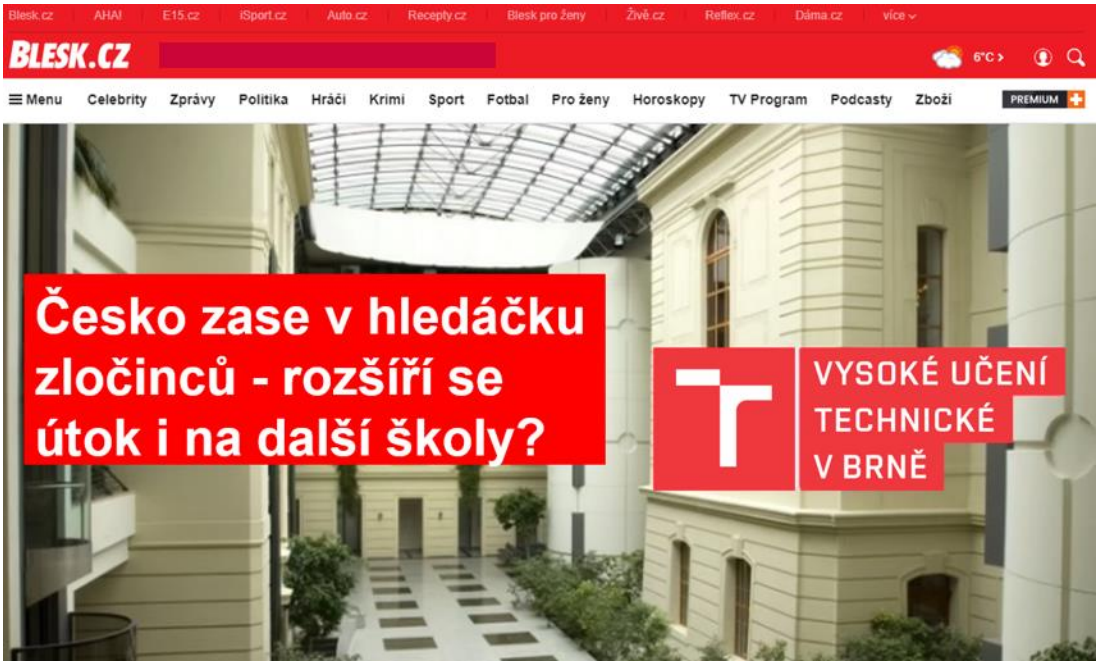
Diskusia 2:

- **Otázka 1:** Boli tieto incidenty posúdené? Definujte úroveň závažnosti incidentov v oblasti kybernetickej bezpečnosti a kritériá eskalácie.
- **Otázka 2:** Máte zodpovedný personál vyčlenený na reakciu na incidenty alebo určený tím pre reakciu na kybernetické incidenty vo vašej organizácii?
- **Otázka 3:** Aké interné a externé oznámenia by ste vykonali?

MODUL 3:

Medzičasom

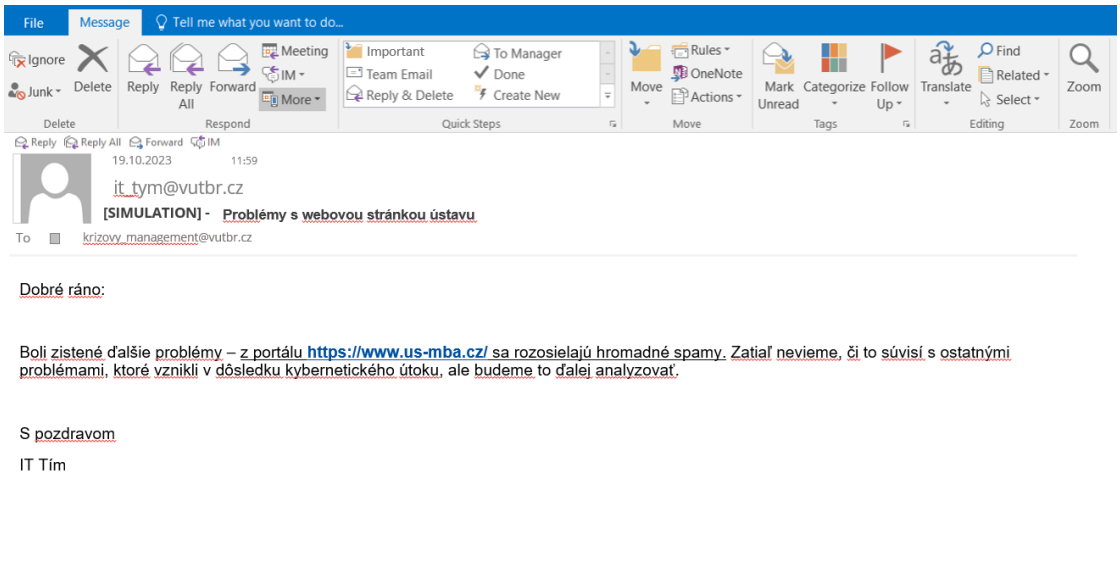
O situácií v ústave informujú média. Sú sviatky. Polovička pracovníkov je doma.



Obrázok 15 Titulok novín [Zdroj: Vlastné spracovanie]

Deň 19

IT tím upozorňuje, že problémy zistené na webovej stránke sú naozaj typom kybernetického útoku. IT oddelenie zisťuje rozposielanie spamov z adresy, ktorá patrí VUT.



Obrázok 16 Email ohľadom MBA[Zdroj: Vlastné spracovanie]

Deň 20

Pre obmedzenú možnosť registrácie pevného termínu sa študenti zhromažďujú na internátoch a čakajú na emaily od vyučujúcich.

Diskusia 3:

- **Otázka 1:** Má vaša univerzita plán obnovy dát? Kde sú uložené zálohy? Sú offline alebo online, uložené na bezpečnom mieste alebo spravované prostredníctvom tretej strany?
- **Otázka 2:** Aké sú obavy ohľadom verejných záležitostí?
- **Otázka 3:** Aké oddelenie a zdroje sú potrebné pre odpoveď na tento incident?

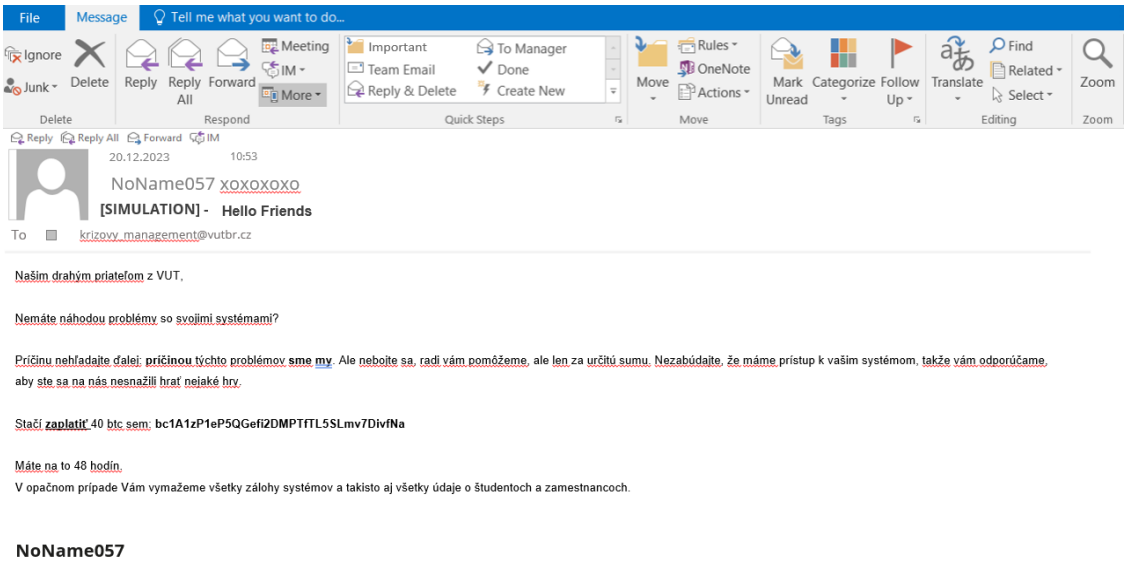
MODUL 4:

Deň 22

Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB) zasahuje a portál MBA pridáva na blacklist. NÚKIB sa snaží kontaktovať univerzitu. Nikto však o tomto pokuse nevie.

Deň 23

VUT IT tímu prichádza email od útočníka. Útočník zosmiešňuje s bezpečnosť univerzity a požaduje výkupné. Ak univerzita nepošle peniaze do 48 hodín, útočník vymaže všetky záznamy študentov.



Obrázok 17 Email od útočníka [Zdroj: Vlastné spracovanie]

Deň 24

Vedenie VUT obdrží odkaz na darkweb, na ktorom je zverejnená vzorka s osobnými údajmi študentov a zamestnancov.

Deň 25

V médiách sa začína písať o zaplatení výkupného. Táto informácia je však falošná.

Obrázok 18 Falošná správa v novinách [Zdroj: Vlastné spracovanie]

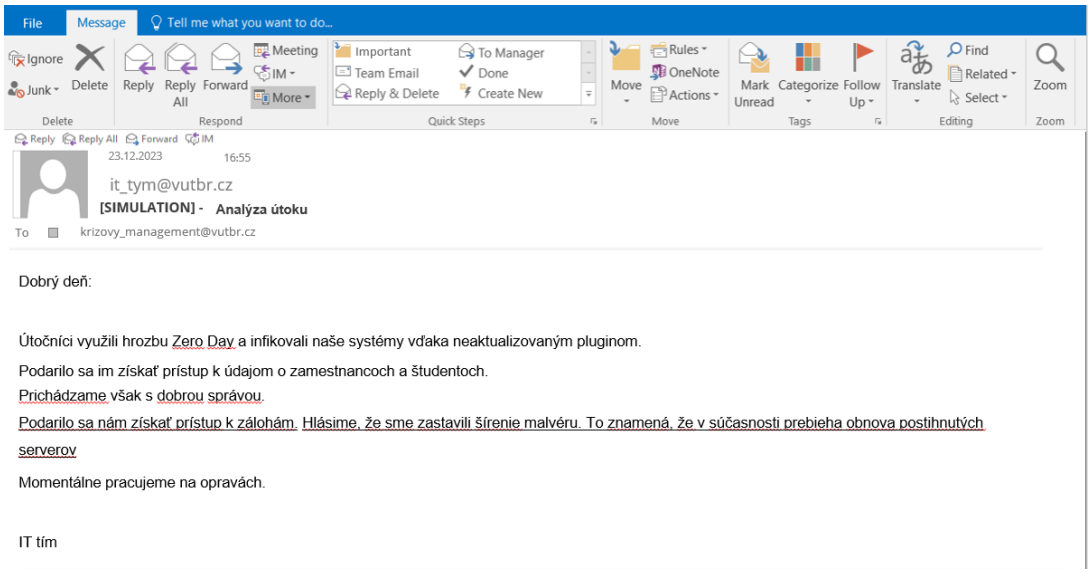
Diskusia 4:

- **Otázka 1:** Koho by ste kontaktovali, ak potrebujete ďalšiu pomoc?
- **Otázka 2:** Aké sú vaše obavy ohľadom verejných záležitostí?

MODUL 5:

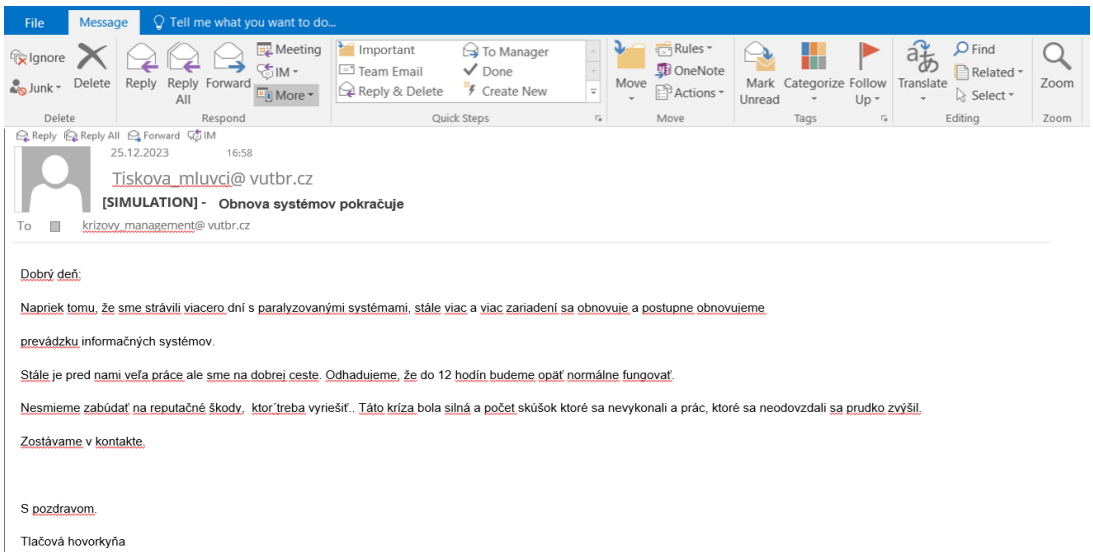
Deň 26

IT tím zistil odkiaľ prichádza problém. Útočníci využili spomínanú zraniteľnosť „ zero day“.



Obrázok 19 Email o zero-day zraniteľnosti [Zdroj: Vlastné spracovanie]

Tlačová hovorkyňa sa vyjadruje k incidentu. Žiada, aby sa problém riešil najmä s prevádzkovateľom samotného portálu MBA.



Obrázok 20 Email od tlačovej hovorkyne [Zdroj: Vlastné spracovanie]

Deň 30

Mnohí žiaci nestíhajú termíny skúšok aj napriek tomu. Ovplyvňuje to dobrú povesť univerzity.

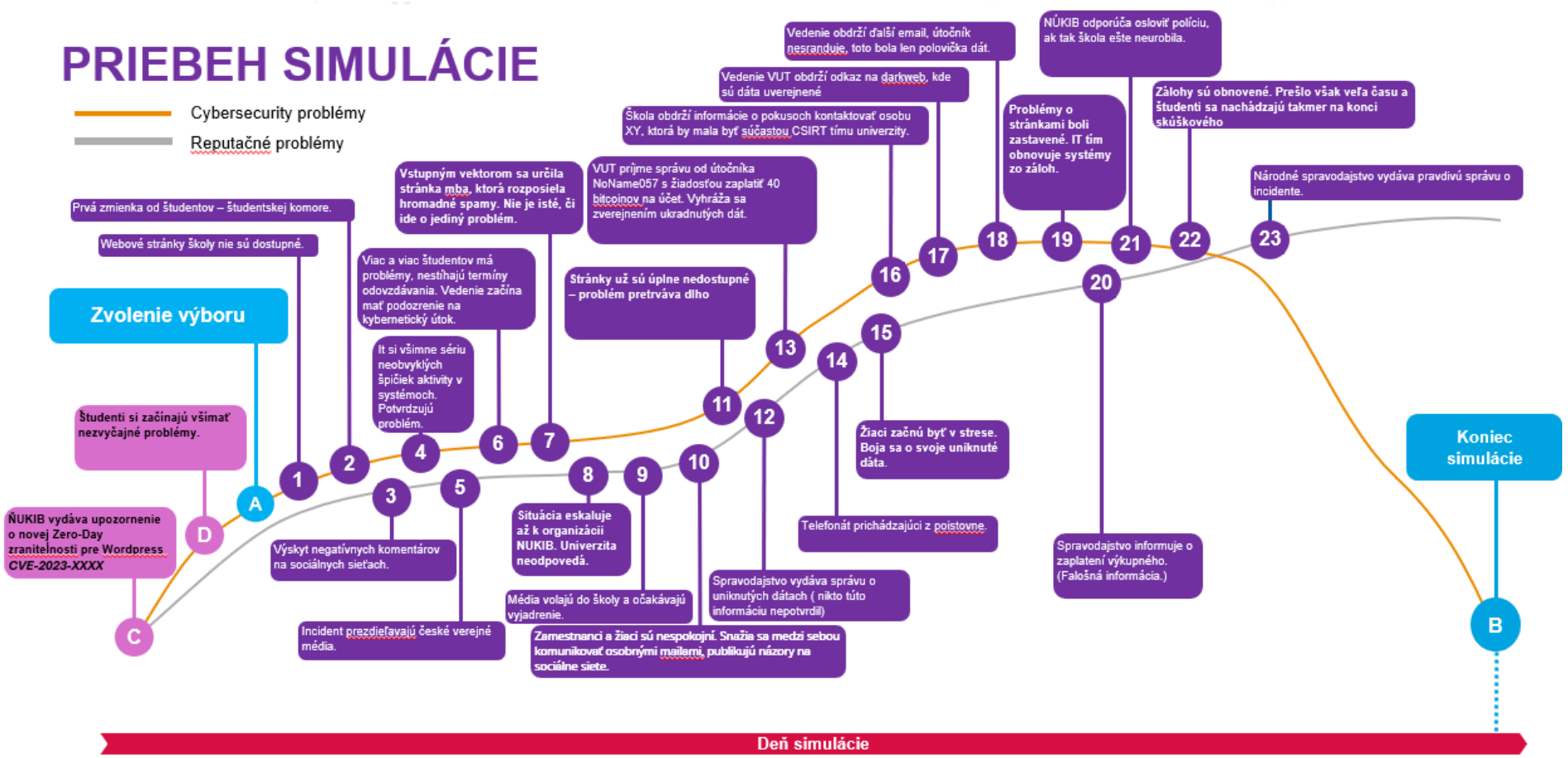
Deň 31

Univerzite bolo oznámené, že žiadne výkupne platiť nemusí, išlo o žart. Páchateľ je však neznámy.

Diskusia 5:

- **Otázka 1:** Aká okamžitá ochrana alebo zmierňujúce opatrenia by mohli univerzite v tomto scenári pomôcť? Kto je zodpovedný za tieto kroky?
- **Otázka 2:** Aké sú obavy vášho konkrétneho oddelenia? Snaží sa Vaše oddelenie urýchlene odstrániť problém alebo spolupracuje na verejnej mienke?
- **Otázka 3:** Aké ochranné opatrenia by ste podnikli v prípade nevzniknutia incidentu?
- **Otázka 4:** Ako sa vyjadríte ohľadom incidentu verejnosti?
- **Otázka 5:** V ktorej fáze bolo potrebné zavolať políciu?

Celý priebeh simulácie je vysvetlený v nasledovnom obrázku:



Obrázok 21 Priebeh simulácie [Zdroj: Vlastné spracovanie podľa (34)]

[7] **„Hot debrief“ simulácie**

V tomto bode sa simulácia zhodnotí tzv. „za horúca“.

Bezprostredne po konci cvičenia povedie direktor a facilitátor rekapituláciu. Rekapitulácia je dôležitá z hľadiska uzatvorenia všetkých otázok a úkonov, ktoré skupina vykonala. V prílohe diplomovej práce bude evidovaný dokument pre hot debrief, kde sa zapisovali odpovede skupiny na všetky otázky. Následne facilitátor vysloví poznatky, ktorou skupine nadobudol, aký bol cieľ každého modulu a či skupina úspešne cieľa dosiahla. Cieľom je identifikovať, čo fungovalo dobre a čo nie – oblasti, ktoré potrebujú zlepšenie. Účastníci môžu poskytnúť okamžitú spätnú väzbu o svojich problémoch, na ktoré narazili, a o efektívnosti plánov a postupov, ktoré boli počas cvičenia testované.

[8] **Spracovanie spätnej väzby**

Informácie získané počas "hot debriefu" sú následne analyzované. Zodpovední koordinátori alebo vedúci tímu zhromaždia pripomienky a zaznamenajú kľúčové poznatky, ktoré pomôžu pri ďalšom zlepšovaní postupov a pripravenosti. Na základe zhromaždených údajov a analýzy feedbacku sa vypracuje **detailný report.** Tento report obsahuje prehľad cvičenia, zdôraznenie hlavných úspechov a oblastí na zlepšenie, a konkrétne odporúčania pre budúce cvičenia a operácie.

[9] **Komplexnejšie vyhodnotenie**

Po "hot debrief" a vypracovaní reportu sa uskutoční hlbšie a podrobnejšie vyhodnotenie, ktoré zahŕňa rozšírenú analýzu údajov, vyhodnotenie reakcii na testovanie, súčinnosť so štandardmi, politikami a pravidlami firmy. Hodnotenie je vedené z dvoch smerov – kvalitatívne a kvantitatívne

V kvalitatívnom hodnotení sú uvedené tri hlavné oblasti a kritéria, ktoré sa týkajú správy, komunikácie a reakcií na udalosti, a ktoré by mali byť adresované.

1. **Riadenie a správa**:
    - Zásady a kritériá dôležité pre manažment.
    - Podpora pri implementácii a prioritizácia.
    - Štruktúrovaná podpora kontrolných procesov.

- Zapojenie a vedenie tímu.
- Plány pre nepretržitú podnikovú činnosť.
- Správa rizík a strategické plánovanie.
- Spolupráca medzi verejným a súkromným sektorom.

2. **Komunikácia**:
   - Nastavenie na krízovú reakciu.
   - Rozdelenie úloh a zodpovedností.
   - Plány na riadenie kríz.
   - Tímy pre podporu.
   - Komunikačné stratégie počas krízy.
   - Interakcia s klientmi.
   - Aktívna účasť zúčastnených strán v reálnom čase.
   - Koordinácia medzi operáciami a komunikáciou.
3. **Reakcie a rozhodnutia**:
   - Manažment informácií (zber, distribúcia).
   - Monitorovacie procesy (analýza informácií).
   - Koordinované operácie v prípade potreby.
   - Nástroje podporujúce rozhodovacie procesy.

Následne sa z všetkých troch kategórii zachytávajú odpozorované procesy a oproti nim sa zapíše správny postup alebo možnosť zlepšenia danej sféry. Tieto body sa ohodnotia stupnicou od 1 po 10, ako dobre boli zvládnuté a pripíše sa **dôkaz** z reakcii počas simulácie. (Príloha č.3.)

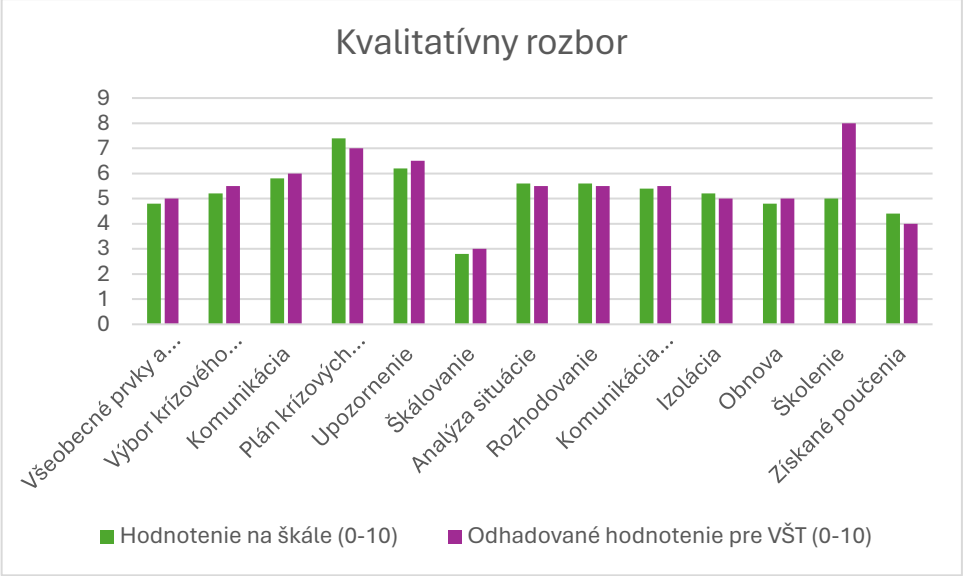
V kvalitatívnom zhodnotení sa v tabuľke budú hodnotiť bodmi od 0-10 nasledovné kritéria. Čísla v tabuľkách sú vymyslené a neodzrkadľujú realitu.

Tabuľka 5 Kategórie kvalitatívneho sledovania [Zdroj: Vlastné spracovanie]

Kategória	Hodnotenie na škále (0-10)	Odhadované hodnotenie pre VŠT (0-10)
Všeobecné prvky a predchádzajúce aktivity	4,8	5
Výbor krízového manažmentu	5,2	5,5
Komunikácia	5,8	6

Plán krízových incidentov	7,4	7
Upozornenie	6,2	6,5
Škálovanie	2,8	3
Analýza situácie	5,6	5,5
Rozhodovanie	5,6	5,5
Komunikácia (opakovanie)	5,4	5,5
Izolácia	5,2	5
Obnova	4,8	5
Školenie	5	8
Získané poučenia	4,4	4

Získane hodnoty si vieme premeniť do grafu pre lepšie pochopenie situácie a postavenia univerzity oproti priemerným hodnotám prostredia.



Graf 2 Porovnanie kvalitatívnych výsledkov [Zdroj: Vlastné spracovanie]

[10] Prezentácia a diskusia výsledkov

Výsledky komplexnejšieho vyhodnotenia sa následne prezentujú vedeniu organizácie a zúčastneným tímom. Toto poskytuje príležitosť na diskusiu o tom, ako implementovať odporúčania a zlepšiť celkovú pripravenosť a reakcie na budúce incidenty.

5 FINANČNÝ PLÁN PROJEKTU

Tabuľka 6 Náklady tvorbu a prevedenie table top [Zdroj: Vlastné spracovanie]

Krok projektu	Počet ľudí	Cena za deň (€)	Počet dní	Celková cena (€)
Analýza prostredia	2	50	10	1 000€
Analýza incidentu	2	50	10	1 000€
Analýza politík a štandardov	2	75	10	1 500€
Dotazníky	1	250	2	500€
Vyhotovenie cvičenia	2	117	15	3 500€
Preklady	1	100	3	300€
Simulácia cvičenia	4	600	1	2 400€
Vyhotovenie výsledkov	1	200	10	2 000€
Prezentácia výsledkov	1	250	1	250€
Celkom				12 450€

Tabuľka poskytuje prehľad o finančných nákladoch spojených s tvorbou a prvotným školením o kybernetickej bezpečnosti v prostredí univerzity. Celkovo sú uvedené tri kategórie nákladov s rozličnými profily odborníkov a príslušnými jednotkovými cenami:

Pri cenovej tvorbe sme brali na vedomie fakt, že ide o štátnu univerzitu a rozpočet na simulované cvičenie bude obmedzený. Alokácia zdrojov v tomto prípade bola prevedená nasledovne:

Preverili sa počiatočné analýzy prostredia, ktorá zahŕňala zhromažďovanie údajov o súčasnom prostredí univerzity, analýza vonkajších a vnútorných faktorov, ktoré univerzitu ovplyvňujú, identifikácia kľúčových vplyvov a prípadných zainteresovaných strán. Cena 50€ na deň na osobu je pomerne nízka, reflektuje základné analýzy a prácu s dostupnými dátami.

Analýza incidentu zahŕňala detailný rozpis predchádzajúceho incidentu a potenciálnych rizík, ktoré by mohli vyústiť do incidentu. Vyhodnotili sa slabé stránky univerzity a vytvoril sa podklad pre cvičenie. Cena odpovedá náročnosti výkonu.

Analýza politík a štandardov vedených na univerzite dodáva prehľad a ohodnotenie aktuálnych politík pre krízový manažment. Vyššia cena za deň odzrkadľuje náročnosť a schopnosť orientovať sa v právnom prostredí.

Cena za dotazníky obsahuje prípravu a distribúciu dotazníkov zameraných na zber potrebných informácii pre simuláciu a následne pre spätnú väzbu.

Vyhotovenie cvičenia zahŕňalo komplexnú prípravu scenárov a materiálov potrebných na realizáciu. Dve osoby pracovali na tejto činnosti za 117 € na deň po dobu 15 dní, čo zabezpečilo kvalitné materiály, ktoré boli esenciálne pre úspešné vykonanie cvičenia.

Preklady boli potrebné pre sprístupnenie materiálov účastníkom, ktorí hovorili rôznymi jazykmi. Jeden prekladateľ pracoval za 100 € na deň, čo bolo ekonomicky efektívne riešenie pre zabezpečenie jazykovej prístupnosti dokumentov.

Simulácia cvičenia predstavovala realizáciu naplánovaného scenára, pričom štyri osoby boli zamestnané na tento jeden deň za 600 € na deň na osobu, čo odzrkadľovalo ich odborné zručnosti a prípravu potrebnú na zvládnutie komplexných situácií počas cvičenia.

Vyhotovenie výsledkov zahŕňalo spracovanie a analýzu údajov získaných počas cvičenia. Jeden pracovník za 200 € na deň analyzoval a dokumentoval výsledky, ktoré boli kritické pre pochopenie účinnosti cvičenia.

Prezentácia výsledkov za cenu 250 € za jeden deň zahrnula sumarizáciu a predstavenie zistení z cvičenia vedeniu organizácie, čo bolo nevyhnutné pre strategické plánovanie a zlepšenia.

Medzisúčet všetkých nákladov spojených s týmto projektom predstavuje 12 450 €. Táto tabuľka poskytuje základné finančné informácie potrebné pre hodnotenie nákladovosti a efektívnosti projektu zavedenia simulácie kybernetického incidentu do vzdelávacieho programu univerzity.

ZÁVER

Na základe predchádzajúcej analýzy prostredia, incidentov v okolí a detailnej analýzy konkrétneho incidentu a odporúčaní je možné konštatovať, že zvýšenie kybernetickej bezpečnosti si vyžaduje komplexný a viacúrovňový prístup. Na základe analýzy incidentu poskytnutého univerzitou, pozorovaní a preverení smerníc sme úspešne vedeli vytvoriť efektívny simulačný nastroj pomocou table top cvičenia, v ktorom sme nie len zrevidovali chyby a nedostatky systému a procesov ktoré univerzita využíva, ale boli sme schopní vytýčiť konkrétne medzery a aplikovať ich na účastníkoch cvičenia za cieľom vyskúšať ich znalosti a upozorniť ich na nedostatky ako v politikách, štandardoch, tak znalostiach a pripravenosti na kybernetický incident. V rámci technických nedostatkov sme prišli k niekoľkým poznatkom.

Implementácia pokročilých detekčných systémov a vylepšenie bezpečnostných pravidiel by mala byť prioritou pre univerzitu v snahe o proaktívnu detekciu a prevenciu kybernetických útokov. Zároveň je vysoko odporúčané zriadiť tím špecializovaný na aktívne hľadanie hrozieb a zraniteľností, čím sa zásadne zníži riziko kompromitácie systémov. Kľúčovým aspektom je tiež prechod k systémom Endpoint Detection and Response (EDR), ktoré poskytujú detailnejší pohľad na bezpečnostný stav zariadení a umožňujú rýchlejšiu reakciu na podozrivé správanie. Manažment aktualizácií je rovnako dôležitý, pretože zabezpečuje, že všetky používané systémy a aplikácie sú aktualizované a chránené pred známymi hrozbami.

Ďalšie kroky by mali zahŕňať zlepšenie interných komunikačných kanálov a školenie zamestnancov, aby boli včas informovaní o incidentoch a disponovali potrebnými zdrojmi na ich riešenie. Formalizácia Service Level Agreements (SLA) pre všetky hosťované služby zabezpečí, že poskytovatelia hostingu budú dodržiavať jasné požiadavky vyplývajúce z dohody. Je tiež nevyhnutné prehodnotiť a posilniť protokoly na riešenie incidentov, čo organizáciám umožní rýchlejšie a efektívnejšie reagovať na bezpečnostné hrozby.

V rámci snahy o simulácie table top cvičenia na bezpečnostné incidenty bola organizovaná simulácia tohto vypracovaného cvičenia, avšak táto simulácia nebola

efektívna, nakoľko testovacia vzorka pozostávala prevažne zo študentov piateho ročníka, ktorí absolvovali všetky predmety pána Ing. Sedláka a majú niekoľko certifikátov od úradu NÚKIB. Títo študenti boli dobre pripravení a oboznámení s možnými scenármi incidentov, čo viedlo k správnym reakciám a odpovediam na scenár. Tento fakt poukazuje na dôležitosť diverzity účastníkov pri plánovaní a vykonávaní simulačných cvičení, aby sa zabezpečilo, že výsledky simulácie realisticky odrážajú schopnosti univerzity, alebo iného podniku reagovať na nepredvídané a variabilné bezpečnostné hrozby. Je nevyhnutné zahrnúť širší rozsah účastníkov s rôznymi úrovňami skúseností a pripravenosti, aby sa simulačné cvičenia stali skutočne hodnotným nástrojom na zvyšovanie bezpečnostnej pripravenosti.

Záverom je, že pravidelné školenia a simulačné cvičenia sú esenciálne pre zvyšovanie pripravenosti zamestnancov a ich schopnosti efektívne reagovať na bezpečnostné incidenty. Tieto kroky vytvárajú robustný bezpečnostný rámec, ktorý zvyšuje obranyschopnosť organizácie proti kybernetickým hrozbám a zabezpečuje jej dlhodobú udržateľnosť a bezpečnosť.

ZOZNAM ZDROJOV

[1] SMEJKAL, Vladimír a RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 4. vydání. Praha: Grada Publishing, 2013, 488 s. Expert. ISBN 978-80-247-4644-9.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST Special Publication 800-53. In: . 2023. Dostupné také z: https://doi.org/10.6028/NIST.SP.800-53r5.

[3] **International Organization for Standardization (ISO).** ISO/IEC 27001:2022, Information technology — Security techniques — Information security management systems — Requirements [online]. 3rd edition. Geneva: ISO, 2022. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en [cit. 2024-05-11].

[4] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. TLP 2.0 Fact Sheet [online]. [cit. 2024-05-11]. Dostupné z: https://www.cisa.gov/resources-tools/resources/tlp-20-fact-sheet

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Cyber Threat Information Sharing. [online]. Gaithersburg: National Institute of Standards and Technology, 2016 [cit. 2024-05-11]. Dostupné z: https://doi.org/10.6028/NIST.SP.800-150

[6] **International Organization for Standardization (ISO) a International Electrotechnical Commission (IEC).** ISO/IEC 27005:2018, Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací [online]. Geneva: ISO/IEC, 2018. Dostupné z: http://www.iso.org/standard/369790.html [cit. 2024-05-11].

[7] SEDLÁK, Petr; ONDRÁK, Viktor a MAZÁLEK, Vladimír. *Problematika ISMS v manažerské informatice*. Akademické nakladatelství CERM, 2014. ISBN 9788072048724.

[8] SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru*. Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-068-2.

[9] **National Institute of Standards and Technology (NIST).** NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide [online]. 2012. Dostupné z: https://doi.org/10.6028/NIST.SP.800-61r2 [cit. 2024-05-11].

[10] LOPES, Rita. *Difference between CERT, CSIRT and SOC*. Online. 2024. Dostupné z: Https://www.linkedin.com/posts/rita-lopes-a2871257_what-is-the-difference-between-cert-csirt-activity-7115273288951488513-SUFq. [cit. 2024-05-11].

[11] **National Institute of Standards and Technology (NIST).** NIST Special Publication 800-63-3, Digital Identity Guidelines [online]. 2017. Dostupné z: https://doi.org/10.6028/NIST.SP.800-63-3 [cit. 2024-05-11].

[12] **International Organization for Standardization (ISO).** ISO/IEC 20000-1:2018, Information technology — Service management — Part 1: Service management system requirements [online]. Geneva: ISO, 2018. Dostupné z: https://www.iso.org/standard/70636.html [cit. 2024-05-11].

[13] **European Union Agency for Cybersecurity (ENISA).** ENISA Threat Landscape 2023 [online]. 2023. ISBN 978-92-9204-645-3. Dostupné z: [https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport] [cit. 2024-05-11].

[14] ROUMANI, Yaman. Patching zero-day vulnerabilities: an empirical analysis. Online. *Journal of cybersecurity*. 2021, roč. 1, č. 7, s. 023. Dostupné z: https://doi.org/10.1093/cybsec/tyab023. [cit. 2024-05-11].

[15] GANDHI, Foram; PANSANIYA, Drashti; NAIK, Swapna. Ethical Hacking: Types of Hackers, Cyber Attacks and Security. **International Research Journal of Innovations in Engineering and Technology**. Dharmapuri: 2022, Vol. 6, Iss. 1, s. 28-32. DOI: 10.47001/IRJIET/2022.601007.

[16] AMERICA'S CYBER DEFENSE AGENCY, CISA. *#StopRansomware: MedusaLocker*. Online. Dostupné z: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a. [cit. 2024-05-11].

[17] *Dark Web Profile: Medusa Ransomware (MedusaLocker)*. Online. Dostupné z: https://socradar.io/dark-web-profile-medusa-ransomware-medusalocker/. [cit. 2024-05-11].

[18] **Auckland University of Technology Breach: Monti** [online]. Dátum publikácie: 2023. Miesto vydania: [s.l.]. Dostupné z: https://thecyberexpress.com/auckland-university-of-technology-breach-monti/ [cit. 2024-05-11].

[19] **Monti Ransomware Returns with New Linux Variant and Enhanced Evasion Tactics** [online]. Dátum publikácie: 2023. Miesto vydania: [s.l.]. Dostupné z: https://mrhacker.co/malware/monti-ransomware-returns-with-new-linux-variant-and-enhanced-evasion-tactics/ [cit. 2024-05-11].

[20] Zákon č. 18/2018 Z. z. [online]. Platnosť od 25.05.2018. Bratislava: Ministerstvo spravodlivosti Slovenskej republiky, 2018. Dostupné z: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525 [cit. 2024-05-11].

[21] Business Continuity Planning (BCP). In: **Investopedia** [online]. Dostupné z: https://www.investopedia.com/terms/b/business-continuity-planning.asp [cit. 2024-05-11].

[22] KAPLAN, S. a GARRETT, T. (2005). The use of tabletop exercises in the evaluation of emergency response systems. **Disaster Prevention and Management: An International Journal**, [online] 14(3), s. 356-363. Dostupné z: https://www.ready.gov/training [cit. 2024-05-11].

[23] National Institute of Standards and Technology (NIST). Tabletop Exercise. In: **CSRC – Computer Security Resource Center** [online]. Dostupné z: https://csrc.nist.gov/glossary/term/Tabletop_Exercise [cit. 2024-05-11].

[24] **AlertMedia.** Tabletop Exercises. In: **AlertMedia Blog** [online]. Dostupné z: https://www.alertmedia.com/blog/tabletop-exercises/ [cit. 2024-05-11].

[25] BAČÍKOVÁ, Mária, PhD. a JANOVSKÁ, Anna, PhD. (2018). **Základy metodológie pedagogicko-psychologického výskumu. Sprievodca pre študentov učiteľstva,** 1. vydanie. Košice: ŠafárikPress, Univerzita Pavla Jozefa Šafárika v Košiciach. 154 s. ISBN 978-80-8152-695-4. Dostupné z: https://unibook.upjs.sk/img/cms/2018/ff/zaklady-metodologie-ped-psych-vyskumu-web.pdf [cit. 2024-05-11].

[26] Hackerský útok na Univerzitu Mateja Bela: aké dáta chcú hackeri zverejniť a čo sa deje. In: **Živé.sk** [online]. Dostupné z:

https://zive.aktuality.sk/clanok/k5rb75w/hackersky-utok-na-univerzitu-mateja-bela-ake-data-chcu-hackeri-zverejnit-a-co-sa-deje/ [cit. 2024-05-11].

[27] Hackeři napadli Univerzitu obrany, měli odcizit data rektorátu. In: **Novinky.cz** [online]. Dostupné z: https://www.novinky.cz/clanek/domaci-hackeri-napadli-univerzitu-obrany-meli-odcizit-data-rektoratu-40444979 [cit. 2024-05-11].

[28] **Národný úrad pre kybernetickú a informačnú bezpečnosť (NUKIB).** Legislativa [online]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/ [cit. 2024-05-11].

[29] **Fakulta podnikatelská Vysokého učení technického v Brně**. Historie a současnost [online]. Dostupné z: https://www.fp.vut.cz/cs/o-fakulte/historie-a-soucasnost/ [cit. 2024-05-11].

[30] **Fakulta podnikatelská Vysokého učení technického v Brně**. Nabídka programů [online]. Dostupné z: https://www.fp.vut.cz/cs/pro-uchazece/nabidka-programu/ [cit. 2024-05-11].

[31] VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Směrnice Č. 1/2024: Řízení kybernetické a informační bezpečnosti VUT [online]. Brno: Vysoké učení technické v Brně, 2024 [cit. 2024-05-11].

[32] GANCARČIK, R. *Informační bezpečnost jako ukazatel výkonnosti podniku.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 86 s. Vedúci diplomovej práce Ing. Petr Sedlák.

[33] What Is a Service Level Agreement (SLA)? In: **The Balance Small Business** [online]. Dostupné z: https://www.thebalancesmb.com/what-is-service-level-agreement-sla-2890233 [cit. 2024-05-11].

[34] ENISA,Participant Handbook: Crisis Simulation [presentation]. [Accessed: 2024-05-11].

ZOZNAM TABULIEK

ZOZNAM GRAFOV

ZOZNAM OBRÁZKOV

ZOZNAM PRÍLOH

- Príloha č.1 – Cvičenie table top
- Príloha č.2 – Hot debrief
- Príloha č.3 – Prezentácia výsledkov