

Lokální síť z pohledu kybernetické bezpečnosti

Bc. David Šikuta

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. David Šikuta
Osobní číslo:	L23347
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Rizikové inženýrství
Forma studia:	Kombinovaná
Téma práce:	Lokální síť z pohledu kybernetické bezpečnosti

Zásady pro vypracování

- Zpracujte hlavní pojmy problematiky za využití aktuálních českých i zahraničních zdrojů.
- Charakterizujte řešenou problematiku a analyzujte současné možnosti řešení.
- Na základě provedené analýzy navrhnete implementaci konkrétního řešení.
- Vyhodnotte teoretické a praktické přínosy diplomové práce.

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

Seznam doporučené literatury:

1. CLARKE, Richard A. a KNAKE, Robert K.. *The fifth domain: defending our country, our companies, and ourselves in the age of cyber threats*. Version_1. New York: Penguin Press, 2019. ISBN 978-0-525-56196-5.
2. JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.
3. KOLOUCH, Jan. *CyberCrime*. CZ.NIC. Praha : CZ.NIC,z.s.p.o., 2016. ISBN 978-80-88168-18-8.
4. KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
5. SCHNEIER, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*. W. W. Norton & Company, 2023. ISBN 978-0-393-86666-7.

Další odborná literatura dle doporučení vedoucího práce.

Vedoucí diplomové práce: **Ing. et Ing. Jiří Konečný, Ph.D.**
Ústav krizového řízení

Datum zadání diplomové práce: **2. prosince 2024**

Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

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

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

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 25.4.2025

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zabývá kybernetickou bezpečností lokálních sítí s důrazem na roli lidského faktoru v oblasti zranitelností a rizik. V rámci praktické části byl realizován penetrační test ve formě quishingového útoku na akademické půdě, jehož cílem bylo nejen prověřit reálné ohrožení, ale i otestovat možnosti edukace studentů v oblasti kybernetických hrozeb. Práce využívá teoretických rámců, jako je triáda CIA a metodika hodnocení rizik dle vyhlášky č. 82/2018 Sb., a na základě získaných dat formuluje návrhy na opatření ke zvýšení odolnosti sítě. Důraz je kladen na propojení technických a behaviorálních prvků bezpečnosti a praktické využití výsledků pro zvyšování povědomí o rizicích v prostředí vzdělávacích institucí.

Klíčová slova: kybernetická bezpečnost, quishing, sociální inženýrství, riziko, penetrační test, edukace, lokální síť

ABSTRACT

This diploma thesis deals with the cybersecurity of local networks with an emphasis on the role of the human factor in the area of vulnerabilities and risks. As a portion of its practical part, a penetration test in the form of a quishing attack was carried out on campus with the aim of not only to verify the real threat, but also to test the possibilities of educating students in the area of cyber threats. The thesis uses theoretical frameworks, such as the CIA triad and the risk assessment methodology according to Decree No. 82/2018 Coll., and based on the data obtained formulates proposals for measures to increase network resilience. The emphasis is placed on the connection of technical and behavioral elements of security and the practical use of the results to raise awareness of risks in the environment of educational institutions.

Keywords: cybersecurity, quishing, social engineering, risk, penetration test, education, local network

Poděkování patří zejména mému vedoucímu práce Ing. et Ing. Jiřímu Konečnému Ph.D. za jeho neocenitelnou ochotu a pomoc a také Ing. Pavlu Valáškoví za jeho věcné rady a pomoc při odborných konzultacích. Poděkování také patří kolegům, kteří si našli čas a pomohli s vypracováním týmových částí práce. Velké poděkování patří i mé manželce Kláře, která mi byla velkou oporou.

OBSAH

ÚVOD.....	12
CÍL PRÁCE, POUŽITÉ METODY A VÝZKUMNÉ OTÁZKY.....	13
OMEZENÍ PRÁCE	14
I TEORETICKÁ ČÁST	15
1 DEFINICE ZÁKLADNÍCH POJMŮ.....	16
1.1 KYBERPROSTOR	16
1.2 BEZPEČNOST V KYBERPROSTORU	17
1.3 BEZPEČNOST	18
1.3.1 Security a safety	18
1.4 FYZICKÁ BEZPEČNOST	18
1.5 ZRANITELNOST.....	19
1.6 HROZBA	19
1.7 RIZIKO.....	19
1.8 AKTIVUM	20
1.9 KYBERNETICKÉ RIZIKO	20
1.10 PROTIOPATŘENÍ.....	20
1.11 KYBERNETICKÝ ZLOČIN	20
1.12 APWG	21
1.13 MALWARE.....	21
1.14 KATEGORIE HACKERŮ	22
1.15 DPIA.....	22
1.16 ENISA	23
1.17 QR KÓD.....	23
2 PROSTŘEDKÝ ÚTOKŮ.....	25
2.1 SOCIÁLNÍ INŽENÝRSTVÍ.....	25
2.2 KLASIFIKACE SOCIÁLNÍHO INŽENÝRSTVÍ.....	26
2.3 PHISHING.....	28
2.4 SPEAR PHISHING	29
2.5 QUISHING	29
3 PROSTŘEDKY OCHRANY.....	30
3.1 KYBERNETICKÁ BEZPEČNOST	30
3.2 PRINCIPY KYBERNETICKÉ BEZPEČNOSTI	30
3.3 TRIÁDA CIA.....	31

3.3.1	C jako důvěrnost.....	31
3.3.2	I jako integrita	32
3.3.3	A jako dostupnost.....	32
3.4	PARKERIAN HEXAD.....	32
3.5	PRVKY KYBERNETICKÉ BEZPEČNOSTI	33
3.5.1	Lidé.....	33
3.5.2	Technologie	34
3.5.3	Procesy	34
4	HODNOCENÍ RIZIK	35
	ZÁVĚREČNÁ KAPITOLA TEORETICKÉ ČÁSTI.....	36
II	PRAKTICKÁ ČÁST	37
5	PŘÍPRAVA ÚTOKU.....	38
5.1	CYBERCRIME V CYBERSPACE	38
5.2	ZRANITELNOST V LOKÁLNÍCH SÍTÍCH	40
5.3	JAK SE DOSTAT DO HLAVY OBĚTI.....	42
5.4	ŠKOLENÍ	45
6	METODOLOGIE ÚTOČNÍKA.....	46
6.1	VÝBĚR MÍSTA	46
6.2	VÝBĚR METODY	47
6.3	PROSTŘEDKY VYBRANÉ METODY	52
6.3.1	Letáková kampaň	52
6.3.2	FLKR_testy	55
6.4	ZDROJE NÁVŠTĚV	56
7	VÝSLEDKY A DATA.....	57
7.1	LETÁKY	57
7.2	FLKR_TESTY	59
7.3	DÍLČÍ ZÁVĚR ZÁCHYTŮ.....	60
8	POROVNÁNÍ KAMPAŇÍ.....	62
8.1	NÁKLADY	62
8.2	ČAS	63
8.3	BILANCE.....	64
9	DOTAZNÍK	65
9.1	STRUKTURA DOTAZNÍKU	65
9.2	VÝSLEDKY PIZZA LETÁK	67
9.3	VÝSLEDKY FLKR_TESTY.....	69
9.4	POROVNÁNÍ.....	70
9.5	VYHODNOCENÍ A OPATŘENÍ	71

9.6	SHRnutí DOTAZNÍKU	74
10	ANALÝZA RIZIK	75
10.1	MODELOVÁ FAKULTA	75
10.2	ZRANITELNOSTI.....	76
10.3	HROZBY	78
10.4	HODNOCENÍ AKTIV	79
10.5	HODNOCENÍ RIZIK	81
11	HODNOCENÍ RIZIK MODELOVÉ FAKULTY	85
12	NÁVRH OPATŘENÍ	90
12.1	OPATŘENÍ DOPORUČENÁ	90
12.2	OPATŘENÍ NAVRHOVANÁ	91
12.2.1	Phishing ve škole.....	91
12.2.2	Quishing na akademické půdě	93
12.2.3	Učebna či chodba	94
12.3	VZDĚLÁVÁNÍ SYSTÉMOVÉ	94
12.4	RIZIKA PO OŠETŘENÍ.....	94
13	DISKUZE	98
	ODPOVĚDI NA VÝZKUMNÉ OTÁZKY	101
	ZÁVĚR	102
	SEZNAM POUŽITÉ LITERATURY	103
	SEZNAM OBRÁZKŮ	107
	SEZNAM TABULEK.....	109
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	110
	SEZNAM PŘÍLOH.....	111

ÚVOD

V době rychlého technologického rozvoje je společnost čím dál více závislá na informačních a komunikačních technologiích. Tento vývoj přináší nejen řadu výhod, ale i významná rizika, která se promítají do každodenního života jednotlivců, firem i veřejných institucí. Jednou z klíčových oblastí, kde tato rizika nabývají reálného významu, je bezpečnost lokálních sítí ať už soukromého sektoru, státního, nebo akademického.

Kybernetická bezpečnost se v tomto kontextu stává komplexní disciplínou, která musí kombinovat technické prostředky s edukací uživatelů a schopností identifikovat a předcházet hrozbám, jež vznikají často z lidské nepozornosti nebo důvěřivosti. Ne náhodou je právě člověk často označován za nejslabší článek bezpečnostního řetězce.

Tato diplomová práce se zaměřuje na praktické ověření bezpečnosti lokální sítě na Fakultě logistiky a krizového řízení v Uherském Hradišti prostřednictvím simulovaného quishingového útoku – moderní formy phishingu založené na zneužití QR kódů. Cílem útoku nebylo způsobit škodu, ale sbírat data o chování uživatelů, ověřit úroveň povědomí o kybernetických rizicích a současně demonstrovat možnosti vzdělávání skrze tzv. bezpečnostní praxi.

Práce dále navazuje na vybrané teoretické koncepty – jako je definice kyberprostoru, triáda CIA (Confidentiality, Integrity, Availability) a uplatňuje je v rámci hodnocení aktiv, zranitelností a rizik podle vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti. Praktická část je podložena sběrem dat prostřednictvím několika kanálů: fyzické quishingové kampaně, dotazníkového šetření a analýzy zpětné vazby.

Výsledky práce mají přímou vazbu na praxi a nabízejí konkrétní návrhy, jak zvyšovat kybernetickou gramotnost studentů a zaměstnanců akademických institucí, jak optimalizovat zabezpečení sítí s ohledem na lidský faktor a jak přistupovat k penetračnímu testování s edukativním přesahem.

CÍL PRÁCE, POUŽITÉ METODY A VÝZKUMNÉ OTÁZKY

Cílem práce je zjištění stavu ochrany místní sítě na fakultě logistiky a krizového řízení v Uherském Hradišti. Ten bude proveden formou penetračního testu za pomoci quishingového útoku. Při penetračním testu proběhne zároveň prověření možností edukace studentů a zvýšení povědomí o problematice. Útok zároveň poslouží k základnímu sběru informací s příkladem možnosti edukace.

Ke zhodnocení ochrany bude využito modelové fakulty, která se bude ve veřejně dostupných informacích shodovat s fakultou logistiky a krizového řízení. Data z fyzického quishingového útoku poskytnou informace k vyhodnocení aktuálního stavu a hodnocení rizik, které bude provedeno podle metodiky vyhlášky 82/2018 Sb. o kybernetické bezpečnosti, kterou se státní správa a instituce řídí. Hodnocení rizik bude řešeno kvalifikovaným týmem a hodnocení po ošetření bude vycházet z teoretické změny po použití praktické edukační kampaně.

VO1: Jaký je aktuální stav povědomí studentů o kybernetických rizicích?

VO2: Jak lze využít penetrační test pro sběr dat?

VO3: Jaký je vztah mezi náklady nebo časem k počtu záchytů obětí?

VO4: Jak se kvalifikovaný tým se zkušenostmi v oblasti kybernetické bezpečnosti dívá na snížení rizik navrhovanou metodou?

VO5: Jakými způsoby lze edukovat studenty na akademické půdě?

OMEZENÍ PRÁCE

Z pohledu kybernetické bezpečnosti není vhodné do veřejně dostupného dokumentu vkládat reálný stav zabezpečení na Fakultě logistiky a krizového řízení v Uherském Hradišti. Takový postup by mohl snížit odolnost zabezpečení a působit návodně pro případné útočníky. Z tohoto důvodu jsou použity jen veřejně dostupné informace a data z penetračního testu. Zranitelnosti a hrozby jsou z rejstříku vybrány na základě týmové diskuse, odráží běžné hrozby v organizacích podobného typu a s Fakultou logistiky a krizového řízení v Uherském hradišti nemají reálný základ. Vybrané zranitelnosti a hrozby jsou kvalifikovaným týmem odhadnuty na základě zkušeností a poté průměrovány.

I. TEORETICKÁ ČÁST

1 DEFINICE ZÁKLADNÍCH POJMŮ

Ke správnému zabezpečení místních sítí je důležité definovat jak samotný kyberprostor, kde se útok odehrává, jednotlivé prvky informačních a komunikačních technologií, tak i prostředky útoku, včetně působení na dané zranitelnosti.

Dnešní doba je na ICT (informační a komunikační technologie) plně závislá a počty útoků neustále rapidně rostou. Jedná se o velmi komplexní a promyšlené útoky za použití mnoha nástrojů a postupů.

Také prvků ICT je k definování nepřeborné množství, stejně tak jako prvků ochrany.

1.1 Kyberprostor

Kyberprostor se napříč odbornou literaturou definuje různě, často vcelku odlišně. Datování první definice pojmu kyberprostor se dá vypátrat do roku 1982, kde pan William Gibson ve své povídce „Jak vypálit Chrom“ tento pojem použil. Následoval jeho román „Neuromancer“, kde se již dostal i k popsání kyberprostoru, a to následnou definicí:

„Konsensuální halucinace každý den zakoušena miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky... Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru myslí, shluky a souhvězdí dat. Jako světla města, ... William Gibson: Neuromancer (1984).“ (Kolouch, 2019)

Definice v Cambridgeském slovníku uvádí dokonce více definic, které jsou však modernějším pojetím kyberprostoru, nicméně ve všech případech se jedná o velmi strohý popis. Tři uváděné definice k pojmu „cyberspace“ uvádí, že se jedná o pomyslný prostor, složený z elektronických systémů, sloužící ke komunikaci, přístupu k informacím, jejich předávání a setkávání lidí. (Oxford dictionary, c2025)

Dále můžeme nahlédnout do českého výkladového slovníku. Tam definici kyberprostoru nenajdeme, ale pod heslem „Český kyberprostor“ nalezneme alespoň odkaz dále na definici „kyberprostor pod jurisdikcí České republiky“ (Kolouch, 2019) Je tudíž zjevné, že v rámci České republiky se pojmem zabývá spíše odborná literatura, která nemá jednotný základní balík definicí.

Velmi moderní a výstižnou definici uvádí pánové Kolouch a Bašta ve své publikaci Cybersecurity (2019):

„Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.“ (Kolouch, 2019)

Velmi rozšířeným pojetím je zákonná definice, která se v oblasti kybernetické bezpečnosti používá velmi často a je zpravidla součástí bezpečnostní dokumentace:

„Kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.“ (Jirásek, 2022)

Je zřejmé, že definovat kyberprostor není jednoduché a výklad je značně rozdílný podle zaměření publikace, či autora samotného. Někteří na pojem nahlíží velmi stroze, ale díky tomu je pojem lépe uchopitelný pro širší publikum, někde se na něj nahlíží sofistikovaně a velmi do hloubky. Například dokument pocházející z dílny americké armády „Cyberspace Operations: Concept Capability Plan 2016-2028“ tento prostor rozděluje do tří vrstev – fyzické, logické a sociální. Poté ještě každou jednotlivou vrstvu definuje a rozděluje do pěti komponent. Definice kyberprostoru je zde v originálním znění následovná:

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (Federation of American Scientists, 2010)

V překladu zní následovně:

„Globální doména v informačním prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních technologií, včetně internetu, telekomunikačních sítí, počítačových systémů a řídicích jednotek.“ (Federation of American Scientists, 2010)

V dnešním pojetí se tedy pojem kybernetický prostor vztahuje převážně k prostoru přenosu informací mezi ICT. Tedy k jakémusi virtuálnímu prostředí, kde probíhá výměna informací, ale také výpočetní operace. To je ten prostor, kde se bavíme o kybernetické bezpečnosti.

1.2 Bezpečnost v kyberprostoru

Bezpečnostní prostředí v kybernetickém prostoru se vyznačuje především přesahem do různých bezpečnostních sfér. Dnešní svět je na ICT závislý a pokud dojde k útoku v kybernetickém prostoru, bude ovlivňovat skutečný svět a v mnoha případech na něj bude mít reálný bezpečnostní dopad. Na pozadí mnoha incidentů v posledním desetiletí zesiluje

význam bezpečnosti v kybernetickém prostoru, a to napříč běžným uživatelem, firmou, nebo dokonce i celým státem. Bezpečnostní politika se mění a nejen stát, ale celý svět se snaží o posunutí komplexní bezpečnostní strategie vpřed. Bezpečnost se dotýká každého jednoho uživatele a ten se tak stává i potencionální zranitelností jak malých systémů, tak ohrožením bezpečnosti reálného světa, do kterého bezesporu účinky útoků pronikají.

1.3 Bezpečnost

Ve všeobecné rovině lze říct, že tento pojem je známý napříč obory i literaturou a důkladně vymezený. Nicméně definice se různí díky výkladu v různorodých vědních oborech a různému uchopení k danému kontextu. Ve většině případů se však protíná definování určitého stavu, ve kterém se jednotlivci, skupiny, subjekty, společnosti či celé státy necítí ohroženi hrozbami, či ochranu před nimi považují za dostatečnou. (Smejkal, 2019)

1.3.1 Security a safety

V anglické literatuře se pojem bezpečnost vyjadřuje konkrétněji ve dvou výrazech – security a safety. Tyto pojmy používá hojně i česká literatura v jejich anglické podobě.

- Security vyjadřuje většinou aktivní ochranu a zabezpečení
- Safety vyjadřuje naopak ochranu pasivní a používá se také k vyjádření a charakteristice stavu.

I v relativně mladé literatuře, která se bezpečnostní tematikou zabývá, najdeme rozdílné vyjádření pojmů. Například mezi publikacemi Cybersecurity od pánů Koloucha a Bašty z roku 2019 a Bezpečnost informačních systémů od pánů Smejkal, Sokola a Kodla z roku 2019 nalezneme u první zmíněné security jako bezpečnost a druhá vyjadřuje stejný český pojem jako safety. Naopak security druhá publikace vyjadřuje jako zabezpečení.

1.4 Fyzická bezpečnost

V obecné rovině se jedná o technické, organizační a režimové opatření, či jejich kombinaci. (Smejkal, 2019)

Ve vztahu k problematice kybernetické bezpečnosti je důležitou součástí. Nejen vzdálený přístup do systému skrze kybernetický prostor je jedinou variantou útoku. Velmi často se jedná právě o útok, který je umožněný díky přímému fyzickému přístupu do sítě.

1.5 Zranitelnost

Vyjadřuje slabé místo na daném aktivu, případně slabinu v jeho ochraně. Může být využita hrozbou k působení negativního vlivu na daný subjekt, tedy aktivum. Dalo by se vyjádřit jako specifická citlivost aktiva na danou hrozbu. (Smejkal, 2013)

1.6 Hrozba

„Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“ (Jirásek, 2022)

Hrozbou chápeme daný fenomén, který může, ale nemusí na dané aktivum působit, a to s nějakou pravděpodobností a různou mírou dopadu. Hrozba tedy je, ale zda a jak bude působit na aktivum nám vyjadřuje riziko.

1.7 Riziko

Pojem definovaný různě, nicméně vždy s velmi podobným cílem. Ve vztahu k tématu se jeví jako vhodné použití definice z výkladového slovníku kybernetické bezpečnosti:

- *„Nebezpečí, možnost škody, ztráty, nezdaru.“*
- *Účinek nejistoty na dosažení cílů.*
- *Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.“* (Jirásek, 2022)

Riziko, na rozdíl od hrozby, lze spočítat či odhadnout. Je to pravděpodobnost působení hrozby na aktivum, důsledků, které hrozba může aktivu způsobit a zranitelnosti. Je tedy součinem pravděpodobnosti, důsledku a hodnoty zranitelnosti působení hrozby na aktivum. Vyjádření rizika je tedy:

$$R = P \times D \times Z$$

Kde **R** je rizikem, **P** pravděpodobností, **D** důsledkem a **Z** zranitelností.
(Sbírka zákonů České republiky, 1993-2023)

1.8 Aktivum

Aktivem se označuje vše, co má nějakou hodnotu pro daný subjekt. Působení hrozby na dané aktivum tuto hodnotu snižuje. Aktiva lze rozdělit do několika skupin, základní dělení lze definovat jako:

Hmotná – mezi ta se řadí například pozemky, budovy, vybavení, stroje, peněžní hotovost.

Nehmotná – pod nimi najdeme mimo jiné informace, morálku, loajalitu zaměstnanců, know-how, autorská práva a mnoho dalších. (Smejkal, 2013)

1.9 Kybernetické riziko

Lze jej definovat jako riziko, které způsobuje hrozba v kybernetickém prostoru. (Jirásek, 2022)

Hrozba způsobující kybernetické riziko však nemusí být jen v kybernetickém prostoru. Naopak hrozby způsobující kybernetické riziko často působí v reálném světě.

1.10 Protiopatření

„Protiopatření je postup, proces, procedura, technický prostředek nebo cokoli, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhuje s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.“ (Smejkal, 2013)

1.11 Kybernetický zločin

„As we rush to put our lives online, we have unwittingly exposed ourselves to a whole new breed of criminal“ (Goodman, 2016) což v překladu znamená:

„S tím, jak spěcháme, abychom mohli žít online, jsme se nevědomky vystavili zcela novému druhu zločinců.“ (Goodman, 2016)

Kybernetický zločin, často pojmenovaný anglickým názvem cybercrime, je jakákoliv nezákonná činnost odehrávající se prostřednictvím počítače nebo internetu. Spadají zde například krádeže identity, šíření škodlivého softwaru, nebo útoky na infrastrukturu. (Goodman, 2016)

1.12 APWG

Anti-Phishing Working Group (APWG) je globální koalice veřejného a soukromého sektoru a zahrnuje:

- technologické firmy (např. Microsoft, PayPal, Symantec),
- banky a finanční instituce,
- vládní agentury (např. FBI, Europol),
- univerzity a výzkumné organizace.

Byla založena v roce 2003 a jejím hlavním cílem je sdílet informace o phishingových útocích a kampaních, koordinovat obranu proti nim a vzdělávat veřejnost i organizace v oblasti kyberbezpečnosti.

Mezi hlavní činnosti patří například:

- publikace čtvrtletních a ročních zpráv o trendech z oblasti phishingu a kybernetického zločinu,
 - monitorování nových typů hrozeb
 - poskytování dat pro výzkum a bezpečnostním týmům,
 - spolupráce s mezinárodními institucemi na potírání kybernetického zločinu.
- (APWG, c2003-2025)

1.13 Malware

Malware (zkratka z malicious software) je software úmyslně navržený tak, aby narušoval, poškozoval nebo získával neoprávněný přístup k počítačovým systémům, sítím či datům. Může ohrozit důvěrnost, integritu a dostupnost informací. Je to vlastně sada instrukcí, které běží na vašem počítači a způsobují, že systém provádí něco, co nechcete. Zahrnuje různé typy škodlivého softwaru, jako jsou viry, červi, trojské koně, spyware, adware, ransomware a další. Každý typ má specifické chování a cíle, ale všechny sdílejí úmysl poškodit nebo zneužít cílový systém. (Mohanta, 2020)

1.14 Kategorie hackerů

Ve světě kybernetického zločinu existují dvě základní kategorie hackerů. A v tomto světě mají i svoje pojmenování, které je velmi často využíváno. Za hlavní kategorie můžeme považovat white hat hacker a black hat hacker.

White hat hacker (etický hacker)

White hat hacker je odborník na kybernetickou bezpečnost, který s povolením testuje systémy a sítě s cílem identifikovat a opravit zranitelnosti.

- Pracuje legálně a eticky.
- Provádí penetrační testy a bezpečnostní audity.
- Spolupracuje s organizacemi na zlepšení jejich bezpečnosti. (Kaspersky, c2025)

Black hat hacker

Black hat hacker je jedinec, který neoprávněně proniká do počítačových systémů s cílem způsobit škodu, krást data nebo získat finanční prospěch.

- Jedná nelegálně a s úmyslem škodit.
- Využívá malware, phishing a další škodlivé techniky.
- Je motivován osobním ziskem, pomstou nebo ideologií. (Porterfield, 2017)

Zajímavostí je pravděpodobný vznik tohoto kloboukového fenoménu. Pojem white hat pochází z klasických westernových filmů, kde hrdinové nosili bílé klobouky na rozdíl od padouchů s černými klobouky. (Kaspersky, c2025)

Gray hat hacker

Postupem času vzniklo i označení pro gray hat hackera. Ten je někde na pomezí mezi white hat (etickými) a black hat (škodlivými) hackery. Obvykle se neřídí žádným oficiálním svolením k průnikům do systémů, ale nemá ani škodlivý úmysl. Cílem bývá upozornění na zranitelnosti nebo vlastní etický kodex, který se ale nemusí shodovat se zákony. (Kaspersky, c2025)

1.15 DPIA

Česky „Posouzení vlivu na ochranu osobních údajů“, je proces určený ke zhodnocení rizik spojených se zpracováním osobních údajů a k přijetí opatření pro jejich zmírnění. Metodika

v příručce určuje dle triády CIA ukázkovou metodiku a poskytuje praktické pokyny pro hodnocení rizik a implementaci bezpečnostních opatření při zpracování osobních údajů. (ENISA, 2017)

1.16 ENISA

Jedná se o Agenturu Evropské unie pro kybernetickou bezpečnost, anglicky European Union Agency for Cybersecurity, Evropskou unií zřízená agentura s cílem posilovat kybernetickou bezpečnost v EU, podporovat členské státy při zvládání kybernetických hrozeb a spolupracovat s veřejným i soukromým sektorem na zajištění kybernetické bezpečnosti místních sítí a informačních systémů. Založena byla v roce 2004 na základě Nařízení (ES) č. 460/2004 a původně se jednalo o dočasnou agenturu. Její mandát byl několikrát prodloužen a rozšířen. Aktuální právní rámec vychází z Nařízení (EU) 2019/881 (známé také jako Kybernetický akt – Cybersecurity Act), které rozšířilo pravomoci ENISy a dalo jí trvalý mandát. Mezi její hlavní činnosti patří:

- Poradenství evropským institucím a členskými státy v oblasti kybernetické bezpečnosti.
 - Podpora implementace směrnic, např. NIS2 (směrnice o bezpečnosti sítí a informací).
 - Koordinace reakce na incidenty a budování kapacit v oblasti kybernetické bezpečnosti.
 - Vzdělávání, školení a osvěta v oblasti kybernetických hrozeb.
 - Spolupráce se soukromým sektorem, výzkumnými institucemi a dalšími evropskými a mezinárodními organizacemi.
 - Vývoj a podpora evropského systému certifikace kybernetické bezpečnosti.
- (ENISA, c2025)

1.17 QR kód

U nás označovaný jako QR kód je částečně počeštěný výraz označující anglický název Quick Response Code. Jedná se o dvourozměrný kód, jenž umožňuje rychlé načtení a dekodování různých informací pomocí zařízení jako jsou například QR scannery, nebo v běžném životě používány smartphony. Na rozdíl od klasických kódů známých pod zkratkou EAN dokáže QR kód uchovat mnohem více dat, jako jsou například celé URL adresy, platební údaje,

textu apod. QR kódy původně vyvinula japonská firma Denso Wave s cílem urychlit sledování dílů v automobilovém průmyslu. Jeho výhodou je čtení kódu i při částečném poškození za pomoci chybové korekce. Další výhodou, díky které se těší takové popularitě je možnost interakce pomocí mobilního telefonu. (Stark, 2013)

2 PROSTŘEDKÝ ÚTOKŮ

Pro útoky a kriminální akce se využívají různé druhy postupů, které se v čase modifikují, vylepšují a s technologickým pokrokem rozšiřují. Často vycházejí, nebo jsou provázány se sociálním inženýrstvím. Každý bezpečnostní manažer tedy musí rizika v kybernetickém prostoru vyhodnocovat dle aktuálních trendů.

2.1 Sociální inženýrství

V éře digitálních technologií, které nás obklopují na každém kroku se rizika každodenního života promítají stále více do kybernetického prostoru. Během dne většina z nás využívá nějaký systém, připojuje se do nějaké sítě. Ať už do banky v rámci správy financí, v zaměstnání v rámci pracovní činnosti, ve škole při studiu, nebo doma pro informace či zábavu. A s masivním rozšířením sítí do našich životů se také mění svět zločinu a bezpečnosti v nich. Vznikají komplexní bezpečnostní systémy, ale i přes jejich sofistikované zabezpečení je možná konfrontace skrze člověka, přesněji řečeno kompromitace skrze psychologickou manipulaci. Tomuto fenoménu dnešní doby říkáme sociální inženýrství. Jedná se o soubor technik s cílem ovlivnit lidské chování a přimět jednotlivce k poskytnutí citlivých informací, přístupových údajů, anebo k provedení jiných akcí, které nejsou běžné, či napomáhají útočníkům dostat se do sítě. (Hadnagy, 2018)

Už Mitnick v roce 2002 definoval sociální inženýrství jako cílenou manipulaci lidského chování, která má za cíl obejít právě bezpečnostní opatření, získat informace anebo přístup do sítě, a to skrze důvěru, klam nebo psychologický tlak. (Mitnick, 2003) Jedná se o netechnický útok, který často předchází technickému útoku.

Jak lze tedy vidět, pojem a praktiky sociálního inženýrství nejsou ničím novým a je to jen pokračování manipulace s lidmi, které se začalo využívat i v kybernetickém prostoru.

Útoky můžeme v zásadě dělit na technické, tedy takové, které provádí hackeři skrze síť přímo do daných systémů a poté na sociální, kdy se hacker snaží pomocí podvodných technik nějakým způsobem obelhat, oklamat, či jinak zmanipulovat oběť. Případně jejich kombinace. Může se tedy jednat o prolamování bezpečnostních IT systémů a v případě problému může útočník využít techniku sociálního inženýrství a například pomocí vishingu si do dané organizace zavolá, představí se jako někdo jiný a zjistí si potřebné informace, například cestu k souborům, tak jak se stalo při útoku na vývojářskou firmu. (Mitnick, 2003)

Ne vždy je využití sociálního inženýrství považováno za hackerský útok. Nicméně pro úspěšný útok bývá často základem. (Kolouch, 2016)

Mezinárodně uznávaný technolog, kterého například „The Economist“ označil za „security guru“ je autorem velice výstižného citátu: (Harvard Kennedy School, c2025)

„Amatéři hackují systémy, profesionálové ,hackují‘ lidi.“

(Schneier, 2023)

2.2 Klasifikace sociálního inženýrství

Ve své podstatě by tedy šly techniky sociálního inženýrství rozdělit na psychologické, digitální a fyzické. Takové dělení lze vyčíst v několika publikacích, jak uvádí například ve své knize Hadnagy (2018). Takové dělení však dnes není úplně přesné. V době kombinací se setkáváme například s quishingem, který může být jak ve formě digitální, tak fyzické.

Jak Hadnagy (2018), tak Mitnick (2002) ve svých publikacích zmiňují převážně tyto metody, ke kterým si v tabulce (Tabulka 1) uvedeme nějaké příklady.

Tabulka 1 Techniky sociálního inženýrství

Technika	Popis	Příklad
Pretexting	Vytvoření falešné identity nebo situace ke zvýšení důvěryhodnosti.	Telefonát od „bankéře“ ověřujícího údaje.
Phishing	Masové rozesílání falešných zpráv s cílem přimět oběť k akci.	E-mail od „Netflixu“ požadující aktualizaci platebních údajů.
Vishing	Phishing prostřednictvím hlasového hovoru.	Volající „policista“ požaduje ověření údajů kvůli „krádeži identity“.
Smishing	Podvodné SMS zprávy.	SMS od „dopravce“ s odkazem na sledování zásilky.
Elicitation	Nenápadné získávání informací konverzací.	„Náhodná“ konverzace na konferenci.
Impersonation	Fyzické nebo digitální vydávání se za jinou osobu.	Falešný IT pracovník žádající přístup.
Baiting	Nabídka fyzické nebo digitální návnady.	USB disk ponechaný na parkovišti.
Quid pro quo	Nabídka výměny za informace nebo přístup.	Nabídka slevy za přihlašovací údaje.
Shoulder surfing	Přímé sledování uživatele (např. zadávání hesla).	V kavárně přes rameno.
Dumpster diving	Hledání užitečných informací ve vyhozených dokumentech.	Faktury, poznámky, seznamy hesel.

(Mitnick, 2003; Hadnagy, 2018)

Ty jsou stále platné, nicméně od doby vydání posledního vydání v roce 2018 od Hadnagyo se seznam technik rozšířil. Trendy popisuje například dokument, který vydala ENISA v roce 2022. Pár příkladů lze uvést v rozšiřující tabulce, nicméně situace pokročila do bodu, kdy je technik a jejich kombinací nespočet a stále přibývají nové, případně dochází k popisu již nějakou dobu praktikovaných technik. O technice, která je uvedena v tabulce (Tabulka 2)

jako poslední, se zmiňuje i jeden etický hacker v podcastu O2 Místo kyberčinu, kdy stál u vstupního terminálu firmy, kde byl prováděn penetrační test a snažil se načíst „ukradenou“ kartu ke vstupu. V tom k němu přistoupil jeden zaměstnanec, přiložil svoji kartu se slovy: *„nechce Vám to načíst? Každou chvíli to blbne, jděte“*. Nic výjimečného, nicméně terminologie k těmto situacím postupně vzniká a vyvíjí se tak, jak roste objem útoků a jejich rozmanitost.

Tabulka 2 Nové trendy v technikách sociálního inženýrství

Technika	Popis	Příklad
Quishing	QR kódy vedoucí na škodlivé stránky.	QR kód na letáku přesměrovává na phishingový web.
Deepfake impersonation	Využití syntetického hlasu/obrazu k napodobení autorit.	Falešný video chat s "ředitelem" požadujícím finanční převod.
Business Email Compromise (BEC)	Cílené útoky na korporátní komunikaci.	Podvržený e-mail od CEO s požadavkem na platbu.
Social media mining	Analýza sociálních sítí za účelem útoku.	Útočník získá jména dětí a použije je pro hádání hesla.
Consent phishing	Získání přístupu pomocí podvodného oprávnění ke cloudovým službám.	Aplikace požaduje přístup k účtu Microsoft 365.
Tailgating / Piggybacking	Fyzické následování autorizované osoby.	Útočník „proklouzne“ do budovy za zaměstnancem.

(Váš hosting, 2023; ENISA, 2022)

2.3 Phishing

Jeden ze stavebních kamenů sociálního inženýrství se stal phishing. V jeho základní podobě využíval spamovou techniku k rozesílání podvodných e-mailů. Jeho nespornou výhodou jsou minimální náklady a možnost masivního zásahu. Někde se přirovnává ke „kobercovému bombardování“ ve světě kybernetické kriminality. (Kolouch, 2016)

Jedná se tedy o hromadné rozesílání podvodných e-mailů, které uživatele pomocí technik sociálního inženýrství nabádají ke kliknutí na odkaz, k otevření přílohy, nebo k provedení nějakého jiného úkonu, jako například dnes moderního načtení QR kódu. (Schneier, 2023)

2.4 Spear phishing

Jedná se o formu phishingového útoku zaměřenou na jednotlivce, nebo organizace. Často je čerpáno z otevřených zdrojů, útočník mapuje oběť a poté díky získaným informacím tvoří velmi precizní formu útoku, která je adresně určena. Dále pak může například oběť, nebo její pravý email využít k šíření důvěryhodného útoku na zbytek organizace, vedení, nebo jiné konkrétní oběti. A to už například i za použití malware v rámci šíření po místní síti. (Kolouch, 2016)

2.5 Quishing

Jedna z metod sociálního inženýrství je quishing. Jedná se o formu phishingového útoku provedeného za pomoci QR kódu. Je to tedy složení zkratky QR a slova phishing. Útokem je v základu phishingová kampaň, avšak oběť nekliká na škodlivý odkaz, nýbrž skenuje QR kód. Cíl je také stejný jako u phishingové kampaně. Zisk přihlašovacích údajů, osobních informací, či instalace škodlivého softwaru. Tyto quishingové útoky tak můžeme najít například ve spamech elektronické pošty, falešných webových stránkách, podvodných letácích ve fyzické podobě, nebo například jako přelepy na bankomatech a místech s informačními QR kódy. (Authentic8, 2024)

K oblibě v používání QR kódu vede uživatele především pohodlí a rychlost. K velkému rozmachu došlo také během a po pandemii COVID-19. Ta přijímání QR kódů velmi urychlila díky práci na dálku a bezkontaktní komunikace. Například jako menu v restauraci, na které nemusí zákazník sahat, nebo informace o dezinfekci či zdraví. Poté se otevřely právě nové možnosti v oblasti kybernetické kriminality a s rozmachem QR kódů došlo i k rozmachu quishingu. (Vipre, b.r.)

3 PROSTŘEDKY OCHRANY

Bezpečnost je v dnešní době velmi aktuální téma v celé společnosti, a ne jinak je tomu i ve vztahu ke kybernetickému prostoru. Ten totiž do bezpečnosti zasahuje ve většině případů, a to díky informačnímu věku. Právě častým zdáním je, že se kybernetická bezpečnost týká pouze kybernetického prostoru. Avšak ten zasahuje do běžných životů nás všech na každém kroku. Proto i otázka bezpečnosti v kybernetickém prostoru se prolíná k otázce bezpečnosti celé společnosti a jejího fungování. V okruhu bezpečnosti si můžeme položit čtyři základní otázky a věnovat se jim:

- O čí bezpečnost jde?
- Jaké hodnoty chráníme?
- Před čím tyto hodnoty chráníme?
- Jaké zdroje vyžaduje ochrana těchto hodnot? (Kolouch, 2019)

Není možné vytvořit stav, kde by bezpečí bylo absolutní. Vždy bude existovat nějaké riziko, zranitelnost, hrozba, které není obsaženo v zabezpečení. Případně si útočník najde cestu, kterou bezpečnostní strategie podcenila, nebo neměla dostatečné zdroje se na ochranu připravit.

3.1 Kybernetická bezpečnost

Pojem kybernetické bezpečnosti se taktéž setkává s mnoha různými definicemi, například jako pojem bezpečnost. Také platí, že definice se liší podle hloubky, do které se daný autor o problematiku zajímá. Existují definice vymezující jen ICT, další se omezují na typy kybernetických útoků, další zase jen na data, případně pouze na on-line kybernetický prostor a ignorují off-line kybernetický prostor. Některé definice se soustředí zase jen na právní rámec.

Pro ujednání potřeb této práce nalezneme definici i v zákoně o kybernetické bezpečnosti, který se na ni dívá jako na bezpečnost v prostředí počítačových sítí, jejich prvků a všech dalších zařízení, která mají přidělenou IP adresu. (Smejkal, 2019)

3.2 Principy kybernetické bezpečnosti

K zabezpečení kybernetického prostoru je využíváno takzvaných triád, tedy trojic zásad, opatření, metod, nebo postupů. (Kolouch, 2019)

3.3 Triáda CIA

Tato triáda patří k nejznámějším a nejpoužívanějším. Opírá se o ni jak ISO 27005, tak vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. Požadované zásady jsou značeny právě písmeny CIA.

C – Confidentiality (důvěrnost)

I – Integrity (celistvost)

A – Availability (dostupnost)



Obrázek 1 Triáda CIA

(Clever and smart, 2010)

Legenda: Obrázek popisuje tři aspekty triády, které při průniku všech zajišťují bezpečnost.

3.3.1 C jako důvěrnost

Srozumitelnou definici nalezneme ve výkladovém slovníku kybernetické bezpečnosti. „Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.“ Důvěrnost tedy zaručuje přístup k ICT a jejich informacím pouze osobám k tomu oprávněným. (Kolouch, 2019)

3.3.2 I jako integrita

Integritu definuje výkladový slovník jako „*vlastnost přesnosti a úplnosti*.“ Ta tedy zaručuje, že data nebyla nijak změněna a ani s nimi nikdo neoprávněný žádným způsobem nemanipuloval. (Kolouch, 2019)

3.3.3 A jako dostupnost

Pod pojmem dostupnosti ve výkladovém slovníku nalezneme „*vlastnost přístupnosti a použitelnosti na žádost oprávněné entity*.“ Což zaručuje přístup k datům, ale pouze osobám k tomu oprávněným, a to v momentě potřeby. (Kolouch, 2019)

3.4 Parkerian hexad

Někdy je poukazováno na fakt, že triáda CIA již v dnešní době nemusí být dostatečná. Proto se již někde uplatňuje metoda parkerian hexad, která z triády CIA vychází a doplňuje ji o další tři rozšiřující prvky.

P/C – Possession/control (držení nebo kontrola)

A – Authenticity (autentičnost)

U – Utility (užitečnost)



Obrázek 2 Parkerian hexad

(Clever and smart, 2010)

Legenda: Obrázek ilustruje informační bezpečnost obklopenou prvky parkerian hexad, které bezpečnost zajišťují.

3.5 Prvky kybernetické bezpečnosti

V základní podobě se triáda CIA opírá o tři prvky. Ty do jisté míry umožňují kybernetickou bezpečnost nastolit. Tyto jednotlivé prvky výstižně popsal bezpečnostní expert Bruce Schneier. Tyto citace byly přeloženy autory knihy Cybersecurity a tyto překlady budou využity vždy v úvodu každého prvku. (Kolouch, 2019)

3.5.1 Lidé

„Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů (Bruce Schneier)“ (Kolouch, 2019)

Hlavním důvodem, proč jsou lidé nejslabším článkem v zabezpečení sítě je více. V první řadě se nabízí velmi krátká doba využívání informačních systémů. Počítače jsou lidmi využívány ve větším počtu až někdy po roce 1990. Masové připojení do globální sítě probíhalo až někdy kolem roku 1995. Například smartphony se ve velkém měřítku dostaly k uživatelům až kolem roku 2007. Dnes už velmi běžné sociální sítě jsou s námi jen něco málo přes deset let. (Kolouch, 2019) Je tedy zjevné, že za sebou kybernetický prostor nemá velkou historii a ve stínu velmi rychlého a dynamického vývoje je jisté, že ne všichni uživatelé vědí, jak se v sítích chovat. Ochrana je tedy pro bezpečnostní správce opravdovou výzvou.

3.5.2 Technologie

„Pokud se domníváte, že technologie dokáže vyřešit vaše bezpečnostní problémy, nerozumíte problémům a nerozumíte technologii. (Bruce Schneier)“ (Kolouch, 2019)

Dalším prvkem jsou právě technologie, které zabezpečují jak interakci uživatele v kyberprostoru, tak také jeho ochranu. Běžný uživatel vnímá technologickou bránu do kyberprostoru pouze jako koncové zařízení. Na úrovni organizace se v technologiích odkrývají další vrstvy zabezpečující místní síť a její funkčnost, jako jsou právě zmíněné LAN a Wi-Fi spojení, servery, firewally apod. Technologie bývají zpravidla tou bezpečnější částí a největším rizikem se stává opět člověk, který například neudrhuje aktualizovaný systém, provádí platby ve veřejné síti aj. (Kolouch, 2019)

3.5.3 Procesy

*„Mantrou dobrého bezpečnostního inženýra je: **Bezpečnost není produkt, ale proces.** Je to víc než navrhnout silnou kryptografii do systému. Je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala. (Bruce Schneier)“* (Kolouch, 2019)

Prvky uzavírá souhrn činností prováděných pro bezpečné používání technologií a služeb uživateli. Jako příklad se dá uvést právě řízení aktiv a rizik, ale také autentizace a autorizace, aktualizace, nebo například testování odolnosti zabezpečení atd.

Tento prvek je na budování zabezpečení sítě nejnáročnější. Zde je kladen právě největší důraz na bezpečnostní správce a je doporučeno jak školit, tak provádět i penetrační testy. (Kolouch, 2019)

4 HODNOCENÍ RIZIK

V oblasti kybernetické bezpečnosti existuje několik variant hodnocení rizik. Přímo vyhláška o kybernetické bezpečnosti č. 82/2018 sb. uvádí možnost hodnocení rizik v příloze č.2. Tato metodika bude využita i zde. Opírá se i o ISO 27000 a se stejnou metodikou pracuje i software CSA 2.0.

Pro určení metodiky je povinné stanovit jednoznačnou funkci. Tuto funkci nejčastěji ovlivňuje dopad, zranitelnost a hrozba. Lze tedy využít běžnou funkci pro výpočet rizik uvedenou ve zmiňované vyhlášce:

$$\text{Riziko} = \text{dopad} \times \text{hrozba} \times \text{zranitelnost}$$

(Sbírka zákonů České republiky, 1993-2023)

U kybernetické bezpečnosti se však nehodnotí dopad jako například u metody PNH, i když vzorec je velmi podobný, a i dopad je vlastně výsledkem názoru hodnotitelů. Dopad se hodnotí před samotným hodnocením rizik, a to na základě triády CIA. Jelikož vyhláška umožňuje určitý rámec volnosti zodpovědné osoby, lze najít různé metodiky, které se liší spíše v drobnostech, avšak v základu vždy musí splňovat rámec vyhlášky.

V příloze 1 vyhlášky 82/2018 Sb. je popsáno hodnocení aktiv, které poté určuje zmíněný dopad. Aktiva se hodnotí pomocí tří atributů – důvěrnosti, integrity a dostupnosti. Z nichž se pro dopad využívá buď nejvyšší hodnota, nebo průměrná. (KYBEZ, 2023a)

Dále je v doporučení povoleno například sloučení hrozby a zranitelnosti, pokud povinná osoba toto nerozlišuje. Také úrovně pro převod do číselné podoby je dovoleno měnit, avšak potom musí povinná osoba také změnit matici rizik.

ZÁVĚREČNÁ KAPITOLA TEORETICKÉ ČÁSTI

Teoretická část diplomové práce položila základy pro hlubší pochopení problematiky kybernetické bezpečnosti v prostředí lokálních sítí, přičemž zvláštní pozornost byla věnována roli lidského faktoru jako jednoho z klíčových aspektů zranitelnosti. Na základě rešerše odborné literatury a legislativních rámců byly sepsány poznatky, které zásadním způsobem ovlivňují přístup k ochraně informačních systémů.

Kybernetická bezpečnost není pouze technickou disciplínou. Ukazuje se, že právě propojení technických a sociálních prvků je nezbytné pro efektivní ochranu lokálních sítí. V této souvislosti je důležitým výstupem poznání, že uživatel – tedy člověk – není jen pasivním článkem, ale aktivním činitelem, který může bezpečnost výrazně ohrozit, nebo naopak právě podpořit. Z toho vyplývá, že v rámci bezpečnostních opatření je nutné klást důraz nejen na technologie, ale především na edukaci a vytváření bezpečnostního povědomí.

Bylo zjištěno, jaký návrh efektivních protiopatření je vyžadován a za pomoci modelů jako triáda CIA bylo možné nahlédnout do struktury ochrany dat a jejich kritických vlastností – důvěrnosti, integrity a dostupnosti. Zároveň jsme získali náhled do moderního pohledu na kybernetická rizika, kde právní rámce, jako je vyhláška č. 82/2018 Sb., poskytují základ pro systematické hodnocení rizik.

Jedním z hlavních přínosů teoretické části bylo zmapování technik sociálního inženýrství, a to nejen z historického hlediska, ale i z pohledu aktuálních trendů – včetně technik jako je quishing, které byly následně využity v praktické části práce. Tyto útoky ukazují, jak sofistikovaným způsobem mohou být zneužívány běžné technologie, a jak snadno lze lidskou důvěru obrátit proti uživateli samotnému. Právě tento typ útoků často obchází technická opatření a staví na psychologickém nátlaku nebo sociální manipulaci.

Na základě výše uvedeného lze říct, že teoretická část práce vymezila klíčové pojmy a souvislosti, které umožnily navazující praktický výzkum. Bez jejich důkladného pochopení by nebylo možné interpretovat výsledky penetračního testu, navrhnout relevantní opatření nebo posoudit dopad edukace na zvýšení kybernetické odolnosti. Z teoretické analýzy tedy vyplývá, že efektivní ochrana lokální sítě není otázkou jednoho opatření, ale výsledkem propojení tří základních rovin – člověka, technologie a procesů – jejichž rovnováha tvoří jádro moderní kybernetické bezpečnosti.

II. PRAKTICKÁ ČÁST

5 PŘÍPRAVA ÚTOKU

Pro podklady praktické části byl naplánován jednoduchý hackerský útok, a to formou dvou quishingových kampaní ve fyzické podobě. Proveden byl na Fakultě logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, situované v Uherském Hradišti, a to formou, která neměla negativní dopad. Útok vedl pouze na dotazníkové řešení, tudíž se nejednalo o žádný sběr osobních informací, či šíření nějakého škodlivého kódu. Nicméně provedení a způsob útoku by v jeho reálné podobě k daným nezákonným aktivitám vést mohl. Právě z důvodu využívání sociálního inženýrství jako zahajovacího aktu většiny útoků byla vybrána tato metoda, která prošla praktickým pokusem a vyhodnocením. Phishing v upravené formě prováděný pomocí QR kódu se tedy stal hlavním podkladem pro řešení rizik v místních sítích a také praktickou ukázkou metody k ošetření rizik vztahujících se právě na sociální inženýrství. Cílem bylo zjistit, zda bezpečnost v kybernetickém prostoru může opravdu z velké části stát na uživateli, případně jak uživatele školit a motivovat k obezřetnějšímu chování. Jak zvyšovat jejich povědomí o problematice a jak se může akademická půda podílet na vzdělávání i mimo daný rámec hodin k problematice určený. Zvyšování povědomí o rizicích u nových trendů, jakým kybernetický prostor a kriminalita v něm bezesporu je, by mělo probíhat na více úrovních, vzdělávací systém nevyjímaje. V rámci ošetření rizik se bude výstup z pokusu aplikovat právě i na způsoby práce s neodbornou veřejností a celkové provedení bude od začátku směřováno právě k poučení studentů. I to byl jeden z hlavních důvodů výběru fakulty jako vhodného místa k provedení útoku včetně formy, jakou byl proveden.

5.1 Cybercrime v cyberspace

Je nepopiratelným faktem, že se trestná činnost přesouvá do kybernetického prostoru. Zločinci využívají moderních technologií a postupů a útočí na nic netušící oběti. Nárůst kybernetické kriminality v České republice jasně ukazuje rostoucí trend. (Vlach, 2020)

Počty registrovaných případů je možno z více zdrojů zapsat do tabulky, a tak si i vypočítat meziroční nárůsty v dlouhodobějším horizontu. Jelikož se nepodařilo dohledat obecnou statistiku obsahující dané období v celku, každý rok byl ověřen nejméně ze dvou zdrojů a tak, aby se rozsah období z jednoho zdroje překrýval alespoň s jedním rokem ze zdroje druhého. Po ověření totožného čísla z překrývaného roku byla potvrzena shoda statistiky tak, aby růst odpovídal konkrétní položce.

Tabulka 3 Statistika růstu případů kybernetické kriminality

Rok	Počet registrovaných případů	Meziroční nárůst (%)
2011	1 502	—
2012	2 195	46,1
2013	3 108	41,6
2014	4 348	39,9
2015	5 023	15,5
2016	5 344	6,4
2017	5 654	5,8
2018	6 815	20,5
2019	8 417	23,5
2020	8 073	-4,1
2021	9 518	17,9
2022	18 554	94,9
2023	19 592	5,6

(Česká justice, 2020; NÚKIB, 2020; ČESKÁ JUSTICE, 2023; ČESKÉ NOVINY, 2024)

Evropská směrnice NIS2 dává alespoň základ ochrany. Nicméně útoky na jednotlivce, ať už za účelem napadnout konkrétní osobu, nebo se s její zpravidla nevědomou pomocí takzvaně „nabourat“ do firemní sítě, jsou stále aktuální a systémové řešení není na dohled. Není divu, přikázat lidem ať se v sítích chovají zodpovědně je spíše nereálná záležitost.

Organizace si samy na sebe často můžou objednat penetrační test, který jejich odolnost vyzkouší v praxi. Ten má za cíl prověřit právě připravenost organizace a také ukáže zodpovědným osobám slabá místa. Bezpečnostní manager se díky penetračnímu testování seznámí s trendy v oblasti kybernetických útoků a zpravidla dostane doporučení, jak jim předcházet. Běžný občan takovou možnost nemá. Dostane se mu spíše krátkého základního školení v organizaci, kde pracuje. Jedním z vedlejších výstupů této práce je i zjištění, zda studenti prošli nějakým školením a zda půda akademie poskytuje vhodné prostředí pro

penetrační testování. Prověří se také možnost školení praxí a aplikovatelnost na organizace vzdělávacího typu.

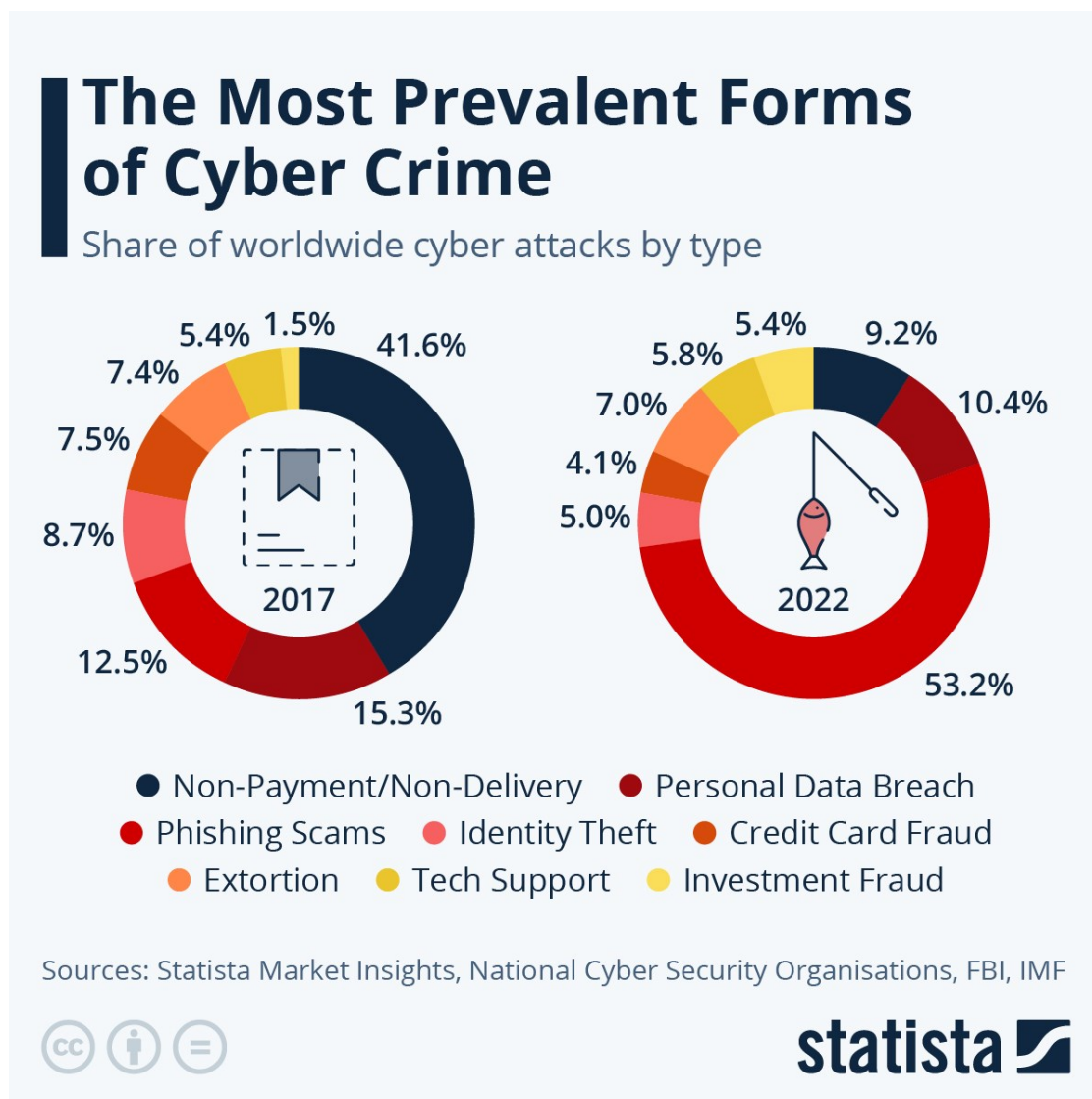
Záměrem pokusu bylo proto nejen prověřit stav v dané organizaci, ale také rovnou poukázat na dané riziko, vzbudit zájem, rozproudít debatu a v neposlední řadě ukázat jednu z mnoha možností popularizace a možné cesty k penetračnímu testování obyvatel, či praktické výuky ve vzdělávacích zařízeních.

5.2 Zranitelnost v lokálních sítích

Pokud se zaměříme na lokální sítě v širokém spektru organizací, odhalíme jednu častou slabinu – člověka. Technické prostředky a odborníci jsou schopni pracovat s celou škálou útoků a technické zabezpečení je dnes na velmi vysoké úrovni. Z tohoto důvodu se velmi často útoky provádějí za pomoci sociálního inženýrství či osobního kontaktu s obětí nebo členy organizace.

Jak je možné vidět na obrázku (Obrázek 3), ještě v roce 2017 byl nejrozšířenějším kybernetickým zločinem falešné internetové obchodování. To znamená vytvoření a zaplacení zboží, které následně není doručeno. Tato činnost zahrnovala celých 42 % kybernetických trestných činů. V té době phishing a útoky na osobní údaje tvořily 28 % útoků. V roce 2022 byl již phishing nejrozšířenějším kybernetickým zločinem s celkovým podílem 53 %. Jedná se tak opravdu o nejrozšířenější typ útoku, který zpravidla nese další druhy, jako například odkaz na malware. (STATISTA, 2023) Phishing je tedy startovní akce důležitá pro další pokračování útoku. Také slouží k vytipování sítí k útoku, kdy se právě čeká až oběť „zabere“ a otevře nám dveře do jedné z mnoha sítí, na které byla kampaň nasazena.

Jak data z roku 2017, tak nová data z roku 2022 nám ukazují ještě další důležitý poznatek. Obě nejrozšířenější metody jsou cíleny na lidi a využívají sociálního inženýrství. Lze tak říct, že nejvíce zkoušeným článkem v řetězci zabezpečení je člověk. Útočníci zpravidla volí tu nejsnazší cestu, ten nejslabší článek. A v době moderních technologií, kdy máme sofistikované systémy a odborníky kvalitně zpracované postupy a ochranná opatření je útok přes člověka pro útočníky bez hlubokých hackerských dovedností jediná možná cesta.



Obrázek 3 Statistika typů útoků 2017 a 2022

(STATISTA, 2023)

Legenda: Obrázek ukazuje nejrozšířenější formy kybernetické kriminality a jejich podíl na celosvětových kybernetických útocích podle typu.

2017

- Nepřijetí platby / nedoručení zboží – 41,6 %
- Zneužití osobních údajů – 15,3 %
- Phishingové podvody – 12,5 %
- Krádež identity – 8,7 %
- Podvody s kreditními kartami – 7,5 %

- Vydírání – 7,4 %
- Technická podpora – 5,4 %
- Investiční podvody – 1,5 %

2022

- Phishingové podvody – 53,2 %
- Zneužití osobních údajů – 10,4 %
- Nepřijetí platby / nedoručení zboží – 9,2 %
- Krádež identity – 7,0 %
- Podvody s kreditními kartami – 5,8 %
- Technická podpora – 5,4 %
- Vydírání – 5,0 %
- Investiční podvody – 4,1 %

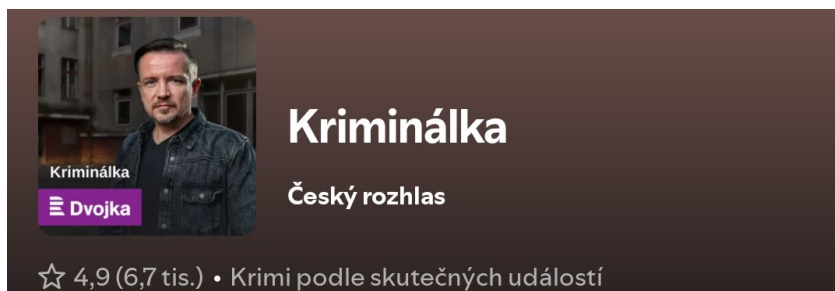
5.3 Jak se dostat do hlavy oběti

Stejně jako útočník, tak i bezpečnostní manažer musí mít postup, jak se dostat do mysli oběti. Útočník díky sociálnímu inženýrství dosahuje svých cílů. Můžeme si položit několik otázek, na které zkusíme najít odpověď praktickým pokusem.

- Je tedy možné techniky kybernetických útoků použít i k popularizaci tématu a seznámení člověka s problematikou?
- Jaký dopad bude mít penetrační testování běžných obyvatel?
- Je možné i při takovém penetračním testu získat určitou zpětnou vazbu?
- Jaké informace můžeme při testu předat dál?

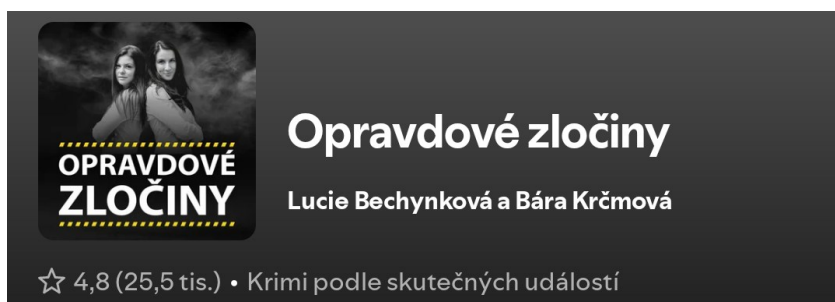
Dalo by se tedy mluvit o určité popularizaci tématu skrze útok. Nejen čistě penetrační test, zjištění stavu a nastavení opatření, jak tomu zpravidla bývá. Ale právě to seznámení s problematikou a předcházení problematice. Popularizace obecně dnes náleží například podcastům, nebo různé infografice či e-letáčkům, které však mezi neodbornou veřejností velký dosah nemají.

Jak lze vidět na příkladu z aplikace Spotify (obrázky níže), počty hodnocení u krimi podcastů a komedií jdou do tisíců a u kybernetické bezpečnosti se jedná o jednotky. I v případě neoborného podcastu, který je hodně zaměřen spíše na činy a osobnosti hackerů se jedná o nižší desítky. A to spadá do stejné kategorie jako podcast „Kriminálka“ a „Opravdové zločiny“, tedy kategorie „Krimi podle skutečných událostí“.



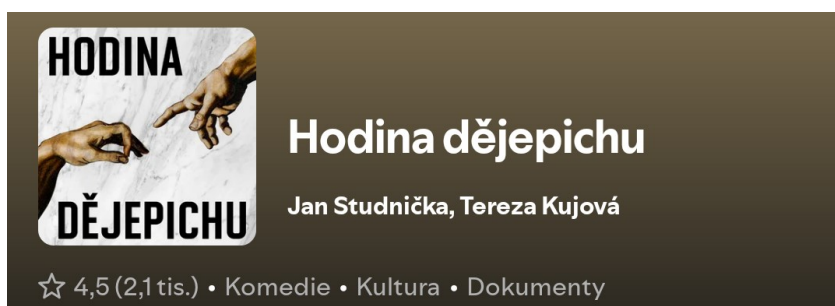
Obrázek 4 Spotify Kriminálka

(SPOTIFY, c2025)



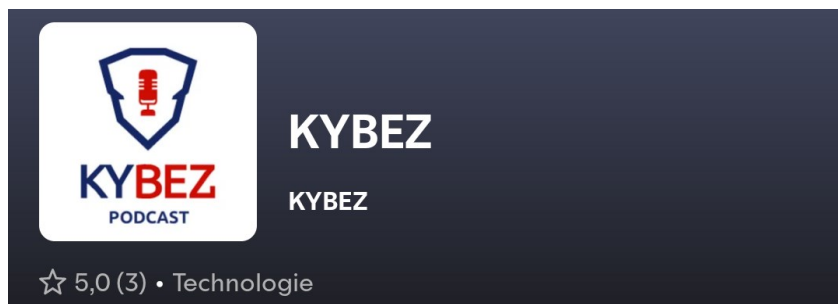
Obrázek 5 Spotify Opravdové zločiny

(SPOTIFY, c2025)



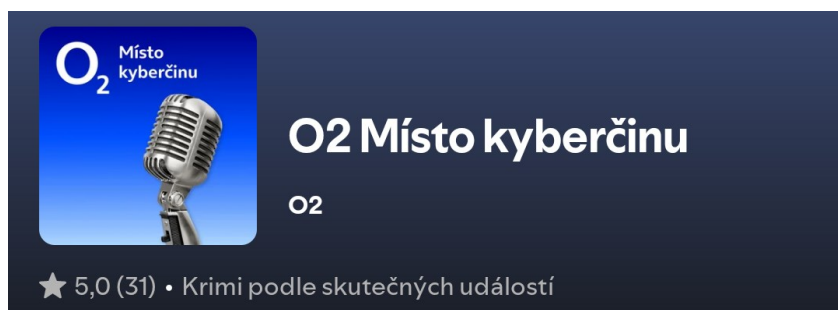
Obrázek 6 Spotify Hodina dějepichu

(SPOTIFY, c2025)



Obrázek 7 Spotify KYBEZ

(SPOTIFY, c2025)



Obrázek 8 Spotify Místo kyberčinu

(SPOTIFY, c2025)

Praktické situace se tedy jeví jako možnost dále rozvíjet povědomí o rizicích v kybernetickém prostoru a tím chránit jak obyvatele, tak dané místní sítě, ať už domácí, nebo sítě organizací kde dané osoby působí. Jak prohlásil na přednášce pan doktor Svoboda:

„Stačí mít lepší zámek, nežli má soused“

Ing. Petr Svoboda, Ph.D.

Můžeme zvyšovat odolnost sítí a snižovat rizika úspěšných útoků díky opatrnosti a povědomí uživatelů. Dalo by se říct, že jedna z těch možných cest k vyšší odolnosti celku vede skrze jednotlivce, kteří považují bezpečnost v kybernetickém prostoru jako konkurenční prostředí a neustále se snaží „mít lepší zámek nežli konkurence“. A s klesající úspěšností útoků může klesat i zájem tyto útoky provádět.

5.4 Školení

Jednou z běžných metod je školení. Týká se zpravidla zaměstnanců a mezi jeho slabiny patří neodbornost publika. V soukromém i státním sektoru již školení zpravidla probíhají, ale posluchači k tomuto tématu často přistupují s nezájmem. Komenského škola hrou pomáhá, pokud se udeří na citlivou notu. Jako příklad lze uvést velmi oblíbené doptání na e-mailovou adresu někoho z publika a využití webu pro ověření úniku hesel. Zájem rapidně vzrůstá, a dokonce se posluchači sami začnou hlásit pro ověření úniků na jejich emailové adrese.

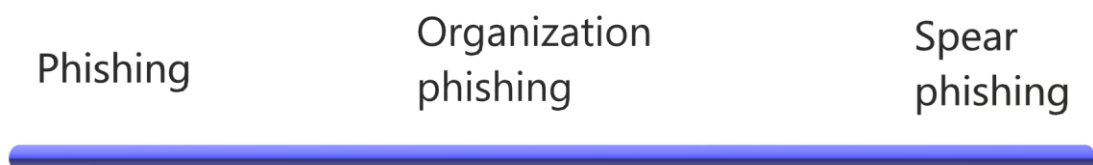
Pokus má tedy i poukázat na možnost zvýšení zájmu, lepší pochopení problematiky a otestovat možnosti praktických ukázek, které jsou cíleny na určité sociální skupiny, či obyvatelstvo jako celek. Praktickým provedením poukazuje na rizika v každodenním životě a chrání tak jak samotné uživatele, tak i celé místní sítě před útokem skrze člověka jakožto článek v bezpečnostním řetězci sítě.

6 METODOLOGIE ÚTOČNÍKA

Z důvodu lepšího sledování a také ochrany konkrétní sítě se útok povede ve fyzické formě. Což pro phishing není úplně typické, ale u quishingu takovou podobu vidět můžeme například v podobě přelepování originálních QR kódů.

6.1 Výběr místa

Jakým způsobem a na co útočit je zpravidla otázka kampaně, která bude vedena. Při masivním zásahu klasickým, tedy tím v elektronické podobě, hromadně rozeslaným phishingem není cílení na místo řešeno vůbec. Při spear phishingu je zase důkladně zkoumáno jak místo, tak zájmová osoba. Díky umělé inteligenci však nastává doba, kdy se bude dát pohodlně zacílit třeba na typ organizací a rozesílat balíky v rozsahu masivní phishingové kampaně, avšak šité na míru organizacím. Jako například zde v pokusu lze leták (6.3.1) pomocí umělé inteligence zbarvit do barev všech univerzit a rozeslat již upravenou verzi například v barvách různých univerzit. Ke konvenčním označením phishing a spear phishing by se dalo přidat i označení ve smyslu organization phishing, které spojuje vybrané prvky v jednu kampaň a pohybuje se po ose blíže jednomu či druhému, a to na základě šíře záběru od obecného až ke konkrétní osobě. Napříč literaturou došlo v průběhu času k označení spear phishing v případech kvalitně připravených kampaní na jednotlivce. Později se označení definovalo k jednotlivci a organizaci. Avšak jak ukazuje i pokus popsáný v této práci, lze najít rozdíly mezi útokem na jednotlivce, fakultu, univerzitu, nebo univerzity jako celek. Tento pohled lze aplikovat na různé sektory, například kampaň připravena na ředitele banky bude jiná než na bankovní dům, banku, nebo bankovní instituce. A poté se znaky kampaně, příprava a s tím spojené varovné signály a obrana při průběhu pravděpodobně budou lišit. Pomyslný organization phishing by se poté posouval po ose vlevo či vpravo podle toho, které ze základních variant by byl blíže. Tak jak je například popsáno v kapitole 8.3 Bilance.



Obrázek 9 Pomyslný Organization phishing

(vlastní)

Výběr vhodného místa pro fyzický quishingový útok probíhal podle následujících kritérií:

- Volný pohyb, nebo přístup.
- Vysoká koncentrace osob.
- Organizace využívající sítě ve větší míře.
- Možnost kontrolovat proces pokusu.
- Přístup k informacím od subjektů.

K pokusu byla vybrána Fakulta logistiky a krizového řízení v Uherském Hradišti. Ta splňuje výše uvedené body následovně:

- Přestože se ke vstupu musí použít přístupová karta, jedná se o měkký cíl, kde není vyžadováno důsledné dodržení režimu vstupu a neprobíhá přísná kontrola každého jednotlivce.
- Koncentrace lidí v budovách je velmi vysoká. Pro pokus byl zvolen termín mimo zkouškové období, kdy se studenti vracejí do lavic a předpokládá se vyšší účast na přednáškách začátkem semestru.
- Studenti i samotná organizace mají kvalitní technické zázemí a pro studium je ve značné míře využíváno moderních technologií, včetně sítí.
- V rámci studia má autor pokusu stálý přístup do prostor fakulty a možnost aktivně komunikovat s několika lidmi pohybujícími se v prostorách fakulty a tím získávat informace o aktuálním dění, včetně průběžné zpětné vazby.
- Možnost obdržet v případě potřeby zpětnou vazbu od dotčených osob či dané organizace.

6.2 Výběr metody

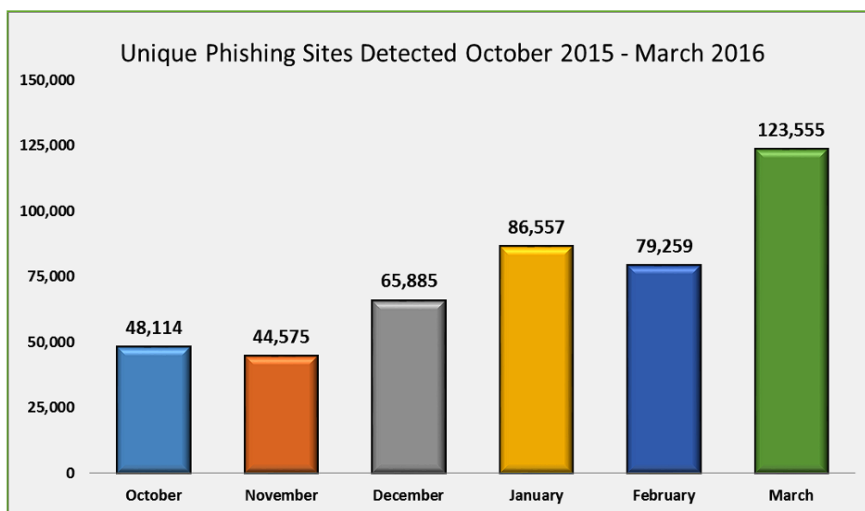
Quishing je aktuální hrozba, u které je podle webu keepnet nárůst za rok 2023 neuvěřitelných 587 %. (Keepnet, 2025) Tento údaj je však nutné brát s rezervou. K útokům se přihlásí jen menší část poškozených, takže se bavíme o nahlášeném minimu. O celkovém počtu pokusů a provedení i neúspěšných útoků pomocí phishingu, nebo nějaké z jeho mutací se dají vést spíše odhady. (Kolouch, 2016) Odhady se však zakládají na záchytech v jednotlivých organizacích, pokusech menšího rozsahu, jako je například pokus provedený v této práci, a dalších podobných metodách zaměřených na lokální sítě, které se poté s různým rozsahem

aplikují na síť jako celek. I NÚKIB pracuje s úspěšností pouze nahlášených incidentů a na jejich webu vydává pravidelné reporty, které trend zvyšování počtu dokládají. (NÚKIB, 2025)

Vysokou vypovídající hodnotu můžeme očekávat u organizace APWG. V publikaci Cybercrime je uvedeno, že dle reportu z Q1_2016 vzrostl celkový phishing o 250 %. (Kolouch, 2016)

Phishing E-mail Reports and Phishing Site Trends – 1st Quarter 2016

The total number of unique phishing websites observed in Q1 was 289,371. The number observed per month rose steadily from the 48,114 detected in October 2015 to the 123,555 detected in March 2016 – a 250 percent increase over six months. The increase in December 2015 was expected, since there is usually a spate of spamming and online fraud during the holiday shopping season. The continuing increase into 2016 is cause for concern.



Obrázek 10 Phishing report Q1_20166

(APWG, 2013)

Legenda: report APWG na který odkazuje publikace Cybercrime znázorňující vzrůstající počet phishingových útoků v průběhu daných měsíců. V té době v reportu ještě označovaných jako „sites“, nicméně v průběhu vydávání dalších postupně do závorky přidáváno „attack“.

Pro porovnání můžeme tedy přidat aktuální report z webu organizace APWG zachycující vývoj od Q3_2022 do Q3_2024.

The number of reported phish has been in a zone since June 2023, varying between 290,000 and 370,000 attacks per month:



Obrázek 11 Phishing report Q3_2022 - Q3_2024

(APWG, 2013)

Legenda: report APWG, který znázorňuje počet phishingových útoků v daném období.

I když meziročně je vidno určitý pokles, tak lze vyčíst rapidní nárůst mezi zmiňovaným reportem z roku 2016 a aktuálním z roku 2024. Zmíněný report v publikaci Cybercrime se pohybuje na hodnotě 48 114 na začátku sledovaného období, potažmo 123 555 reportů na konci. V roce 2024 graf ukazuje, že sledované období má už 400 000+ reportů na začátku sledovaného období, potažmo kolem 350 000 reportů na konci. (APWG, 2013)

Trend je však takový, že phishing ve své klasické podobě ustupuje a za nárůstem stojí spíše jeho modifikace, jako je například zde použitý quishing. (Kolouch, 2016) Dnes se tedy můžeme setkat často s jinými formami phishingových útoků, které jsou lépe cíleny na konkrétní platformy, místa, či sociální skupiny. Klasický phishing se doplňuje například o QR kód a dochází tak ke kombinaci.

Tuto kombinaci popisoval již v roce 2014 Jaromír Hořejší ze společnosti Avast, kdy se po masivní phishingové akci mohl uživatel dostat až na stránku s požadavkem na zavedení dvoufázového ověření k připojení mobilního telefonu jako druhého zařízení. Po zvolení operačního systému android byl právě použit QR kód, který po spuštění stáhnul malware. (AVAST, 2014)

Vážení kliente!

SMS byla odeslána na číslo: +. Doručení SMS do 5 minut.

Pokud Vám nepřišel SMS, naskenujte QR kód



Je třeba nainstalovat aplikace OTPdirekt. Stiskněte tlačítko "Zobrazit instrukce".

[Zobrazit instrukce](#)

Pozor! Nemůžete pokračovat dále bez OTP hesla.

OTP heslo:

[Pokračovat](#)

Obrázek 12 Útok v roce 2014 s použitím QR kódu

(AVAST, 2014)

Jak lze tedy vidět, v různých podobách je využíváný dlouhodobě. Z obrázku (Obrázek 12) můžeme ještě dobře vidět spousty chyb, zejména gramatických. Je zřejmé, že se používaly automatické překlady a ty byly v té době značně nepřesné zejména ve stavbě vět a interpunkci. O deset let později můžeme říct, že tento jev není tak častý díky lepším systémům pro překlad mezi cizími jazyky. A i když jazykové chyby lze vidět stále i v dnešní době a lze je tak použít jako identifikátor, není dáno, že pokud zpráva jazykové chyby neobsahuje je důvěryhodná.

Pro pokus byl tedy vybrán útok pomocí QR kódu. Ten je vhodný k použití právě i ve fyzické formě. Okamžité načtení odkazu přesměruje oběť z QR kódu rovnou na požadovanou stránku a může tak posloužit i výchovným účelům. Mezi studenty je používání QR kódů zcela běžné. Na samotné fakultě se jich vyskytuje několik. Jako jeden z příkladů je QR kód na FLKR_memes (Obrázek 13), který se stal i inspirací na sekundární prostředek útoku. Pracovalo se s variantou nahrazení, ale QR kód se na fakultě vyskytoval již delší dobu,

a proto byl předpoklad sníženého zájmu. Jiná situace by nastala na začátku akademického roku, kde by záměna měla úspěšné záchyty převážně nově příchozích studentů.



Obrázek 13 FLKR_memes

(vlastní)

Zde nastupuje právě sociální inženýrství a pomocí jeho technik se vybírá metoda pro co největší zásah a úspěšnost. Opět se tedy musí bezpečnostní manažer držet aktuálních trendů a vyhodnocovat rizika i na základě sofistikovaných metod sociálního inženýrství.

Obliba mezi mladší populací předurčuje quishing k úspěchu právě na půdě fakulty. Metody phishingu a jiných útoků jsou často upravovány právě podle prostředí a cíle. Útočník sleduje trendy a snaží se maximalizovat úspěšnost. Buď může použít nějaký běžný postup, jako phishingová kampaň pomocí e-mailů, případně může tyto akce modifikovat právě podle cíle.

Hlavním účelem pokusného útoku je sběr počtu přístupů přes dva quishingové útoky, jejich porovnání, vyhodnocení rizik takového útoku na danou organizaci, posouzení rizik lokální sítě v organizacích tohoto typu a možnosti prevence, či snížení účinnosti útoku na jednotlivce a organizaci. Mimo jiné se díky tomu podařilo sesbírat informace od části obětí, kteří byli ochotni vyplnit dotazník i po zjištění, že se jedná o útok. Nicméně informace z dotazníku jsou jen doprovodným výstupem. Dotazník byl primárně zvolen jako tzv. „počítadlo přístupů“ přes dané QR kódy ve vybraném časovém období. Tvorba alespoň základního dotazníku byla řešena až chvíli před spuštěním útoku jako další sběr informací. Záměrně nebyl rozsáhlý ani zbytečně komplikovaný vzhledem k povaze přístupu do něj. Pokud by se pokus opakoval, určitě by bylo vhodné dotazník nastavit lépe. Do dotazníku již bylo použito i určité školicí kampaně a oběti tak neškodnou formou dostanou zpětnou vazbu o novém fenoménu a kybernetické bezpečnosti.

6.3 Prostředky vybrané metody

Pokud se zaměříme na vybrané místo a metodu, nabízí se nám několik vhodných vektorů útoku. Pro výzkumné účely je potřeba vytvořit alespoň dvě kampaně z důvodu porovnání úspěšnosti, nákladů na jeden záchyt, úspěšnost v daném časovém období, průběh kampaně v čase a účinnost na různé skupiny.

Způsob provedení byl zvolen tak, aby odrážel co nejvěrněji obyčejný masivní útok, tedy aby byl co nejblíže phishingu a co nejvzdálenější od spear phishingu i přesto, že byl provedený na konkrétní organizaci.

Zvoleny byly tedy dvě kampaně, jedna formou letáků na pizzu a druhá formou napodobení probíhající kampaně na FLKR_memes, která odkazuje na sociální síť Instagram.

6.3.1 Letáková kampaň

Jako první varianta byly vybrány letáky na pizzu v akci 1 + 2 pizzy zdarma. Pizza se subjektivně mnoha lidem jeví jako nějaké studentské jídlo a pokud je v nějaké velmi výhodné akci, tak studenti můžou ztrácet ostražitost. Z toho důvodu byla vybrána akce, která běžná není – jedna pizza a k ní další dvě zdarma. Důvodem bylo vložení něčeho typického pro phishing, tedy jakéhosi marketingového „wow efektu“, který má za úkol oběť navnadit na nějakou úžasnou a neodolatelnou nabídku, která se vidí jen velmi výjimečně. A zároveň se právě tato metoda, nebo tento markant uvádí často jako signál, který nás má varovat před podvodem.

Záměrně bylo přistoupeno k tvorbě takovým způsobem, aby byla kampaň podobná nezainteresované straně útočníka z vně organizace, tedy klasicky nastavená kampaň pro plošný zásah. Tvorba letáku byla pod 20 minut celkového času i s úpravami. Na rozdíl od spear phishingu nebyl řešen detailní sběr informací o cílech. K tvorbě byl zvolen jen MS Word, obrázek byl volně dostupný z fotobanky a barva písma byla vybrána v barvách univerzity, což byla jediná informace konkrétně se vztahující k cíli a má vzbudit důvěru.

I toto ukazuje, jak jednoduché je připravit kampaň a s trochou cviku lze tvořit cílenější kampaně na vysoké počty organizací. Samotná tvorba trvala osm minut. Necelých dvanáct poté trvaly úpravy a ladění, nicméně použitelná byla hned první hotová varianta. Neobsahovala fragmenty, grafické ani gramatické chyby, byla srozumitelná a hotová.

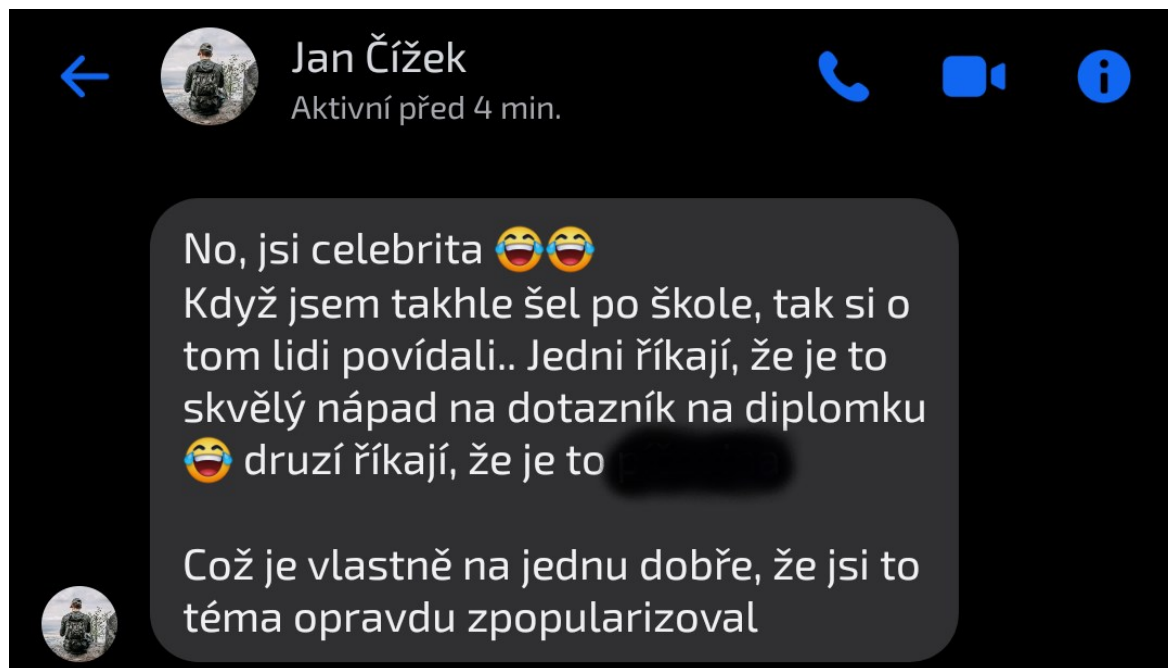


Obrázek 14 Leták na pizzu

(vlastní)

Jak lze vidět na obrázku, leták je jednoduchý, černé barvy, písmem v barvách univerzity. Neobsahuje adresu, informace o pizzerii, nebo jakémkoliv podnikatelském subjektu, který by za akcí stál. Dokonce ani město, ve kterém by se případná pizzerie měla nacházet. Tudíž se ani nesnaží působit jako pravý, který zpravidla obsahuje adresu pobočky, další informace, akce, webové adresy, nebo identifikační číslo podnikatelského subjektu, a naopak obsahuje stále údaje a vzhled, který má varovné prvky. I přes varovné signály je přidanou hodnotou profesionální tisk. Ten je jako jediný prvek na vysoké a uvěřitelné úrovni. Důvodem takového postupu je možnost útočníků využívat, nebo dokonce i zneužívat těchto služeb, například na pracovišti, případně si pro větší útoky pořídit tiskárnu s možností foto tisku. I přes profesionální tisk nebyla provedena profesionální grafická práce, aby i tady bylo simulováno vytvoření letáku útočníkem, který nemusí být profesionálním grafikem.

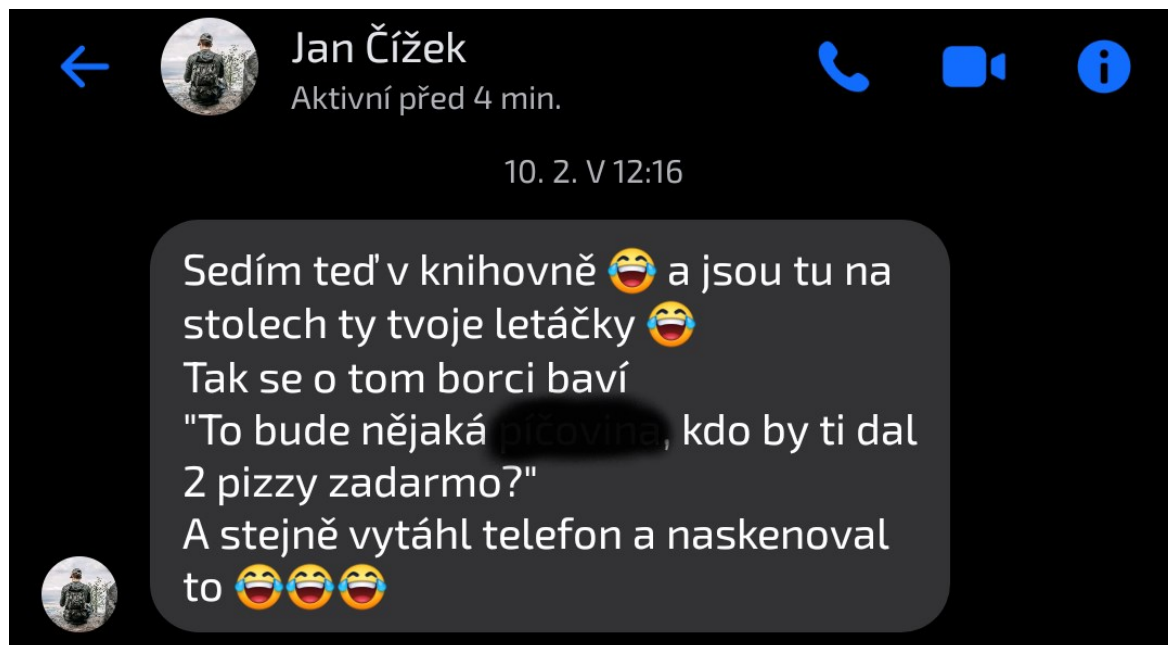
Podle svědectví studenta Bc. Jana Čížka, který na fakultě studuje denní formou, tudíž ve sledovaném prostředí pobývá dlouhodobě a do života na fakultě má mnohem lepší vhled než student kombinované formy, se útok stal i debatním tématem. Jedni nápad chválí, jiní pomlouvají. Názor obětí však není důvodem provedení. Debata poukazuje na to, že se téma popularizuje, studenti se zamýšlí nad problematikou, bezpečnost roste, riziko klesá.



Obrázek 15 Písemné svědectví první

(vlastní)

I když někteří studenti zajisté rizika znají, opatrnost není vždy samozřejmostí. Cíleně vložený varovný signál byl v jednom doloženém případě rozpoznán, a přesto došlo k naskenování a otevření odkazu.



Obrázek 16 Písemné svědectví druhé

(vlastní)

Jelikož můžeme dnes vidět i profesionálně provedené útoky, kdy například při spear phishingu je kampaň připravena opravdu důkladně, lze se domnívat, že kvalita i u větších kampaní poroste dále tak jako tomu bylo doposud.

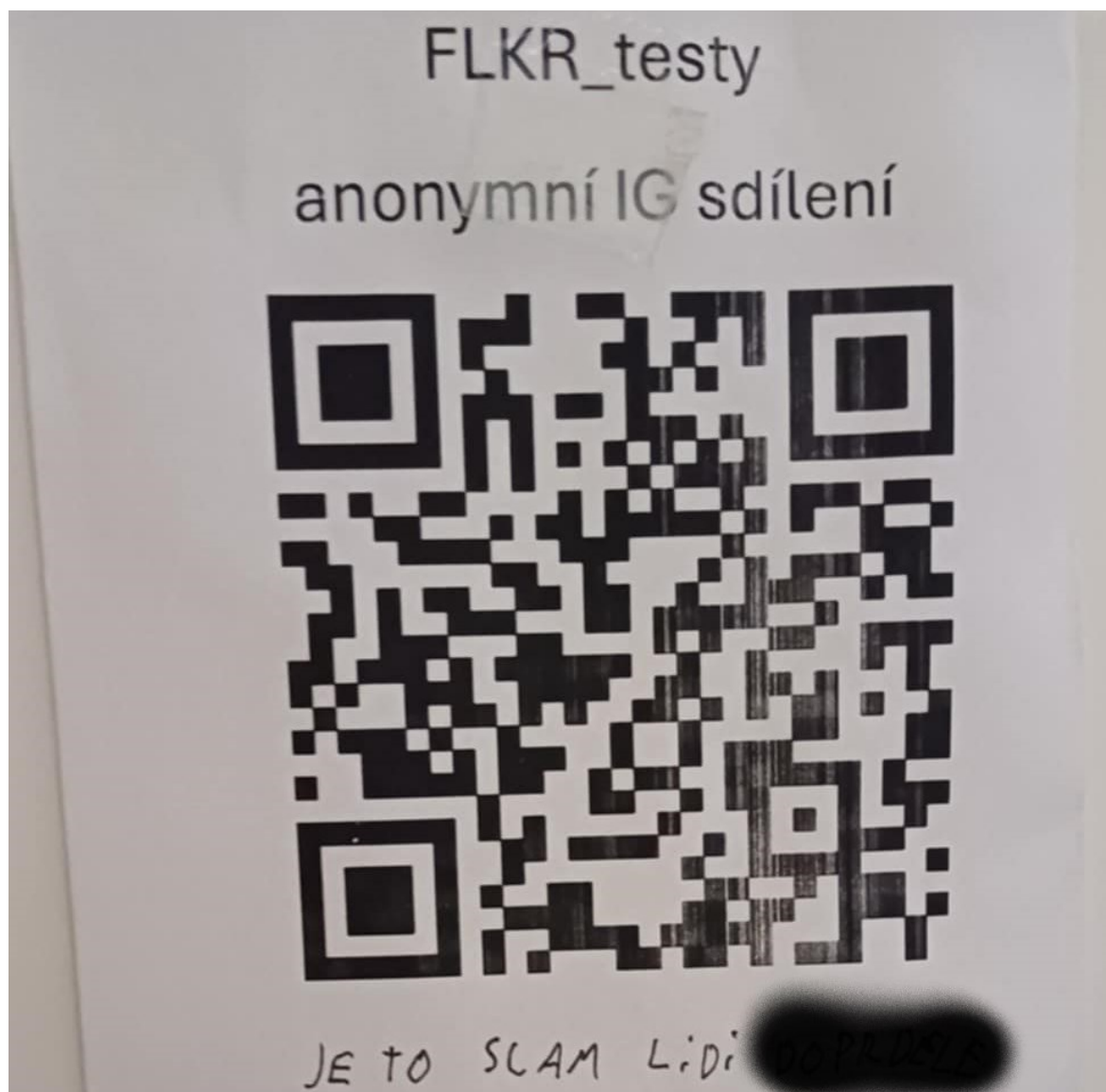
Nakonec byl tedy přidán pouze QR kód na dotazník a leták byl tedy neškodný. Důvěryhodnost způsobuje právě dojem z vynaložených nákladů a je otázkou, zda by útočník očekával určitou rentabilitu vkladu. Účelem však bylo poukázat i na trend zkvalitňování phishingových útoků obecně.

6.3.2 FLKR_testy

Za druhou variantu byl zvolen obyčejný černobílý letáček pouze s nápisem FLKR_testy, anonymní IG sdílení, který byl vytvořen během necelých dvou minut a jehož předlohou byl právě na fakultě se vyskytující letáček FLKR_memes.

Původní záměr byl nahradit letáčky FLKR_memes, nicméně kolem poloviny akademického roku, kdy drtivá většina zájemců o odběr FLKR_memes již kód naskenovala nebyl předpoklad většího záchytu oskenování QR kódu. Tento způsob neměl působit zvlášť důvěryhodným dojmem a náklady měly být zanedbatelné. Z tohoto důvodu byl použit obyčejný černobílý tisk, grafická úprava byla zvolena jen vložením QR kódu a nápisem, bez žádných doprovodných grafických prvků či obrázků a po vytisknutí se letáčky stříhaly ručně tak, aby ruční stříh byl i poznat. Prvek důvěry a vodítko pro neopatrnost oběti byla právě podoba s letáčkem FLKR_memes, který studenti vídají v delším časovém horizontu a může tedy narušit obezřetnost u jemu podobných letáčků. Prvkem nedůvěry bylo právě popsání provedení tvorby. Exponování tohoto způsobu bylo omezeno na toalety a jednu nástěnku tak, aby působil komunitně a utajeně. Tomu odpovídalo právě i samotné provedení. Po nějaké době byl jeden z letáčků právě označen jako „scam“, tedy podvod.

Druhá doprovodná kampaň byla zvolena pro porovnání výsledků při různých nákladech a časové náročnosti. Tato kampaň byla velmi levná a časově absolutně nenáročná. Zatímco hlavní kampaň byla zpracována za pomoci profesionálního tisku a byla provázena nezanedbatelnými náklady.



Obrázek 17 Úprava útoku obětí

(vlastní)

Zřejmě zklamaným studentem, který se těšil na výsledky testů. Dostal tak zdarma zkušenost a nevědomě pomohl ostatním účastníkům, jelikož opět částečně oživil zájem o téma, přidal něco nového do průběhu pokusu a upozornil studenty, že se jedná o podvod, a tudíž je obecná obezřetnost na místě.

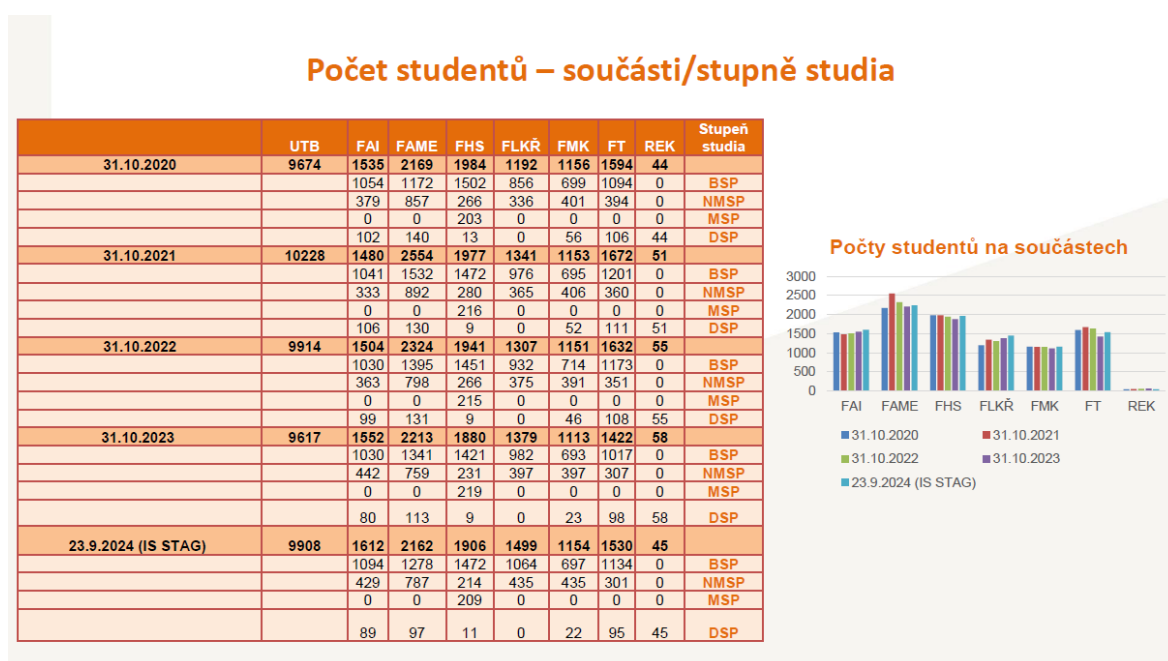
6.4 Zdroje návštěv

QR kódy byly otestovány předem a načtení odkazu bylo testováno bez kliknutí na odkaz. Důvodem bylo ošetření přístupů čistě z útoku tak, aby nebylo potřeba jakkoliv čistit údaje o testovací přístupy. Oba dotazníky shodně vykazují ve statistice také 100 % přístupů pomocí QR kódu, tudíž opravdu přístupy pouze zamýšleným způsobem.

7 VÝSLEDKY A DATA

Penetrační test tedy proběhl v termínu 7.2.2025 – 24.2.2025. Vybráno bylo období po započetí letního semestru, kdy probíhá výuka, a tudíž se na vybraných místech pohybuje maximum lidí. Jako nevhodné se jevílo dělat útok v době zkouškového období, kdy část studentů zpravidla pobývá mimo prostory fakulty anebo kolejí a vždy se dostaví jen v určitý konkrétní termín na případnou zkoušku.

Odhadnout kolik přesně studentů bylo na fakultě není bez interních údajů možné. Maximum studujících v prezenční formě k 23.9.2024 bylo dle informací univerzity z dokumentu Pedagogická oblast: počty studentů a statistiky související s PŘ a se studiem na UTB 2024/2025 celkem 1499 osob.



Obrázek 18 Počet studentů univerzity Tomáše Bati

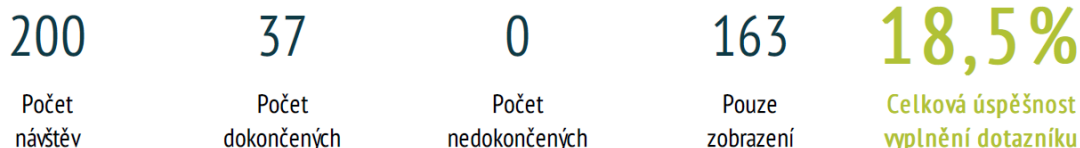
(UTB, 2024)

7.1 Letáky

Distribuce letáků proběhla v pátek v odpoledních hodinách na kolejích. Z důvodu akce „den otevřených dveří“ pořádané v sobotu 8.2.2025, která proběhla na budově fakulty logistiky a krizového řízení, byla provedena distribuce letáků na fakultu se záměrným zpožděním. Přesunuta byla na sobotní podvečer, a to v rozsahu pro prostory učebních bloků fakulty. Důvodem bylo riziko zkreslení výsledků návštěvníky akce. Tudíž největší zásah se očekával v pondělí, dne 10.2.2025 po návratu denních studentů z domova. Celkový počet návštěv se

zastavil na čísle 200, kdy z tohoto počtu respondentů jich 37 vyplnilo dotazník. Jedná se o 18,5% úspěšnost s vyplněním.

Statistika respondentů

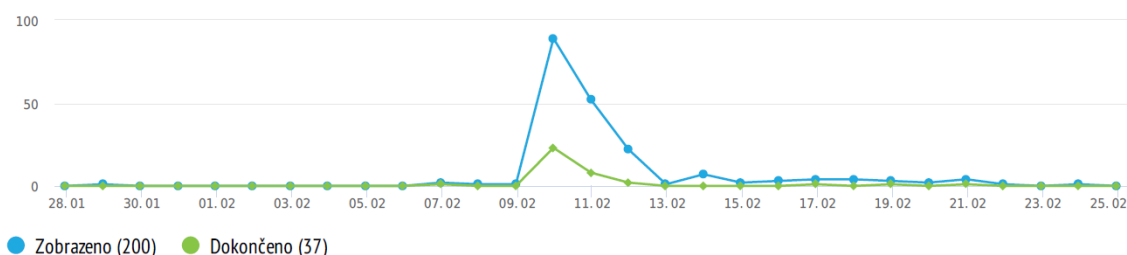


Obrázek 19 Statistika respondentů – akce pizza leták

(vlastní – statistika dotazníku ze serveru Survio)

Z grafu přístupů vidíme následující.

Historie návštěv (07. 02. 2025 – 21. 02. 2025)



Obrázek 20 Historie návštěv – akce pizza leták

(vlastní – statistika dotazníku ze serveru Survio)

Modrá barva nám ukazuje počet návštěv, tedy samotné oskenování QR kódu a následné otevření odkazu. Přístupů bylo za sledované období přesných dvě stě, což je na leták s varovnými prvky vysoké číslo. Jak lze vidět, peaku, tedy maximálního počtu návštěv, dosáhl dotazník hned první den, a to téměř polovinu z celkového počtu. Druhý den následoval pokles na přibližně 25 % z celkových návštěv, třetí den přibližně 10 % a následuje období dvanácti dnů, které je již velmi podprůměrné k celkovému počtu přístupů.

Pokud budeme uvažovat nad důvodem takového poklesu, nalezneme mimo jiné několik možných důvodů:

- Vyčerpání zájemců
- Povšimnutí si přihlížejících, že se jedná o podvod

- Rozšíření informace o podvodu
- Vyčerpání letáků (někteří studenti si brali celé hromádky)
- Propojení informace s kampaní FLKR_testy a vyšší obezřetnost

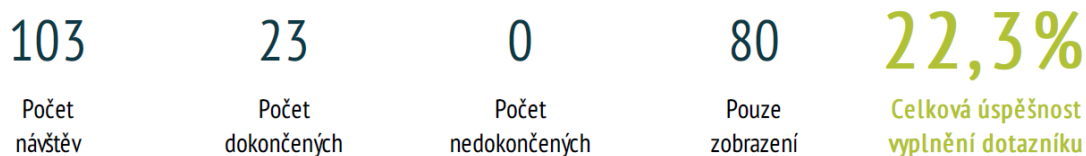
Pokud se o této akci otevřeně mluvilo, je zjevné, že bylo docíleno stavu, kdy studenti leták vidí a už vědí, že se jedná o podvod zprostředkovaně.

Sledovat stav zásob letáčků v reálném čase u fyzické formy nebylo možné. Nicméně z celkového počtu 500ks, kdy bylo k distribuci použito minimálně 480ks. Jelikož několikrát došlo k doplnění letáků z míst odkud byly odneseny, ale počet návštěv po několika málo dnech spadl k několika jednotkám denně, můžeme se domnívat, že po vyzkoušení a zjištění, o co se jedná, nasbírané zásoby jednotlivců skončily v koši.

7.2 FLKR_testy

Stejně jako při distribuci letáků, i druhá metoda v podobě QR kódu FLKR_memes byla odložena na pondělí. Jako místo pro vystavení QR kódu byly vybrány pouze toalety a jedna nástěnka na chodbě. Záměrem bylo, aby byl minimalizovaný počet kusů, tím pádem proběhla minimalizace nákladů, a letáčky zůstávaly na místě. Oproti kampani na pizzu, kdy si někteří studenti brali letáků několik, zřejmě ve víře, že slevu dostanou opakovaně podle počtu letáků.

Statistika respondentů

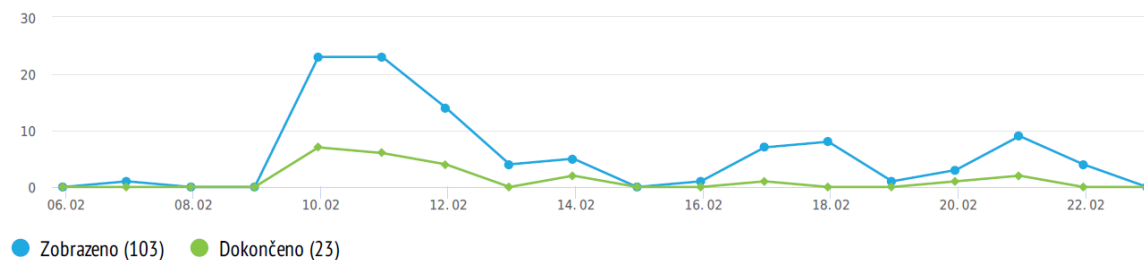


Obrázek 21 Statistika respondentů – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

Otázkou bylo, zda nám i místo může ovlivnit počet oskenování. Graf přístupů nám ukazuje následující:

Historie návštěv (10. 02. 2025 – 21. 02. 2025)



Obrázek 22 Historie návštěv – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

Zjevně jiný průběh v čase. Opět nejsilnější moment na začátku, což by mohlo potvrdit klesající zájem díky rozšíření informace o podvodu. Avšak se poté průběh kontinuálně držel v určitých intervalech až do ukončení pokusu. Předpokládaný útlum byl 15.2 a 16.2, což připadlo na víkend. I zde můžeme uvést několik teoretických důvodů o prvotním poklesu:

- Vyčerpání zájemců
- Rozšíření informace o podvodu
- Propojení informace s letákovou kampaní a vyšší obezřetnost

Zajímavostí je kontinuita v dalších dnech po prvotním útlumu, která se u letákové kampaně neprojevila, tedy alespoň ne v takové míře.

7.3 Dílčí závěr záchytů

Pokus tedy jasně prokázal, že skenování QR kódu velké množství studentů neřeší jako něco škodlivého a docela aktivně skenují kódy z podezřelých zdrojů. Za pomoci interních údajů a podrobnějšího zkoumání počtu osob na budově fakulty a kolejích by bylo možno přesněji zjistit procento studentů, kteří nastražený QR kód oskenovali. Ale i v případě, že autor tyto informace nemá a budeme vycházet z celkového počtu přihlášených studentů 1499, je souhrnný počet oskenování ve výši 303 přístupů velmi vysoké číslo. A to v kontextu toho, že kampaň se ani nesnažila působit co nejvěrohodněji, a naopak bylo účelně ponecháno vždy nějaké varovné vodítko vychází jako velmi znepokojující údaj. Co vedlo studenty k takové neopatrnosti není úplně jasné. Ale pokud to byla jen neopatrnost, nabízí se řešení školením, nebo opakovaným útokem, což je opět školení hrou. Pokud je k neopatrnosti vedlo prostředí, ve kterém se cítili bezpečně, opět se nabízí stejné řešení. Důvodem je, že není možné tyto útoky úspěšně blokovat v reálném čase. A to ani fyzické provedení. Vždy je potřeba nějaká

reakční doba a tohoto období využívá útočník právě ve svůj prospěch. Než email zmizí ze schránky, než někdo strhne QR kódy, než se mezi studenty dostane informace o problému, může být 303krát zkoušeno, což odpovídá 20,2 % z celkového počtu studentů, zda se lze dostat do systému. A i když školení a výuka v oblasti probíhá, lze jasně vidět, že ten slabý článek stále jako vstupní akce funguje. Ale také je zjevné, že téma se dostalo do povědomí studentů a ti vedli aktivní debatu.

8 POROVNÁNÍ KAMPANÍ

Pokud se zaměříme na společné ukazatele obou kampaní, můžeme porovnat několik společných faktorů. Mezi ty hlavní bezesporu patří náklady a čas vůči počtu oskenování a interakci, za kterou budeme považovat vyplnění dotazníku. Ten svým způsobem nahrazuje podvody jako například:

- Odkaz na stránku (např. se slevovým kódem, avšak vedoucí k malware)
- Odkaz na škodlivou aplikaci
- Vyžadování údajů jako e-mail

8.1 Náklady

Finanční náklady na každou kampaň byly zcela odlišné. Jako jedno z možných kritérií na zvýšení úspěchu útoku můžeme náklady uvažovat.

Celkové náklady se skládají čistě z vynaložených finančních prostředků pro tvorbu a tisk. I když s letákem měla tiskárna trochu práce s úpravou tak, aby byla vyšší výsledná kvalita, tak cena byla čistě za tisk letáků. Tiskárna byla srozuměna s tím, že kvalita nemusí být absolutně profesionální, jelikož lehké chyby jsou žádoucí jako jedno z upozorňujících znamení podvodu. Tiskárna nicméně alespoň upravila nějaké prvky tak, aby alespoň barvy odpovídaly předloze. V akci FLKR_testy šlo o domácí tisk, kde cena vychází z ceny toneru děleného mezi počet stran a ceny jednoho balíku papíru děleno počet listů v něm. Vytisknuty byly čtyři listy, kde každý obsahoval čtyři pole s QR kódem k vystřížení.

Tabulka 4 Tabulka finančních nákladů

Název	Celkové náklady	Celkový počet oskenování	Náklady na jedno oskenování	Náklady na jedno vyplnění
Pizza leták	805,00 Kč	200x	4,02 Kč	21,76 Kč
FLKR_testy	1,40 Kč	103x	0,01 Kč	0,06 Kč

(vlastní)

V nákladové složce je vítěz jednoznačný. Takzvaný „lowcost“ je mnohonásobně výhodnější. Na jedno oskenování je varianta FLKR_memes 402krát výhodnější než profesionální tisk. V počtu záchytů je však značně popředu dražší varianta pizza leták, a to téměř

s dvojnásobným počtem oskenování. Je tedy zjevné, že s rostoucí profesionalitou roste i ochota k oskenování, a tudíž se zvyšuje počet záchytů. Z pohledu útočníka je tedy jen otázkou, kolik může získat. Quishing ve fyzické podobě je celkově nákladný a provedený by byl jen v případech, kdy je přínos pro útočníka rentabilní.

8.2 Čas

I zde platí známá poučka – „čas je relativní“. Aby šlo posoudit nějakou časovou náročnost na záchyt je důležité očistit časový rozpočet na měřitelnou část. Vymyslet útok a varianty byl zdoluhavější proces, ale ta jednotka času je u obou variant stejná. Čas budeme tedy počítat od konce nápadu, kdy na pomyslný stůl vypadly dvě varianty útoku a až od tohoto momentu se dělí mezi dvě různé varianty. Z pohledu útočníka by se jednalo o časovou náročnost od momentu, kdy se rozhodl provést útok vybranou formou a nezapočítává se výběr formy.

Do celkového času přípravy letáku je započítaná tvorba, posléze úpravy požadované z tiskárny a komunikace s tiskárnou, kde proběhlo několik emailů. Započítává se jen časová náročnost kolem tvorby. Řešení problému s QR kódem, který nastal po tisku se nezapočítává, jelikož nejde o běžnou situaci a ve většině případů by nenastala, či by se jí předcházelo při dalších útocích. Tudíž z obecného hlediska by šlo o zkreslení.

Při přípravě letáku soubor Word vykazoval 2 minuty úprav. Střih byl za minutu, kdy se daly stříhnout všechny čtyři listy najednou. Opět se nedbalo na nějakou estetiku střihu, účelem byla minimalizace času.

Tabulka 5 Tabulka časové náročnosti

Název	Celkový čas	Celkový počet oskenování	Čas na jedno oskenování	Čas na jedno vyplnění
Pizza leták	1800 sekund	200x	9 sekund	48,6 sekund
FLKR_testy	180 sekund	103x	1,7 sekundy	7,8 sekundy

(vlastní)

I když se časová náročnost může jevit jako nepodstatná, je důležitá právě v momentě, kdy by se plánoval větší útok. Na ose z Obrázek 9, kde je na jedné straně obyčejný masivní phishing a na straně druhé spear phishing bude čas hrát roli právě při plánování zásahu. Pokud se bavíme o přípravě jedné kampaně na jedné fakultě, čas na zisk jedné oběti je více

jak pětikrát větší u letákové kampaně. Pokud by se útočník zaměřoval na maximalizaci počtu obětí, zřejmě bude volit rychlejší variantu.

8.3 Bilance

Náklady i čas se tedy různí a různé jsou i zisky. Pokud se budeme bavit o kampaních blíže klasickému phishingu, kde je hlavním účelem maximalizace obětí s minimem času a nákladů, tak pořad bude výborně fungovat jakákoliv obyčejná kampaň plná varovných prvků. Čím blíže se na ose z Obrázek 9 budeme posouvat doprava, tedy více cílit a profesionalizovat kampaň na danou organizaci, skupiny až vybrané jednotlivce, tím nám porostou náklady a čas. Posun na dané ose by mohl být zapříčiněn právě požadovaným ziskem. Pokud bude útočník chtít získat například jen emaily, nebo nějaká osobní data, stačí jednoduchá kampaň, kde například email bude podmínkou pro vstup do skupiny na sdílení testů, pod záminkou eliminace vyučujících. V případě malware také postačí jednoduchá kampaň. Jde jen o naskenování kódu, otevření odkazu a pokud člověk nemá antivirový program, malware se může vcelku jednoduše stáhnout do zařízení. Zde může osobám pomoci osvěta v důležitosti používání antivirových programů a aktualizací systémů, ať už v mobilním telefonu, nebo počítači. Časově a finančně náročnější kampaň se poté jeví jako výhodná mimo jiné pro sběr citlivých údajů, bankovních přístupů, průmyslové špionáže či zcizení nějakého duševního vlastnictví. Například pro objednání pizzy z letáku by jistě bylo možné využít jednoduché stránky s požadavkem na platbu předem, přičemž by výsledkem byl hladový student jako v našem pokusu, nicméně o sumu za jednu pizzu chudší. Případně se u sofistikovanějších podvodů jeví jako varianta požadavek na stažení vlastní aplikace, kde bude poukaz na dvě pizzy zdarma, přičemž takový student může ztratit i kontrolu nad zařízením.

9 DOTAZNÍK

I když bylo dotazníkové řešení původně zamýšleno jen jako počítadlo přístupů s přidanou hodnotou v podobě o něco sofistikovanějších a podrobnějších údajů o přístupech, nakonec byl vytvořen alespoň jednoduchý a krátký dotazník jako doprovodný projekt této práce. Nakonec se ukázalo několik zajímavých poznatků, a to nejen v rámci odpovědí na otázky. Než přejdeme k samotným otázkám, jedna zajímavost je vyšší úspěšnost vyplnění u kampaně FLKR_testy. Jelikož byly vyvěšeny na toaletách, a jedna kopie na nástěnce na chodbě, nepočítalo se zde s vysokou úspěšností vyplnění. Předpokladem bylo, že po cestě z toalety, či u nástěnky nikdo nebude ochotný dotazník vyplnit, defacto ani k tomu nebude ideální prostor. Je to zajímavá ilustrace toho, jak i levná kampaň může vést k vyššímu procentu osob ochotných k interakci i při menším počtu oskenování, a to v nepohodlném, nebo nevhodném prostředí. Když tento předpoklad aplikujeme na akci pizza leták, tak se předpokládala vyšší ochota k vyplnění, jelikož bylo vyrobeno 500ks letáků a lidé si je tak brali s sebou, což mělo vést právě k tomu, aby ke skenování došlo na místě, které bude k interakci příhodnější.

Celkový počet vyplnění z obou akcí nakonec předčil očekávání natolik, že musela být aktivována placená verze pro zvýšení prostoru k záznamu odpovědí. V tomto ohledu se jeví původní plán na dotazníkové řešení jako okrajové špatný. Původní námět vycházel z předpokladu nízké vypovídající hodnoty dotazníků v diplomových pracích, kdy si studenti posílají dotazníky mezi sebou a vyplňují je jako zájmová osoba. Nicméně po proběhnutém testu se ukazuje, že tento nešvar je díky útoku odstraněn a relevantnost dotazníku může být vysoká. Útokem je zaručeno vyplnění dotazníku přesně zarámovanou zájmovou skupinou osob. Proto také dotazník nakonec dostává prostor k vyhodnocení a jako podklad pro analýzu rizik.

Dotazník měl však jeden původní účel vedle počítání přístupů nastavený už od momentu plánování. Ukázku toho, jak by mohla případná metoda fungovat a seznamovat například studenty ve vzdělávacích institucích. Pod danou otázkou byla vždy informace ohledně bezpečnosti.

9.1 Struktura dotazníku

Místo nápovědy k otázce bylo použito právě už nějaké poučení a informace. Znění otázek bylo v obou případech stejné, lišila se jen úvodní a závěrečná obrazovka. Nebude tedy

uvedeno dvojí znění dotazníku, jen se rozliší výše zmíněné rozdíly. Náповěda k otázce byla využita pro informaci, jak s daným tématem nakládat v rámci ukázky

Úvodní obrazovka – pizza leták

Bohužel Vás zklamal, ale pizza zdarma nebude. Stali jste se obětí **NEŠKODNÉHO** útoku, který vede pouze na dotazník a nijak Vás neohroží. Jedná se pouze o sběr dat o počtu oskenování neznámého QR kódu. Pokud obětujete chvíli svého času k vyplnění čtyř otázek, dozvíte se něco málo o bezpečnosti v síti a pomůžete v bádání nad obranou proti hackerským útokům.

Úvodní obrazovka – FLKR_testy

Bohužel Vás zklamal, ale tady testy nenajdete :) Stali jste se obětí **NEŠKODNÉHO** útoku, který vede pouze na dotazník a nijak Vás neohroží. Jedná se pouze o sběr dat o počtu oskenování neznámého QR kódu. Pokud obětujete chvíli svého času k vyplnění čtyř otázek, dozvíte se něco málo o bezpečnosti v síti a pomůžete v bádání nad obranou proti hackerským útokům.

První otázka

Čtete si při skenování QR kódu adresu odkazu?

Náповěda k otázce: Je důležité kontrolovat kam vede odkaz, či jestli se shoduje číslo účtu při platbě QR kódem. Častým podvodem bývá záměna QR kódu například na prosbě o pomoc lidem postiženým živelní pohromou.

Možné odpovědi – Ano, Ne

Druhá otázka

Prošel jste nějakým školením, nebo výukou v oblasti kybernetické bezpečnosti?

Náповěda k otázce: Školení bývá často doprovázeno sledováním hodin a vyhlížením konce. Je důležité připomenout si, že se jedná o bezpečí Vašich dat, anebo finančních prostředků!

Možné odpovědi – Ano, Ne

Třetí otázka

Sledujete aktivně trendy v oblasti kybernetické bezpečnosti?

Nápověda k otázce: Útoky podléhají rychlému vývoji, zůstaňte v obraze a sledujte nové trendy!

Možné odpovědi – Ano, Ne

Čtvrtá otázka

Používáte nějaký antivirový software?

Nápověda k otázce: Jakákoliv forma zabezpečení je lepší než žádná. Dle pravidla "mít o něco lepší zámek, než má soused".

Možné odpovědi – Ano, Ne, Nevím

Závěrečná obrazovka – pizza leták

Věřím, že zamezení útoku v budoucnu bude odpustkem za absenci slevy na dnešní pizzu :)

Závěrečná obrazovka – FLKR_testy

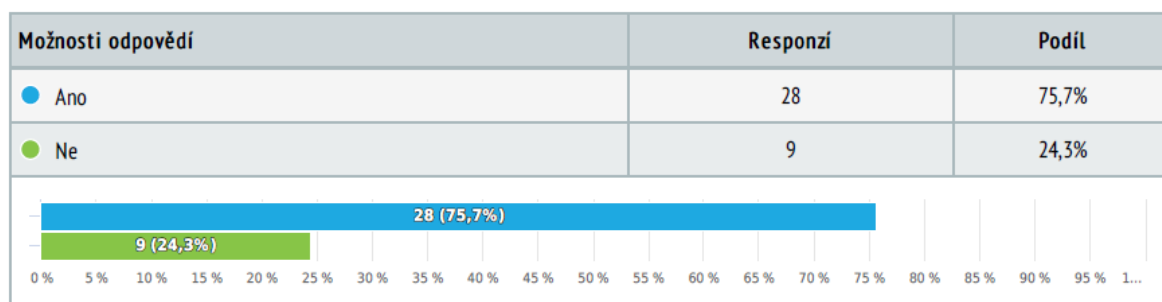
Věřím, že zamezení útoku v budoucnu bude odpustkem za absenci testů :)

9.2 Výsledky pizza leták

Otázka první:

Čtete si při skenování QR kódu adresu odkazu?

Výběr z možností, zodpovězeno 37x, nezodpovězeno 0x



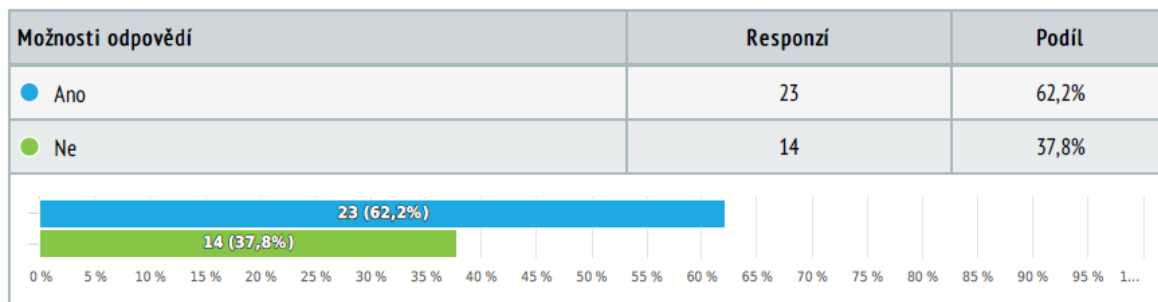
Obrázek 23 Otázka první – akce pizza leták

(vlastní – statistika dotazníku ze serveru Survio)

Otázka druhá:

Prošel jste nějakým školením, nebo výukou v oblasti kybernetické bezpečnosti?

Výběr z možností, zodpovězeno 37x, nezodpovězeno 0x

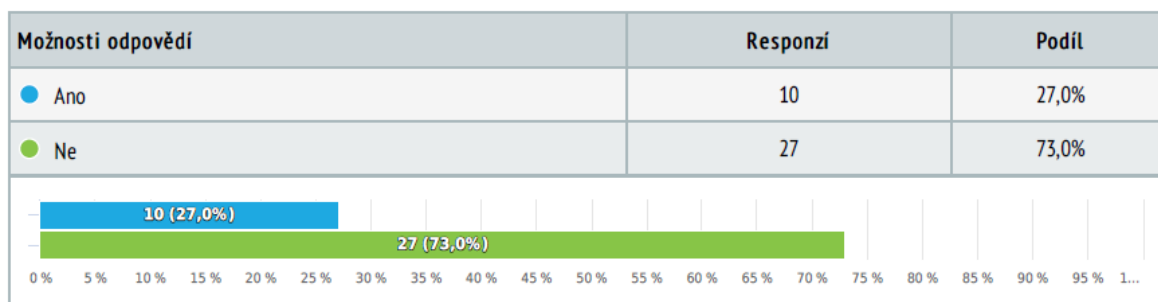


Obrázek 24 Otázka druhá – akce pizza leták
(vlastní – statistika dotazníku ze serveru Survio)

Otázka třetí:

Sledujete aktivně trendy v oblasti kybernetické bezpečnosti?

Výběr z možností, zodpovězeno 37x, nezodpovězeno 0x

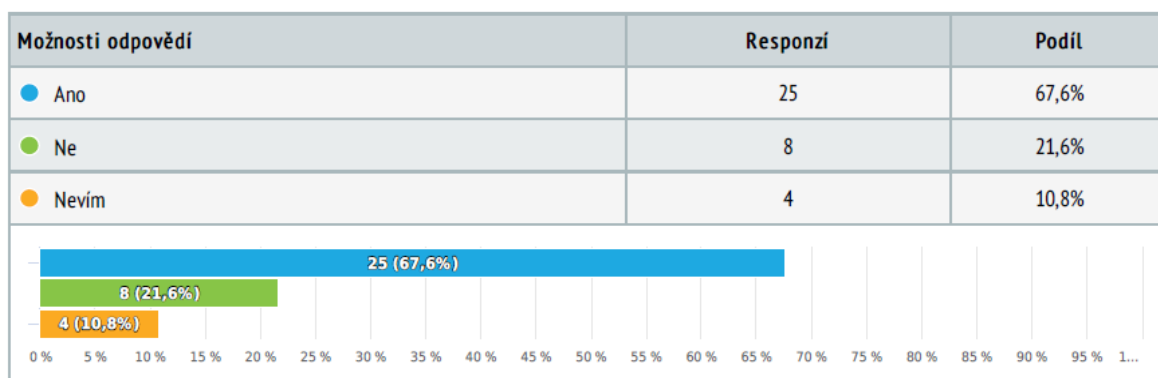


Obrázek 25 Otázka třetí – akce pizza leták
(vlastní – statistika dotazníku ze serveru Survio)

Otázka čtvrtá:

Používáte nějaký antivirový software?

Výběr z možností, více možných, zodpovězeno 37x, nezodpovězeno 0x



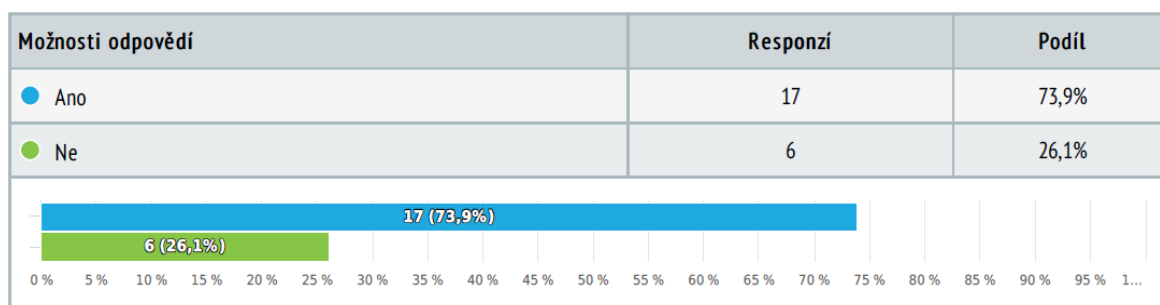
Obrázek 26 Otázka čtvrtá – akce pizza leták
(vlastní – statistika dotazníku ze serveru Survio)

9.3 Výsledky FLKR_testy

Otázka první:

Čtete si při skenování QR kódu adresu odkazu?

Výběr z možností, zodpovězeno 23x, nezodpovězeno 0x



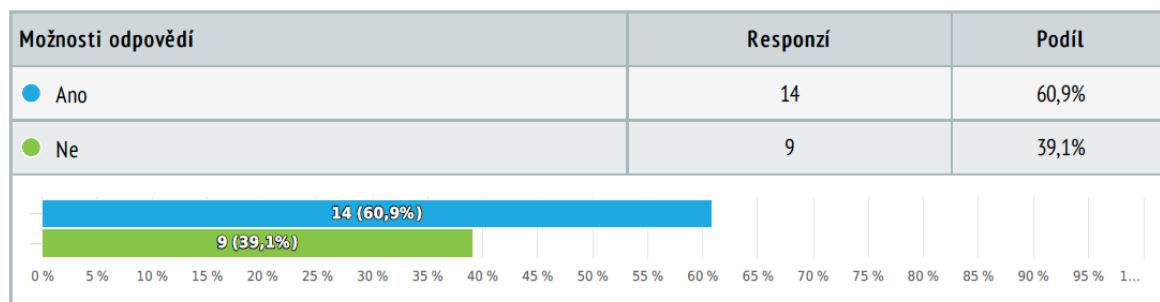
Obrázek 27 Otázka první – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

Otázka druhá:

Prošel jste nějakým školením, nebo výukou v oblasti kybernetické bezpečnosti?

Výběr z možností, zodpovězeno 23x, nezodpovězeno 0x



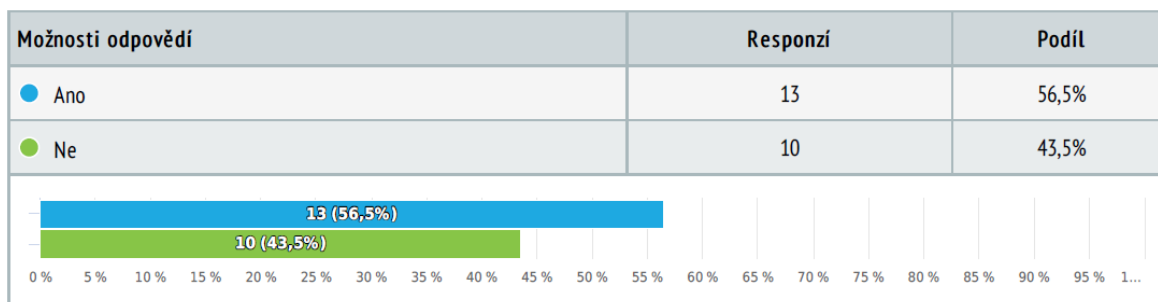
Obrázek 28 Otázka druhá – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

Otázka třetí:

Sledujete aktivně trendy v oblasti kybernetické bezpečnosti?

Výběr z možností, zodpovězeno 23x, nezodpovězeno 0x



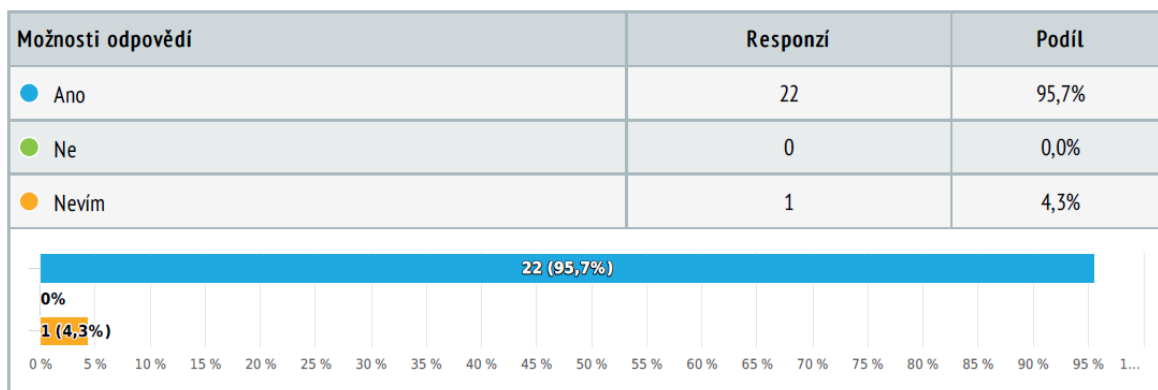
Obrázek 29 Otázka třetí – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

Otázka čtvrtá:

Používáte nějaký antivirový software?

Výběr z možností, více možných, zodpovězeno 23x, nezodpovězeno 0x



Obrázek 30 Otázka čtvrtá – akce FLKR_testy

(vlastní – statistika dotazníku ze serveru Survio)

9.4 Porovnání**Otázka první:**

U první otázky se v obou případech jedná o podobný poměr.

Otázka druhá:

I druhá otázka vykazuje velmi podobný poměr odpovědí.

Otázka třetí:

Až u třetí otázky se nám poměr mění a odpovědi se zásadně liší, kdy nejenom je různý poměr, ale u kampaně pizza leták větší část odpovídá „ne“ k otázce sledování trendů

v oblasti kybernetické bezpečnosti, zatímco u kampaně FLKR_testy větší část trendy sleduje.

Otázka čtvrtá:

U poslední otázky se dozvídáme to nejzajímavější. V akci FLKR_testy nikdo neodpověděl, že antivirový software nepoužívá. Jako „nevím“ byla odpověď označena pouze jednou a přes 95 % odpovědí bylo kladných k používání antivirového softwaru. Zatímco u akce pizza leták kladně odpověděly jen dvě třetiny dotazovaných. Zajímavostí je, že tady již přes 20 % odpovídá negativně a přes 10 % ani neví, zda antivirový software používá.

U posledních dvou otázek se nám tedy protíná zajímavý poznatek. A to, že skupina, která více sleduje trendy v oblasti kybernetické bezpečnosti má tendenci k vyšší zodpovědnosti a v zařízení používá antivirový software.

9.5 Vyhodnocení a opatření

Otázka první:

Jedna čtvrtina dotazovaných v obou případech odpovídá, že si adresu odkazu při skenování nechte. U tří čtvrtin dotazovaných, kteří odpověděli kladně je poté otázkou, jak důkladně si odkaz přečtou. Pokud by se jednalo například o napodobení FLKR_memes a QR kód by odkazoval na Instagram, všimne si každý například toho, že by adresa jen vypadala jako pravá, ale ve skutečnosti by mohla mít třeba vynechané písmenko a místo odkazu ve znění Instagram/flkr_memes by mohla adresa vypadat následovně – Instgram/flkr_memes (tedy chybějící písmeno „a“ ve slově Instagram) a vést na web se škodlivým obsahem.

Jako opatření by se jevílo udávání adresy nad QR kód, což dnes lze často vidět. Pokud instituci důvěřujeme, adresa je napsaná například nad QR kódem, lze si ji přečíst předem a následná záměna by mohla být zřetelnější a lépe rozpoznatelná než jen na obrazovce mobilního telefonu, kde často nemusí být vidět adresa celá. Také přidání emailu může být nápomocno a místo skenování kódu může uživatel využít emailové adresy ke kontaktování.

Otázka druhá:

Tato otázka byla položena záměrně jako kontrolní a byl očekávaný vysoký počet kladných odpovědí, jelikož výuka na fakultě logistiky a krizového řízení zahrnuje i kybernetickou a informační bezpečnost, a to pro všechny studijní odbornosti. Výuka však probíhá až ve čtvrtém semestru, což by při obvyčejném průměrování znamenalo, že první a druhý akademický rok danou výuku neměl, zatímco třetí, čtvrtý a pátý akademický rok již výukou

prošel. Obě kampaně mají téměř 40 % negativních odpovědí, což odpovídá výše zmíněnému a potvrzuje pravdivost informací v obou kampaních. Jeden ze záměrů otázky byl právě ten, jestli studenti vnímali přednášky jako průpravu i pro vlastní bezpečnost.

Opatření směřující k neproškoleným osobám se nabízí právě ve školení. Na tomto místě se otevírají dveře jak klasickým formám, tak například více interaktivním jako jsou použity například v této práci.

Otázka třetí:

Tato otázka se nám v poměru odpovědí rozchází. Důvodů může být několik a zjistit ten pravý bez dalších informací nebude možné. Pro další práci můžeme zmínit nějaké teoretické domněnky, které můžou být návodné pro doplňující otázky v případě replikování pokusu v podobné formě:

- Studenti, kteří se aktivně zajímají o jakékoliv IT téma budou spíše nakloněni k využití sítí, ať už třeba právě sociálních, nebo například nějakých cloudových, k využití při studiu a sdílení informací
- Studenti, kteří sledují podcasty na téma kybernetického zločinu, případně se o kybernetickou bezpečnost a zločin v kybernetickém prostoru zajímají tak vědí, že na sítích se informace tohoto typu dají nalézt a jsou tedy více motivováni tento druh informace vyhledávat a vyzkoušet
- Běžně používaný model propagace, jako je právě leták, i přes varovné prvky ochotněji naskenuje právě člověk s menším povědomím o kybernetickém zločinu

U neodborné veřejnosti je opatření ke sledování trendů velmi náročnou disciplínou. Existují různé popularizační kanály, ale jak bylo poukázáno například v kapitole 5.3 Jak se dostat do hlavy oběti, není aktuálně o téma významný zájem. Jako varianta se jeví interaktivní metody, které uživatelé dostanou zábavnou nebo zajímavou formou, případně důraz na pravidelná školení.

Otázka čtvrtá:

Prvotní vyhodnocení bylo provedeno již v předchozí kapitole při porovnání a vykazuje provázanost s otázkou třetí. Samotné odpovědi poté ukazují, že drtivá většina nějakou formu zabezpečení používá. Z celkových šedesáti odpovědí bylo jako „ano“ označeno čtyřicet sedm. Což dělá 78,3 %. Zde by bylo na místě opět zjistit jakou ochranu využívají, případně v jaké reálné míře se konkrétní zabezpečovací aplikace používají. Pokud se na tyto údaje

podíváme blíže, můžeme dle průběžných průzkumů zjistit, kolik uživatelů používá aplikace k zabezpečení mobilních zařízení. Sesbíraná data budou umístěna do tabulky k vizualizaci celkového přehledu. Nejedná se o navazující průzkumy, nicméně poslouží jako vhodná ilustrace trendu v této oblasti napříč několika léty.

Tabulka 6 Počty uživatelů používající zabezpečovací aplikaci

Rok	Procento uživatelů	Zdroj průzkumu
2016	40 %	Seznam.cz a ESET
2017	38 %	Seznam.cz a ESET
2018	39 %	Seznam.cz a ESET
2022	52.7 %	Samsung
2025	47 %	ESET
2025	78,3 %	vlastní – statistika dotazníku ze serveru Survio

(CHIP, 2018; MOBILMANIA, 2022; ESET, 2025)

Jak lze tedy vidět, nárůst je zjevný, avšak průzkum u studentů na fakultě logistiky a krizového řízení vykazuje vyšší číslo, než byl předchozí trend. Důvodů proč tomu tak je může být hned několik. Mimo jiné například tyto:

- Zvyšující se povědomí o důležitosti zabezpečení mobilních zařízení.
- Zodpovědnost studentů na zmíněné fakultě vybočuje z průměru.
- Vysoká kvalita pedagogů na fakultě.
- Obory fakulty zaměřující se na bezpečnost společnosti.
- Špatně pochopená/položená otázka.

V jakékoliv variantě vysvětlení by si přesně taková informace zasloužila další výzkum. Lépe nastavit dotazník a zaměřit se na něj jako na primární zdroj informací.

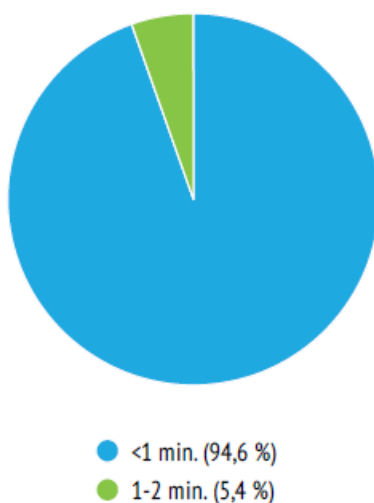
Základní variantou opatření je edukace. Zde není ani tak potřeba vzbudit zájem, ale vysvětlit důležitost použití. Po instalaci uživatel dál nemusí na nic myslet, je hotovo a opatření je aplikováno. Při dalším školení je vhodné zapojit kontrolu aktualizací.

9.6 Shrnutí dotazníku

I když byl původně dotazník vedlejším projektem, nakonec poskytnul spoustu zajímavých informací. Nabízí se tedy prostor pro variantu útoku zaměřenou právě na dotazník, kdy je jedním velkým benefitem vyplněný dotazník osobou, která v ten moment porušila bezpečnostní pravidla. Určitě by se jednalo o velmi zajímavý zdroj informací.

Do této práce nebyl rozsáhlejší dotazník aplikován záměrně, jelikož nebylo účelem studenty odradit od vyplnění a opravdu je připravit o přibližně minutu času. Defacto „chvilíčku“ tak, jak je napsáno na úvodní obrazovce po otevření odkazu z QR kódu. A opravdu se toto podařilo.

Čas vyplňování dotazníku



Obrázek 31 Čas vyplnění dotazníků

(vlastní – statistika dotazníku ze serveru Survio)

10 ANALÝZA RIZIK

Předlohu k analýze rizik vztahující se ke kybernetické bezpečnosti nalezneme v přílohách vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti a jedná se o metodu semikvantitativní. Pro posouzení rizik v lokální síti ukázkové organizace poslouží právě data z penetračního testu quishingovým útokem tak, aby byla minimalizována subjektivita, hodnocení rizik stálo na reálném podkladu a ošetření rizik bylo použitelné v praxi na reálné subjekty, nikoli jen na modelové situace. Bude vyhodnocen vliv sociálního inženýrství a jeho působení na vybrané hrozby uvedené v příloze vyhlášky č. 82/2018 Sb. Hrozby i zranitelnosti budou vybrány ve vztahu k povaze útoku.

V příloze 1, odstavci 2 je uvedeno následující:

„Je doporučeno, aby si každá povinná osoba tyto dopadové matice přizpůsobila svým potřebám.“ (Sbírka zákonů České republiky, 1993-2023)

Pro potřeby této práce bude použita forma základní tak, jak je uvedena v příloze vyhlášky. Jelikož autor práce není s reálným stavem bezpečnosti na fakultě seznámen, není možné objektivně rizika posoudit na daný subjekt, na který byl útok proveden. Hodnocení rizik bude tedy tvořeno průměrem hodnocení od osob aktivně pracujících v oboru IT a bezpečnosti, potažmo přímo na pozici vztahující se ke kybernetické bezpečnosti.

Důležitý krok je vytipování hrozeb a zranitelností. I když vyhláška o kybernetické bezpečnosti základní výběr uvádí v příloze 3, tak zároveň opět upozorňuje na následující:

„Tato příloha obsahuje jen vybrané kategorie zranitelností a hrozeb. Identifikace konkrétních zranitelností a hrozeb je odpovědností povinné osoby.“ (Sbírka zákonů České republiky, 1993-2023)

10.1 Modelová fakulta

Reálný stav samozřejmě znám není. I když se nabízí se varianta rozhovorů s pracovníky na fakultě, či univerzitě, do veřejně dostupného dokumentu jako je tato diplomová práce reálný stav rozhodně nepatří, a to zejména u zranitelností. Dokument by poté mohl působit návodně pro skutečné útočníky. Budeme tedy předpokládat, že zranitelnosti, hrozby a rizika uvedené ve vyhlášce jsou reálné a hodnocení provedeme na modelové organizaci, která bude mít známé parametry totožné s danou fakultou. Veřejně dostupné informace budou použity z fakulty logistiky a krizového řízení, zbytek bude subjektivně vybrán s ohledem na

náhodnost, aby bylo zamezeno jakékoliv podobnosti s reálným stavem a znemožněno zneužití.

Modelová organizace bude tedy vzdělávací instituce, konkrétně samostatná fakulta, na kterou bude proveden útok pomocí quishingu. Počet studentů 1499. Ošetření rizik proběhne pomocí praktické a interaktivní vzdělávací kampaně. Poté proběhne modelování snížení rizika podle teoretického odhadu kvalifikovaným týmem. Pokud by bylo možné provádět pokus opakovaně, například vždy na začátku akademického roku, byly by výsledky mnohem přesnější a dozajista by se jednalo o zajímavou vědeckou studii.

10.2 Zranitelnosti

Z celkového výčtu zranitelností uváděných v příloze 3 vyhlášky č. 82/2018 lze o všech uvažovat i pro fakultu logistiky a krizového řízení, stejně tak na vzdělávací instituce obecně. Výčet je následující, přičemž jeden bod byl odstraněn, jelikož je uveden v seznamu dvakrát:

- *„nedostatečná údržba informačního a komunikačního systému,*
- *zastaralost informačního a komunikačního systému,*
- *nedostatečná ochrana vnějšího perimetru,*
- *nedostatečné bezpečnostní povědomí uživatelů a administrátorů,*
- *nevhodné nastavení přístupových oprávnění,*
- *nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,*
- *nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,*
- *nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,*
- *nedostatečná ochrana aktiv,*
- *nevhodná bezpečnostní architektura,*
- *nedostatečná míra nezávislé kontroly,*
- *neschopnost včasného odhalení pochybení ze strany zaměstnanců.“ (Sbírka zákonů České republiky, 1993-2023)*

Pokud budeme brát v potaz rizika spojená se sociálním inženýrstvím, tedy započítí útoku skrze quishing, bude se jednat o níže uvedené zranitelnosti. Ke každé si vytipujeme nějaký ilustrační příklad zneužití zkoumanou formou. Vytipována byla první polovina zranitelností uvedených ve výše zmíněné příloze vyhlášky, které se sociálního inženýrství dotýkají nejvíce a jsou schopny ilustrovat rizika.

Tabulka 7 Vybrané zranitelnosti

Zranitelnost	Popis
Nedostatečná údržba informačního a komunikačního systému	Absence aktualizací a bezpečnostních záplat může přispět k využití malwaru staženého po oskenování QR kódu a útočník může dostat přístup do systému, či sítě.
Zastaralost informačního a komunikačního systému	Zvyšující se bezpečnost a její prvky bezesporu přispívají k vyššímu zabezpečení, jako například WPA3.
Nedostatečná ochrana vnějšího perimetru	Zde je riziko zneužití právě u fyzické formy. Jedná se tedy o zranitelnost, kterou lze využít i u určitých forem phishingu.
Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	Uživatelé, kteří nejsou řádně proškoleni bývají nejčastějším bezpečnostním rizikem v řetězci ochrany místní sítě v dané organizaci.
Nevhodné nastavení přístupových oprávnění	Pokud již dojde k prolomení účtu, samozřejmostí by měl být omezený přístup v duchu pravidla CIA. Útočník se tak nemůže dostat do všech systémů a ke všem datům.
Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	V případě nějaké formy sociálního inženýrství je důležité reagovat co nejdříve, incident nahlásit bezpečnostnímu správci a ten musí adekvátně reagovat. V rámci sociálního inženýrství je rychlá a adekvátní reakce velmi důležitá, jelikož se dá předejít například infikování systému nějakým škodlivým kódem. Bezpečnostní správce má nastavit postupy a možnosti hlášení takových incidentů.

10.3 Hrozby

V příloze 3 vyhlášky č 82/2018 Sb. najdeme také základní hrozby. Povinná osoba má identifikovat konkrétní hrozby pro vlastní organizaci. Výčet hrozeb je následující:

- *„porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,*
- *poškození nebo selhání technického anebo programového vybavení,*
- *zneužití identity,*
- *užívání programového vybavení v rozporu s licenčními podmínkami,*
- *škodlivý kód (například viry, spyware, trojské koně),*
- *narušení fyzické bezpečnosti,*
- *přerušování poskytování služeb elektronických komunikací nebo dodávek elektrické energie,*
- *zneužití nebo neoprávněná modifikace údajů,*
- *ztráta, odcizení nebo poškození aktiva,*
- *nedodržení smluvního závazku ze strany dodavatele,*
- *pochybení ze strany zaměstnanců,*
- *zneužití vnitřních prostředků, sabotáž,*
- *dlouhodobé přerušování poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,*
- *nedostatek zaměstnanců s potřebnou odbornou úrovní,*
- *cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,*
- *zneužití vyměnitelných technických nosičů dat,*
- *napadení elektronické komunikace (odposlech, modifikace).“ (Sbírka zákonů České republiky, 1993-2023)*

Na první pohled se zde nabízí jako jediná vhodná hrozba *„cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik“*. Nicméně z daného seznamu lze při řešení konkrétního útoku vyjmout více hrozeb, jelikož sociální inženýrství cílí sice na lidi

jako prvek zabezpečení, ale také jej kombinuje například právě s pochybením zaměstnance. Hrozby si však poté rozdělíme v rámci aktiv na více konkrétní příklady vztažené právě k daným aktivům.

Tabulka 8 Výběr hrozeb pro modelovou situaci

Hrozba	Popis	Varianta/příklad
Užívání programového vybavení v rozporu s licenčními podmínkami	S neoriginálním softwarem se do počítače, a tudíž i do sítě, může dostat malware.	Namísto kampaně FLKR_testy lze udělat kampaň na jakoukoliv aplikaci nabízenou zdarma, která bude obsahovat škodlivý kód.
Škodlivý kód (například viry, spyware, trojské koně)	Právě pomocí sociálního inženýrství lze často škodlivý kód stáhnout.	Po naskenování může dojít k automatickému stažení, nebo výzvě ke stažení ze stránky, například v podobě nějakého „PDF sborníku testů“.
Pochybení ze strany zaměstnanců	„Amatéři hackují systémy, profesionálové ‚hackují‘ lidi.“ Bruce Schneider	Sociální inženýrství využívá právě pochybení zaměstnanců, či uživatelů.
Cílený kybernetický útok pomocí sociálního inženýrství	Tato hrozba přímo vystihuje provedený útok.	Provedené varianty.

(Sbírka zákonů České republiky, 1993-2023)

10.4 Hodnocení aktiv

Hodnocení aktiv je rozděleno do čtyř úrovní, které určují úroveň dopadu. Dále se dělí podle pravidla CIA a každá kategorie má svoji vlastní tabulku. Ty budou použité ve variantě uvedené ve vyhlášce. (Sbírka zákonů České republiky, 1993-2023) Hodnocení aktiv poté určuje dopad při hodnocení rizik, která vychází z metodiky DPIA, či doporučené metodiky úřadu pro ochranu osobních údajů. Bude použita jedna úprava, která vychází právě z posouzení aktiv za pomoci triády CIA, kdy se v metodikách pouze určuje vliv na jednotlivé

aspekty označením „X“, avšak zde do tabulky přímo vepíšeme danou hodnotu, která poté určuje dopad. Důvodem je lepší přehlednost a také přímá viditelnost rozdílů mezi dvěma doporučenými metodikami hodnocení dopadů pomocí aktiv.

Určení dopadu má také metodické varianty a to dvě. Rozdíl mezi nimi můžeme ilustrovat tak, že hodnocení rizik se stejným vstupem provedeme dvakrát podle obou metodických postupů.

První metodickou variantou vycházející ze softwarového řešení Cyber Security Audit 2.0 a z webu kybez je hodnocení průměrem. Tedy tak, že se jako dopad určí průměr z hodnot aktiv, které jsou ohodnoceny triádou CIA. (KYBEZ, 2023a)

Editace aktiva: Notebooky obchodní oddělení

Obecné | **Hodnocení aktiva** | Hodnocení důležitosti | Identifikace hrozeb/zranitelností | Způsoby používání a manipulace | Vlastní atributy

C - Důvěrnost
 Střední
 Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.

I - Integrita
 Vysoká
 Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.

A - Dostupnost
 Nízká
 Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).

Stanovte pravidla ochrany

B I :: !=

Výsledné hodnocení
2
DOBŘÝ

< Předchozí krok | Zrušit | **Uložit** | Následující krok >

Obrázek 32 Hodnocení aktiv dle CIA průměrem

(KYBEZ, 2023a)

Druhá varianta pracuje s nejvyšší hodnotou v hodnocení aktiv. Tedy v každém aspektu se udělá průměr od všech hodnotitelů a do dopadu se použije ta hodnota, která je nejvyšší, tedy nejrizikovější. (KYBEZ, 2023a)

Obrázek 33 Hodnocení aktiv dle CIA nejvyšší hodnotou

(KYBEZ, 2023a)

Jak lze vidět na obrázcích (Obrázek 32 a Obrázek 33) výsledné hodnocení dopadu na aktivum je vypočítáno z hodnot určených za pomoci triády CIA. Aktivum se podle této metody hodnotí dle tabulek z přílohy 1 vyhlášky 82/2018 Sb. o kybernetické bezpečnosti.

Způsob hodnocení vychází z tabulek uvedených ve vyhlášce 82/2018 Sb. o kybernetické bezpečnosti, které se řídí triádou CIA. Byly použity výchozí tabulky z přílohy zmíněné vyhlášky, které nalezneme také v příloze 1.

10.5 Hodnocení rizik

Jako poslední musíme určit hodnoty daných rizik. Funkce pro výpočet rizika je opět na povinné osobě, nicméně běžně používaná funkce je uvedena i ve vyhlášce 82/2018 Sb. v příloze č. 2. Pro analýzu odpovídající hodnotící tabulce v této práci vzorec tedy vypadá následovně:

$$R = P \times D \times Z$$

Kde ve vzorci R je rizikem, které se rovná součinu P, tedy pravděpodobnosti hrozby, D jako dopadu, který je výsledkem hodnocení aktiv triádou CIA a Z jako vybrané zranitelnosti.

Následující tabulka slouží k určení úrovně pravděpodobnosti realizace hrozby na základě její odhadované četnosti. Tabulka rozlišuje čtyři úrovně: nízkou, střední, vysokou a kritickou. Každá úroveň je definována kombinací míry pravděpodobnosti a časového intervalu, ve kterém se může hrozba reálně vyskytnout – od výjimečných situací (méně než jednou za 5 let) až po velmi časté výskyty (více než jednou za měsíc). Toto hodnocení umožňuje lépe identifikovat závažnost jednotlivých hrozeb a efektivněji plánovat opatření k jejich zvládnutí. Hodnocení vychází z metodiky uvedené ve vyhlášce č. 82/2018 Sb.

Tabulka 9 Hodnocení hrozby

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

(Sbírka zákonů České republiky, 1993-2023)

Další tabulka slouží k určení míry zranitelnosti informačního systému na základě pravděpodobnosti jejího zneužití a účinnosti bezpečnostních opatření. Tabulka rozlišuje čtyři úrovně: nízkou, střední, vysokou a kritickou. Nízká úroveň značí dobře zabezpečené prostředí s minimální pravděpodobností zneužití. Střední úroveň odráží částečně omezenou účinnost opatření a potenciální, avšak dosud neprokázané pokusy o zneužití. Vysoká úroveň značí reálné riziko zneužití a známé případy prolomení bezpečnosti. Kritická úroveň pak představuje situaci s velmi vysokou pravděpodobností útoku a nefunkčními nebo chybějícími opatřeními.

Tabulka 10 Hodnocení zranitelnosti

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

(Sbírka zákonů České republiky, 1993-2023)

Poslední tabulka popisuje úrovně přijatelnosti rizik v závislosti na jejich závažnosti. Rozlišuje čtyři úrovně: nízké, střední, vysoké a kritické. Nízké riziko je považováno za akceptovatelné bez nutnosti dalších opatření. Střední riziko může být přijatelné nebo vyžaduje méně náročná opatření. Vysoké riziko je již nepřijatelné a vyžaduje systematické kroky k jeho snížení. Kritické riziko je považováno za nepřijatelné a musí být řešeno okamžitě. Tabulka slouží jako podklad pro rozhodování o dalším postupu při řízení kybernetických rizik.

Tabulka 11 Hodnocení rizika

Úroveň	Popis
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

(Sbírka zákonů České republiky, 1993-2023)

Zde je ještě vhodné přidat matici hodnoty rizik a barevně dané úrovně rozlišit. Barevné rozlišení přiřazuje číselné hodnoty jednotlivým úrovním rizika a umožňuje jejich rychlé vizuální rozlišení. Rozlišuje čtyři skupiny: bezvýznamné, akceptovatelné, nežádoucí a nepřijatelné riziko. Toto rozdělení usnadňuje rozhodování o prioritách při řízení rizik.

Tabulka 12 Hodnocení rizik – barevné rozlišení

Skupina	Hodnota
Nepřijatelné riziko	48-64
Nežádoucí riziko	32-47
Akceptovatelné riziko	16-31
Bezvýznamné riziko	0-15

(vlastní)

11 HODNOCENÍ RIZIK MODELOVÉ FAKULTY

V momentě, kdy máme výchozí tabulky tak, jak nám vyhláška 82/2018 Sb. určuje, a to i v upravené formě, což také umožňuje, můžeme si vytipovat obecná aktiva a provést hodnocení rizik.

Tabulka 13 Aktiva modelové organizace

Aktivum	Typ	Podrobnosti
Finanční	Bankovní účet	Získání přístupu k bankovním účtům
		Přesměrování plateb a poplatků na vlastní účet
Informační systémy	Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle)
		Systémy pro provoz a fungování fakulty
	Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití
Nehmotné	Reputace	Poškození důvěry k fakultě a její bezpečnosti
	Duševní vlastnictví	Krádež vědeckých projektů, nebo know-how fakulty, jejích zpracovaných postupů.
Fyzické	Počítače a servery	Poškození či zašifrování dat
	Přístupové údaje	Krádež údajů použitelných k fyzickému přístupu do budovy (kódy k zámekům, údaje pro tvorbu přístupové karty)

(vlastní)

Bodování rizik provedeme pomocí bodovací tabulky, kde uvedeme rovnou i ohrožené aspekty aktiv. To nám zpřehlední, na jaké aspekty v rámci triády CIA má daná hrozba vliv a jaká je hodnota. Pokud se bude dotýkat hrozba více aspektů, bude využito v jednom případě průměru hodnot, v druhém případě nejvyšší hodnoty pro porovnání obou možností metodiky.

Veškeré tabulkové hodnoty ve vyhlášce č. 82/2018 Sb. jsou uváděny slovně. Do hodnotící tabulky však zapisujeme hodnoty číselné. K tomu je potřeba ještě převést slovní hodnocení

do číselné podoby. To buď tak, že v si každou tabulku upravíme, nebo pro převod použijeme jednoduchou převodní tabulku (Tabulka 14 Převodní tabulka). V této fázi jsme připraveni na distribuci hodnotících podkladů a listů hodnotícímu týmu.

Tabulka 14 Převodní tabulka

Číselná hodnota	Slovní hodnota
1	Nízký
2	Střední
3	Vysoký
4	Kritický

(vlastní)

Hrozby v tabulce vypíšeme jako popis konkrétní akce útočníka vycházející z: Tabulka 8 Výběr hrozeb pro modelovou situaci. U zranitelnosti vycházíme z toho, že uživatel udělá chybu a další prvek v řadě nám nezabrání v dokončení útoku. Ošetření těchto zranitelností nám poté může v budoucnu částečně eliminovat chyby uživatelů. Jedná se o výběr několika zranitelností a záměrně nemají přímo reflektovat skutečný stav.

Samotná tabulka s hodnocením obsahuje ilustrativní příklady a je hodnocena týmem tří osob, které všechny pracují v IT odvětví a buď nyní, nebo v minulosti zastávaly funkci místního bezpečnostního správce v oblasti kybernetické bezpečnosti. Tabulka a celkové hodnocení je tedy stavěno pro vyplnění kvalifikovanou osobou, která se v problematice orientuje a do tabulky bude vepsán průměr týmu hodnotitelů. Samotný vzor k hodnocení je poté uveden v příloze 1 a konkrétní hodnocení jednotlivých členů týmu v příloze 2.

Tabulka 15 Hodnocení rizik – průměrem

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	3	4	3	36
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	3	3	2	18
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	2	3	3	3	27
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	3	3	3	27
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	3	2	3	18
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	3	3	3	27

(vlastní a kolektiv)

Tabulka 16 Hodnocení rizik – nejvyšší hodnotou

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	3	4	3	36
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	3	4	2	24
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	2	3	3	3	27
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	3	4	3	36
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	3	3	3	27
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	3	4	3	36

(vlastní a kolektiv)

Pokud porovnáme oba způsoby hodnocení rizik, díky barevnému rozlišení lze na první pohled vidět jasný rozdíl mezi oběma metodami. Při hodnocení průměrem se do nežádoucího rizika dostává pouze jedenkrát, zatímco nejvyšší hodnota nám vykazuje nežádoucí riziko v polovině případů. Je tedy na každém bezpečnostním správci, jakou variantu zvolí.

Pokud se na tabulky podíváme důkladněji, jako jediné společné žluté riziko zůstal přístup k bankovním účtům. Je to ukázka toho, jak vypracování obou metod může odhalit rizika, která celý tým hodnotitelů považuje shodně za nejvyšší. Což se u bankovních účtů potvrdilo. Zájem o jejich napadení bývá vysoký a často jsou útoky doprovázeny právě sofistikovanějšími metodami. Zřejmě je to zapříčiněno vysokou finanční výtěžností útoku, oproti třeba sběru emailových adres.

Dále zůstávají ve žlutém riziku už jen napadení systémů a poškození či šifrování dat. Opět se jedná o varianty útoků, kde je velmi vysoká finanční výtěžnost díky požadavku na platbu za dešifrování dat, nebo znovu zpřístupnění systémů.

Zelená rizika v tabulce s nejvyšší hodnotou zůstávají tedy u přesměrování plateb, což může a nemusí být zajímavé, pokud jde například o různé stipendia a školní poplatky vzhledem k dlouhodobosti, kdy nestačí jeden úder, ale platby se sbírají. A dále už jen přístup do účtů a osobní údaje. Ty nemají tak vysokou hodnotu.

Díky rozdílům a vyhodnocení oběma způsoby lze pozorovat soulad týmu i přes to, že hodnocení prováděl každý zcela samostatně.

V této fázi byla hodnotitelům předložena druhá tabulka přílohy 1 a byli seznámeni s plánem edukace.

12 NÁVRH OPATŘENÍ

Na tomto místě jde rozdělit navrhovaná opatření na dvě úrovně. Jednou je nějaký běžně užívaný model bezpečnostních opatření, který nám rizika sníží jen díky implementaci. Avšak je zde i ta druhá rovina – vzdělávání. Určitě probíhá jak v pracovním životě v podobě školení, tak i ve vzdělávacích institucích, jako výuka. Jenže v prostředí, kdy prokazatelně kybernetická kriminalita roste a větší část kybernetických útoků začíná, nebo využívá nějakou formu sociálního inženýrství je potřeba povědomí uživatelů o těchto hrozbách neustále zvyšovat. Akademická půda se ukazuje jako jedno z vhodných míst k realizaci. A i v této práci se ukázalo, že lze zkombinovat jak výzkum, tak penetrační test a také do toho všeho přimíchat vzdělávací program.

12.1 Opatření doporučená

Opatření přímo proti hrozbě sociálního inženýrství vychází velmi často právě ze školení. Pokud se podíváme přímo na KYBEZ a jejich doporučení, skládá se z těchto bodů:

- „Edukace zaměstnanců: Zajistěte, aby vaši zaměstnanci byli seznámeni s riziky sociálního inženýrství a věděli, jak se bránit.
- Silná hesla a autentizační metody: Používejte silná hesla a dvoufaktorovou autentizaci pro ochranu přístupu k důležitým systémům.
- Omezení sdílení citlivých informací: Dbejte na to, aby citlivé informace byly sdíleny pouze s oprávněnými osobami a že existují přiměřená opatření pro jejich uchovávání.
- Politika kontroly přístupu: Zavedení jasných pravidel a omezení týkajících se přístupu k citlivým datům a systémům.“ (KYBEZ, 2023b)

Ze čtyř doporučených bodů se jeden dotýká přímo školení, tedy vztahu na člověka. Další tři jsou v gesci administrátorů a místních bezpečnostních správců, ale jedná se právě o omezení chyb uživatelů, tedy o to, že i v případě selhání člověka zafunguje další ochranný aspekt.

Školením zajistíme prevenci a povědomí uživatelů o možném riziku. Tím děláme odolnou tu první linii. Tu, která je nejčastěji využívána k napadení sítě. Vedle plánu pro ochranu před případnými útoky musí organizace pravidelně školit své zaměstnance, ale také další uživatele vstupujících do sítě. Jako například v případě fakulty studenty. Aktuální informace

musí dostávat v pravidelných intervalech tak, aby byla organizace schopna odolávat neustále se měnícím formám útoků. (KYBEZ, 2023b)

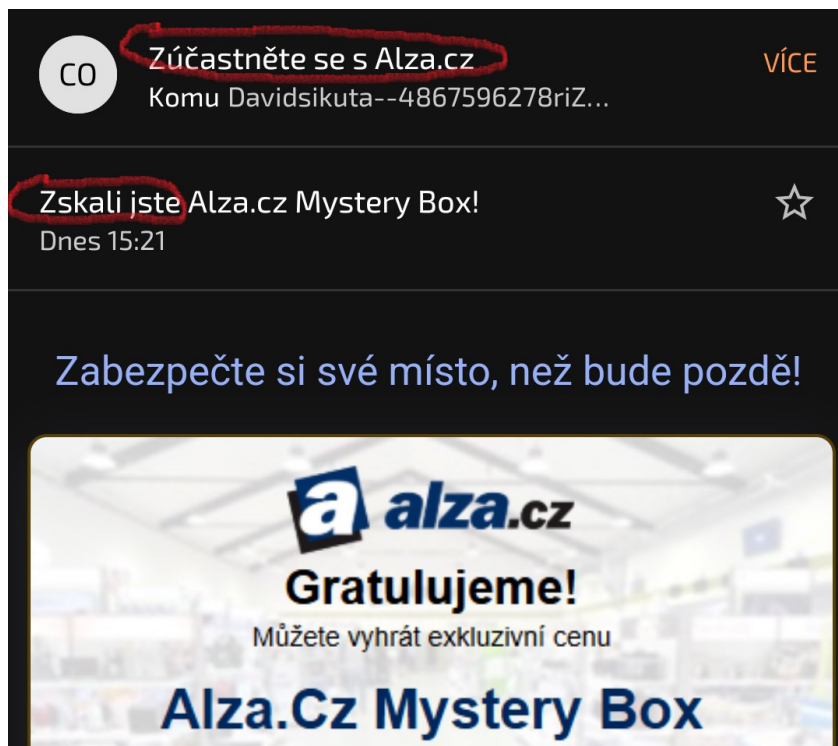
12.2 Opatření navrhovaná

Varianty navrhovaných opatření byly již zmíněny v některých předchozích kapitolách. Jedná se především o vzdělávací program formou určitého penetračního testování studentů, případně osob v organizaci, na níž by opatření mohlo být také aplikováno.

Vytvořením souboru určitých phishingových kampaní, se kterými by studenti přišli do kontaktu a jejich vyústěním by bylo poučení v chování. Tak, aby práce s moderními technologiemi nevzbuzovala strach, ale určitý respekt a opatrnost. Povědomí o problematice si student může vypěstovat mimo jiné i díky následujícím ilustrovaným příkladům.

12.2.1 Phishing ve škole

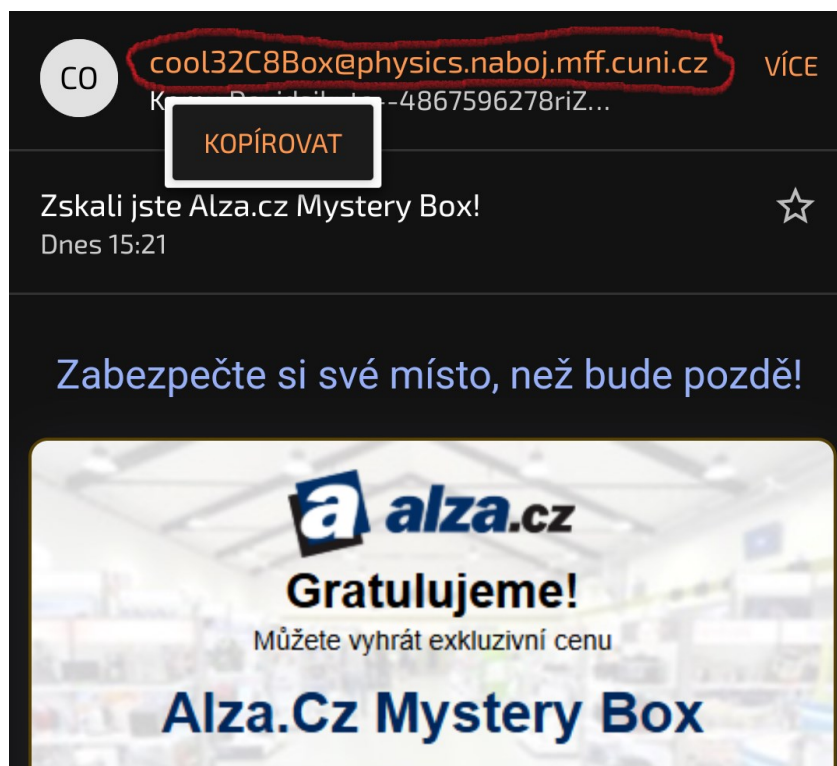
Každý student na fakultě má přidělený email. Ve vytipované době, kdy má čas a prostor vnímat nové informace, lze všem zaslat hromadný e-mail, který by vedl právě na nějakou stránku, která by vysvětlovala, jak se chovat při práci s odkazem v e-mailu a seznámila jej i s variantou obdržení emailu z oficiální školní adresy. Lze například vytvořit e-mailovou adresu pod fiktivním jménem a ilustrovat možnost útoku zevnitř. Vrátit studenta zpět do e-mailového klienta a ukázat mu, jak se pracuje s ověřením adresy, kdy pod zobrazovaným jménem můžeme najít často nesmyslnou adresu. Shodou okolností lze jako příklad ukázat e-mail, který se právě v tento moment hlásí z osobního účtu. Většinou do pár minut zmizí jako hlášený spam. I to může být důvodem, proč uživatelé schopnost tyto podvody odhalit ztrácí.



Obrázek 34 Spamový e-mail se jménem

(vlastní)

Jak lze vidět na Obrázek 34 Spamový e-mail se jménem, jméno zakrývá e-mailovou adresu, a tak si oběť ani nemusí všimnout nesmyslné adresy. K tomu pořád obsahuje i chybu v textu. Penetrační email může vést na web ukazující, jak s obdrženým mailem naložit a jaké základní kroky podniknout pro ověření.



Obrázek 35 Spamový e-mail s e-mailovou adresou

(vlastní)

Na webu může být právě obdržený email ze školní adresy včetně ukázky jak si adresu zkontrolovat včetně ukázky různých poznávacích znamení. Zpracování by mělo být zajímavé, ideálně interaktivní s cílem zaujmout. A ve své podstatě lze takovou akci vytvořit a plánovaně používat na studenty prvního ročníku, kdy již žádný náklad kromě času na odeslání připraveného e-mailu všem není. Jednalo by se tak o velmi levný provoz s vysokým počtem záchytů.

12.2.2 Quishing na akademické půdě

U této varianty je možná i inspirace u provedeného útoku z této práce. S určitou modifikací, či i jako další průběžný výzkumný projekt. V rámci opatření lze touto metodou doajista zvyšovat povědomí uživatelů o hrozbách v kybernetickém prostoru. Po fakultě lze se zanedbatelným finančním nákladem provést kampaň například z kraje prvního semestru nových studentů. Stejně jako u phishingu a návrhu na e-mailovou kampaň i zde lze odkazovat na vzdělávací projekt ke quishingu a vytvořit vzdělávací prezentaci. Tato metoda má předpoklad využití převážně na mobilních zařízeních a tím pádem i stavba vzdělávací webové prezentace může mít úpravu vzhledu pro mobilní zařízení.

12.2.3 Učebna či chodba

V rámci ukázky pro zájemce lze vybavit i nějakou místnost interaktivními předměty, k jejichž využití postačí mobilní telefon studenta. V zásadě se může jednat i o nevyužitou část chodby, kde se udělá určitá Cybercrime ulička, jejíž návštěvu může doporučit vyučující v předmětech zaměřených na kybernetickou a informační bezpečnost, či IT.

12.3 Vzdělávání systémové

Může se zdát, že taková opatření jsou vhodná spíše na fakultu aplikované informatiky, či obecně na vzdělávací instituce zabývající se problematikou kybernetické bezpečnosti. Nicméně pod tíhou čísel je zřejmé, že při pokračujícím trendu se jedná, případně v brzké době jednat bude, o celospolečenský problém se všeobecně oborovým rozsahem. A s rostoucím rozmachem umělé inteligence, rostoucí počítačové gramotnosti, která stejným dílem roste i na straně black hat skupin, informatizace organizací a celé společnosti je jistý předpoklad v pokračování růstu tohoto druhu kriminality. Obecné povědomí by tedy mělo být prioritní, jelikož i jeden jediný člověk může svojí chybou připravit firmu o milióny, či stát o strategickou výhodu.

12.4 Rizika po ošetření

Ošetření rizik bylo odhadnuto týmem složeným z lidí aktivně pracujících v IT a aktuálně, nebo v minulosti zastávajících pozice místních bezpečnostních správců, kdy někteří provádějí také školení v oblasti kybernetické bezpečnosti.

Tým byl složen následovně:

Bc. David Šikuta

Mgr. Leoš Pašek

David Štefaňák

Členové byli seznámeni s postupem a návrhem opatření. Také byli seznámeni s průběhem kampaně již v počátku a o celém záměru jako aktivní školící kampani měli přehled. Ošetření bylo hodnoceno podle změny po zavedení školící kampaně na úrovni interaktivní činnosti vůči studentům.

Tabulka 17 Hodnocení rizik – kvalifikovaný odhad po opatřeních průměrem

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	2	4	2	16
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	2	3	2	12
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	2	3	3	2	18
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	2	3	2	12
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	2	2	2	8
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	2	3	2	12

(vlastní a kolektiv)

Tabulka 18 Hodnocení rizik – kvalifikovaný odhad po opatřeních nejvyšší hodnotou

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	2	4	2	16
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	2	4	2	16
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	2	3	3	2	18
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	2	4	2	16
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	2	3	2	12
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	2	4	2	16

(vlastní a kolektiv)

Odhad rizik po ošetření lze také zpracovat dle metodiky podle průměru z triády CIA a nejvyšší hodnotou. I zde vidíme zásadní rozdíly ve výsledném hodnocení rizika. Kdy průměrem spadají do akceptovatelného, tedy zeleného rizika dvě položky, zatímco při hodnocení nejvyšší hodnotou pět. Naopak v bezvýznamném riziku, tedy modrém najdeme při hodnocení rizik průměrem čtyři položky, zatímco při hodnocení rizik nejvyšší hodnotou pouze jednu.

I když jsou dle dvou různých metodik značné rozdíly, tak se obě varianty dostaly do stavu, kdy veškeré rizika spadají do kategorií bezvýznamného rizika a akceptovatelného rizika. V hodnocení rizik po ošetření bylo bráno v potaz právě to, že se minimalizuje chyba uživatele a díky znatelně nižšímu riziku již budou dostatečně dobře působit další obranné linie.

Pokud by se dalo toto hodnocení opřít o aktualitu při dokončení této práce, lze zmínit napadení účtu premiéra Fialy 8.4.2025.

„Podle experta na kybernetickou bezpečnost prolomení dvoufázového ověření účtů značí útok špičkových hackerů, kterým ale s největší pravděpodobností pomohla chyba někoho v premiérově týmu.“ (NOVINKY, 2025)

I zde se stále ukazuje, že špičková práce hackerů využívá chyb uživatelů. A je to perfektní ukázka toho, jak velká uživatelská chyba může pomoci prolomit i další obranné linie. V této konkrétní situaci bylo zřejmě sdíleno heslo a díky tomu se zřejmě podařilo i obejít dvoufaktorové zabezpečení.

13 DISKUZE

I přes vzrůstající povědomí o důležitosti kybernetické bezpečnosti na straně odborníků a opatrném chování v sítích na straně veřejnosti stále dochází k nezodpovědnému chování. Jak ukazují data, sociální inženýrství patří stále mezi nejvyužívanější bránu vstupu do sítě. Nejen data, ale i odborníci stále poukazují na člověka jako nejslabší článek zabezpečení sítě. Jako příklad můžeme uvést několik citací, které tento fakt potvrzují již mnoho let a stále se tato situace nemění.

„Amatéři hackují systémy, profesionálové ‚hackují‘ lidi.“ (Harvard Kennedy School, c2025)

„Humans The weakest link in cyber security“ (SECURITY AFFAIRS, 2012)

„Nejslabším článkem v bezpečnostním řetězci je člověk“ (CNews, 2011)

„Lidský faktor je nejslabší článek v řetězci, který je opravdu potřeba posílit.“ (HOSPODÁŘSKÉ NOVINY, 2023)

„Nejčastějším vstupním bodem pro získání informací a dat, jež jsou dostupné v interních sítích organizací, je už několik let uživatel. Útočníci na něj jako na nejslabší článek kybernetické bezpečnosti cílí pomocí technik sociálního inženýrství.“ (NÚKIB, 2018)

„Velkým problémem jsou samotní uživatelé, kteří se vás snaží obejít, zařídit si věci po svém a nerespektovat pravidla.“ (ROOT, 2022)

„Můžete se snažit, jak chcete a uživatel pak na něco klikne a způsobí průšvih. Asi 95 % bezpečnostních incidentů je způsobeno uživateli“ (ROOT, 2022)

Je tedy zřejmé, že sociální inženýrství bude i nadále v oblibě. Jedná se o nejméně technické útoky v kybernetickém prostoru a díky tomu je určeno pro velkou část zločinců a podvodníků.

V rámci pokusu bylo prověřeno, že i letité poučky o phishingu stále mnoho uživatelů ignoruje a stále je možné tyto metody v různých modifikacích používat. Přestože se investuje do vzdělávacích kampaní, dosah k běžným uživatelům nebude stoprocentní.

Z dat získaných pokusem můžeme říct, že velká část studentů bez zaváhání otevírá odkazy z nedůvěryhodného zdroje, který vykazuje známky phishingu. A to i v době, kdy tyto varovné prvky umí útočník již skrýt.

Dále se prokázalo, že i s velmi levnou a časově nenáročnou kampaní je dosaženo výborných výsledků, a tudíž je phishing stále formou útoku, který se bude využívat ve velkých objemech.

V rámci sběru informací skrze dotazníkové řešení se nám poté dostalo odpovědí na několik základních obecných otázek. Zde se jeví prostor pro další výzkum a důkladnější zkoumání. Dotazníkové řešení skrze quishingovým útok se ukázalo jako zajímavý nápad, který rozproudil debatu a dozajista vzbudil zájem o bezpečnost v kybernetickém prostoru.

Varianta ukázala i jeden ze způsobů, který lze ve vzdělávacích institucích provádět v rámci školení studentů. A nemusí se jednat jen o letáčky. V rámci vzdělávání lze například na chodbě umístit QR kódy, které povedou na jednoduché poučky a vysvětlí, co student udělal špatně při skenování kódu. Je to už jen o fantazii odpovědné osoby, která se může držet hesla „škola hrou“.

Jako dílčí zpětnou vazbu k účinnosti šíření povědomí o rizicích lze uvést i informace z rozhovoru s panem inženýrem Pavlem Valáškem, který byl jako zaměstnanec fakulty pověřen se zpracováním a rozvěšením plakátů s QR kódem na akci „silový trojboj“. Zatímco v minulém ročníku v roce 2024 se pomocí QR kódu přihlásilo 22 zájemců, zatímco e-mailem 0. O letošní ročník 2025 byly pomocí QR kódu pouze 4 přihlášky, zbytek, tedy 13 zájemců, za pomoci e-mailu uvedeného na plakátu. Může to být jako příklad opatrného přístupu uživatelů, tak také toho, že QR kód by v rámci ošetření rizik měl obsahovat více údajů, jako například možnost využití e-mailové adresy.

Je také důležité uvědomit si, že nejde o šíření paniky, ale o vzdělávání. Není účelem říct lidem, aby QR kódy nepoužívaly, ale naučit je, jak k nim přistupovat správně a jak je používat bezpečně. Jednou z cest je právě výše zmíněná interaktivní metoda, založená na vlastní zkušenosti. Pokud budeme jen zkoumat stav bezpečnosti, stačí například zkusit odkazovat QR kódem na stránku, ze které je automatické přesměrování. Nicméně je vhodnější nastavit kampaň tak, aby dotyčný věděl, co udělal za chybu, co se může stát a jak tomu předcházet. Tento pomyslný trojúhelník by měl být základem interaktivního vzdělávání v rámci bezpečnosti. Jelikož interakce v kybernetickém prostoru bude drtivá většina absolventů provádět jak v zaměstnání, tak i v osobním životě. Nabízí se tedy varianta další živé ukázky, anebo možnost věnovat nějaký kousek chodby na fakultě neškodným ukázkám těchto útoků v duchu „vzdělávací uličky“ tak, aby si studenti mohli projít různé varianty a prakticky se naučili rozpoznávat podezřelé indicie a získávali návyky bezpečného přístupu. To vše buď na doporučení při výuce, nebo jako zahrnutí do výuky samotné.

V rámci řešení rizik se ukázala jako vhodná varianta semikvantitativní bodová metoda, která se uvádí v přílohách vyhlášky 82/2018 Sb. o kybernetické bezpečnosti. V rámci ošetření se práce drží zavedených doporučení autorit, jako je například NÚKIB. Výsledné hodnoty rizik po ošetření lze zjistit nejlépe opakovaným pokusem a zkoumáním rozdílů v interakci.

ODPOVĚDI NA VÝZKUMNÉ OTÁZKY

VO1: Jaký je aktuální stav povědomí studentů o kybernetických rizicích?

Data z dotazníkového šetření ukázala, že velký počet studentů nemá dostatečné povědomí o moderních formách útoků, jako je quishing. Překvapivě vysoký počet studentů reagoval na podněty z kampaně bez podezření, což potvrzuje nedostatečnou edukaci.

VO2: Jak lze využít penetrační test pro sběr dat?

Penetrační testování formou simulovaného útoku umožnilo nejen sběr kvantitativních dat o chování uživatelů, ale i kvalitativní vhled do jejich chyb a uvažování. Test sloužil i jako nástroj edukace a vyvolání diskuse mezi studenty.

VO3: Jaký je vztah mezi náklady nebo časem k počtu záchytů obětí?

Porovnáním jednotlivých metod (letáková a "záchodová" kampaň) se ukázalo, že jednodušší a levnější forma měla vyšší účinnost. Nejvyšší počet interakcí přinesly nenápadné a snadno přístupné QR kódy v kombinaci s jednoduchou výzvou.

VO4: Jak se kvalifikovaný tým se zkušenostmi v oblasti kybernetické bezpečnosti dívá na snížení rizik navrhovanou metodou?

Odborné hodnocení potvrdilo, že edukační forma penetračního testování může významně přispět ke snížení rizik, pokud je správně zpracována a interpretována.

VO5: Jakými způsoby lze edukovat studenty na akademické půdě?

Jako účinné metody se jeví právě ty interaktivní. Přímá účast na „útocích“ zájem vzbudila a rozšířila povědomí o existenci rizik.

ZÁVĚR

Cílem této práce bylo prověřit úroveň kybernetické bezpečnosti lokálních sítí z hlediska jejich nejzranitelnějšího prvku – člověka. Zaměřením na lidský faktor v kombinaci s praktickým penetračním testem pomocí quishingové kampaně se podařilo získat nejen zajímavá data, ale také odhalit praktické nedostatky ve vnímání kybernetických rizik studenty. Výzkumné šetření ukázalo, že i když je kybernetická bezpečnost součástí každodenního digitálního života, většina uživatelů stále nepřistupuje k ochraně osobních údajů či síťového prostředí s dostatečnou obezřetností.

Analýza výsledků praktické části ukázala, že i jednoduchý útok, jako je fyzicky umístěný QR kód, může být velmi efektivní, pokud cílí na běžného, neproškoleného uživatele. Práce zároveň prokázala, že tato forma penetračního testu může být nejen nástrojem odhalování zranitelností, ale i způsobem vzdělávání. Právě propojení testování, edukace a následného vyhodnocení se ukazuje jako možný funkční model pro akademické prostředí i mimo něj.

Navržená opatření – technická i organizační – reflektují aktuální trendy v oblasti kybernetických hrozeb. Zjištěné zranitelnosti a navržené edukační aktivity ukazují, že pro efektivní ochranu je nezbytné budovat tzv. kybernetickou kulturu, tedy prostředí, v němž jsou bezpečnostní návyky přirozenou součástí uživatelského chování. Velký potenciál se skrývá ve spojení preventivních kampaní s interaktivními formami výuky, které studenty nejen informují, ale i aktivně zapojují.

SEZNAM POUŽITÉ LITERATURY

APWG, 2013. *Trends reports APWG* [online]. 2025 [cit. 2025-02-24]. Dostupné z: <https://apwg.org/trendsreports/>

APWG, c2003-2025. *Quishing: QR code phishing* [online]. [cit. 2025-04-14]. Dostupné z: <https://apwg.org/>

AUTHENTIC8, 2024. *Quishing attacks 101: how QR codes are exploited for phishing* [online]. [cit. 2025-04-13]. Dostupné z: <https://www.authentic8.com/blog/quishing-qr-code-phishing>

AVAST, 2014. *Avast blog* [online]. [cit. 2025-02-22]. Dostupné z: <https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>

CLEVER AND SMART, 2010. *CIA:duvernost-integrita-dostupnost* [online]. 2008. Dolní Břežany: Miroslav Čermák [cit. 2025-04-24]. ISSN 2694-9830. Dostupné z: <https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/>

CNEWS, 2011. *Zásady bezpečnosti na počítači: nenechte se okrást na internetu* [online]. [cit. 2025-03-31]. Dostupné z: <https://www.cnews.cz/clanky/zasady-bezpecnosti-na-pocitaci-nenechte-se-okrast-na-internetu/>

ČESKÁ JUSTICE, 2020. *Kybernetická kriminalita v ČR stoupá, loni to bylo 8417 činů. ČESKÁ JUSTICE* [online]. [cit. 2025-03-22]. Dostupné z: <https://www.ceska-justice.cz/2020/02/kyberneticka-kriminalita-cr-stoupa-loni-bylo-8417-cinu/>

ČESKÁ JUSTICE, 2023. *Útoky na účty nebo erotické materiály. Kyberkriminalita stále roste* [online]. [cit. 2025-03-22]. Dostupné z: <https://www.ceska-justice.cz/2023/10/utoky-na-ucty-nebo-eroticke-materialy-kyberkriminalita-stale-roste/>

ČESKÉ NOVINY, 2024. *V roce 2016 tvořila kyberkriminalita v ČR 2 % trestné činnosti, loni 11 %* [online]. [cit. 2025-03-22]. Dostupné z: <https://www.ceskenoviny.cz/zpravy/2475774>

ENISA, 2017. *Handbook on Security of Personal Data Processing*. ENISA. ISBN 978-92-9204-251-6.

ENISA, 2022. *ENISA Threat Landscape 2022. Version_1*. ENISA. ISBN 978-92-9204-588-3.

ENISA, c2025. *Enisa* [online]. [cit. 2025-04-18]. Dostupné z: <https://www.enisa.europa.eu/>

ESET, 2025. *Třetina Čechů nemá přehled o obsahu smartphonu, pětina si není jistá jeho zabezpečením* [online]. [cit. 2025-03-29]. Dostupné z: <https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-tretina-cechu-nema-prehled-o-obsahu-smartphonu-petina-si-neni-jista-jeho-zabezpecenim/>

FEDERATION OF AMERICAN SCIENTISTS, 2010. *United states army's cyberspace operations concept capability plan 2016-2028* [online]. USA: The United States Army's [cit. 2023-04-16]. Dostupné z: <https://irp.fas.org/doddir/army/pam525-7-8.pdf>

GOODMAN, Marc, 2016. *Future crimes: inside the digital underground and the battle for our connected world*. New York: Anchor Books, a division of Penguin Random House. ISBN 978-0-8041-7145-8.

HADNAGY, Christopher, 2018. *Social engineering: the science of human hacking*. Second edition. Indianapolis, IN: Wiley. ISBN 978-1-119-43373-6. Dostupné také z: <https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=5436552>

HARVARD KENNEDY SCHOOL, c2025. *Bruce Schneier* [online]. [cit. 2025-04-18]. Dostupné z: <https://www.hks.harvard.edu/faculty/bruce-schneier>

HOSPODÁŘSKÉ NOVINY, 2023. *V bezpečnosti nejde jen o boj systémů* [online]. [cit. 2025-03-31]. Dostupné z: <https://hn.cz/c1-67257330-v-bezpecnosti-nejde-jen-o-boj-systemu-nejslabsim-clankem-je-clovek>

CHIP, 2018. *Průzkum: Antivir v mobilu používá méně než polovina studentů, smartphone má 96 % z nich* [online]. [cit. 2025-03-29]. Dostupné z: <https://www.chip.cz/pruzkum-antivir-v-mobilu-pouziva-mene-nez-polovina-studentu-smartphone-ma-96-z-nich>

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2022. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA. ISBN 978-80-908388-4-0.

KASPERSKY, c2025. *Black hat, White hat, and Gray hat hackers – Definition and Explanation* [online]. [cit. 2025-04-15]. Dostupné z: <https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>

KEEPNET, 2025. *2025 QR Code Phishing Trends: In-Depth Analysis of Rising Quishing Statistics* [online]. [cit. 2025-02-19]. Dostupné z: <https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of-rising-quishing-statistics>

KOLOUCH, Jan a Pavel BAŠTA, 2019. *Cybersecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, Jan, 2016. *Cybercrime*. Praha : CZ.NIC,z.s.p.o. CZ.NIC. ISBN 978-80-88168-18-8.

KYBEZ, 2023a. *Jak hodnotit aktiva* [online]. [cit. 2025-04-06]. Dostupné z: <https://kybez.cz/analyza-bezpecnosti-3-jak-hodnotit-aktiva/>

KYBEZ, 2023b. *Jak chránit sebe i své podnikání* [online]. [cit. 2025-04-06]. Dostupné z: <https://kybez.cz/socialni-inzenyrstvi-jak-chranit-sebe-i-sve-podnikani-pred-manipulaci/>

MITNICK, Kevin a William L. SIMON, 2003. *Umění klamu: Kevin Mitnick nejslavnější hacker na světě*. Gliwice: Helion. ISBN 83-736-1210-6.

MOBILMANIA, 2022. *Znepokojivé výsledky průzkumu. Každý třetí má ve svém telefonu citlivé fotky, polovina uživatelů nemá antivirus* [online]. [cit. 2025-03-29]. Dostupné z: <https://mobilmania.zive.cz/clanky/znepokojive-vysledky-pruzkumu-kazdy-treti-ma-ve-svem-telefonu-citlive-fotky-polovina-uzivatelu-nema-antivirus/sc-3-a-1355566/default.aspx>

MOHANTA, Abhijit a Anoop SALDANHA, 2020. *Malware analysis and detection engineering: a comprehensive approach to detect and analyze modern malware*. New York: Apress. ISBN 978-1-4842-6192-7.

NOVINKY, 2025. *Někdo v týmu chyboval* [online]. [cit. 2025-04-12]. Dostupné z: <https://www.novinky.cz/clanek/domaci-nekdo-v-tymu-premiera-zrejme-chyboval-rika-expert-k-utoku-na-fialuv-ucet-40516501>

NÚKIB, 2018. *Zpráva o stavu KB NÚKIB* [online]. [cit. 2025-03-31]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

NÚKIB, 2020. *Zpráva o stavu KB 2020* [online]. [cit. 2025-03-22]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

NÚKIB, 2025. *Analýzy a Souhrnné zprávy* [online]. [cit. 2025-02-19]. Dostupné z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/analyzy/>

OXFORD DICTIONARY, c2025. *Cyberspace* [online]. [cit. 2025-04-19]. Dostupné z: <https://dictionary.cambridge.org/dictionary/english/cyberspace>

PORTERFIELD, Jason, 2017. *White and Black Hat Hackers*. Rosen Young Adult. ISBN 978-1-5081-7314-4.

ROOT, 2022. *Nejslabším článkem je ... uživatel* [online]. [cit. 2025-03-31]. Dostupné z: <https://www.root.cz/clanky/nejslabsim-clankem-je-nepouceny-ci-nezodpovedny-uzivatel-tvrdi-bezpecaci/>

Sbírka zákonů České republiky, 1993-2023. Praha: Ministerstvo vnitra. ISSN 1211-1244. Dostupné také z: <http://www.sbirkyzakonu.cz>

SECURITY AFFAIRS, 2012. *Why humans could be the weakest link in cyber security chain?* [online]. [cit. 2025-03-31]. Dostupné z: <https://securityaffairs.com/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html>

SCHNEIER, Bruce, 2023. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*. W. W. Norton & Company. ISBN 978-0-393-86666-7.

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4644-9.

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

SPOTIFY, c2025. *Podcasty* [online]. [cit. 2025-04-24]. Dostupné z: <https://open.spotify.com/search/podcasty/podcastAndEpisodes>

STARK, Michael, 2013. *QR Codes: The Technical Guide*. A K Peters/CRC Press. ISBN 978-1-4665-9146-2.

STATISTA, 2023. *Nejrozšířenější formy kybernetické kriminality* [online]. [cit. 2025-02-22]. Dostupné z: <https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/>

UTB, 2024. *Pedagogická oblast, Univerzita Tomáše Bati ve Zlíně* [online]. [cit. 2025-04-15]. Dostupné z: <https://www.utb.cz/?mdocs-file=69391>

VÁŠ HOSTING, 2023. *Jak na kybernetickou bezpečnost: 1. díl Sociální Inženýrství* [online]. [cit. 2025-04-13]. Dostupné z: <https://www.vas-hosting.cz/blog-jak-na-kybernetickou-bezpecnost-1-dil-socialni-inzenyrstvi#tailgating>

VIPRE, b.r. *What is Quishing, a.k.a. QR Code Phishing?* [online]. [cit. 2025-04-13]. Dostupné z: <https://vipre.com/glossary-terms/what-is-quishing>

VLACH, Jiří, Kateřina KUDRLOVÁ a Viktorie PALOUŠOVÁ, 2020. *Kyberkriminalita v kriminologické perspektivě*. Vydání: první. Praha: Institut pro kriminologii a sociální prevenci. Studie. ISBN 978-80-7338-189-9.

SEZNAM OBRÁZKŮ

Obrázek 1 Triáda CIA.....	31
Obrázek 2 Parkerian hexad	33
Obrázek 3 Statistika typů útoků 2017 a 2022	41
Obrázek 4 Spotify Kriminálka	43
Obrázek 5 Spotify Opravdové zločiny.....	43
Obrázek 6 Spotify Hodina dějepichu.....	43
Obrázek 7 Spotify KYBEZ.....	44
Obrázek 8 Spotify Místo kyberčinu.....	44
Obrázek 9 Pomyslný Organization phishing	46
Obrázek 10 Phishing report Q1_20166	48
Obrázek 11 Phishing report Q3_2022 - Q3_2024	49
Obrázek 12 Útok v roce 2014 s použitím QR kódu.....	50
Obrázek 13 FLKR_memes	51
Obrázek 14 Leták na pizzu	53
Obrázek 15 Písemné svědectví první.....	54
Obrázek 16 Písemné svědectví druhé	54
Obrázek 17 Úprava útoku obětí	56
Obrázek 18 Počet studentů univerzity Tomáše Bati.....	57
Obrázek 19 Statistika respondentů – akce pizza leták	58
Obrázek 20 Historie návštěv – akce pizza leták	58
Obrázek 21 Statistika respondentů – akce FLKR_testy	59
Obrázek 22 Historie návštěv – akce FLKR_testy.....	60
Obrázek 23 Otázka první – akce pizza leták.....	67
Obrázek 24 Otázka druhá – akce pizza leták.....	68
Obrázek 25 Otázka třetí – akce pizza leták.....	68
Obrázek 26 Otázka čtvrtá – akce pizza leták	68
Obrázek 27 Otázka první – akce FLKR_testy	69
Obrázek 28 Otázka druhá – akce FLKR_testy	69
Obrázek 29 Otázka třetí – akce FLKR_testy	70
Obrázek 30 Otázka čtvrtá – akce FLKR_testy	70
Obrázek 31 Čas vyplnění dotazníků	74
Obrázek 32 Hodnocení aktiv dle CIA průměrem	80
Obrázek 33 Hodnocení aktiv dle CIA nejvyšší hodnotou	81
Obrázek 34 Spamový e-mail se jménem	92

Obrázek 35 Spamový e-mail s e-mailovou adresou.....	93
---	----

SEZNAM TABULEK

Tabulka 1 Techniky sociálního inženýrství	27
Tabulka 2 Nové trendy v technikách sociálního inženýrství	28
Tabulka 3 Statistika růstu případů kybernetické kriminality	39
Tabulka 4 Tabulka finančních nákladů	62
Tabulka 5 Tabulka časové náročnosti	63
Tabulka 6 Počty uživatelů používající zabezpečovací aplikaci	73
Tabulka 7 Vybrané zranitelnosti	77
Tabulka 8 Výběr hrozeb pro modelovou situaci	79
Tabulka 9 Hodnocení hrozby	82
Tabulka 10 Hodnocení zranitelnosti	83
Tabulka 11 Hodnocení rizika	84
Tabulka 12 Hodnocení rizik – barevné rozlišení	84
Tabulka 13 Aktiva modelové organizace	85
Tabulka 14 Převodní tabulka	86
Tabulka 15 Hodnocení rizik – průměrem	87
Tabulka 16 Hodnocení rizik – nejvyšší hodnotou	88
Tabulka 17 Hodnocení rizik – kvalifikovaný odhad po opatřeních průměrem	95
Tabulka 18 Hodnocení rizik – kvalifikovaný odhad po opatřeních nejvyšší hodnotou	96

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APWG	Anti-Phishing Working Group
CIA	Confidentiality, Integrity, Availability
D	Dopad
DPIA	Data Protection Impact Assessment
ENISA	European Union Agency for Cybersecurity
FLKR	Fakulta logistiky a krizového řízení
KB	Kybernetická bezpečnost
Moodle	Modular Object-Oriented Dynamic Learning Environment
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
P	Pravděpodobnost
QR	Quick Response
R	Riziko
STAG	Studijní agenda
VO	Výzkumná otázka
Z	Zranitelnost

SEZNAM PŘÍLOH

Příloha P I: Hodnotící tabulky

Příloha P II: Vyplněné hodnotící tabulky

PŘÍLOHA P I: HODNOTÍCÍ TABULKY

Tabulka 1 Běžný stav

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.					X		X
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.					X		X
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.					X		X
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X

(zdroj: vlastní)

Jméno:
 (v případě vyplnění jména bude zveřejněno v diplomové práci)

X – označuje hodnoty, které se nevyplňují
 (budou dopočítány)

Tabulka 2 Po ošetření rizik

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.					X		X
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.					X		X
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.					X		X
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.					X		X

(zdroj: vlastní)

Jméno:
 (v případě vyplnění jména bude zveřejněno v diplomové práci)

X – označuje hodnoty, které se nevyplňují
 (budou dopočítány)

Rizika se vztahují k phishingovému útoku na fakultu školy a vyplňujeme je tedy ve vztahu k tomuto druhu útoku. Například – zda může phishingový útok pomoci získat přístup k bankovnímu účtu.

Kde u **P** vyplníme na škále 1–4 s jakou pravděpodobností – dle tabulky níže popis hrozby.

U zranitelnosti **Z** zase vyplníme na škále 1–4 jak je pravděpodobné, že se daná zranitelnost ke konkrétnímu útoku (phishing) na danou hrozbu využije.

U aspektů vyplníme dle triády CIA, viz tabulky níže.

Vyplňujeme:

C – Důvěrnost, I – Integritu, A – Dostupnost

Škála je 1-4, kdy 1 znamená, že není vyžadována žádná akce, tudíž vliv není, nebo je zanedbatelný.

Pokud tedy dané aktivum není ohroženo například důvěrností, jelikož se jedná o veřejně dostupnou informaci, tak vyplníme číslo 1. Viz tabulky níže.

Tabulka 1: jsou rizika běžné modelové fakulty o 1499 studentech.

Tabulka 2: jsou rizika po masivní vzdělávací kampani a penetračním testu studentů formou letáků, které simulují phishingový útok, nicméně namísto škodlivého kódu či podvodu šíří povědomí o problematice a vzdělávací informace. Ve zkratce – jak sníží vzdělávací kampaň s penetračním útokem daná rizika.

U tabulky 2 tedy nebude zřejmě vliv na aspekty, jelikož vzdělání neovlivní například to, zda provedený útok poškodí data, ale bude mít vliv hlavně na **P**, jakožto pravděpodobnost, že daná hrozba nastane a poté i **Z**, jakožto zranitelnost, kterou útočník úspěšně využije.

Úroveň	Popis důvěrnosti C	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítě jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabírající zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4.

Úroveň	Popis integrity I	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Úroveň	Popis dostupnosti A	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Úroveň	Popis Hrozba P
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Úroveň	Popis Zranitelnosti Z
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

PŘÍLOHA P II: VYPLNĚNÉ HODNOTÍCÍ TABULKY

Tabulka 1 Běžný stav

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	4	3	3	X	4	X
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	3	X	3	X
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	2	2	4	X	3	X
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	2	3	X	3	X
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	2	4	X	4	X
Počítače a servery	Poškození či zafixování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	1	4	3	3	X	4	X

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)

Jméno: David Šilka
(v případě vyplnění jména bude zveřejněno v diplomové práci)

Tabulka 2 Po ošetření rizik

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko				
			C	I	A	P	D	Z	R	
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	4	3	2	X	2	X	
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	2	X	2	X	
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	2	2	3	X	2	X	
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	2	2	X	2	X	
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	2	2	X	2	X	
Počítače a servery	Poškození či zafixování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	1	4	3	3	X	2	X	

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)

Jméno:
(v případě vyplnění jména bude zveřejněno v diplomové práci)

Tabulka 1 Běžný stav

Aktivum	Hrozba	Zranitelnost	Aspekty				Riziko			
			C	I	A	P	D	Z	R	
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	3	X	3	X	
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	3	4	3	2	X	2	X	
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	1	3	X	3	X	
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	3	3	3	3	X	3	X	
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	3	X	3	X	
Počítače a servery	Poškození či zajišťování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	3	X	3	X	

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)Jméno: Leaš Pásek
(v případě vyplnění jména bude zveřejněno v diplomové práci)

Tabulka 2 Po ošetření rizik

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	2	X	2	X
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	5	4	3	2	X	2	X
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	3	3	1	3	X	3	X
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	3	3	3	3	X	3	X
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	2	X	2	X
Počítače a servery	Poškození či zasíťování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	2	4	4	2	X	2	X

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)Jméno:
(v případě vyplnění jména bude zveřejněno v diplomové práci)

Tabulka 1 Běžný stav

Aktivum	Hrozba	Zranitelnost	Aspekty			Riziko			
			C	I	A	P	D	Z	R
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	3	X	3	X
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	4	3	3	3	X	2	X
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	2	3	2	3	X	2	X
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	2	X	3	X
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	3	X	3	X
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	4	4	2	X	3	X

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)Jméno: DAVID ŠTEFÁNEK
(v případě vyplnění jména bude zveřejněno v diplomové práci)

Tabulka 2 Po ošetření rizik

Aktivum	Hrozba	Zranitelnost	Aspekty				Riziko			
			C	I	A	P	D	Z	R	
Bankovní účet	Získání přístupu k bankovním účtům.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	4	4	4	3	X	2	X	
Bankovní účet	Přesměrování plateb a poplatků na vlastní účet.	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.	4	3	3	2	X	2	X	
Účty	Získání přístupu do účtů studentů a pracovníků fakulty (STAG, Moodle).	Zastaralost informačního a komunikačního systému.	2	3	2	2	X	2	X	
Účty	Napadení systémů důležitých pro provoz fakulty.	Zastaralost informačního a komunikačního systému.	4	3	3	2	X	2	X	
Osobní údaje	Krádež identity nebo sběr osobních údajů k dalšímu využití.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	2	1	3	X	2	X	
Počítače a servery	Poškození či zašifrování dat.	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů.	3	4	4	2	X	2	X	

(zdroj: vlastní)

X – označuje hodnoty, které se nevyplňují
(budou dopočítány)Jméno: DAVID ŠTEFÁNEK
(v případě vyplnění jména bude zveřejněno v diplomové práci)

