**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačního inženýrství**

# Diplomová práce

## Obrana proti phishingovým útokům

**Petr Podskalský**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petr Podskalský

Systémové inženýrství a informatika
Informatika

Název práce

**Obrana proti phishingovým útokům**

Název anglicky

**Defence against phishing attacks**

---

**Cíle práce**

Hlavním cílem práce je navrhnout vhodnou formu obrany proti phishingovým emailům, kterým čelí zaměstnanci vybraného podniku. Obrana bude navržena ve formě vhodných organizačních a technických opatření, které zvýší: povědomí zaměstnanců o možnostech phishingových útoků, kybernetickou bezpečnost v rámci organizace.
V rámci organizačních opatření budou formulovány způsoby, jak nejlépe vzdělávat zaměstnance, aby dokázali identifikovat a patřičně reagovat na phishingové emaily. Technická opatření budou zaměřena na navržení účinných obraných akcí proti phishingovým emailům z hlediska prevence a reaktivního přístupu, aby phishingové emaily zaměstnancům vůbec nedorazily.
Dílčím cílem bude vytvoření phishingových kampaní pro testování zaměstnanců vybraného podniku.

**Metodika**

Pro navržení vhodné formy obrany proti phishingovým emailům budou nastudovány existující druhy phishingových útoků jako spear phishing, vishing, whaling, smishing. Následně budou zjištěny taktiky a techniky útočníků, které pro svůj útok využívají. K rozšíření znalostí bude také sloužit osvojení si dostupných opatření, jak se škodlivým emailům bránit.

Na základě získaných znalostí bude navrženo několik phishingových kampaní, které budou sloužit pro testování zaměstnanců. Kampaně budou napodobovat převážně notifikace z používaných systémů ve firmě. Při testování zaměstnanců prostřednictvím kampaně se bude sledovat jejich reakce vůči daným emailům. Zda email smažou, přepošlou, správně reportují nebo přejdou na škodlivou testovací stránku a zadají své přihlašovací údaje. Údaje zaměstnanců nebudou v rámci testování nijak monitorované ani ukládané. Následně bude z těchto kampaní zjištěno a vyhodnoceno chování subjektů. Poté bude navržena efektivní forma edukace pro zaměstnance, která zajistí lepší povědomí o problematice a v budoucích testovacích kampaních i lepší výsledky zaměstnanců.

**Doporučený rozsah práce**

50-60 stran

**Klíčová slova**

phishing, kybernetická bezpečnost, sociální inženýrství, kybernetické útoky

---

**Doporučené zdroje informací**

ABAGNALE, Frank, 2019. Scam Me If You Can: Simple Strategies to Outsmart Today's Rip-off Artists. New York: Penguin Random House. ISBN 978-0525538967.

BROTHERSTON, Lee a BERLIN, Amanda, 2017. Defensive Security Handbook. California: O'Reilly Media, Inc. ISBN 978-1491960387.

HADNAGY, Christopher, 2018. Social Engineering: The Science of Human Hacking. 2nd ed. New Jersey: John Wiley & Sons. ISBN 978-1119433385.

OZKAYA, Erdal, 2019. Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Birmingham: Packt Publishing. ISBN 978-1789616194.

RAINS, Tim, 2020. Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks. Illustrated edition. Birmingham: Packt Publishing. ISBN 978-1800206014.

---

**Předběžný termín obhajoby**

2022/23 LS – PEF

**Vedoucí práce**

Ing. Marek Pícka, Ph.D.

**Garantující pracoviště**

Katedra informačního inženýrství

Elektronicky schváleno dne 9. 3. 2023

**Ing. Martin Pelikán, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 13. 3. 2023

**doc. Ing. Tomáš Šubrt, Ph.D.**

Děkan

V Praze dne 23. 03. 2023

**Čestné prohlášení**

Prohlašuji, že svou diplomovou práci Obrana proti phishingovým útokům jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.03.2023 _____

**Poděkování**

Rád bych touto cestou poděkoval Ing. Markovi Píckovi, Ph.D. za vedení a důležité rady, které mi poskytoval v průběhu tvorby mé diplomové práce. V neposlední řadě také za čas, který mi věnoval při všech mých konzultacích. Rád bych také poděkoval mému nadřízenému, který mi umožnil zpracovat praktickou část této práce ve firmě.

# Obrana proti phishingovým útokům


## Abstrakt

Tato diplomová práce se věnuje obraně před kybernetickými útoky prováděnými formou phishingu a dalšími souvisejícími technikami.

V teoretické části práce jsou rozebrány různé způsoby kybernetických útoků (např. smishing, vishing, whaling), princip fungování e-mailové komunikace, podstata phishingových útoků a jejich životní cyklus. Dále jsou v práci rozebrány jednotlivé důvody a hlavní motivace obětí zareagovat a zadat své osobní údaje při obdržení škodlivého e-mailu. V práci je také popsáno, jaké existují organizační aspekty ochrany před phishingem, včetně vzdělávání zaměstnanců. Následně je rozebrán systém prevence proti phishingu a technikám sociálního inženýrství a technické aspekty kybernetické bezpečnosti (DKIM, DMARC, SPF, spam filter, filtrování příloh). Pro úplnost je v práci věnován prostor i současným trendům souvisejícím s phishingem a ochranou před ním a krátké historii kybernetické bezpečnosti, legislativně související s ochranou kyberprostoru, a to primárně na území České republiky.

Praktická část této práce řeší, jaká je nejlepší forma obrany proti phishingovým e-mailům jak z hlediska organizačních opatření, tak z hlediska technických opatření při nutných omezeních z důvodu velikosti vybraného podniku a jím nastaveného systému. Nejprve je v praktické části zkoumáno, jestli dokáží zaměstnanci rozeznat škodlivé e-maily a jak na ně reagují. Následně je pro tyto zaměstnance navržena vhodná forma školení a je zkoumáno, zda jsou všechna technická opatření správně nastavena a zda phishingový e-mail bude na e-mailovém serveru zachycen a k zaměstnanci tedy vůbec nedoručen.



**Klíčová slova:** phishing, kybernetická bezpečnost, kybernetické útoky, phishingové simulace, sociální inženýrství

# Defence Against Phishing Attacks


## Abstract

The thesis focuses on defending against cyberattacks made by phishing and other techniques related to it.

The theoretical part of the thesis describes different types of cyber-attacks (e.g. smishing, vishing, whaling), the principle of e-mail communication, the nature of phishing attacks and their life cycle. Furthermore, the motivation of victims when they receive a malicious email is discussed. The thesis also describes what organizational aspects exist to protect against phishing, including employee training. Subsequently, the prevention system against phishing and social engineering techniques and technical aspects of cyber security (DKIM, DMARC, SPF, spam filter, attachment filtering) are described. For the sake of completeness, the thesis also deals with current trends related to phishing and protection against phishing and a short history of cybersecurity, legislation related to the protection of cyberspace, primarily in the Czech Republic.

The practical part of this thesis deals with the best form of defense against phishing emails both in terms of organizational measures and technical measures, reflecting the necessary limitations due to the size of the selected company and the system it has set up. First, the practical part investigates whether employees can recognize malicious emails and how they react to them. Then, there is an appropriate training is designed for these employees and it is examined whether all technical measures are set up correctly and whether a phishing e-mail will be intercepted on the e-mail server and therefore not delivered to the employee at all.



**Keywords**: phishing, cyber security, cyber-attacks, phishing simulations, social engineering

# Obsah

# 1 Úvod

Tato práce se věnuje tématu ochrany proti phishingovým útokům. Primárním cílem práce je návrh vhodné formy obrany proti phishingovým e-mailům, kterým čelí zaměstnanci vybraného podniku. Protože i tento podnik (respektive vedoucí zaměstnanci) si velmi dobře uvědomuje možné riziko, které hrozí právě skrze phishingové útoky. Z důvodu ochrany osobních údajů zaměstnanců, dobré pověsti dané společnosti a informační bezpečnosti bude nadále používán pouze pojem vybraný podnik či vybraná firma a další identifikátory, podle kterých by bylo možno vybraný podnik identifikovat, budou anonymizovány.

Phishing („rhybaření“) (6, s. 246), ať už ve formě kampaní nebo jednotlivých útoků, je od poloviny 90. let minulého století (18, s. 2) jedním z největších problémů firem, státních organizací i jednotlivců. Jedná se o podvodnou techniku sociálního inženýrství, která má donutit cíl útoku, v práci je použit i pojem oběť, k nějaké akci. Například kliknout na určitý odkaz, vyplnit své osobní údaje na falešné stránce, poskytnout své údaje útočníkovi (v práci jsou užity pojmy útočník i phisher neboli „rhybář“), umožnit přístup do systému nepovolané osobě nebo poskytnout útočníkovi informace vhodné k dalším, sofistikovanějším útokům.

V současné době je téma phishingu zvláště aktuální. S rostoucím využíváním a fungováním lidí v digitálním světě, rostou i počty krádeží a podvodů, které souvisí s online prostředím. Podvodnému jednání nejsou vystavováni pouze spotřebitelé, ale často také podniky a jejich zaměstnanci. V současnosti je phishing zdaleka nejvyužívanější technikou při kybernetických útocích. Zvláště od roku 2020, kdy v důsledku pandemie onemocnění COVID-19 došlo k výraznému využívání vzdáleného připojení v rámci soukromé i veřejné sféry, enormně vzrostly počty phishingových útoků (mezi lednem a únorem roku 2020 konkrétně o 510 %) (42). Podle analýzy NÚKIB z roku 2018 se s spear phishingem, propracovanější verzí phishingu, setkalo 64 % odborníků v oblasti IT a kybernetické bezpečnosti, což oproti roku 2017 představovalo 11 % nárůst (43). Podle informací z roku 2015 jsou phishingové útoky stále úspěšnější. V tomto roce trvalo v průměru 82 vteřin, než phishingová kampaň měla svou první oběť, 23 % recipientů phishingových zpráv tyto otevřelo a 11 % z nich otevřelo i přílohu těchto zpráv (3, s. 87). Nemluvě o tom, že podle ročního přehledu agentury Proofpoint podlehlo 83 % všech britských společností alespoň jednou phishingovému útoku (44). I v souvislosti s těmito daty se téma práce jeví velice aktuální.

# 2 Cíl práce a metodika

## 2.1 Cíl práce

Hlavním cílem práce je navrhnout vhodnou formu obrany proti phishingovým e-mailům, kterým čelí zaměstnanci vybraného podniku. Obrana bude navržena ve formě vhodných organizačních a technických opatření, které zvýší:

a. Povědomí zaměstnanců o možnostech phishingových útoků,
b. Kybernetickou bezpečnost v rámci organizace,
c. Organizaci práce a bezpečnosti ve vybraném podniku obecně.

Tyto tři faktory lze vnímat jako dílčí cíle práce, které vedou k žádoucímu pozitivnímu výsledku u cíle hlavního.

V rámci organizačních opatření budou v práci formulovány patřičné způsoby, jak nejlépe vzdělávat zaměstnance, aby dokázali identifikovat a patřičně reagovat na phishingové e-maily.

Technická opatření se budou věnovat návrhu účinných obraných opatření a akcí proti phishingovým e-mailům, a to z hlediska prevence a reaktivního přístupu. Výsledkem by měla být situace, za které phishingové e-maily k zaměstnancům vůbec nedorazí, nebo se k nim dostanou v co nejnižší míře.

Dílčím cílem této práce pak bude vytvoření a realizace phishingových kampaní pro testovaní zaměstnanců vybraného podniku, ze kterých bude vyhodnoceno, zda zaměstnanci dokáží odhalit škodlivý e-mail.

## 2.2 Metodika

Pro navržení vhodné formy obrany proti phishingovým e-mailům budou v této práci popsány klíčové pojmy kybernetické bezpečnosti, techniky sociálního inženýrství související s tématem této práce, druhy kybernetických útoků (např. spear phishing, whaling, smishing apod.) a technické a organizační aspekty prevence proti phishingu (2FA, druhy vzdělávacích kampaní apod.). Následně budou zjištěny taktiky a techniky útočníků, které pro svůj útok využívají. Pro nasimulování phishingového útoku bude v praktické části této práce vytvořena podvodná stránka pro aplikaci všech předchozích poznatků ohledně zabezpečení vybraného podniku po stránce technické (DKIM, DMARC, SPF) i organizační (průběžné vzdělávání zaměstnanců formou kampaní, testování jejich vnímavosti falešných zpráv, e-mailů a podvodných stránek apod.).

Na základě získaných znalostí z prostředí firmy, provedené metodou bait, bude navrženo několik různých phishingových kampaní. Tyto kampaně budou sloužit pro testování zaměstnanců a jejich kompetencí a potažmo i kybernetické bezpečnosti v rámci vybraného podniku. Kampaně budou napodobovat převážně notifikace z interních systémů užívaných ve firmě. Bude se tedy jednat nikoliv o klasický phishing, ale z větší části o jeho variantu spear phishing. Při testování zaměstnanců prostřednictvím kampaně budou sledovány jejich reakce vůči daným e-mailům, primárně z pohledu:

1. Jak budou s podvodnou zprávou zacházet neboli zda podvodnou zprávu smažou, přepošlou, nebo správně reportují,
2. Zda přejdou na škodlivou testovací stránku,
3. Zda zadají své přihlašovací či osobní údaje.

Osobní údaje zaměstnanců nebudou v rámci testování nijak monitorované, ani ukládané. Následně bude z těchto kampaní zjištěno a vyhodnoceno chování subjektů podle výše stanovených pozorovaných reakcí, a to včetně kvantifikovatelných výstupů.

Na základě výsledků phishingových kampaní bude navržena efektivní forma edukace pro zaměstnance např. formou intenzivních školení, zlepšení interních reportů v rámci vybraného podniku, zapojení managementu do školení o kybernetické bezpečnosti apod., která zajistí lepší povědomí o problematice a v budoucích testovacích kampaních i případné lepší výsledky zaměstnanců a zajistí zachování bezpečnosti a renomé firmy. Navržení technických opatření bude řešeno převážně v systému Microsoft 365 Defender, kde bude ověřeno, že firma využívá plně všechny bezpečnostní opatření ať již v oblasti označení externích e-mailů, správné využívání technik spf, dkim, dmarc, správné nastavení spam filteru a filtrování příloh. Pokud budou v podniku v rámci těchto opatření zjištěny nějaké nedostatky, bude navrženo jejich zlepšení či eliminování.

# 3 Teoretická východiska

## 3.1 Kybernetická bezpečnost

Tato kapitola je věnována základním pojmům a elementům kybernetické bezpečnosti, které mají návaznost na ochranu před phishingem u vybraného podniku. Oblasti evropského práva, které jsou sice významné pro celek kybernetické bezpečnosti, ale ne pro vybraný podnik, jsou pouze zmíněny. Jedná se primárně o směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (7, s. 93), a návrh nové směrnice EU v této oblasti.

### 3.1.1 Definice pojmu kybernetická bezpečnosti

Samotný pojem kybernetická neboli informační bezpečnost je podmnožinou pojmu bezpečnost a lze ho chápat několika různými způsoby (7, s. 42). Definice níže nejsou vyčerpávajícím výčtem. Naznačují pouze rozsah zkoumané problematiky a vychází jak ze slovníkových definic, tak z mezinárodně používaných dokumentů např. „Definition of Cybersecurity – Gaps and overlaps in standardisation“ agentury ENISA (7, s. 44-45):

a. Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů – tato definice je zaměřena spíše na vnější možnosti bezpečnosti,
b. Schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených – tato definice spíše akcentuje vnitřní možnosti informační bezpečnosti.

Tato práce bude mít na zřeteli oba pojmy, případné odlišnosti od těchto definic, pokud to bude nutné, budou v textu reflektovány.

### 3.1.2 Legislativní ukotvení kybernetické bezpečnosti

Oblast kybernetické bezpečnosti je upravena větším množstvím právních a dalších předpisů, které často ani přímo nehovoří o kyberprostoru (7, s. 94). Týkají se ale oblasti bezpečnosti např. kritické infrastruktury, státu, obyvatel apod., případně postihů za protiprávní chování spojené s informačními technologiemi.

Část bezpečnostních pravidel a regulací není upravena na úrovni zákonů, ale mezinárodních dohod např. Úmluva o počítačové kriminalitě, známá jako Budapešťská úmluva, norem ISO 27000 (7, s. 46) o řízení bezpečnosti informací a dalších více či méně oficiálních návodů a doporučení pro zajištění bezpečnosti informací. V českém prostředí je to např. vzdělávací portál NÚKIB (57), který se ale zaměřuje hlavně na prvky kritické infrastruktury a státní organizace; propracovanou metodickou pomoc nabízí britský NCSC včetně rozšířené spolupráce s nestátními organizacemi (58).

Kybernetickou bezpečnost v České republice primárně upravuje ZKB (zákon o kybernetické bezpečnosti) a navazující prováděcí předpisy (viz § 6 ZKB). Garantem kybernetické bezpečnosti v rámci České republiky je od doby svého zřízení v roce 2017 NÚKIB (7, s. 93). Část agendy informační bezpečnosti, zvláště ve vztahu k vnitřní bezpečnosti státu, nebo např. kontroly Policie ČR, má na starosti Ministerstvo vnitra (7, s. 739). Ačkoliv obě organizace poskytují i podporu organizacím, které nespadají pod působnost ZKB a navazujících vyhlášek, nejsou, na rozdíl třeba od Velké Británie, garanty kybernetické bezpečnosti celé IT infrastruktury v daném státě. Naopak, předpisy týkající se kybernetické bezpečnosti v rámci České republiky i evropského práva primárně poukazují na prvky kritické infrastruktury a poskytovatele digitálních služeb (viz § 2 a 3 ZKB).

Trestněprávní odpovědnost, související mimo jiné s phishingem, je popsána v zákoně č. 40/2009 Sb., trestním zákoníku, konkrétně v § 230 - § 232. Odborná právnická literatura téma phishingu, malware a obecně neoprávněného přístupu do počítačových sítí (14, s. 1744) reflektuje. Právě seznamování všech částí veřejnosti, nejen odborníků, s kybernetickou bezpečností je nejnutnější prevencí negativních jevů, kam se řadí phishing a jemu obdobné techniky (6, s. 14).

### 3.1.3 Vybrané techniky kybernetické bezpečnosti

Vzhledem k široké působnosti bezpečnostních opatření, které mají zajistit jak kybernetickou, tak fyzickou bezpečnost, a které spolu často úzce souvisí, (27, s. 3), je vhodné si zmínit některé obecné postupy, které mají působit jako vodítka pro specifické způsoby obrany např. podle zaměření dané společnosti, zda se jedná o státní či soukromou organizaci apod. V případě této práce jsou tyto specifické způsoby zaměřeny na oblast phishingu, spoofingu a zajištění ochrany dat a osobních údajů zaměstnanců vybraného podniku. Vymezit kybernetickou bezpečnost v jejích praktických dopadech lze následovně (vzato podle 7, s. 411 - 424):

1. Fyzická bezpečnost – neboli zajištění prostoru, ve kterém se nachází serverovna, počítačové stanice zaměstnanců a citlivé informace využitelné k útoku. Fyzickou bezpečnost lze dále rozdělit na:
    a. Zajištění perimetru – tím se rozumí zabezpečení oblasti (místnosti, budovy), ve které se nachází chráněná aktiva (data, informace, prvky infrastruktury, počítačové stanice apod.),
    b. Kontrola přístupu – vymezuje, kdo (pracovníci IT, management, servisní technik) má k chráněným aktivům přístup a zda je přístup omezen, jestli musí zaměstnanci chodit v určitém počtu, aby nedošlo ke zneužití aktiv ze strany insidera apod. Také za jakých podmínek (jestli je třeba mít bezpečnostní prověrku, specifickou funkci, zda je třeba před vstupem kontrolovat biometrické údaje) a v jakém čase např. nemožnost přístupu do určitých chráněných částí budovy po skončení pracovní doby apod.,
    c. Vnitřní bezpečnost – ochrana před vstupem neoprávněných osob na pracoviště či do chráněných částí budovy, za jakých podmínek mohou nepovolané osoby vstupovat do zabezpečených oblastí budovy, rozmístění kamerového systému apod.,
    d. Ochrana počítačových systémů před rozebráním, úpravou či připojením periferií (USB disk) ke vstupům do systému.
2. Bezpečnost sítí a služeb – do této kategorie spadají i technické prostředky k ochraně před spamem a phishingem, vybraným metodám se bude tato práce věnovat v 4. kapitole.

Kromě tohoto dělení lze nalézt i jiné možnosti rozdělení kybernetické bezpečnosti, např. podle způsobu vniknutí do systému, podle jednotlivých ohrožených systémů, podle možností zranitelnosti skrz metody sociálního inženýrství apod. (27, s. 21).

## 3.2 Princip fungování e-mailové komunikace

E-mailová komunikace je rozlišována:

1. Z hlediska fungování v rámci protokolů,
2. Z hlediska infrastruktury.

SMTP funguje v základním nastavení na portu TCP 25 nebo na portu TCP 587 a jedná se o komunikační protokol, který zajišťuje přenos e-mailů. V okamžiku, kdy uživatel vytvoří e-mail, je odeslán na SMTP server organizace, který e-mail přepošle na další SMTP server.

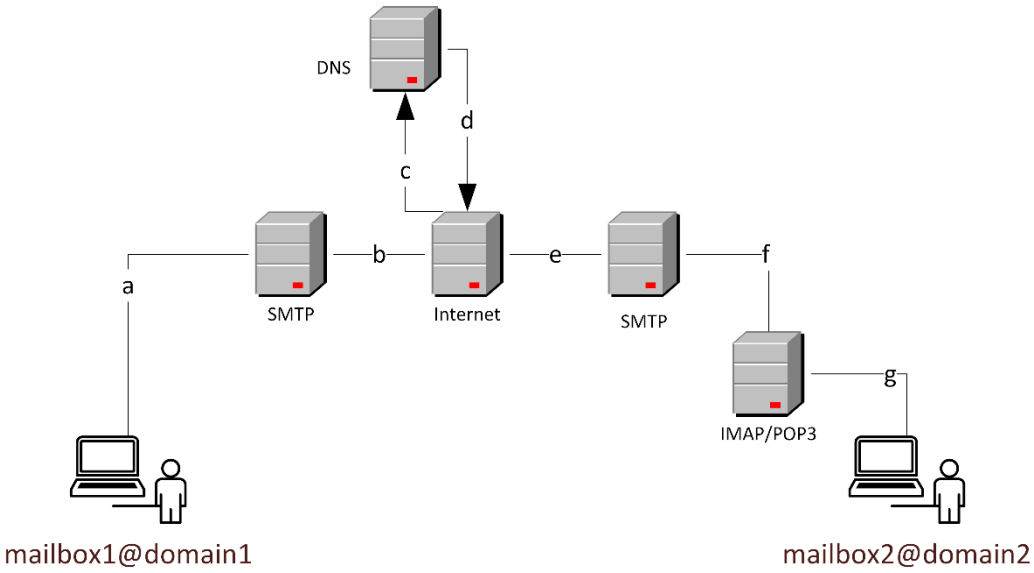
To se opakuje do momentu, než se e-mail dostane k cílovému SMTP serveru. Port TCP 587 na rozdíl od portu TCP 25 zajišťuje spolu se šifrováním TLS bezpečné odeslání zprávy (38).

POP3 neboli Post Office Protocol 3 je základní protokol aplikační vrstvy. Tento protokol využívají e-mailoví klienti k získání e-mailu ze SMTP serveru. POP3 kontaktuje SMTP server a následně si z tohoto serveru stáhne všechny e-maily. Po stažení jsou ale e-maily ze SMTP serveru odstraněny. Následně je k e-mailu možné přistupovat pouze z cílového počítače, na který byl e-mail stažen (28, s. 5).

IMAP umožňuje přístup k e-mailům z jakéhokoliv zařízení. IMAP protokol dovoluje číst e-mailové zprávy přímo ze SMTP serveru, nedochází tedy ke stažení zprávy přímo do počítače, jako je tomu v případě POP3 protokolu. Stažení e-mailové zprávy je i tak možné, ale nedochází k němu automaticky (38).

V následujícím obrázku bude znázorněna komunikace od vytvoření e-mailu až k jeho doručení (28, s. 3):

a. Uživatel domain1 napíše ve svém klientovi e-mail, který je následně zaslán na odchozí SMTP server jeho organizace. V tento okamžik server nedokáže určit, kde se domain2 nachází,
b. Odchozí server SMTP se dotáže DNS, aby zjistil IP adresu, která souvisí s domain2,
c. Výsledek z DNS serveru je odeslán zpět na SMTP server,
d. Zpráva je poslána přes internet a cestou projde přes několik dalších SMTP serverů,
e. E-mail dorazil na cílový SMTP server, který souvisí s domain2,
f. Následně je nutné e-mail přesunout ze SMTP serveru na jiný server, na kterém běží buďto POP3 nebo IMAP protokol. Tento server následně umožní příjemci přihlásit se do systému a k e-mailu přistupovat.




*Obrázek 1 - Odesílání e-mailu (upraveno podle 28, s. 3)*

## 3.3 Phishingový útok

Phishing do češtiny překládáno i jako rhybaření nebo rhybolov (6, s. 247) je možno chápat v užším smyslu jako donucení či oklamání oběti k navštívení podvodné stránky, na které oběť zadá své osobní údaje, nebo je podvodná stránka jiným způsobem získá. (6, s. 247). V širším smyslu je phishing jakékoliv jednání, které má donutit oběť jednat podle scénáře připraveného útočníkem např. dárcovské scamy, falešné e-maily předstírající osobu nadřízeného či kolegy ve firmě apod. (6, s. 247). Název „phishing“ odpovídá filozofii phishingových útoků – útočník hodí do pomyslného internetového rybníku návnadu a čeká, až se cíl útoku (ryba) chytí (18, s. 2).

Termín phishing byl poprvé použit v druhé polovině 90. let minulého století (18, s. 2). Masivní nástup phishingových útoků je spojen s využíváním platebních bran a webových obchodů, jakými jsou PayPal či eBay, na začátku tohoto století, a následně s nástupem sociálních sítí např. Facebook, Myspace, Twitter a další. Současná situace, jak je již řečeno v úvodu, naznačuje, že množství phishingových útoků neustále roste. To je v praxi usnadněno častějším využíváním vzdáleného přístupu zaměstnanců různých institucí za poslední tři roky v důsledku pandemie onemocnění COVID-19 (20, s. 324). Přes phishingové kampaně ve spojení s napadnutelným rozhraním vzdáleného přístupu se v posledních třech letech snáz šíří např. ransomware (malware, který brání uživateli ve využívání počítače např. zašifrováním dat do doby, než uživatel zaplatí výkupné, ang. ransom – od toho název) (6, s. 221) Buran, nástupce VegaLocker (21, s. 306).

Phishing jako takový je technikou tzv. sociálního inženýrství, která může být definována jako „účelová manipulace lidí s cílem přimět je k provedení určité akce nebo k vyzrazení důvěrné informace," (15, s 172), nebo „jakákoliv technika mířící k přesvědčení cíle, aby prozradil specifickou informaci či provedl specifickou akci z nezákonných důvodů" (definice ENISA, přeloženo autorem) (45). Sociální inženýrství není vždy spojeno s IT. Před nástupem osobních počítačů a využíváním internetu širokou veřejností byly techniky sociálního inženýrství častěji označovány lidově jako „podraz" neboli scam či „podvod" (fraud) (1, s. 12). Jejich podstata byla stejná, jako v případě sociálního inženýrství či konkrétněji phishingu, ale s možnostmi automatizovaného sběru informací, dostupnosti osobních údajů a anonymizací osobního kontaktu, telefonicky, e-mailem, je pole pro podvodné jednání mnohem širší (1, s. 122).

Hlavní důvody pro využití phishingu lze rozdělit do tří základních kategorií (3, s. 229):

1. Zajištění vstupu do uzavřeného systému, který poslouží ke kybernetickému útoku,
2. K získání osobních údajů a citlivých informací (hesla, přihlašovací údaje),
3. K získání informací využitelných pro další útoky.

Phishing a s ním související techniky jsou navíc velice variabilní, mohou být tzv. „šité na míru" (k tomu více u popisu jednotlivých typů útoků v této práci).

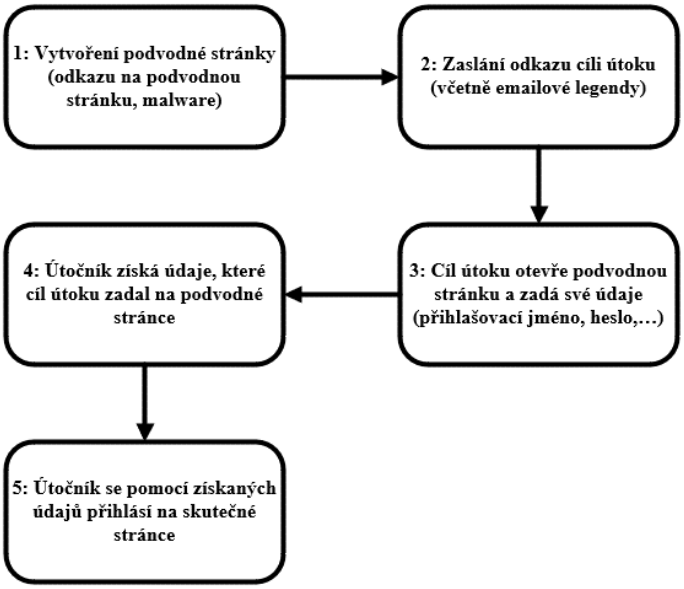
### 3.3.1 Životní cyklus phishingové útoku

Phishingové útoky se skládají ze tří základních fází (3, s. 196) (18, s. 2):

1. Získání informací (Bait neboli návnada):
    a. V této první fázi phisher získává informace o potenciálním cíli a upravuje svou strategii v závislosti na osobě, proti které plánuje útok. Zjišťuje, jaké jsou její motivace, technické zázemí, věk. Nebo v případě organizace zkoumá, jaká je firemní kultura, pokud jsou dostupné informace o vyšším managementu, zda lze využít jména a osobní údaje pracovníků, lze-li zneužít osobních údajů významných partnerů organizace apod.
2. Příslib (Hook neboli zaháčkování):
    a. Útočník v této fázi u svého útoku vytvoří pocit nutnosti kliknout na falešný odkaz. Takovou situací může být oficiálně vypadající e-mail od finanční instituce, urgentní zpráva od dodavatele zabezpečení ohledně bezpečnostní aktualizace, e-mail od vedoucího pracovníka týkající se nutnosti provedení finanční transakce apod.

3. Samotný útok (Catch neboli úlovek):
    a. Závěrečnou fází je samotný odkaz na falešnou stránku, malware obsažený na této stránce, hyperlink a další způsoby, kterými útočník získá osobní informace zamýšleného cíle na základě předchozích fází.
    b. Silnou stránkou každého phishignového útoku je obrovské množství variací, které lze použít, proto jsou výše popsané fáze pouze orientační.

Konkrétnější popis phishingového útoku lze vyjádřit následujícím jednoduchým obrázkem:




*Obrázek 2 - Popis phishingového útoku (upraveno podle 18, s. 2)*

První bod diagramu odpovídá fázi bait. Vytvořená podvodná stránka je co nejpodobnější skutečné stránce např. firemnímu účtu, stránce pojišťovny, banky apod. Druhý bod diagramu vychází z fáze bait a navazuje na fázi hook – cíl útoku musí být dostatečně znám, aby vytvořený e-mail, odkaz či obdobný způsob byly dostatečnou motivací k provedení nutných akcí, kliknutí na odkaz, zadání osobních údajů. Třetí a čtvrtý bod odpovídají fázi catch neboli provedení útoku, pátý bod je potom samotným zneužitím získaných informací podle motivace útočníka (viz kapitolu 3.3 této práce) (18, s. 2).

Alternativně lze hovořit o plánování phishingového útoku, vytváření podmínek phishingového útoku a o vlastním phishingovém útoku (6, s. 247).

### 3.3.2 Typizovaný phishingový útok

Vzhledem k personalizaci phishingových útoků např. formou spear phishingu není úplně přesné hovořit o typizovaném phishingovém útoku. Přesto jsou některé znaky a

okolnosti útoků natolik typické, že je lze celkem jednoznačně rozpoznat (6, s. 247). Pro phishing jsou nejpodstatnější tři aspekty (6, s. 247):

1. Motivace útočníka (viz část 3.3 této práce), kterých může být více, ale všechny jsou podvodným jednáním s nekalým záměrem jako zneužití osobních údajů nebo neoprávněný vstup do systému,
2. Motivace oběti tedy otevřít podvodný e-mail, kliknout na podvodný link, stáhnout infikovanou přílohu apod.),
3. Poznávací znaky útoku k rozdílu např. mezi phishingem a spoofingem (viz část 3.6 této práce).

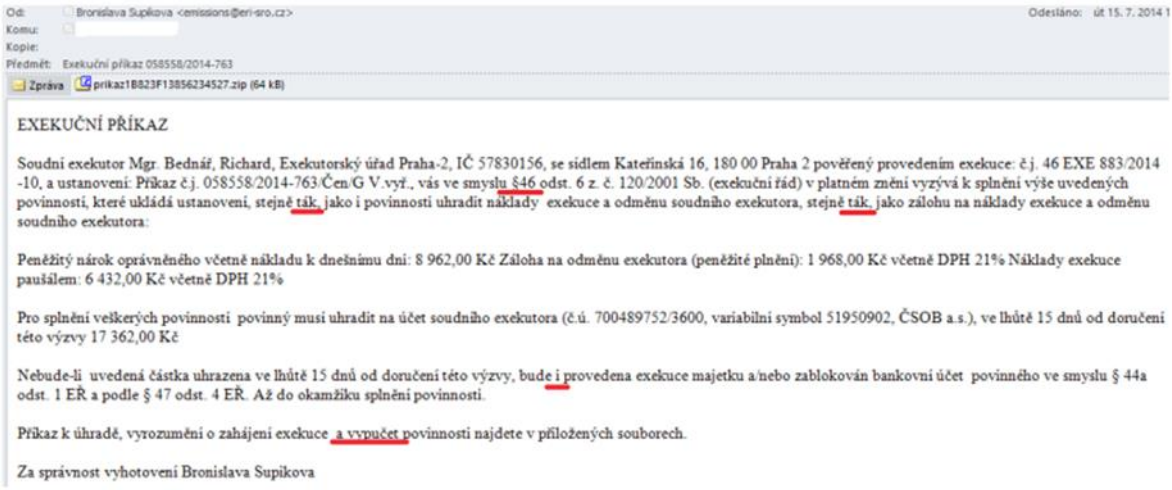
### 3.3.3 Motivace oběti

Phishing předpokládá aktivní jednání obětí, které se liší podle toho, zda se jedná o phishingu v užším, či širším smyslu (6, s. 246). Aby oběť provedla požadovanou akci, musí k ní být motivována. Následující seznam podává přehled nejobvyklejších motivací (25, s. 56). Většinou je ale motivací vícero a základem úspěšného phishingového útoku je vyvolání silné emoce – strachu, chamtivosti, překvapení, smutku, soucitu (3, s. 230):

1. Chamtivost/finanční nouze; phishingový e-mail, pokud působí přesvědčivě, může slibovat např. výhodnou půjčku, zápis do loterie apod.,
2. Strach; phisher se vydává za autoritu např. státní zaměstnanec, notář, exekutor, nadřízený, zaměstnanec IT oddělení a vytváří na oběť útoku nátlak. Typické jsou formulace typu: klikněte ihned, důležitá zpráva, Váš účet byl zneužit, zašlete znovu přihlašovací údaje apod. (3, s. 9). Nátlak může být zvýšen ve chvíli, kdy je k útoku zneužita e-mailová adresa, která působí dostatečně důvěryhodně, spolu s některými osobními údaji autority např. jméno nadřízeného zjistitelné z webových stránek, některé typické formulace v psaném textu, které phisher mohl získat z předchozí komunikace s autoritou a zneužít je proti oběti apod.,
3. Důvěřivost; oběť předpokládá, že odesílatel je důvěryhodný a spolehlivý. V Českém kontextu takto proběhlo více kampaní např. Dluh-Banka-Exekuce v roce 2014–2015, kdy ve třech vlnách přišly velkému množství osob zprávy o dluhu, následně výzva k úhradě a následně oznámení o exekuci; v přílohách těchto e-mailů byl obsažen malware (6, s. 255).

### 3.3.4 Poznávací znaky útoku

Příkladem lze využít nejtypičtější phishingový útok, se kterým se pravděpodobně setkala většina uživatelů – podvodným e-mailem, často se lze setkat i s falešnou SMS zprávou v rámci SMiShingu, nebo např. vyskakovacím oknem provedeným u určité akce, v českém kontextu se tak stalo například u kauzy Seznam – One Time Password. (3, s. 9) (6, s. 261).


Od: Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014 1
Komu:
Kopie:
Předmět: Exekuční příkaz 058558/2014-763
Zpráva prikaz1B823F13856234527.zip (64 kB)

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně tak, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně tak, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vyúčtě povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Bronislava Supikova

*Obrázek 3 - Phishingový e-mail (6, s. 252)*

Na výše uvedeném příkladu lze snadno rozpoznat typické znaky phishingové podvodné zprávy (7, s. 602):

1. Časté pravopisné chyby, zvýrazněno červeně. Včetně opakujících se slov ták, absence správné interpunkce apod.,
2. Nevhodná syntaxe. Slovní spojení „bude i provedena," absence čárek při citaci zákona apod.,
3. Nesmyslné věty, ve čtvrtém odstavci chybí kus věty, v prvním se opakuje pojem „odměna soudního exekutora",
4. Nevhodné technické prostředky. Exekuční příkaz je zasílán doporučeně poštou, nebo do datové schránky; i znalost podobných procesů či dotaz na kolegu nebo blízkou osobu může napovědět, že se nejedná o pravý exekuční příkaz,
5. Podezřelá příloha, .zip, .iso, .exe,
6. Podezřelý odkaz, jednou ze základních zásad kybernetické bezpečnosti je neotevírat odkazy zaslané e-mailem, a to i v případě, kdy vypadají jako legitimní. Důvěryhodná organizace či společnost málokdy zasílá e-mailem odkaz na stránku, kde je třeba zadat své přihlašovací údaje,

7. Zaslání oficiální zprávy, zde exekuční příkaz, ale může se jednat o falešné vyrozumění ze soudu, od finanční instituce apod., na soukromý e-mail, nebo obráceně osobně laděné zprávy na pracovní e-mail.

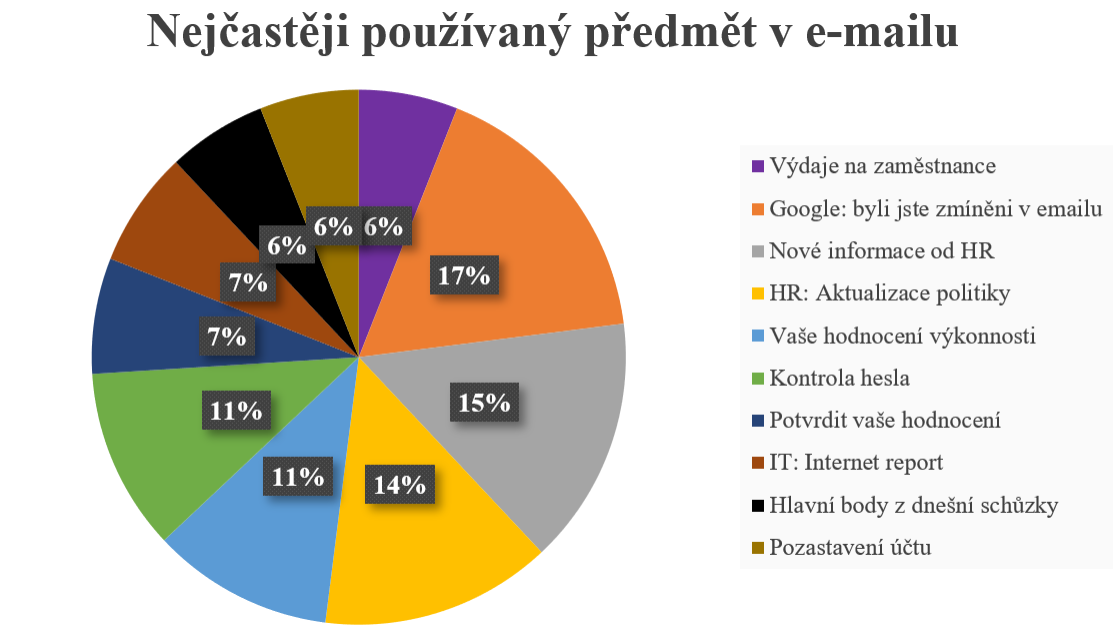
Podstatou tohoto konkrétního útoku byla snaha donutit oběť, aby otevřela přílohu obsahující malware (6, s. 253). Jiné typy útoků se zaměřují primárně na krádež osobních a přihlašovacích údajů. Odborná literatura (3, s. 243) popisuje jednoduchý e-mail, který obdrželi zaměstnanci nejmenované společnosti. Falešná adresa vypadala, že patří zaměstnanci personálního oddělení. V samotném e-mailu byl jednoduchý, krátký text s možností získat nový telefon ve firemní soutěži, pokud zaměstnanec klikne na níže přiložený, důvěryhodně se tvářící, odkaz a zadá své přihlašovací jméno a heslo do firemního intranetu.

V tomto experimentu, který vycházel z (3, s. 244):

1. Informací získaných předchozím průzkumem ve společnosti. E-mail přišel zhruba v době, kdy se na trhu objevil nový typ telefonu iPhone, většina zaměstnanců iPhone používala. E-mail přišel z důvěryhodné adresy,
2. Z primárních motivací k participaci na phishingovém útoku (touha po majetku, důvěřivost),

a který měl kontrolní vzorek necelých tisíc osob, zadalo své přihlašovací údaje skoro 75 % z nich (3, s. 244).

Aby útočníci dokázali správně zaujmout oběť pro zobrazení e-mailové zprávy, často používají podobné či opakující se e-mailové předměty, mnohdy využívající emocí obětí (1, s. 131). V kontextu vybraného podniku a útoků na zaměstnance firem může být příkladem graf, který znázorňuje procentuálně jednotlivé typy předmětů, které byly používány ve třetím čtvrtletí roku 2022. Z tohoto grafu je patrné, že až 40 % předmětů se týká lidských zdrojů.

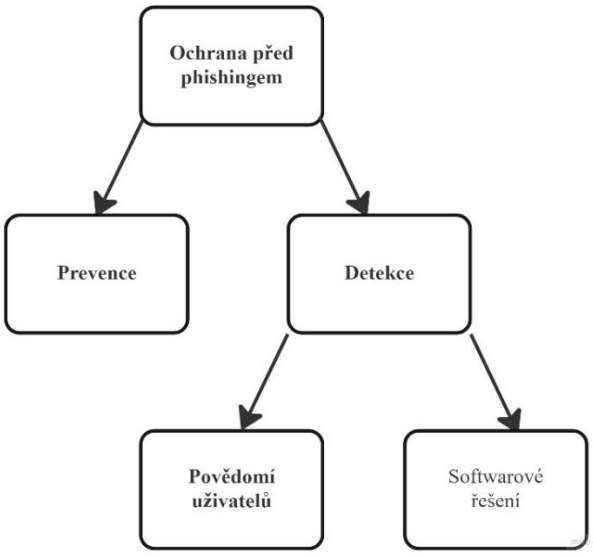



*Obrázek 4 - Nejčastěji používané předměty v e-mailu (upraveno podle 29 )*

## 3.4 Organizační aspekty ochrany před phishingem

Nejlepší obranou je prevence (18, s. 3). Toto základní pravidlo si uvědomuje nebo by si měla uvědomovat každá osoba zodpovědná za bezpečnost svěřené organizace, aktiva nebo třeba pouze soukromého firemního účtu. Prevence je základem jedné z triád kybernetické bezpečnosti (životního cyklu kybernetické bezpečnosti sestávajícího z prevence, detekce a reakce) (7, s. 45). Prevence jako taková je součástí vzdělávání zaměstnanců čili koncových uživatelů, proto jí je třeba věnovat nejvyšší pozornost u vytváření efektivních obranných metod před phishingovými útoky (viz praktickou část této práce).

Opatření proti phishingu, často nabízené jako plně automatizovaná řešení pod názvem anti-phishing, např. firmou Eset, Kaspersky či AVG, lze pro potřeby organizačních aspektů kybernetické bezpečnosti zjednodušeně shrnout následujícím obrázkem:




*Obrázek 5 - Opatření proti phishingu (upraveno podle 18, s. 3)*

Na tučně zvýrazněných pasážích u diagramu může, a měl by, zaměstnanec neboli koncový uživatel spolupracovat s oddělením IT a být seznámen s bezpečnostními řešeními. Participace uživatele je též součástí systému řízení bezpečnosti informací neboli ISMS (Information Security Management System), vycházejícím z mezinárodně uznávané normy ISO/IEC 27001 – Systém řízení bezpečnosti informací – Požadavky (7, s. 254). Normy ISMS lze aplikovat ve společnosti bez ohledu na počet zaměstnanců (22, s. 1). Potom je však třeba přizpůsobit nejlepší řešení podmínkám dané instituce či jednotlivce. Např. specifická řešení pro oblast nemocnic, finančních institucí, bezpečnostních složek, státních organizací apod.

### 3.4.1 Vzdělávání zaměstnanců

Dlouhodobé výzkumy a praktické poznatky odborníků na oblast informační bezpečnosti naznačují, že pro prevenci před phishingovými útoky je nejlepší jít příkladem a odměňovat pozornost zaměstnanců (2, s. 91). Jelikož nelze, kvůli rozdílnému stupni vzdělání, nedostatečným lidským zdrojům apod., mít každého zaměstnance dostatečně technicky zdatného v oblasti IT a kybernetické bezpečnosti, je hlavním cílem vzdělávání v oblasti prevence před kybernetickými hrozbami zvýšení základních znalostí a dovedností týkajících se kybernetické bezpečnosti. Těmi jsou např. jak rozpoznat falešný e-mail, ověřování podezřelých zpráv, reportování podezřelých e-mailů apod. (2, s. 91).

Mezi základní metody vzdělávání patří (2, s. 88-98):

1. Prezentace; toto by měli provádět experti z IT oddělení v pravidelných intervalech, přizpůsobených pro konkrétní podnik či oddělení,

2. Testování; to může být prováděno formou e-learningu s testy, případně formou edukačního phishingu nebo penetračního testování (zasíláním falešných e-mailových zpráv apod.) s následným zapracováním získaných poznatků a nedostatků do bezpečnostní politiky podniku či instituce,
3. Cvičný útok; na ten mohou být zaměstnanci připravováni, nebo může být nečekaný.

Edukační phishing a penetrační testování zaměstnanců se od sebe navzájem příliš nerozlišuje. Rozdíl je především v očekávání od hlavního cíle. Cílem edukačního phishingu je pouze vzdělání zaměstnanců, o potenciální hrozbě v podobě phishingového útoku a samotné existenci takového útoku. Zatímco penetrační testování má hlavní cíl v získání přístupu, zpronevěření či osvojení si jiného typu informací od zaměstnanců (3, s. 253-254). Veškeré metody popsané v přehledu výše mohou být samozřejmě kombinovány a nejsou vyčerpávajícím výčtem.

Vzdělávání zaměstnanců popsanými metodami by se mělo věnovat dvěma základním předpokladům úspěšné obrany před phishingovým útokem – prevenci a detekci (viz předchozí kapitolu).

#### 3.4.1.1 Detekce

Základem detekce je povědomí uživatelů o nebezpečí phishingu a rozpoznání phishingového e-mailu. V případě pochybností musí vyvolat v zaměstnancích vhodné chování, tj. informovat o potenciálně nebezpečné zprávě či příloze IT oddělení či nadřízeného pracovníka podle vnitřních předpisů organizace. Zaměstnanec by měl být seznámen s nejčastějšími podezřelými částmi e-mailu (17, s. 602):

1. Hlavička e-mailu:
    a. Od (From): zaměstnanec by měl na první pohled zkontrolovat, zda daná adresa nemá překlepy, nadbytečná čísla a zda alespoň částečně odpovídá autorovi e-mailu. Např. zda u zprávy, pod kterou je podepsaný zaměstnancův nadřízený, odpovídá jméno domény firemní doméně a nejsou v ní překlepy apod. Zároveň by si měl být zaměstnanec vědom, že hlavička e-mailu je snadno zfalšovatelná,
        i. Display name,
        ii. E-mailová adresa: Mailbox@domain.
    b. Komu (To): zda nebyl e-mail rozeslán hromadně,

c. Předmět (Subject): Zda je předmět srozumitelný. Zvážit svou reakci v případě neznámého odesílatele, u kterého chybí název předmětu apod.,
d. Zobrazení celé hlavičky e-mailu; toto opatření může být pro technicky méně zdatné zaměstnance méně příjemné, ale umožní lépe rozpoznat případnou falešnou zprávu (7, s. 603).

2. Tělo e-mailu:
   a. Obsahuje čistý text zprávy, hypertextové odkazy, obrázky a html styling,
   b. Před každým kliknutím na link, by si měl zaměstnanec zkontrolovat, kam link odkazuje,
   c. Ověřit, zda nejsou ve zprávě evidentní nesrovnalosti jako např. chybná gramatika, nesmyslné věty a neodpovídající logo,
   d. Je-li v těle digitální podpis, nejlépe zaručený či uznávaný. Ten totiž zvyšuje míru autenticity přijaté zprávy (7, s. 476).
3. Příloha:
   a. V jakém formátu je příloha (apriorně neotevírat žádnou přílohu s koncovkou .exe, .iso apod.),
   b. Pokud není odesílatel zprávy či zpráva důvěryhodná, tak přílohu neotevírat (7, s. 154).

Praktické způsoby seznámení s těmito pravidly budou rozvedeny v další části této práce.

#### 3.4.1.2 Prevence

Prevencí je v kontextu vzdělávání zaměstnanců jak obecně preventivní chování ve vztahu ke kybernetické bezpečnosti, jako např. dodržování doporučené délky a síly hesla, nezadávání osobních údajů na podezřelých stránkách, nevyužívání firemní počítačové stanice k soukromým aktivitám apod., tak školení v oblasti kybernetické bezpečnosti. Toto by mělo probíhat ze strany managementu a oddělení IT či smluvního dodavatele zajišťujícího informační bezpečnost (4, s. 289-290).

Součástí prevence je mimo jiné dostatečná komunikace mezi všemi zaměstnanci (2, s. 88–98):

1. Mezi jednotlivými zaměstnanci na stejných pozicích např. přijde-li podezřelá zpráva s podpisem kolegy, je vhodné se na něj obrátit,

2. Mezi podřízenými a nadřízenými. V případě urgentní zprávy či okamžité nutnosti splnit úkol, který si zaměstnanec vyhodnotí jako potenciální pokus o spoofing či phishing, musí mezi podřízeným a nadřízeným existovat elementární důvěra. V opačném případě může být, např. ze strachu z kázeňského postihu, podřízený motivován k vyplnění požadavku v jinak podezřelé zprávě),
3. Mezi zaměstnanci a IT oddělením.

Důležitý je též systém reportování problematických či podezřelých zpráv – ten musí být jednoduchý, rychlý a dostupný (řešení bude představeno v praktické části této práce). V opačném případě zaměstnanec může ztratit motivaci případné bezpečnostní incidenty nahlašovat a riziko úspěšného phishingového útoku se tak zvýší (1, s. 115).

Jedním z předpokladů úspěšného reportování je individuální řešení jednotlivých incidentů – díky němu získává zaměstnanec zpětnou vazbu a povzbuzení k dalšímu preventivnímu chování, jakož i motivaci pokračovat v dobré praxi. Možným řešením je vyčlenění jedné až dvou osob v rámci stávajícího týmu či týmů IT, podle velikosti podniku či instituce, které se budou věnovat jen reportu, řešení bezpečnostních incidentů a vzdělávání zaměstnanců v této oblasti, nebo vyčlenění specifické pozice/oddělení (25, s. 2).

## 3.5 Technické aspekty ochrany před phishingem

Technickými aspekty se rozumí protokoly, software a podobné prostředky ochrany před nevyžádanými e-maily a odkazy. Tyto fungují bez aktivního zasahování ze strany běžného uživatele a jejich praktické aspekty budou dále zmíněny v praktické části této práce. Primárním rozdílem mezi organizačními opatřeními, které naopak závisí na participaci jednotlivých uživatelů, jsou technické aspekty ochrany automatizovány a pro běžného uživatele neviditelné. Zároveň platí, že jsou tyto aspekty schopny zmírnit následky případných útoků (16, s. 201). Pro úplnost je třeba uvést ty nejvýznamnější z nich, které jsou nejpodstatnější pro zajištění bezpečnosti jak obecně, tak konkrétně v případě vybraného podniku. Zvláštní pozornost práce věnuje konkrétnímu obrannému nástroji, a to systému Microsoft 365 Defender, ve kterém jsou realizována obranná opatření (k tomu viz metodiku a praktickou část této práce).

### 3.5.1 Obranné nástroje

Vzhledem k již zavedenému způsobu kybernetické bezpečnosti ve vybraném podniku a nutnosti přizpůsobit se těmto postupům je v práci zvolen jako výchozí obranný nástroj a primární způsob ochrany **Microsoft 365 Defender** (k tomuto omezení viz kap. 5).

#### 3.5.1.1 Microsoft 365 Defender

Microsoft 365 Defender, primární nástroj pro kontrolu a ochranu vybraného podniku (jak je dále popsáno v praktické části), je integrovaný ochranný systém, který nabízí nativní ochranu kancelářského balíku Microsoft Office (39). Podle požadavků na úroveň kybernetické bezpečnosti a oblasti ochrany je Defender možno dělit podle funkcionalit a oblasti ochrany (39). V této práci jsou nejpodstatnější funkce Microsoft Defender for Endpoint (zaměřené na jednotlivé koncové uživatele, tedy zaměstnance a klíčové zaměstnance vybraného podniku, kdy toto řešení je jak preventivní ochranou před kybernetickými útoky, tak ho lze využít k rozpoznání úspěšného útoku a adekvátní reakce na něj) (39) a Microsoft Defender for Office 365 (zvláště u automatického rozpoznávání spamu, phishingových e-mailů a hyperlinků na falešné stránky, jak je popsáno v této kapitole dále, a simulovaných phishingových útoků, jak je popsáno v praktické části této práce).

Jednou z výhod Microsoft 365 Defender pro ochranná opatření v rámci firem je širší podpora firmy Microsoft, která sdružuje komunitu vývojářů, expertů na kybernetickou bezpečnost a uživatelů, a pravidelné informování uživatelů o novinkách u tohoto produktu včetně možnosti dalšího vzdělávání (47).

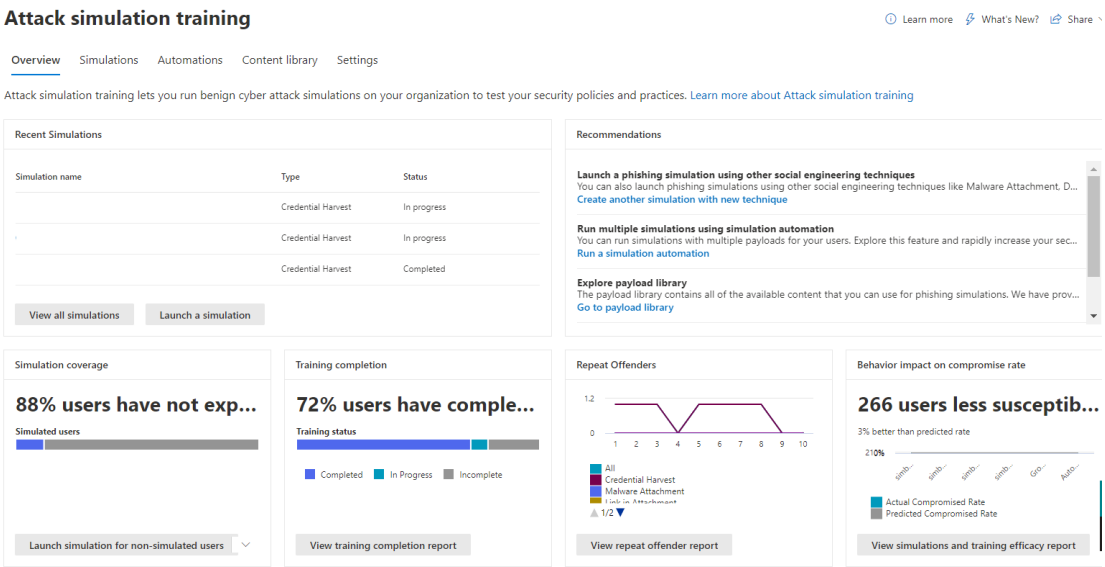
**Attack Simulation Training**

Jednou z největších výhod Microsoft Defender je možnost vytvoření simulovaného útoku, který prověří bezpečnost podniku, připravenost zaměstnanců a odhalí případné bezpečnostní problémy. Simulované útoky mohou využít následujících metod sociálního inženýrství, jak je dále popsáno v praktické části této práce (seznam není vyčerpávající) (46):

1. Credential Harvest (sběr hesel) – útočník zašle oběti zprávu obsahující URL na falešnou stránku, která si vyžádá přístupové jméno a heslo oběti. Daná stránka je co nejpodobnější některé z obecně známých a využívaných webových stránek (více v kapitole 4 této práce);

2. Malware Attachment (příloha se škodlivým kódem) – útočník zašle oběti přílohu, která po otevření spustí na počítači oběti libovolný kód (např. makro), jež útočníkovi umožní lépe zaútočit, nebo je rovnou škodlivý;
3. Link in Attachment (odkaz v příloze) – URL na škodlivou stránku je obsaženo v příloze e-mailové zprávy. Tato škodlivá stránka, podobně jako u techniky Credential Harvest, má nejčastěji podobu okna, do kterého oběť zadá své přihlašovací údaje a heslo.

V rámci vytvoření simulovaného útoku poskytuje Microsoft Defender rozsáhlý výběr falešných webových stránek pro potřeby simulace (46).



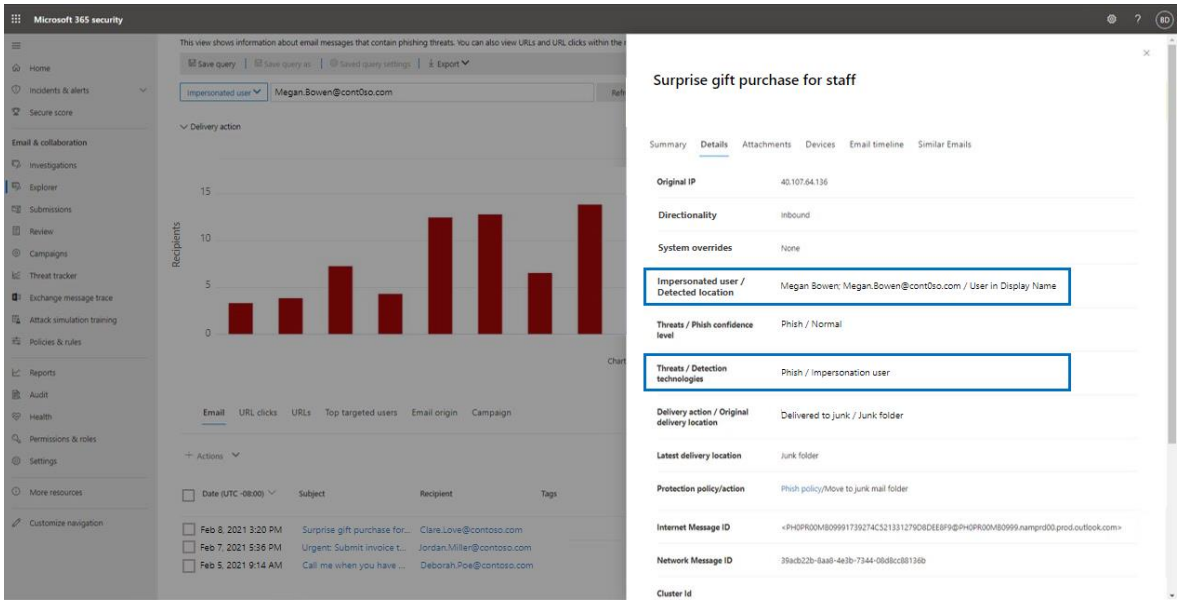

*Obrázek 6 - Příklad Attack Simulation Training v prostředí vybrané společnosti*

## Threat Explorer

Jednou z podstatných částí Microsoft Defender je funkcionalita Threat Explorer. Ta umožňuje např. (52):

1. Zkoumat malware detekovaný dalšími bezpečnostními funkcemi Microsoft Defender,
2. Zobrazení URL adresy, která byla součástí phishingového útoku,
3. Automatizaci detekce a reakce na různé druhy bezpečnostních incidentů,
4. Zkoumání škodlivé e-mailové komunikace.

Tyto možnost jsou v praktické rovině rozebrány v následující části práce.




*Obrázek 7 - příklad užití Threat Explorer (52)*

**Doporučená nastavení pro Defender**

Praktická část této práce (konkrétně kapitola 4.4.1.3) vychází z nativního doporučeného nastavení Microsoft Defender, optimalizovaného pro využití všech potřebných funkcionalit Defenderu (anti-phishing a anti-spam kampaň) (53).

### 3.5.2 Internetové standardy pro ověřování e-mailových zpráv

V následujících podkapitolách jsou popsány nejdůležitější standardy internetové komunikace.

#### 3.5.2.1 DKIM

DKIM neboli DomainKeys Identified Mail je protokolem, který verifikuje odesílatele zprávy, doménu, ze které byl odeslán, i obsah e-mailu, jakož i to, že e-mail nebyl po odeslání modifikován třetí stranou (4, s. 226). DKIM umožňuje rozpoznat doménu, ze které byl e-mail skutečně odeslán. DKIM funguje na principu asymetrické kryptografie – odeslání e-mailu MTA, který do všech odesílaných e-mailů vloží digitální podpis. Ten server vytvoří na základě soukromého klíče a hashe e-mailu (hlaviček i těla). Digitální podpis je do e-mailu uložen jako nová hlavička jménem DKIM-Signature. Pojem hash znamená, že se e-mail před odesláním jednosměrně (z hashe nelze získat zpětně podobu soukromého klíče, ani obsah e-mailové korespondence) zašifruje, přičemž výsledkem je krátký shluk písmen a číslic. Tento řetězec lze využít k ověření pravosti odesílané zprávy, hash tedy slouží jako otisk původního e-mailu. V případě změny e-mailu by neodpovídal hash (4, s. 229).

Zmíněný digitální podpis je u příjemce verifikován serverem pomocí tzv. veřejného klíče, z nějž si vytvoří vlastní hash a ten následně porovná s hashem e-mailu. Veřejný klíč si server stáhne z DNS domény, kde je vložen v TXT záznamu (4, s. 230).

### 3.5.3 SPF

SPF čili Sender Policy Framework je formou e-mailové autentifikace, zaměřené podobně jako DKIM na ochranu před spamem, tedy jakákoliv nevyžádaná pošta, většinou hromadná a obtěžujícího charakteru, spoofingem a phishingem. Umožňuje přidat záznam SPF do DNS, čímž vytváří seznam ověřených odesílatelů, kteří mohou posílat e-maily z dané domény (25, s. 185). Server příjemce e-mailové zprávy tak může ověřit, zda daný odesílatel má povolení zasílat zprávy přes odesílatelovu doménu. Výsledkem tedy je, že SPF spojuje odesílatele domény s konkrétní IP adresou, ze které byl daný e-mail odeslán. Lze tedy říci, že zatímco DKIM ověřuje, zda nebyl e-mail pozměněn, SPF potvrzuje, že daná zpráva skutečně byla poslána z domény patřící legitimnímu odesílateli (25, s. 186).

### 3.5.4 DMARC

DMARC neboli Domain-based Message Authentication, Reporting and Conformance sytém rozšiřuje a doplňuje existující techniky SPF a DKIM, které provádí ověření domény e-mailů, ale neobsahují možnost sdělit příjemci, jak se má chovat ke zprávám, kde ověření selže (25, s. 186). Také nemají možnost informovat majitele domény, jak bylo naloženo s přijatými zprávami, což naopak DMARC umožňuje. V případě, že zpráva neprojde SPF a DKIM, mohou nastat tři akce podle nastavení DMARC (25, s. 187):

1. E-mail se k příjemci nedostane,
2. E-mail se přesune do virtuálního prostředí, kde je spuštěn a otestován na přítomnost škodlivého obsahu,
3. E-mail se dostane k příjemci.

Zároveň DMARC umožňuje správci domény kontrolovat, kdo z ní zasílá zprávy, kolik zpráv z domény odchází a jakým způsobem jsou zprávy vyhodnocovány na straně příjemce.

### 3.5.5 Další způsoby zabezpečení

Pro úplnost jsou dále zmíněny navazující a doplňující způsoby ochrany vybraného podniku, které lze ale vztáhnout na kybernetickou bezpečnosti obecně.

#### 3.5.5.1 Vícefaktorové ověření

Vícefázové ověření (multi-factor authentication) slouží k ověření identity osoby, která se chce přihlásit na webové stránce či v aplikaci (26, s. 4). Využívá principu vícefázového ověření, tedy kombinace alespoň dvou pověření ze tří následujících při každém pokusu o přihlášení (26, s. 5):

1. Něco, co vím (PIN, heslo, ID),
2. Něco, co mám (token, jednorázově vygenerované heslo),
3. Něco, co jsem (biometrický údaj, například otisk prstu).

Tento způsob ověřování i v případě, kdy útočník odcizí přihlašovací údaje oběti, zajišťuje další možnost zabezpečení a chrání před nepovolaným přístupem do systému.

#### 3.5.5.2 Spam filter

Spamový filtr je pravděpodobně nejzákladnější e-mailovou ochranou, kterou může organizace využívat. Filtr spamu je využíván k rozeznávání nevyžádané pošty jako reklamní akce, hromadné e-maily apod., kdy poté, co je e-mail rozezná jako spam nebo ho za spam označí, provede určitou akci. Ta může spočívat v (25, s. 64):

1. Smazání zprávy,
2. Přesunu zprávy do složky Nevyžádaná pošta/spam. V závislosti na nastavení spam filtru,
3. Odeslání nevyžádané pošty na jinou e-mailovou adresu.

Aby filtry spamu správně fungovaly, musí být správně nakonfigurovány. Nejlépe tak, aby veškerá pošta, kterou spam filter jako spam vyhodnotí, rovnou nebyla smazána. Filtry fungují na základě různých způsobů filtrování spamu, například (25, s. 65):

1. Content filter – jako spam označuje takové zprávy, které obsahují určitá slovní spojení, často užitá vícekrát v rámci jedné zprávy, například „Úžasná sleva," „Skvělá nabídka" apod.,
2. Blacklist filter – jako spam jsou označeny zprávy od těch odesílatelů, kteří jsou na listině nevyžádaných odesílatelů zpráv,
3. Bayesian filter – jako spam jsou označeny ty zprávy, které nejčastěji samy označujeme za spam. Např. od určitých odesílatelů, s určitými slovními spojeními, v určitém jazyce apod. Tento filtr vychází z Bayesova teorému.

#### 3.5.5.3 Filtrování příloh

Jedním z dalších způsobů, jak zabránit, aby zaměstnanci nebyl doručen škodlivý soubor, je využití techniky attachment filtering. Tato technika funguje na principu zablokování předem definovaných typů souborů. Je velmi důležité si předem definovat, jaké soubory se využívají pro škodlivé účely, a hlavně, jaké soubory je možné ve firmě zablokovat. Mezi nejzákladnější a běžně blokované koncovky patří: .exe (Executable), .vbs (Visual Basic Script), .js (JavaScript), .ps (PowerShell Scripts) (28, s. 61).

## 3.6 Další techniky sociálního inženýrství

Některé další techniky s phishingem úzce souvisí, jsou s ním komplementární, nebo se využívají na základě informací získaných phishingem (viz předchozí kapitoly). V některých případech, například u spear phishingu, lze popsané techniky chápat jako podskupiny phishingu (6, s. 246).

Pro úplnost rozebírané problematiky budou zmíněny některé případné rozdíly. Spojujícími prvky níže popsaných technik, velmi podobných či přímo totožných jako u obecně phishingového útoku, lze definovat následovně (6, s. 246):

1. Donucení cíle zadat na podvodné stránce své osobní informace, nebo je jiným způsobem odhalit,
2. Kompromitace organizace či jednotlivce pomocí falešné webové stránky,
3. Vytvoření falešné identity útočníka. Nejčastěji významné osoby či instituce, např. bankovního ústavu, firemního vedení apod.

Phishing, jak je popsáno dále, je úzce spojen se spoofingem (48), jehož nejvýznamnější varianty jsou v kapitole dále popsány. Kromě níže uvedeného výčtu jednotlivých technik lze na příbuzné phishingové techniky nahlížet přes tzv. bezpečnostní vektor (3, s. 9), který hovoří o sociálním inženýrství v negativním smyslu, s cílem poškodit cíl. Ten dělí tyto techniky primárně na SMiShing, vishing, phishing a krádež identity. Kam by se řadil i spoofing (3, s. 10), tedy spíše podle média použitého k podvodnému jednání (SMS, telefon, e-mail a doména).

### 3.6.1 Spear phishing

Spear phishing, též rybaření oštěpem či rhybaření oštěpem, je cílenější metodou phishingu, která využívá dříve získané informace o cíli útoku. Využívá důvěrných informací

o cíli, detailnější znalosti organizační struktury společnosti, které je cíl zaměstnancem,[1] a/nebo cílí na konkrétní informace, které chce získat. Např. duševní vlastnictví, utajované informace (6, s. 264). U spear phishingu cíl méně často odhalí, že se jedná či může jednat o útočníka, a méně prověřuje útočníkovy zprávy a požadavky (6, s. 265). Primárním rozdílem oproti phishingu je tedy personalizace a zamíření útoku vůči konkrétnímu cíli.

Spear phishing souvisí též se zneužitím konkrétní domény, nejčastěji patřící společnosti, u které cíl útoku pracuje. Cíl útoku tak častěji ztrácí obezřetnost, protože považuje danou zprávu za důvěryhodnou (9, s. 116).

### 3.6.2 Vishing

Vishing je podmnožinou phishingových útoků. Jedná se v podstatě o telefonický phishing, při kterém je cílem útoku získat osobní informace na základě falešné identity útočníka, který při telefonickém hovoru od cíle útoku tyto informace požaduje (6, s. 265. Typický příklad: útočník se představí jako zástupce banky s nesrovnalostí při transakci či vedení účtu, po cíli požaduje informace pro „ověření identity“ cíle. Např. datum narození, číslo občanského průkazu. Tyto informace může zneužít při dalším, cílenějším útoku (viz spear phishing výše).

Vishing se využívá primárně pro (3, s. 233):

1. Sběr hesel (Credential harvesting),
2. Zpravodajství z otevřených zdrojů (OSINT),[2]
3. Kompromitaci cíle.

Vishing využívá nejčastěji technologie VOIP (jak kvůli nižším nákladům pro podvodné jednání, tak horší možnosti vystopování podvodného jednání).

### 3.6.3 SMiShing

Také smishing, složeno ze slov SMS a phishing (6, s. 266). Jedná se o podobnou techniku, jakou je vishing, ale namísto telefonního hovoru je využito zaslání SMS. Tedy krátké textové zprávy. Tato technika spočívá v zaslání krátké, oficiálně vypadající zprávy nejčastěji od finanční či podobné instituce s falešným odkazem, často zkráceným. Většina uživatelů telefonních zařízení odkazy otevře bez předchozí kontroly.

[1] Pod pojmem zaměstnanec se v této práci rozumí i dodavatelé vázaní smlouvou a další osoby, které se podílí na ochraně a chodu organizace.
[2] OSINT (Open-Source Intelligence) – Shromažďování informací o osobě či organizaci z veřejně dostupných zdrojů jako například noviny, webové stránky, sociální média, knihy (54).

Vzestup SMiShingu souvisí s politikou BYOD[3], zde je myšlen vlastní mobilní telefon, který nemusí být dostatečně zabezpečen u velkého množství firem (3, s. 240). Úspěšný SMiShing závisí na (3, s. 242):

1. Krátkosti textové zprávy,
2. URL cílové podvodné stránky. Resp. na tom, aby daný odkaz nevypadal na první pohled podezřele,
3. Co nejmenším množství úkonů, které musí cíl útoku podniknout.

### 3.6.4 Whaling

Jedná se o jednu z variant phishingu, velice podobnou spear phishingu. Dala by se přeložit jako „lov velryb," nebo novotvarem „velrybaření." Název naznačuje, že na rozdíl od pouhého „rhybaření" se zde jedná o útok na vysoce postavené osoby, manažery a další pozice, nikoliv na pouhé „ryby," ale na „velryby." Whalingový útok je co nejosobnější, využívá předchozích poznatků získaných dalšími technikami sociálního inženýrství či z jiných zdrojů a často je koncipován jako urgentní zpráva od jiné vysoce postavené osoby např. obchodního partnera (17, s. 603).

### 3.6.5 Pharming

Jde o složeninu slov „farming" (farmaření) a „phreaking" (nezákonné napojení se na cizí telefonní linku a její využívání) (6, s. 263). Pharming je specifickou metodou phishingu, která spočívá ve dvou možných variantách útoku (6, s. 263):

1. Útok na DNS server; doménové jméno je zde přeloženo na IP adresu, a ve chvíli, kdy uživatel zadá adresu originálního serveru, je přesměrován na adresu falešnou,
2. Napadení počítače koncového uživatele pomocí malware, který přesměruje uživatele při zadání IP adresy na stránku podvodnou.

### 3.6.6 Catphishing a catfishing

Technika spočívá ve vytvoření falešného profilu na sociálních sítích a následného spojení se zamýšleným cílem útoku (19, s. 199). Vzhledem k anonymitě komunikace a vytvoření pocitu konformity a spojení může útočník využít emocionálního obsahu komunikace, např. na různých seznamovacích fórech a zamýšlený cíl bývá k útoku méně

[3] BYOD (Bring Your Own Device) neboli přineste si své vlastní zařízení. Znamená, že si zaměstnanec může přinést své vlastní zařízení do firmy.

opatrný. V extrémních případech může cíl prozradit důvěrné informace téměř bez nátlaku – kuriózním případem je únik informací na fóru k počítačové hře World of Tanks, kdy jeden z uživatelů poskytl tajné informace o jednom z tanků bez důraznějšího nátlaku (50).

Catfishing je spojen s prostředím seznamovacích aplikací a fór a zaměřením se na získání finančního obnosu od cíle. Catphishing se soustřeďuje na zisk informací (19, s. 199).

### 3.6.7 Watering hole phishing

Tato technika se zaměřuje převážně na společnosti. Útočník lokalizuje ty webové stránky, které zaměstnanci společnosti nejčastěji navštěvují, a infikuje je pomocí automaticky stažitelného malware. Ten následně umožňuje útočníkovi jednoduchý přístup k osobním údajům, utajovaným informacím, nebo například obchodním tajemstvím (23). Jedná se o agresivnější phishingovou techniku (19, s. 213), jejíž jméno je odvozeno od napajedla (waterhole). Podobně jako u ostatních názvů, které jsou spojeny s rybařením či říší zvířat, vychází tato technika z toho, že cíle útoku, podobně jako zvířata, chodí k jednomu napajedlu, kde na ně číhá útočník (predátor).

### 3.6.8 Clone phishing

Princip této techniky spočívá v odeslání e-mailu identického se skutečným, ne-phishingovým e-mailem. Podvodný e-mail je odeslán po skutečném, z e-mailové adresy, která na první pohled působí důvěryhodně a cíl útoku, vzhledem k tomu, že před krátkou dobou obdržel od téměř totožné adresy stejný e-mail, nemusí pojmout podezření. Podvodný e-mail většinou obsahuje vysvětlení či omluvu v tom smyslu, že linky z předchozí zprávy nemusí správně pracovat, došlo k drobné chybě apod. Nový, podvodný e-mail má v přílohách malware, nebo při otevření odkazu dostane cíl útoku na falešnou stránku (23). Pro automatizaci této (i většiny výše uvedených) technik slouží v rámci PEN testování tzv. SET – Social Engineering Toolkit (Souprava sociálního inženýrství), vyvinutý Davidem Kennedym (3, s. 59) a jednoduše využitelný v rámci „etického hackingu.“[4]

### 3.6.9 Typo Squatting

Jedná se o další typ útoku sociálního inženýrství, který využívá překlepů v doméně, aby tato vypadala co nejpodobněji té, na kterou se útočník zaměřil (nejčastěji se jedná o známé firmy či instituce). Oběť má uvěřit tomu, že se jedná o legitimní stránku, kdy útočník

[4] The Social-Engineer Toolkit (SET) je souprava sociálního inženýrství (dostupná z 55).

využívá doménu velmi obdobnou; útočník si proto koupí doménu velmi podobnou té, na kterou zaměřuje svůj útok. Relativní podobnost může navodit například vynecháním písmena, jména domény (například namísto .cz .eu) či záměrného překlepu, útočník tím získá platnou doménu a zvýší svou šanci tím, že pakliže oběť na tuto stránku narazí, ať již náhodně nebo přes nějaký odkaz v e-mailu, nemusí si všimnout, že se jedná o doménu podvrženou. Typo označuje drobné chyby, kterých se lidé mohou dopustit při psaní na klávesnici (6, s. 326).

### 3.6.10 Homograph Attack

Přestože se jedná o velmi starý typ útoku, stále proti homografickému útoku neexistuje ideální obrana. Pro uživatele je prakticky nemožné odhalit, že doménové jméno není v pořádku. Útok zneužívá situace, existence mnoha různých znaků působících stejným dojmem. Je to způsobeno tím, že je možné při registraci domény využít IDN (národní) znaky. Díky IDN lze vytvořit doménové jméno nejen pomocí ASCII[5] znaků, ale i za pomoci jakéhokoliv Unicode[6] znaku. Unicode má pro každý znak (i když na první pohled velmi podobný) jiný kód, proto „o“ v latince a „o“ psané v cyrilici mají odlišný kód. Nicméně uživatel „o“ psané cyrilicí vidí úplně stejně, jako kdyby se jednalo o „o“ napsané v latince. Právě toho mohou útočníci velmi jednoduše zneužít a například namísto webové stránky PayPal vytvořit stránku PayPaI. Oběť by pro identifikaci musela adresu překopírovat do textového editoru, ve kterém je již tento rozdíl snadno rozpoznatelný (16, s. 33). Typickým příkladem u předchozího použití této techniky může být název g00gle.com (použití nul namísto písmena o), goog1e, googIe (číslice 1 a velkého písmena I namísto písmena l apod.) (16, s. 33).

### 3.6.11 Využití subdomény

Pokud si útočník zaregistruje jakoukoliv doménu, může si velice snadno udělat jakoukoliv subdoménu, protože ty se již neregistrují. Proto mohou vzniknout i takové domény jako www.google.xyz.cz. Pro nepozorného uživatele by se tento na první pohled mohlo jevit jako legitimní e-mail (28, s. 31).

[5] ASCII neboli American Standard Code. Tabulka, která převádí znaky na čísla.
[6] Unicode – Jedná se o mezinárodně definovanou normu v kódování znaků (56).

### 3.6.12 Spoofing

Obecně je spoofingem jakákoliv činnost, při které útočník předstírá, že je jinou osobou nebo falšuje stránku, IP adresu apod., aby uvedl svůj cíl v omyl a nezákonně získal informace, či vstup do systému. Přičemž nejdůležitější je právě vytvoření falešné identity (16, s. 37). Typickým příkladem je zaslání odkazu na podvodnou stránku z oficiálně vypadající e-mailové adresy, kde je změna oproti oficiální adrese napodobené osoby či instituce na první pohled těžko rozpoznatelná a v některých případech vůbec (16, s. 37).

Kromě výše uvedené obecné definice existuje pro spoofing více důvodů, které mohou být analogické s cíli phishingu, např (16, s. 37).:

1. Krádež identity; kdy útočník získá od cíle útoku dostatek informací, aby se za něj mohl vydávat,
2. Šíření malware,
3. Poškození dobrého jména společnosti či jednotlivce pomocí získaných osobních údajů,
4. Možnost útoků MitM (Man-in-the-middle) neboli útok, při kterém je předpokládána komunikace mezi dvěma stranami narušena prostředníkem, který má k zasílaným informacím přístup, nebo komunikaci aktivně ovlivňuje.

### 3.6.13 Domain spoofing

Domain spoofingem se rozumí vytvoření velice přesvědčivé falešné stránky či e-mailové domény, která má za cíl oklamat cíl útoku (uživatele, zaměstnance apod.). Falešná doména musí být co nejpřesvědčivější, a protože lze majitele domény v případě webových stránek zjistit, v prostředí českého internetu například na stránkách správce domény .cz www.nic.cz, obecněji velkým množstvím volně přístupných stránek, je třeba, aby stránka nevyvolávala na první pohled podezření (3, s. 42).

Domain spoofing se dělí na tři základní typy útoků (3, s. 42):

1. E-mail spoofing – oběť útoku obdrží e-mailovou zprávu od známé osoby, firmy či instituce (přítel, kolega, státní správa). Tato zpráva ale obsahuje malware či odkaz na falešnou stránku,
2. Website spoofing – útočník (spoofer) vytvoří webovou stránku se vzhledem a názvem domény co nejpodobnějším ověřené, legitimní a oblíbené stránce např. namísto linkedln.com stránku linkedin.com. Následně rozešle odkaz na tuto stránku, která sbírá přihlašovací údaje, obsahuje škodlivý software apod.,

3. DNS Poisoning také Domain Name System poisoning – u tohoto typu útoku je oběť při kliknutí na skutečný odkaz přesměrována na jinou webovou stránku, než kterou původně otevřela.

## 3.7 Trendy a výzvy v oblasti kybernetické bezpečnosti

Podvodníci se v jednotlivých praktikách kybernetických útoků stále více zlepšují. Čím propracovanější technika a dlouhá příprava, tím se zvětšuje šance útočníku na úspěch a zisk, a to i vzhledem k tomu, že závislost všech složek společnosti na virtuálním prostředí se neustále zvyšuje (6, s. 181).

Že se phishingové útoky podvodníků stále zdokonalují, potvrzuje i společnost AEC, která se dlouhodobě zabývá informační bezpečností. Útočníci dokáží s téměř dokonalou přesností imitovat jakýkoli oficiální e-mail a problém jim nedělá ani grafická podoba e-mailů (34), což je oproti minulosti (viz příklad v kapitole 3.3.4) o to více signifikantní.

Společnost ESET publikovala zprávu, ve které uvádí trendy a výzvy v kybernetické bezpečnosti v roce 2023, přičemž těmto problémům se věnují i průběžné zprávy NÚKIB a česká legislativa (7, s. 79). Jedná se především o (35):

1. Nárůst kyberkriminality,
2. Nedostatek odborníků,
3. Práce na dálku a hybridní práce, při které musí firmy věnovat kybernetické bezpečnosti větší pozornost,
4. Růst dark webu a s tím související trestné činnosti,
5. Stále nové metody a taktiky kyberkriminality,
6. Zvýšení počet útoků v rámci ransomwaru,
7. Zlepšit vzdělanost a informovanost. Zaměstnanci firem představují nejslabší článek kybernetické obrany.

Z průzkumu realizovaného v roce 2022, který si nechala vypracovat společnost Sophos, celosvětový lídr v řešení kybernetického zabezpečení, vyplývá, že až 85 % vedoucích pracovníků z českých firem narazilo ve své práci na spam nebo podezřelé zprávy, které jim přišly do e-mailu. S phishingem se setkalo 60 % manažerů, kdy se podvodníci snažili získat jejich přihlašovací údaje. Ve velkých organizacích s vyšším počtem zaměstnanců než 100 pak toto číslo představuje až 64 %. Přičemž se podvodníci nejvíce zaměřují na získání citlivých dat od top managementu (76 %), marketingových ředitelů (75 %) a HR manažerů (67 %).

Klíčovými faktory, jak takovému jednání zamezit, je dostatečná kybernetická hygiena,[7] a především vzdělanost v této oblasti. Z průzkumu také vyplynulo, že 58 % vedoucích pracovníků v českých firmách z jiných oddělení než IT, nebyli proškoleni v oblasti kybernetické bezpečnosti (36).

Každých 10 sekund je uskutečněn ransomware útok na nějakou společnost. Každý den je vytvořeno 300 000 nových druhů malware a z 91 % stojí za kybernetickým útokem e-mail (37). Všechna tato čísla, doplněná o vstupní informace z úvodu této práce, mají za cíl opakovaně doložit nutnost dostatečné kybernetické bezpečnosti a preventivních opatření.

[7] Kybernetická hygiena značí činnosti, pomocí kterých jsme schopni se bránit proti kybernetickým hrozbám v digitálním prostředí (51).

# 4 Vlastní práce

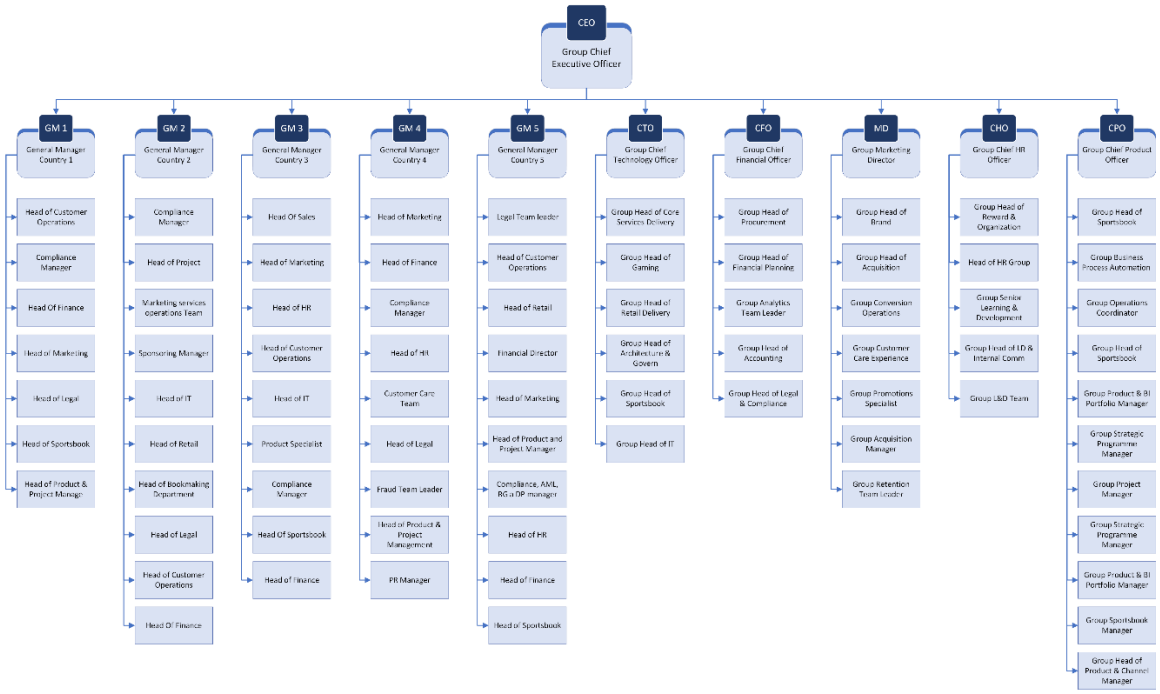
Praktická část diplomové práce byla autorem zpracována a implementována v existující firmě. Pro zajištění anonymity vybraného podniku, zajištění jeho dobrého jména, ochrany zaměstnanců a zajištění jeho ochrany jsou veškerá data anonymizována. Toto se týká též poznávacích znaků vybraného podniku (logo, webové stránky apod.), díky kterým by ho bylo možno identifikovat. Tento přístup byl zvolen mimo jiné z důvodu, že se v práci vyskytují výsledky phishingových kampaní, jsou zde popsány aktuální bezpečnostní opatření využívané vybraným podnikem, jakož i velké množství dalších citlivých údajů. Anonymizace poslouží pro lepší navržení univerzálně využitelných bezpečnostních opatření, jelikož autor práce bude takto nucen své závěry zobecňovat a koncipovat do podoby využitelné dalšími podniky, firmami či institucemi.

## 4.1 Popis společnosti

Vybraná firma má mezinárodní působnost, působí v několika zemích světa včetně České republiky a zaměstnává několik tisíc lidí. Hlavní centrála firmy se nachází v Praze, kde pracují všichni zaměstnanci z kancelářského zázemí, kteří spadají pod celou skupinu nebo pod český trh. Firma má také větší množství poboček v České republice. Tato práce se zaměřuje na všechny interní zaměstnance ze všech zemí, kde firma působí, vyjma pobočkových zaměstnanců, kteří nedisponují vlastním firemním počítačem.

Firma se specializuje na poskytování služeb nabízených jak přes internet, tak osobně na pobočkách. Díky fungování v online prostředí je firma výrazně digitálně zaměřená, a proto má mnoho svých vlastních aplikací, webových stránek a interních systémů, které má pod správou nebo zprostředkované třetí stranou. Vybraná firma z toho důvodu musí zabezpečit veškeré údaje, které uchovává o svých zákaznících, finančních transakcích, jednotlivých systémech, osobních údajích zaměstnanců včetně zvláštních kategorií osobních údajů (41, s. 37), o svém know-how, kontaktech na zákazníky a obchodní partnery, datových centrech, budovách a jejich zabezpečení a dalších informacích. Díky tomu zaměstnává výrazné množství profesionálů z IT odvětví, jako například vývojáře, administrátory, správce operačních systémů a sítí, IT podporu pro uživatele či specialisty na IT bezpečnost.

## 4.2 Organizační struktura firmy




*Obrázek 8 - Organizační struktura podniku (Interní materiály, Vlastní zpracování)*

Organizační struktura byla graficky znázorněna pro lepší zobrazení struktury firmy a jejího řízení. Z organizační struktury je patrné, že je firma rozdělena do 5 států a na jednu skupinu, která má přesah do všech jednotlivých zemí. Veškerá firemní koncová zařízení jsou onboardovaná[8] do firemního prostředí a díky tomu je možné provádět efektivně detekci na těchto zařízeních. Zaměstnanci si mohou zvolit i své osobní zařízení, u kterých má pak firma daleko více limitované možnosti pro sledování systémů. Nicméně veškerá firemní e-mailová komunikace probíhá skrze firemní Outlook, tedy i na takovýchto zařízeních je firma schopna sledovat veškeré příchozí i odchozí zprávy. Firma pro své účely využívá licenci Office 365 E5, která poskytuje jednotlivé kancelářské aplikace zaměstnancům a služby jako Office 365 Cloud App Security a Microsoft Defender for Office 365 – Plan 2. Tyto služby firma využívá pro komplexní zajištění informační bezpečnosti, protože nabízí souhrnné informace o užívaných aplikacích a možnost nastavit si správnou, personalizovanou ochranu proti kybernetickým hrozbám, jakými jsou malware či dále probíraný phishing.

Proto i veškerá navržená bezpečnostní opatření v této práci budou zaměřena na výše zmíněné služby a phishingové kampaně budou zajištěny nástrojem **Attack simulation training** od společnosti Microsoft, který je taktéž dostupný díky licenci E5.

[8] Tímto pojmem je myšleno připojení zařízení do Defenderu

Pro firemní intranet je využívaný SharePoint, na kterém jsou zaměstnanci informováni o novinkách ve firmě, jsou zde dostupné všechny platné bezpečnostní politiky a možnost sdílet soubory mezi jednotlivými pracovníky. Pro rychlou a efektivní komunikaci ve firmě se využívá MS Teams.

Pro hlášení bezpečnostních incidentů zaměstnanci využívají Jira Ticket systém,[9] přičemž za kybernetický incident lze považovat jakékoliv narušení či jen možnost narušení IT systémů, služeb a síti v podniku, způsobené konkrétní událostí (další definici poskytuje např. zákon o kybernetické bezpečnosti v § 7) (47). Tento nástroj je dostupný pro všechny zaměstnance, ti ale zároveň musí být připojeni na firemní síti přes LAN nebo pomocí VPN. Jira systém slouží pro hlášení incidentů, v jeho rámci probíhají všechny schvalovací úkony u těchto incidentů a jsou zde zaznamenány a uloženy veškeré projekty včetně jejich fází.

Firma se v posledních dvou letech zaměřila na zlepšení své IT bezpečnosti i z toho důvodu, že umožňuje svým zaměstnancům pracovat z domovů (tzv. home office) a do kanceláří docházet pouze občasně. Firma si uvědomuje, že by zaměstnanci mohli mít lepší povědomí o IT bezpečnosti (z důvodu zvýšené zranitelnosti interních systémů, zhoršené možnosti pravidelně kontrolovat zařízení, ze kterých zaměstnanci vstupují do interní sítě apod.), a proto podporuje rozvoj činností, které zaměstnance na možné hrozby připraví a naučí je, jak se mají správně zachovat, pokud tato situace nastane.

Za nastavení a dodržování všech bezpečnostních opatření ve všech zemích je zodpovědný Group IT Security Manager a jeho oddělení (viz obrázek na začátku kapitoly).

## 4.3 Organizační opatření

Firma si uvědomuje, že vysoké riziko spočívá už v samotných zaměstnancích a jejich povědomí (respektive jeho absenci) v oblasti kybernetické bezpečnosti. Kybernetické bezpečnostní incidenty mohou vznikat:

1. Úmyslně (viz kapitolu 3.3 této práce),
2. Neúmyslně.

Na oblast neúmyslného způsobení bezpečnostních incidentů zaměstnancem se právě další část této práce zaměřuje (i s ohledem na téma práce, tedy phishing a phishingové kampaně). Kvůli zvýšenému riziku spojeným s neúmyslným poškozením je tato firma připravena zaměstnance dostatečně proškolit a prohloubit jejich znalosti, díky kterým budou

[9] Jira tiketový nástroj, slouží pro nahlášení problémů či dotazů a efektivní komunikaci v rámci jednotlivých týmů.

poté zaměstnanci schopni v krizových situacích adekvátně reagovat. Důvodem je mimo jiné skutečnost, že v současné době firma nedisponuje dostatečnými školícími materiály či technikami, díky kterým by odpovědní zaměstnanci mohli své kolegy vzdělávat a prohlubovat jejich znalosti a vědomosti v oblasti kybernetické bezpečnosti. Stěžejní z pohledu autora práce i managementu podniku je, aby zaměstnanec věděl, jak správně reagovat a uměl vhodně vyhodnotit e-mailový útok, který je nejčastějším rizikem pro bezpečnost firmy (viz teoretickou část práce, např. kapitolu 3.3.4). Ve firmě v současnosti existuje pouze povinné vstupní školení pro nově přijaté zaměstnance. Nicméně ani tento způsob školení není ve firmě zaběhnutý a je využíván teprve 2 roky. Mnoho zaměstnanců, kteří ve firmě působí již několik let, toto školení tedy neměli k dispozici a jsou tak paradoxně zranitelnější, než nově příchozí zaměstnanci; i tento faktor je jedním z důvodů, proč rozšířit stávající systém vzdělávání zaměstnanců přes další komunikační kanály a formy.

**Závěr analýzy**

Tato kapitola se bude zaměřovat na nové vzdělávací techniky ve firmě, jejichž úspěšnost a výsledky budou následně vyhodnoceny. V rámci rozšířeného vzdělávání budou realizovány následující kroky:

1. Příprava a spuštění phishingových kampaní mířených na zaměstnance,
2. Proškolení všech zaměstnanců,
3. Následné opětovné otestování.

V rámci praktické části práce byly stanoveny následující hypotézy (vycházející z teoretické části práce a obecných poznatků týkajících se sociálního inženýrství a nutnosti preventivních opatření pro efektivní ochranu systémů), které budou ověřeny v průběhu této kapitoly a krátce vyhodnoceny v kapitole 5:

1. Zaměstnanci vybrané společnosti budou při iniciačních phishingových kampaních více náchylní k rizikovému chování (zadání přihlašovacích údajů, kliknutí na odkazy v podezřelém e-mailu) a kompromitaci společnosti; tato hypotéza vychází z následujících předpokladů:
    a. Osoby bez dostatečného povědomí o alespoň základních technikách kybernetické hygieny jsou náchylnější k rizikovému chování (viz např. kap. 3.4),
    b. Osoby, které se dříve nesetkaly s phishingovým útokem, nejsou schopny adekvátně reagovat (viz např. kap. 3.4).

2. Po alespoň základním informování o probíhajícím cvičném útoku a následném nastavení základních organizačně-vzdělávacích opatření (více v následujících kapitolách) výrazně vzroste počet zaměstnanců, kteří provedou doporučený postup při podezření na phishing.

Jelikož jsou tyto hypotézy poměrně jednoduché, bude následně možné je též relativně snadno v průběhu práce ověřit.

### 4.3.1 Simulační phishingové kampaně zaměřené na zaměstnance firmy

Dle názoru autora této práce je využívání simulačních phishingových kampaní, obohacených o vzdělávací indikátory, jedním z nejlepších způsobů vzdělávání zaměstnanců, a to z důvodu získání praktických dovedností, možnosti ilustrovat dopady útoku a uvědomění si mezer ve vzdělávání a pozornosti zaměstnanců. Z toho důvodu byla tato metoda zvolena, navržena a implementována ve firemním prostředí.

Pro simulační phishingové útoky byl využit nástroj od společnosti Microsoft Attack simulation training. Jak již bylo výše zmíněno, firma používá jejich služby dlouhodobě a tento nástroj pro simulaci útoků má zdarma v rámci licenčních služeb, nejedná se tedy o další výdaj nad rámec stávajícího rozpočtu na IT vybavení (právě vstupní investice bývají často překážkou pro kvalitní ochranu IT systémů a vzdělávání zaměstnanců a jsou obecně nejnákladnější součástí vývoje kybernetické bezpečnosti) (6, s. 185). Výběr stávajícího simulačního nástroje ovlivnilo i to, aby nebyl do firmy zbytečně implementován další systém, který by firma musela spravovat a tím zvýšit rozsah práce stávajících zaměstnanců a snížit obeznámenost zaměstnanců IT oddělení s využívaným softwarovým řešením.

#### 4.3.1.1 Způsob provedení

Otestování zaměstnanců skrze simulované phishingové e-maily bylo schváleno vedením firmy, které nechalo formát a realizaci simulací čistě na uvážení a spravování autora této práce. Jednotlivé kroky při sestavení a provedení této simulace byly konzultovány s IT Security manažerem, který má v této oblasti širší zkušenosti a znalosti. Na základě těchto konzultací vzniklo strukturované zadání, podle kterého se postupuje při každé nové simulaci.

Aby bylo provedeno co nejrozsáhlejší otestování, simulace byla mířena na všechny firemní zaměstnance, tzn. skupinové zaměstnance, a zaměstnance v rámci všech zemí (viz organizační schéma vybraného podniku). Jedinou skupinou zaměstnanců, kteří se simulace neúčastnili, byla skupina zaměstnanců pracujících na pobočkách.

S testováním se začalo po jednotlivých odděleních. Bylo to z důvodu, aby byla pro jednotlivá oddělení (která jsou relativně uzavřenými jednotkami) zrealizována personalizovaná simulace, která bere v potaz systémy, ve kterých zaměstnanci pracují a které používají v rámci běžné pracovní náplně. Vždy před spuštěním kampaně byl informován IT Security manažer a SOC tým.[10] Pokaždé jim byl předán vzorový phishingový e-mail, který byl zaměstnancům odeslán, aby obě zodpovědná místa byla informována o průběhu testování a v případě nutnosti mohla zareagovat na dotazy testovaných zaměstnanců. Každá kampaň trvala minimálně dva týdny a během této doby nebyla spuštěna žádná další kampaň, přičemž tento interval byl stanoven po domluvě s IT Security manažerem, aby nedocházelo k velkému množství dotazů a testování bylo regulované. Kampaně sloužily mimo jiné k tomu, aby uživatele informovaly o existenci nebezpečí souvisejících s phishingovými e-maily. Žádnému zaměstnanci nehrozil postih, pokud na základě podvodného e-mailu zadal své přihlašovací údaje či stáhl škodlivý soubor. V žádné kampani nebyly sbírány osobní údaje zaměstnanců, a to i v případech, kdy zaměstnanec použil své heslo; v takovém případě heslo nikdy neopustilo jeho počítač a zůstalo nekompromitované. Také byl kladen důraz na zachování anonymity zaměstnanců, proto nebyl zveřejněn seznam lidí, kteří nerozpoznali testovací škodlivý e-mail. Vedení firmy byl poskytnut pouze zobecněný report, kde byly publikovány výsledky v rámci jednotlivých odděleních. Po ukončení phishingové kampaně byl každý zaměstnanec informován, že byl součástí testování.

#### 4.3.1.2 Nastavení kampaní a jejich realizace

Nástroj Attack simulation training (dále též pouze nástroj) nabízí široké spektrum funkcionalit. Aby bylo možné spustit novou kampaň, musí se nejdříve vytvořit payload (datový obsah), který reprezentuje škodlivý e-mail s určitým typem útoku. V nástroji existuje velká knihovna již vytvořených payloadů připravených k okamžitému použití. Jedná se o univerzální šablony, které nejsou přizpůsobené jednotlivé firmě, a tím pádem jsou pro zaměstnance vybraného podniku i více nápadné; Proto bylo v nástroji vytvořeno několik vlastních payloadů, přizpůsobených pro danou firmu (např. vizuální stránkou) a konkrétním oddělením.

Prvním krokem při vytváření payloadů bylo vždy vybrání techniky útoků. Pro testování byly využity techniky Credential harvest a Malware attachment (viz kapitolu 3.6

[10] SOC tým (bezpečnostní operační centrum) – tým odborníků na bezpečnost IT, který analyzuje data a hledá bezpečnostní problémy v celé IT infrastruktuře firmy.

této práce). Tyto techniky byly zvoleny z toho důvodu, že se jedná o jedny z nejzákladnějších a nejběžnějších typů útoků a také jsou tyto techniky v nástroji Attack simulation training nejvíce propracované.

V druhém kroku bylo nutné nastavit již konkrétní konfiguraci pro payload. Pro každou simulaci bylo nastaveno:

1. Jméno odesílatele,
2. E-mail odesílatele,
3. Předmět e-mailu,
4. V případě techniky Credential harvest URL, které slouží pro phishingovou stránku,
5. V případě Malware attachment typ a název souboru,
6. Jazyk; byla zvolena angličtina kvůli mezinárodní působnosti firmy,
7. Definování e-mailu – zde byla vytvořena finální podoba e-mailu. Úprava byla provedena dvěma způsoby, jelikož nástroj umožňuje tvorbu e-mailu přes:
    i. textové pole, nebo
    ii. pomocí html kódu. Podoba konkrétních e-mailů a důvody jejich podob jsou blíže specifikovány u jednotlivých kampaní,
8. Vložení indikátorů – indikátory se zobrazí každému zaměstnanci, který se stal obětí útoku. Tyto indikátory byly použity pro školení zaměstnanců, aby tito zaměstnanci měli informaci a zpětnou vazbu k tomu, v čem pochybili a na jaké detaily u e-mailů si dát větší pozor, jakož i jak efektivněji rozpoznat podvodné e-maily.

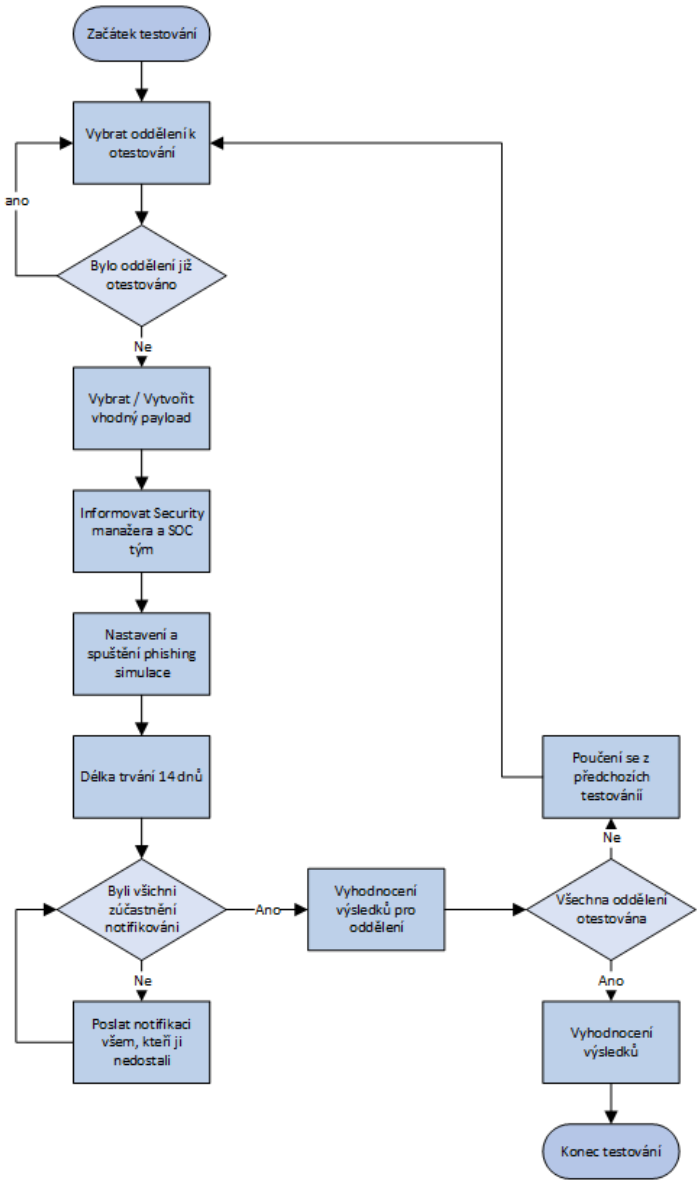
Po vytvoření payloadu bylo nutné nastavit spuštění simulace. V nastavení nástroje bylo v rámci testování zaměstnanců nakonfigurováno:

1. Technika útoku – Credential Harvest. Malware Attachment,
2. Název simulace – pro přehlednost byla simulace vždy pojmenovaná na základě oddělení, kterému byla určena,
3. Vybrán payload,
4. Cíloví uživatelé – nahráno pomocí souborového formátu .csv dle aktuální organizační struktury,
5. Přiřazení školení – zde bylo vybráno vždy jedno až dvě školení pro všechny zaměstnance, kteří byli kompromitováni a zadali v simulovaném phishingovém útoku osobní údaje nebo stáhli škodlivý soubor. Toto školení má podobu krátkých videí, která byla doplněna důležitými informacemi od společnosti Microsoft (tyto

jsou součástí řešení Microsoft 365 Defender). V příštích 15 dnech ode dne ukončení simulace bylo zaměstnancům umožněno školení absolvovat, nebylo ale povinné,

6. Nastavení stránky, která se zobrazila všem kompromitovaným zaměstnancům a přidání vzdělávacích indikátorů,
7. Notifikace uživatelů – Každá notifikace byla upravena potřebám firmy. Byly přidány firemní informace a logo, aby tato notifikace nebyla zaměstnanci považována za další ze škodlivých e-mailů. Jednalo se o:
    i. Notifikace o školení,
    ii. Notifikace v případě správného nahlášení škodlivého e-mailu – poděkování zaměstnancům za odvedení dobré práce,
8. Doba trvání simulace nastavena vždy na 14 dnů.

Pro lepší porozumění této a předchozí kapitoly byl vytvořen vývojový diagram, který popisuje průběh od počátku testovací kampaně až k jejímu ukončení.




*Obrázek 9 - Vývojový diagram - Proces testování*

#### 4.3.1.3 Očekávané cíle

Hlavním cílem tohoto testování bylo zjistit aktuální stav povědomí o této oblasti (tj. o možnostech útoku) mezi zaměstnanci a jejich reakce na škodlivý e-mail (zda e-mailu smažou, přepošlou, stáhnou přílohu nebo zadají své osobní údaje) a zda tyto škodlivé emaily správně, tedy v souladu s interními předpisy vybrané firmy, nahlásí. Záměrem bylo každého ze zaměstnanců, který nereagoval odpovídajícím způsobem, poučit a proškolit v této problematice (ke vzdělávání více v kapitole 4.3). Dílčím cílem bylo poté identifikovat, zda procento lidí, kteří nesprávným způsobem reagovali na e-mail, po absolvování edukativních akcí klesá a zda se procento nahlášených incidentů bude zvyšovat.

#### 4.3.1.4 Jednotlivé kampaně a jejich vyhodnocení

V této kapitole budou popsány vybrané kampaně, které byly v rámci testování zaměstnanců realizovány. Dále budou jednotlivých kampaní vždy popsány následující parametry:

1. téma e-mailu;
2. identifikátory podle kterých bylo poznatelné, že se jedná o škodlivý e-mail (viz kapitolu 3.4.1 této práce);
3. celkový počet zaměstnanců, kteří byli součástí této kampaně.

U vybraných kampaní budou reprezentovány výsledky jejich úspešnosti.

**1. Phishingová kampaň – Jira**

Tato phishingová kampaň byla navržena na základě znalostí o vnitřním fungování firmy a napodobuje notifikaci ze systému Jira, který je ve firmě využíván. Touto kampaní bylo otestováno celkem 619 zaměstnanců. Jedná se o osobnější (personalizovaný) typ útoku, který využívá právě interních znalostí o daném cíli (v tomto případě nikoliv o jednotlivcích, ale o určitém vzorku osob), a proto jej lze označit za spear phishing. Tento e-mail byl koncipován tak, aby upozorňoval uživatele na nově přiřazený úkol, který čeká na jejich potvrzení. Task (přiřazený úkol) řešil žádost o získání účtu lokálního admina. V e-mailu se nacházely jak statické, tak dynamické prvky, přičemž samotná podoba e-mailu nebyla oproti skutečné podobě notifikačního e-mailu z Jira přesná a vykazovala anomálie, díky kterým se e-mail lišil od originálního. Na první pohled byla vidět i nepřesná grafická úprava zprávy.

**Mezi statické prvky jsou zahrnuty:**

1. Předmět e-mailu; [JIRA] (USRSUP-28x) ASSIGNED,
2. Odesílatel; Jira Jira@domenafirmy.com; domenafirmy zde nahrazena z důvodu zachování anonymity. V emailu byla využita technika Homograph Attack (viz kapitola 3.6.10),
3. Odkazy; Zpráva obsahovala mnoho odkazů (hypertextové linky, tlačítko), které odkazovaly na adresu, na které se nacházela škodlivá stránka,
4. Upozornění, že zpráva pochází od externího odesílatele. Toto opatření bylo implementováno v rámci technických opatření (viz kapitola 4.4.1.1).

**Dynamický prvek:**

1. Jméno příjemce v těle zprávy; Validation by jméno (viz Obrázek 10), se vždy upravilo dle jména příjemce.

V momentě, kdy zaměstnanec klikl na hypertextový odkaz nebo na tlačítko, byl přesměrován na webovou stránku (https://www.officentry.com; poskytnuto a registrováno od společnosti Microsoft pro využívání phishingových simulací), přičemž tato stránka vzhledově připomínala přihlašovací stánku společnosti Microsoft.


*Obrázek 10 - Ukázka útoku – Jira*

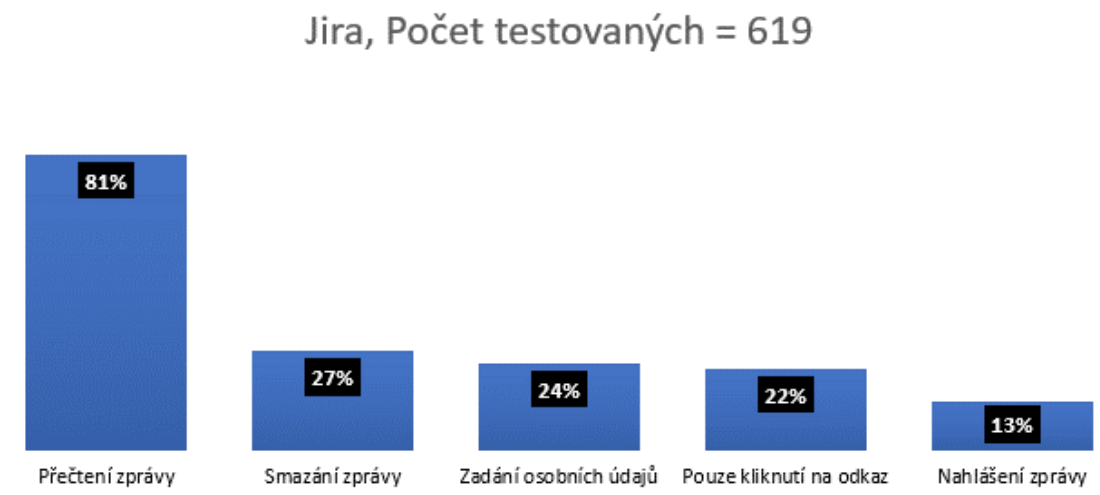
**Identifikátory, podle kterých lze rozpoznat, že se jedná o phishingový email:**

a. Ve firmě se takový formát ticketu nepoužívá: USRSUP-28x (místo x by mělo být číslo),
b. V emailu byla využita technika Homograph Attack (viz kapitola 3.6.10), která napodobila legitimní doménu,
c. Je očekáváno, že e-mail přichází z vnitřní sítě firmy; proto by zaměstnanec měl zpozornět, jelikož je v samotném e-mailu upozorněn, že tento e-mail pochází od externího odesílatele,
d. Na první pohled je vidět, že e-mail není správně graficky strukturován (špatné odrážky, místo obrázků prázdné čtverce),
e. Změna provedena manažerem; Správně by se mělo jednat o typizovaný e-mail, tedy by mělo být v e-mailu uvedeno jméno zaměstnancova manažera (nadřízeného),

f. Pokud zaměstnanec namíří kurzorem myši na odkaz, zobrazí se mu https://www.officentry.com; Správně by měl odkaz odkazovat na: jira.domenafirmy.com,
g. Máte omezený čas na splnění úkolu; Snaha vyvolat okamžitou reakci a strach v uživateli, že něco promešká (technika sociálního inženýrství, notifikační e-mail ze systému Jira takovýto explicitní, reakci vyvolávající text neobsahuje).

Pokud uživatel klikl na odkaz a následně na falešné webové stránce zadal i své osobní údaje, byl přesměrován na vzdělávací stránku, na které byl informován:

1. O situaci, že se jednalo o testovací phishing ze strany oddělení IT bezpečnosti,
2. O tom, že uživatel testem neprošel,
3. O důvodu testování,
4. O jednotlivých identifikátorech, na základě, kterých lze škodlivý email odhalit.




*Obrázek 11 - Výsledky testování - Jira*

Výsledky z grafu (viz Obrázek 11) vždy vychází z celkového počtu testovaných zaměstnanců, tedy z 619 vzorků (detailní hodnocení bude doplněno v následující části práce, zde zobrazený graf je pouze informativní). Tento přístup byl zvolen z toho důvodu, že zaměstnanec mohl provést více akcí současně (např. přečíst zprávu a zároveň nahlásit zprávu, zadat své osobní údaje a následně zprávu smazat apod.). Na základě těchto skutečností lze graf interpretovat následujícím způsobem: 81 % (501) zaměstnanců z 619 si zprávu minimálně otevřelo; 27 % (167) z celkového počtu zprávu smazalo; 24 % (149) zaměstnanců zadalo své osobní údaje a 22 % (136) si přes odkaz v emailu zobrazilo škodlivou webovou stránku. Zaměstnanci, kteří zadali své osobní údaje, museli škodlivou

webovou stránku rovněž navštívit. Na základě toho lze předpokládat, že skoro polovina testovaných zaměstnanců si mohla uvědomit, že se nejedná o legitimní cílovou stránku. Celých 46 % (285) zaměstnanců tuto stránku navštívilo, a dokonce 24 % (149) zaměstnanců zadalo i své osobní údaje; pouze 13 % (80) z celkového počtu nahlásilo škodlivý e-mail prostřednictvím správného interního postupu.

**2. Phishingová kampaň – PPL**

Druhá phishingová kampaň napodobovala informační e-mail od společnosti PPL[11], který informoval o změně údajů k doručení zásilky. Pomocí této kampaně bylo otestováno 480 zaměstnanců. Testovací e-mail byl v tomto případě navržen jednodušeji; Grafická podoba byla velmi jednoduchá, v e-mailu nebyly zmíněny žádné osobní identifikátory, pouze jméno příjemce. Jednalo se tedy o phishingový e-mail, který simuloval situaci, kdy útočník nezná prostředí firmy a pouze zkouší náhodnou zprávou, zda se nenajde nějaký nepozorný zaměstnanec. Byl zde tedy předpoklad nižšího procenta kompromitovaných zaměstnanců právě kvůli méně propracované podobě oproti první (Jira) verzi kampaně.

**Mezi statické prvky patří:**

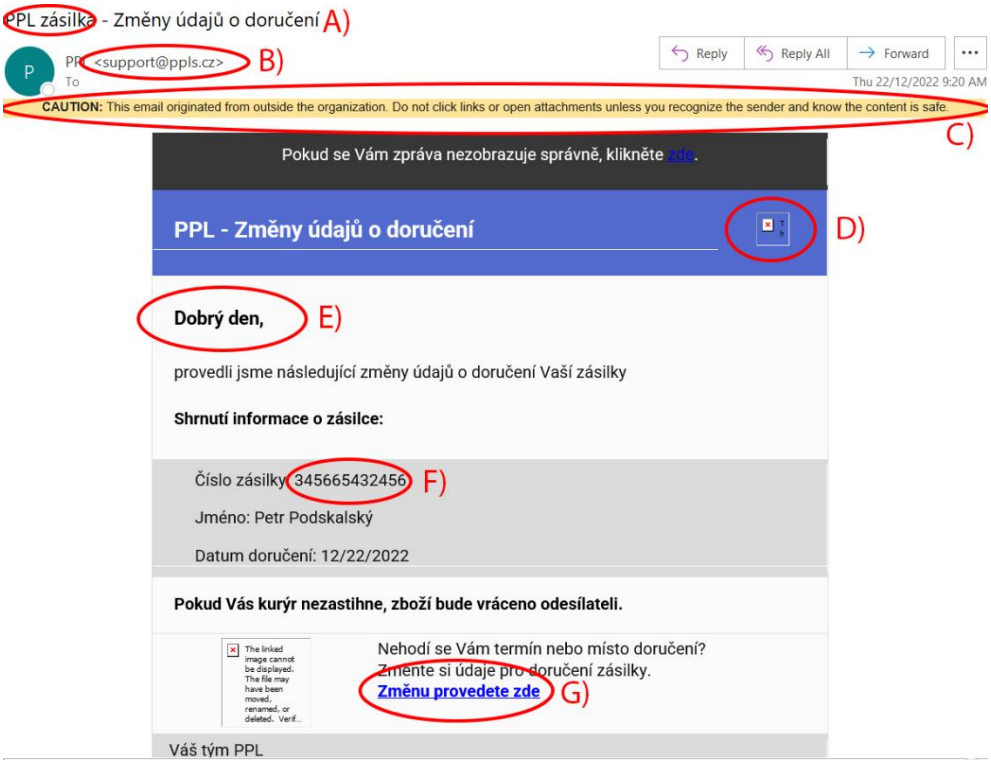
1. Předmět e-mailu; PPL zásilka – Změny údajů o doručení
2. Odesílatel; PPL support@ppls.cz; V emailu byla využita technika Typo Squatting (viz kapitola 3.6.09),
3. Odkazy; Zpráva obsahovala odkazy (hypertextové linky, tlačítko), které odkazovaly na stejnou adresu, na které se nacházela škodlivá stránka,
4. Upozornění, že zpráva pochází od externího odesílatele. Toto opatření bylo implementováno v rámci technických opatření (viz kapitola 4.4.1.1).

**Dynamický prvek:**

1. Jméno příjemce v těle zprávy.

V momentě, kdy zaměstnanec klikl na hypertextový odkaz nebo na tlačítko, byl přesměrován na webovou stránku (https://www.prizewel.com; poskytnuto a registrováno společností Microsoft pro využívání phishingových simulací), přičemž webová stránka vzhledově nepřipomínala přihlašovací stánku společnosti PPL (šablona poskytnutá společností Microsoft byla autorem upravena).

[11] Firma zabývající se přepravou.




*Obrázek 12 - Ukázka útoku – Confluence*

**Identifikátory, podle kterých lze rozpoznat, že se jedná o phishingový email:**

a. Nefiremní e-mail; Jelikož se jedná o e-mail, který napodobuje osobní záležitosti nikoliv firemní; zaměstnanec by měl ihned zpozornit, proč mu takovýto e-mail přišel do firemní pošty,
b. Na první pohled byly viditelné překlepy v doméně,
c. Je očekáváno, že e-mail přichází z vnější sítě firmy; proto byl zaměstnanec správně upozorněn, že e-mail pochází mimo vnitřní síť firmy,
d. Neexistující loga,
e. Velice neosobní pozdravení;
f. Pokud by zaměstnanec očekával nějaké zboží; Měl by si všimnout neexistujícího čísla objednávky,
g. Pokud zaměstnanec namíří kurzorem myši na odkaz, zobrazí se mu https://mcsharepoint.com; správně by měl odkaz odkazovat na: cnfl.domenafirmy.eu.
h. Graficky e-mail neodpovídá legitimním emailům odesílaným z tohoto systému,


*Obrázek 13 - Výsledky testování - PPL*

Výsledky z grafu (viz Obrázek 13) byly vyhodnoceny stejným způsobem jako u předchozí kampaně (viz podkapitola 1. Phishingová kampaň – Jira, výše). Díky tomu lze interpretovat zjištěné výsledky následujícím způsobem: 82 % (181) lidí z celkem 221 si zprávu minimálně otevřelo; 22 % (49) zaměstnanců zprávu smazalo; 1 % (2) zaměstnanců zadalo své osobní údaje a 19 % (42) si přes odkaz v emailu zobrazilo škodlivou webovou stránku. Celkový počet kompromitovaných uživatelů je tedy 20 % (42). Z výsledků daného testování vyplývá, že méně personalizovaný e-mail má daleko menší úspěšnost. Z druhého testování bylo zjištěno, že uživatelé zpozornili v momentě, kdy se přes odkaz dostali na škodlivou webovou stránku. Jelikož přihlašovací formulář zde byl naprosto odlišný oproti přihlášení do PPL. Proto v zadávání svých osobních údajů přestali a pokračovalo pouze 1 % zaměstnanců.

#### 4.3.1.5 Celkové vyhodnocení všech phishingových kampaní

V předchozí kapitole byly podrobněji rozebrány dvě kampaně (Jira - se znalostí firemního prostředí; PPL - bez znalosti firemního prostředí), které byly zaměstnancům firmy rozeslány. K celkovému prvotnímu protestování zaměstnanců ve firmě byly vytvořeny 4 kampaně (Jira, Confluence, PPL, Helpdesk). V této kapitole jsou prezentovány výsledky ze všech těchto kampaní pomocí jednotlivých grafických zobrazení.

**Souhrn všech phishingových kampaní**

V souhrnné tabulce pro lepší přehled budou uvedeni pouze ti uživatelé, kteří si zprávu otevřeli.

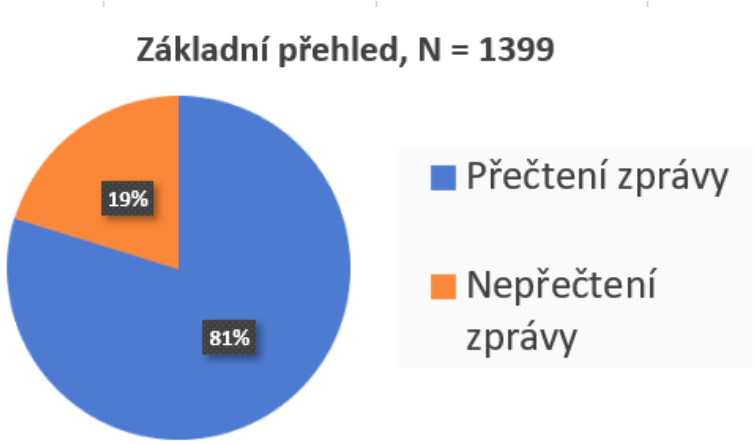
| Kampaně | Přečtení e-mailu | Včasné nahlášení | Ignorování / Smazání zprávy | Kompromitovaní zaměstnanci (minimálně klikli na link) |
|---|---|---|---|---|
| **Jira** | 502 | 40 (8 %) | 177 (35 %) | 285 (57 %) |
| **Confluence** | 278 | 8 (3 %) | 139 (50 %) | 131 (47 %) |
| **PPL** | 181 | 0 (0 %) | 136 (75 %) | 45 (25 %) |
| **Helpdesk** | 166 | 17 (10 %) | 98 (59 %) | 51 (31 %) |
| **Celkem** | 1127 | 65 | 550 | 512 |
| **Průměr** | 281,75 | 16,25 (5,25 %) | 137,5 (54,75 %) | 128 (40 %) |

*Tabulka 1 - Souhrnný přehled testování zaměstnanců 1. kolo*

1. Jira (viz 1. Phishingová kampaň – Jira)
2. Confluence - phishingová kampaň vycházela ze systému Confluence, který je ve firmě využíván pro uchování souborů, plánů, nápadů, specifikací a dalších návodů pro konkrétní projekty. Pomocí této kampaně bylo otestováno 480 zaměstnanců. Testovací e-mail byl v tomto případě navržen jednodušeji; Grafická podoba byla velmi jednoduchá, v e-mailu nebyly zmíněny žádné osobní identifikátory, pouze jméno příjemce. Jednalo se tedy o phishingový e-mail, který simuloval situaci, kdy útočník zná nebo odhadl systém, který firma využívá, a využije této obecné znalosti k útoku (viz příloha 2),
3. PPL (viz 2. Phishingová kampaň – PPL)
4. Helpdesk – Tato kampaň napodobovala situaci, kdy útočník poslal zaměstnanci e-mail, který se tvářil jako zpráva od firemního Helpdesku. Tento e-mail informoval zaměstnance o situaci, že jim do 48 hodin bude deaktivován účet na žádost jejich přímého nadřízeného, pokud se nepřihlásí do systému, aby změně zabránili. E-mail přišel z vnějšího prostředí a znal pouze jméno příjemce a jméno nadřízeného. (viz příloha 3).

Výsledky, které jsou v rámci jednotlivých grafů reprezentovány, pochází z prvotního testování zaměstnanců firmy. Žádný ze zaměstnanců nebyl v rámci kampaní testován vícekrát (i z důvodu, aby jeho reakce na podvodné e-maily nebyla ovlivněna a výsledek zkreslen předchozí znalostí). **Výsledná čísla naznačují, že první pracovní hypotéza je tímto potvrzena; bez předchozích znalostí jsou počty kompromitovaných zaměstnanců**

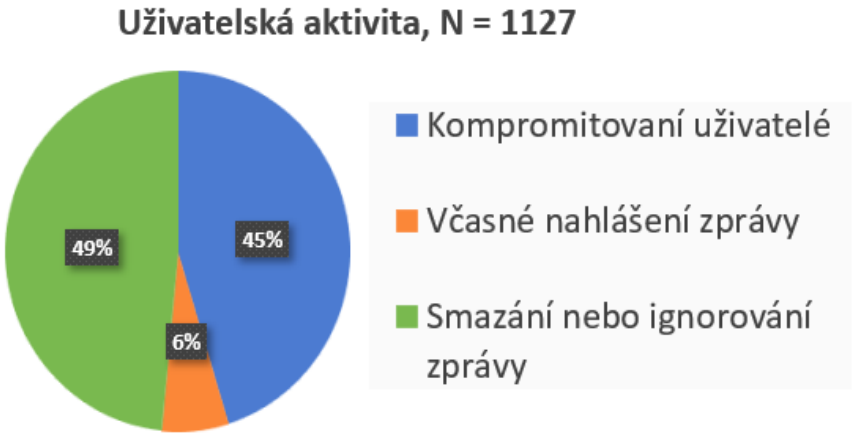
**dosti vysoké (v rozptylu od 25 % do 57 % v závislosti na konkrétní kampani, jak je rozepsáno dále).**




*Obrázek 14 - Celkové vyhodnocení testů – Základní přehled*

Z prvního grafu (viz Obrázek 14) je patrné, že z celkového počtu 1 399 testovaných zaměstnanců pomocí phishingových kampaní si 81 % (1127) z nich přečetlo testovací email. Zbylých 19 % (272) zaměstnanců si e-mail nezobrazilo. Způsobeno

to mohlo být tím, že byl zaměstnanec po dobu testování na dovolené, e-mail mohl být také pomocí filtračních pravidel přesměrován do jiné složky v e-mailovém klientu, kterou uživatel nekontroluje. Pro další statistiky je uvažováno pouze se zaměstnanci, kteří si phishingový email zobrazili. Následující statistiky vychází z 1 127 vzorků.

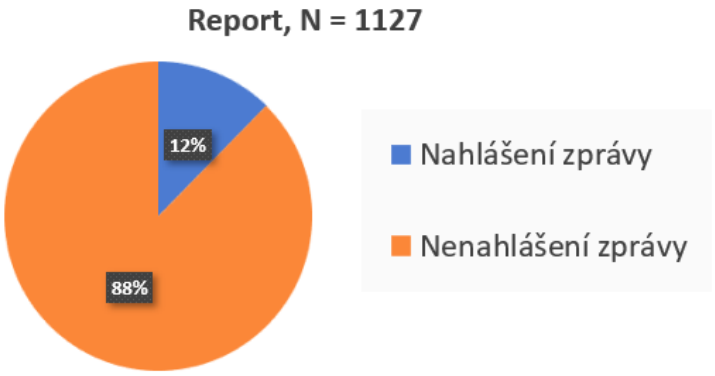



*Obrázek 15 - Celkové vyhodnocení testů - Uživatelská aktivita*

Graf (viz Obrázek 15) popisuje uživatelskou aktivitu vůči obdrženému e-mailu. Mezi kompromitované uživatele patří všichni, kteří pomocí odkazu navštívili škodlivou stránku a následně ve svých aktivitách dále nepokračovali a zároveň i ti, kteří na škodlivé webové stránce zadali i své osobní údaje. Včasné nahlášení zprávy reprezentuje uživatele, kteří po zobrazení zprávy tento e-mail nahlásili. To znamená, že škodlivou stránku vůbec

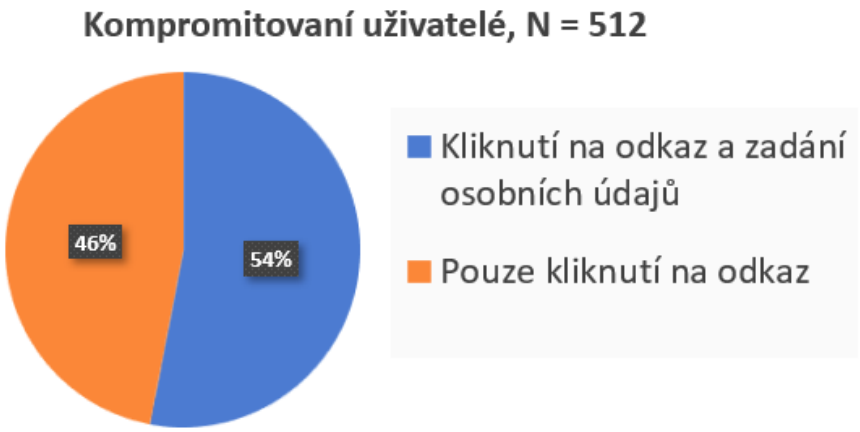
nenavštívili. Poslední kategorie reprezentuje ty zaměstnance, kteří po zobrazení e-mailu žádnou aktivitu nevykonali či e-mail pouze smazali. Tato kategorie je sloučena z důvodu, že z hlediska bezpečnosti není rozhodující, zda dojde pouze ke smazání nebo ignorování zprávy.

V rámci všech testování bylo zjištěno vysoké procento kompromitovaných zaměstnanců. Téměř každý druhý testovaný zaměstnanec určitým způsobem ohrozil bezpečnost v rámci dané firmy 45 % (512) a pouze 6 % (67) zaměstnanců odpovídajícím způsobem nahlásilo škodlivý e-mail.



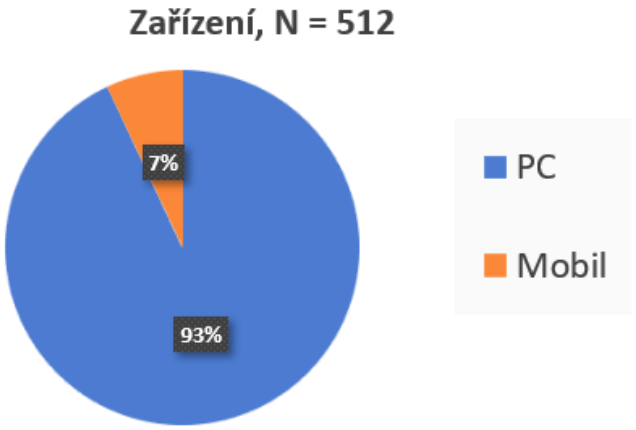

*Obrázek 16 - Celkové vyhodnocení testů – Report*

Pro úplnost a přesnost výsledků testování je na grafu (viz Obrázek 16) zobrazen i procentuální podíl zaměstnanců, kteří zprávu nahlásili během celého procesu testování. Určitá skupina zaměstnanců navštívila škodlivou webovou stránku či zadala své osobní údaje a poté email nahlásila jako škodlivý. Možné příčiny tohoto jednání mohou spočívat např. v tom, že si zaměstnanec uvědomil nepřesnosti či chyby v emailu a zpětně zprávu nahlásil. Do této skupiny jsou zahrnuti rovněž zaměstnanci, kteří byli informováni o neúspěchu v rámci testování pomocí vzdělávacího emailu (viz kapitola 4.2.1.4 Jednotlivé kampaně a jejich vyhodnocení) a zpětně na základě instrukcí o správném nahlašování emailů, tento email nahlásili.




*Obrázek 17 - Celkové vyhodnocení testů – Kompromitovaní uživatelé*

Celkový počet kompromitovaných zaměstnanců byl 512 zaměstnanců. Graf (viz Obrázek 17) znázorňuje, že více než polovina kompromitovaných jsou zároveň ti, kteří zadali i své osobní údaje na falešné stránce, tedy 54 % (278). To znamená, že méně jak polovina testovaných, tedy 46 % (234), si ověřuje, zda cílová stránka opravdu odpovídá té, které má.




*Obrázek 18 - Celkové vyhodnocení testů – Zařízení*

Poslední graf (viz Obrázek 18) zobrazuje zařízení, které kompromitovaní uživatelé využívali. Škodlivou stránku si zobrazilo pouze 7 % (35) testovaných z mobilních zařízení, 93 % (477) zaměstnanců k otevření stránky využilo počítač. Většina mobilních e-mailových klientů zobrazuje daleko méně informací o e-mailové zprávě oproti počítačovým klientům. Toto zjištění proto lze interpretovat buďto tak, že částečně odporuje některým teoretickým předpokladům z první části této práce (srov. Kapitolu 3.6.3), kdy politika užívání mobilních zařízení ve firmách (např. na principu BYOD) naopak vedla ke zvýšenému počtu útoků. S tím je spojena i často horší kvalita zobrazovaných stránek, která lépe maskuje nedokonalosti falešné stránky. Nebo lze předpokládat, že zaměstnanci využívají pro vyřizování své e-

mailové korespondence počítačových stanic spíše než mobilních zařízení – tato informace je ověřitelná (nad rámec této práce) např. dotazníkovým šetřením a lze jí následně přizpůsobit bezpečnostní politiku vybrané firmy.

**Celkové shrnutí:**

Z výsledků získaných v rámci testování lze prohlásit, že firemní vzdělávání v oblasti phishingu a kybernetické bezpečnosti jako takové není dostatečné. Téměř polovina testovaných zaměstnanců neodhalila phishingový e-mail a svou aktivitou vytvořila situaci, která může ohrozit bezpečnost celé firmy. Tím, že se schopnosti a znalosti útočníků neustále zdokonalují, jak po stránce formální úpravy falešného e-mailu, tak po stránce obsahové, měla by firma z těchto výsledků vyvodit odpovídající důsledky v nastavení interních procesů, od podpory vzdělávání zaměstnanců přes pokračující podporu oblasti kybernetické bezpečnosti a zjednodušení možnosti reportovat podezřelou e-mailovou komunikaci. Jedním z důvodů tak vysokého čísla neúspěšných pokusů o rozpoznání phishingového e-mailu může být i to, že firma má implementované poměrně vysoké zabezpečení v této oblasti, a tak se zaměstnanec příliš často se škodlivým e-mailem v rámci plnění svých pracovních povinností nesetká, ať už se jedná o phishing, nebo spam. Proto mohou být zaměstnanci méně ostražití a bez ohledu na možné důvody je tento výsledek dalším důvodem pro preventivní opatření v rámci vzdělávacích kampaní či podobných způsobů informování zaměstnanců.

Alarmující je velmi nízké procento nahlášených e-mailů; pouze 12 % (135) všech testovaných zaměstnanců škodlivou zprávu správně nahlásilo, přičemž právě takovéto nahlášení je pro bezpečnost firmy klíčové. V momentě, kdy je škodlivá zpráva nahlášena a je o ní informován bezpečnostní tým, mohou být provedena potřebná opatření, která by například zprávu smazala ostatním zaměstnancům, jimž byl rovněž tento e-mail adresován. Takto nízké číslo u nahlašování nelze vysvětlit novým nahlašovacím způsobem, který byl implementován v rámci technických opatření této diplomové práce (popsáno v kapitole 4.4.1.2), neboť v případě starého způsobu nahlašování incidentů (popsáno v kapitole 4.1), byly nahlášeny pouze dva incidenty. Proto nový způsob lze považovat za efektivnější, za předpokladu zvýšení povědomí o tomto způsobu nahlašování mezi zaměstnanci.

Nejvyšší procento kompromitovaných zaměstnanců (45 %) bylo u kampaní, jež využívaly znalostí firemních systémů, tedy při využití techniky spear phishing. Oproti tomu phishingová zpráva zaslána pod falešnou e-mailovou adresou společnosti PPL nezaznamenala tak vysoký počet kompromitovaných uživatelů. Z toho lze vyvodit, že

zaměstnanci si dávají větší pozor, pokud jim přijde do firemního e-mailu soukromá zpráva. Naopak pokud se jedná o firemní notifikace, ostražitost zaměstnanců klesá a legitimnost e-mailu tolik nekontrolují. V rámci dalších školení by tato skutečnost měla být reflektována, a to vícerým upozorňováním zaměstnance na riziko toho, že i zpráva velmi podobná notifikaci z interního systému může být škodlivou zprávou. Zaměstnanci by v případě jakýchkoliv nejasností či abnormálních požadavků měli tedy preventivně tuto skutečnost oznámit.

V rámci testování bylo také vypozorováno, že největší dopad škodlivých e-mailů byl právě na české a skupinové zaměstnance. Bylo to způsobeno z toho důvodu, že tito zaměstnanci dostávají denně zprávy v angličtině, proto jim nepřišlo zvláštní, že i škodlivá zpráva byla v tomto jazyce. Naopak v jednotlivých zemích pak procento kompromitovaných zaměstnanců tak vysoké nebylo, jelikož nejsou na anglické e-maily zvyklí na denní bázi a kvůli tomu u takové zprávy byli více ostražití. Z tohoto důvodu by bylo lepší a pro komplexnější otestování připravenosti zaměstnanců u budoucího testování vhodnější připravit payload v lokálním jazyce.

Nejlépe z testování vyšlo oddělení financí a oddělení pro dodržování předpisů. Zde byli kompromitováni pouze dva zaměstnanci, ale ani jeden z nich neposkytl své osobní údaje. Naopak nejméně úspěšným oddělením, které přesáhlo 50 % celkových kompromitovaných uživatelů, bylo oddělení, které se zaměřuje na propagaci služeb. Alarmující je také zjištění, že velké riziko představuje i top management, v rámci kterého 50 % manažerů kliklo na odkaz ve škodlivém e-mailu a poté 60 % z nich zadalo na škodlivé stránce i své osobní údaje. Nikdo z top managementu navíc škodlivý e-mail správně nenahlásil. Na základě těchto zjištění byly v dané firmě ihned podniknuty odpovídající kroky, a to v návaznosti na to, že právě top management je častým terčem útočníků a útoky na něj zaměřené jsou sofistikovanější, s výrazně větším negativním dopadem na celou společnost (viz kapitolu 3.7 Trendy a výzvy v oblasti kybernetické bezpečnosti).

### 4.3.2 Navržení vhodného školení pro zaměstnance

Z prvotního testování zaměstnanců, které bylo provedeno v předchozí kapitole (viz 4.2.1), lze pozorovat, že vědomosti zaměstnanců v oblasti odhalování podvodných e-mailů jsou ve firmě na velmi nízké úrovni. Zaměstnanci mnohdy nekontrolují ani základní prvky v e-mailech, které by jim mohly pomoci při odhalení škodlivých zpráv, a na základě předchozích výsledků je také vidět, že zaměstnanci tyto e-maily ani neumí správně nahlásit pomocí ve firmě již zavedených postupů.

Z tohoto důvodu bylo nutné navrhnou školení, které zaměstnancům vysvětlí základní identifikátory, na které by si při kontrole e-mailů měli dávat pozor, jakož i základní pravidla, kterých by se měli zaměstnanci držet, aby co nejvíce eliminovali možná rizika (k tomu viz též teoretickou část práce, kap. 3.4.1). Jak již bylo zmíněno dříve, ve firmě existuje pouze základní školení pro nastupující zaměstnance, kdy jim tým IT bezpečnosti za pomoci jednoduché prezentace představí základní pravidla bezpečnosti a užívání firemního vybavení. Pravidelné školení, které by bylo k dispozici pro všechny zaměstnance, v současné době neexistuje. Tento fakt může být do jisté míry také příčinou, proč výsledky z testování vykazují tak nízkou úspěšnost.

Na základě těchto zjištění byl pro zaměstnance navržen nový formát vzdělávání. Tím, že se jedná o první způsob edukace tohoto typu ve vybraném podniku, bude školení koncipováno co nejjednodušeji s důrazem na základní informace a bude zaměřeno na hlavní indikátory, které by zaměstnanci měli pokaždé v e-mailu kontrolovat. V době příprav této diplomové práce zároveň probíhá ve firmě implementování nového školícího systému, který nahrazuje stávající systém a který nebylo možné v tomto období využít pro tvorbu nových školení. Z tohoto důvodu bylo jako prvotní školení zvolena edukace formou informativního kvízu za pomoci nástroje Microsoft Forms.

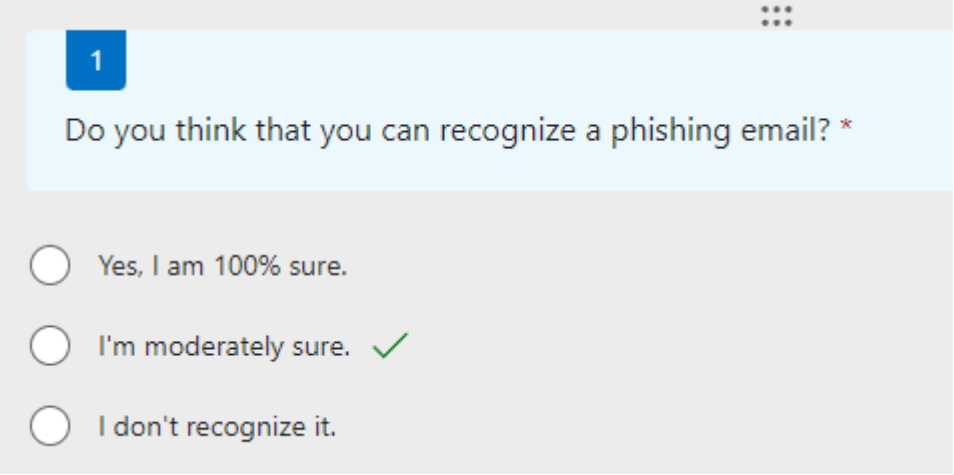
Cílem školení bude edukovat zaměstnance v činnostech:

1. Správného nahlašování podezřelých emailů,
2. Rozpoznávání jednotlivých identifikátorů u podezřelých zpráv v rozsahu:
    a. Kontrolovat adresu odesílatele,
    b. Kontrolovat cílovou adresu, kam link v e-mailu odkazuje,
    c. Zvýšení pozornosti v případě externích e-mailů,
    d. Že škodlivé e-maily mohou mít podobu interních zpráv.

Zaměstnanci budou také proškoleni v oblasti nakládání s podezřelým e-mailem, tj. aby:

1. Nestahovali přílohy z neověřených e-mailů;
2. Navzájem mezi sebou e-maily nepřeposílali;
3. Zkontrolovali cílovou webovou stránku, než provedou jakoukoliv akci.

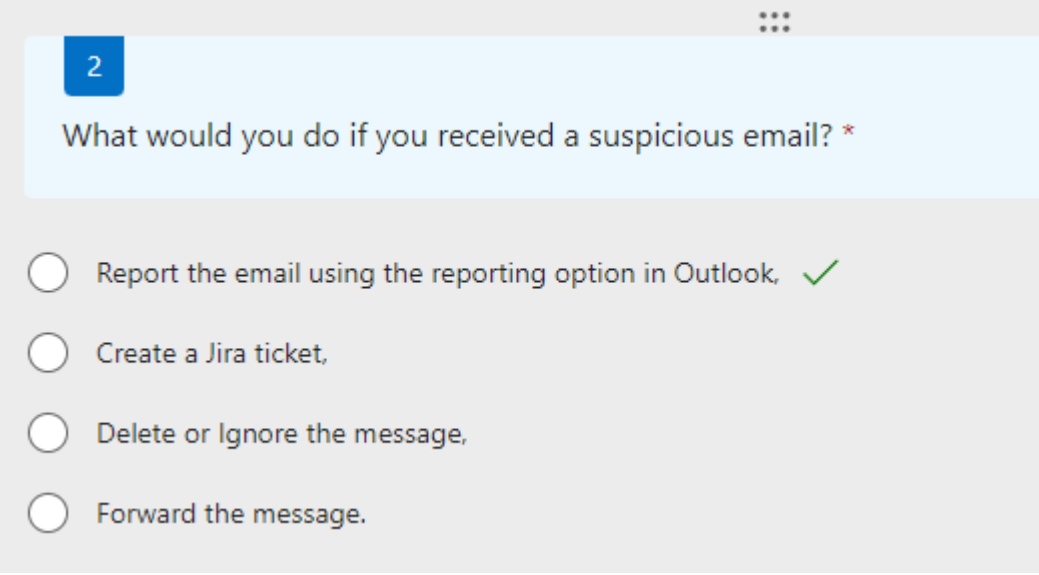
Edukativní kvíz nebyl vytvořen jako hodnotící, tj. nebude nijak vyhodnocován; slouží pouze pro informování zaměstnanců interaktivní formou spolu s vysvětlivkami k jednotlivým tématům a oblastem.




*Obrázek 19 - Školení zaměstnanců - Úvod*

První otázka byla koncipována tak, aby si každý zaměstnanec uvědomil, že byť byl v testování úspěšný, příště se může nedopatřením stát obětí phishingu. V následné informační doložce bylo respondentovi vysvětleno, že taktiky jednotlivých útočníků se neustále zlepšují (viz kapitola 3.7), a tak by měl být zaměstnanec neustále ostražitý (posiluje se zde preventivní složka ochrany před phishingem).

Pakliže zaměstnanec v kvízu označil, že si je na 100 % jistý, že by dokázal identifikovat phishingový e-mail, je informován o tom, že se phishingové útoky neustále vyvíjejí, a proto nelze spoléhat, že zaměstnanec zná všechny typy útoků, které útočníci využívají. Pokud si naopak zaměstnanec není vůbec jistý, dozví se, že je pro něj právě tento kvíz vhodný, jelikož zde bude seznámen se všemi důležitými aspekty, na které by si měl dávat pozor.




*Obrázek 20 - Školení zaměstnanců - Otázka 2*

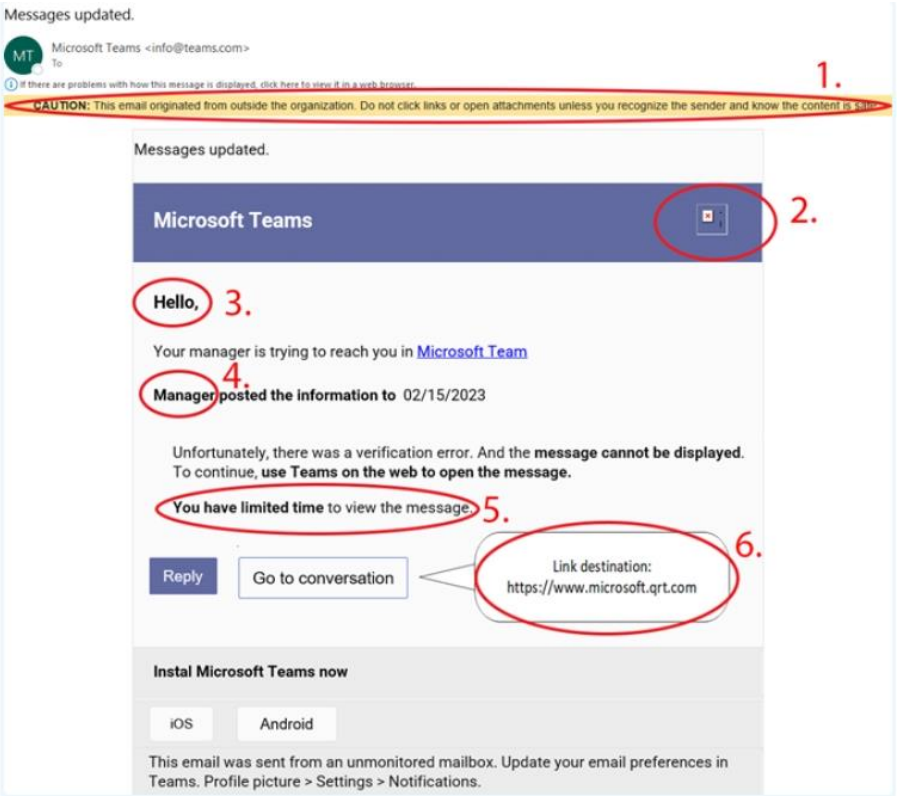
Druhá otázka testovala formou gamifikace zaměstnancovy znalosti v reakčních činnostech na phishingový e-mail. Otázka zněla:

Co byste udělali, pokud byste obdrželi podezřelý e-mail?

1. Reportovali e-mail pomocí reportovacího tlačítka v Outlooku,
2. Vytvořili Jira ticket,
3. Zprávu smazali nebo ignorovali,
4. Přeposlali zprávu.

Následně byli zaměstnanci přesměrováni na další oddíl, který byl přizpůsoben dle jejich odpovědi. Pokud zaměstnanec odpověděl, že zprávu smaže, ignoruje nebo přepošle, bylo mu vysvětleno, že tyto způsoby vhodné nejsou (viz příloha 4). Nahlášení incidentu pomocí Jira ticketu je způsob, který ve firmě existoval předtím, než se zavedlo nové, jednodušší řešení, tedy pomocí reportovacího tlačítka přímo v Outlooku (viz kapitola 4.4.1.2). Zaměstnancům byl následně popsán konkrétní postup, jak toto tlačítko mohou využívat, a objasnění důvodu, proč by zprávy měli nahlašovat. Jelikož zaměstnanci mohou využívat ve firmě různé operační systémy, byl jim popsán postup pro všechny tyto systémy včetně mobilního zařízení (viz příloha 4).

Dalších 5 otázek z kvízu je zaměřeno již na konkrétní e-maily. Zde si zaměstnanci nejdříve mohou zkusit, zda e-mail dokážou správně identifikovat. Nejdříve musí u jednotlivých otázek rozhodnout, zda se jedná o phishing, či legitimní zprávu. Následně jim jsou označeny všechny podezřelé aspekty, kterých si měli všimnout a které jim měly pomoci při rozhodování o správnosti e-mailu. Do kvízu byly zařazeny dva legitimní e-maily a 3 phishigové emaily, vytvořené pro potřeby kvízu.



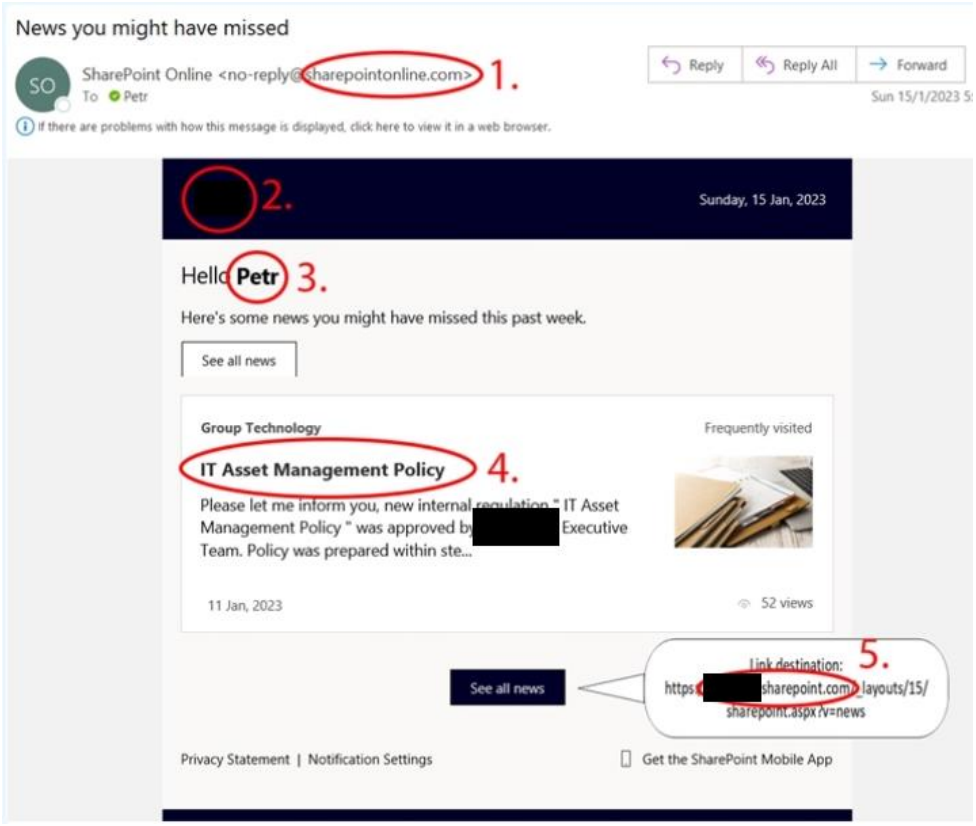

*Obrázek 21 - Školení zaměstnanců - Teams*

Tento obrázek (viz Obrázek 21) již reprezentuje druhý bod, ve kterém jsou zaměstnanci upozorněni na jednotlivé ukazatele škodlivého e-mailu. Zaměstnancům zde bylo doporučeno několik kroků, jak se zachovat při obdržení jakéhokoliv e-mailu, a to:

1. Nejprve si prohlédnout identifikátory v e-mailu, než kliknete na odkaz,
2. Pro zobrazení URL adresy je vždy nutné pouze najet na odkaz kurzorem,
3. Zkontrolovat adresu odesílatele.

**Popis všech ukazatelů, které naznačují, že se jedná o podvodný e-mail:**

1. Legitimní zpráva od služby Teams by neobsahovala varování o externím odesílateli; pokud uvidíte externí varování, buďte opatrní, než něco podniknete,
2. Logo nelze zobrazit,
3. Nachází se zde pouze obecný pozdrav,
4. Legitimní e-mail by měl obsahovat jméno manažera; ne pouze obecný název pozice,
5. Tento e-mail využívá časového nátlaku k získání rychlé odpovědi,
6. Na všechny odkazy vždy najeďte kurzorem, než na ně kliknete; pokud se vám URL adresa hypertextového odkazu nezdá správná, nebo neodpovídá kontextu e-mailu, nevěřte jí.



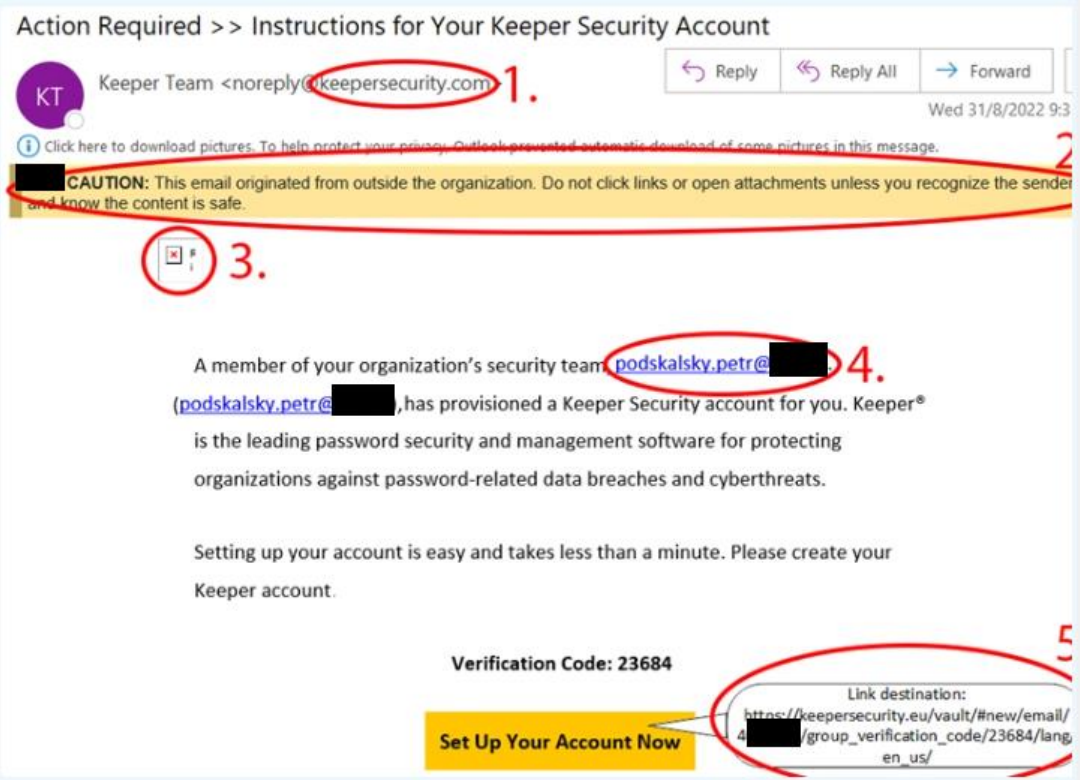

*Obrázek 22 - Školení zaměstnanců - Sharepoint*

Druhý obrázek (viz Obrázek 22) byl navržen tak, aby odpovídal přesné podobě interního e-mailu, který notifikuje zaměstnance o novinkách na intranetu. Zde se jednalo o legitimní e-mail. Je stěžejní, aby si zaměstnanci sami dokázali ověřit pravost e-mailové zprávy a rozlišit jej od phishingu (nebo, v případě nejistoty, se obrátit doporučeným postupem na příslušné oddělení). V následujících popisech je zvoleno přímé oslovení zaměstnanců.

**Popis všech ukazatelů, které naznačují, že se jedná o běžný e-mail:**

1. Pokud jste zkontrolovali adresu odesílatele, mohli jste si všimnout, že se jedná o platnou doménu,
2. Vždy je lepší být obezřetný; pokud vám e-mail přijde podezřelý, můžete si zkopírovat e-mailovou adresu odesílatele a vyhledat, zda jste od tohoto odesílatele v minulosti nějakou zprávu obdrželi,
3. Mohli jste si všimnout oficiálního loga,
4. V e-mailu je uvedeno jméno příjemce:
    a. To ale nemusí nutně znamenat, že se jedná o validní e-mail. Útočníci mohou snadno zjistit jméno příjemce a zneužít této znalosti.

5. Pokud byste otevřeli náš firemní Sharepoint a vyhledali název tohoto článku, zjistili byste, že skutečně existuje,
6. Pokud byste na odkaz najeli myší, viděli byste, že URL adresa je v pořádku.




*Obrázek 23 - Školení zaměstnanců - Keeper*

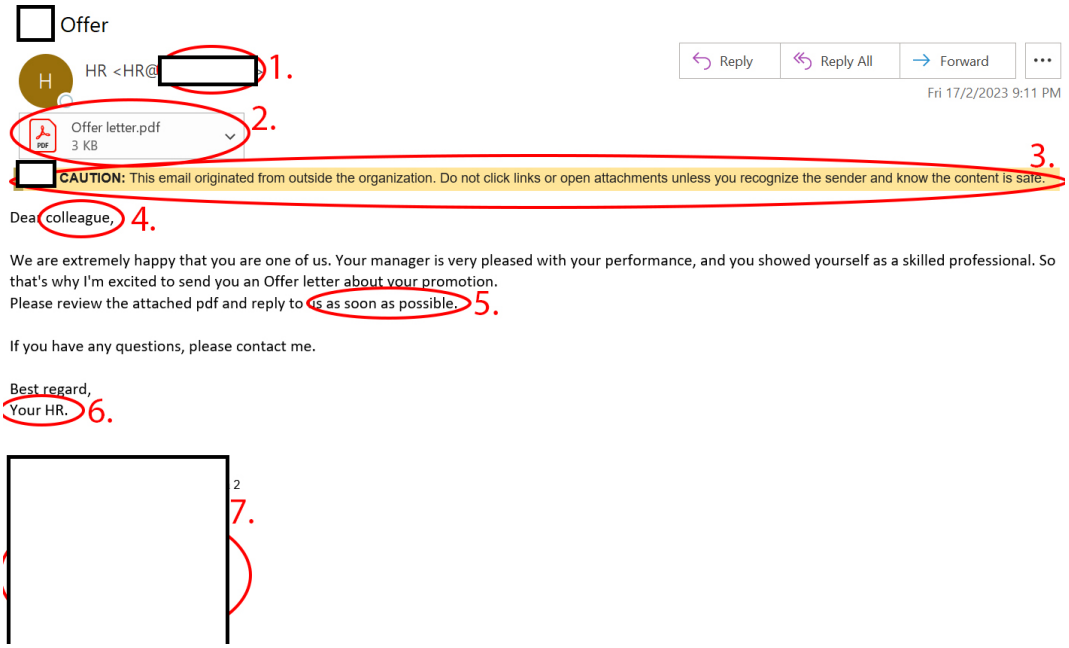
Třetím obrázkem (viz Obrázek 23) byla notifikace, která zaměstnancům přišla ze společnosti Keeper. Jedná se o legitimní e-mail, který zaměstnance informoval o vytvoření nového účtu ve firemním systému pro správu hesel. Mnozí zaměstnanci tento legitimní e-mail označili jako phishingový, a proto byl umístěn do tohoto kvízu, aby zaměstnancům demonstroval správný postup, na základě kterého si sami dokáží legitimitu ověřit.

**Bezpečnostní ukazatele:**

1. Pokud byste se podívali na oficiální webové stránky společnosti Keeper, zjistili byste, že e-mail obsahuje správnou e-mailovou doménu,
2. Upozornění, že e-mail pochází zvenčí,
    a. Jak již bylo zmíněno, neznamená to automaticky, že se jedná o škodlivý e-mail. Tuto službu poskytuje třetí strana, a proto se zobrazilo toto varování.
3. Aplikace Outlook může zabránit stažení některých obrázků,
    a. Tedy i pokud se vám správně nezobrazí, nemusí to automaticky znamenat, že se jedná o phishingovou zprávu.
4. Mohli jste si zkontrolovat, zda tento uživatel ve společnosti existuje,

a. Útočníci samozřejmě mohou jména některých zaměstnanců zjistit různými způsoby poměrně snadno. Existence zaměstnance proto automaticky neznamená, že je e-mail bezpečný,
b. Vždy je lepší kontaktovat danou osobu jiným způsobem, např. prostřednictvím služby Teams, a ověřit, zda se jedná o platný e-mail (zda daná osoba e-mail skutečně odeslala), nebo ne.

5. Pokud byste na odkaz najeli myší, zjistili byste, že se jedná o správnou doménu.



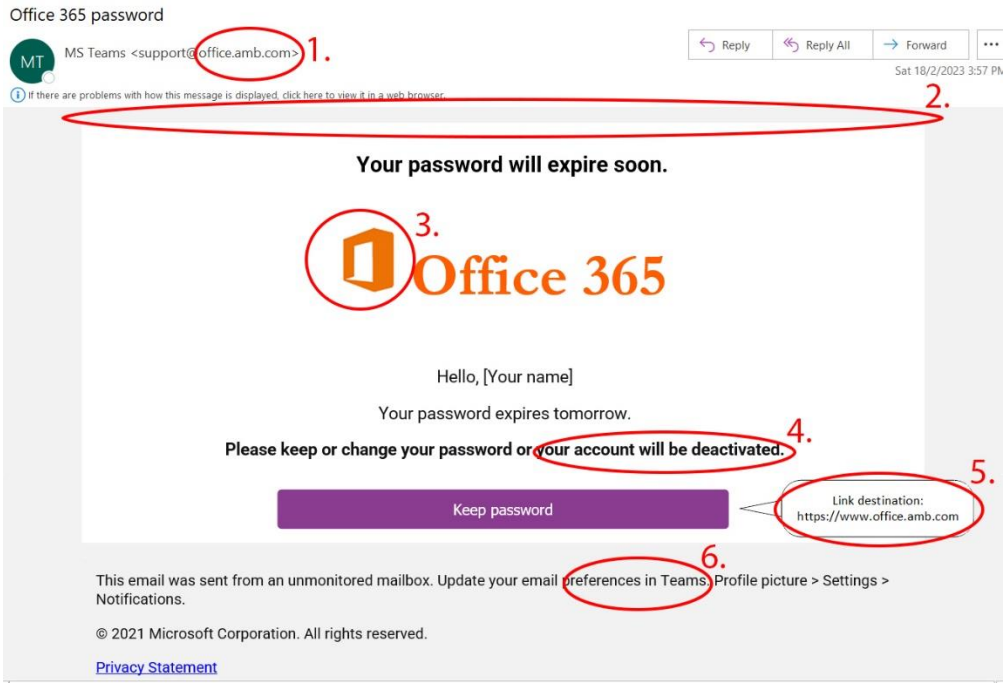

*Obrázek 24 - Školení zaměstnanců - HR Offer*

Následující kvízová otázka měla zaměstnance upozornit na podvodné e-maily, které se zaměřují na jejich důvěřivost či chamtivost, tedy na stěžejní zranitelnosti zneužívané při užití technik sociálního inženýrství (viz kapitola 3.3.3 Motivace oběti). V příkladu je zaměstnanci nabídnuto od personálního oddělení povýšení a přiložena příloha s více informacemi.

**Popis všech ukazatelů, které naznačují, že se jedná o podvodný e-mail:**

1. Doména odesílatele; Je možné si všimnout, že doména odesílatele je [nazev firmy]eg.com, což není správná firemní e-mailová doména,
    a. Jedním z běžných typů útoku je podvržení e-mailové domény. Útok je založen na vynechání jednoho písmene, jeho nahrazení velmi podobným písmenem nebo použití subdomény ([nazev firmy].anything.com), nebo na změně 1. domény ([nazev firmy].onsite) (viz kapitolu 3.6),
    b. Proto je velmi důležité, abyste si vždy pečlivě prohlédli adresu odesílatele.

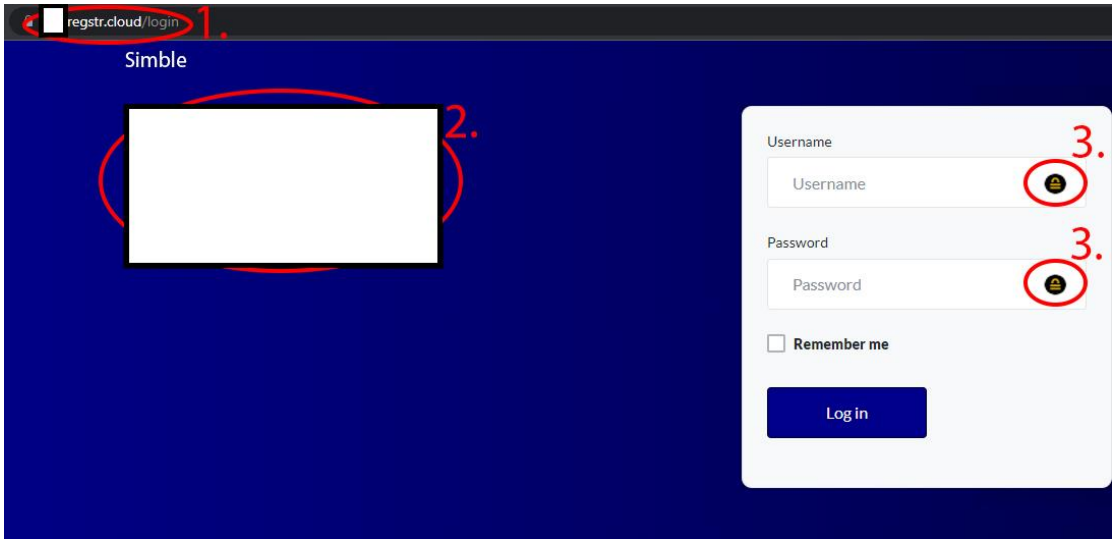
2. Přiložený soubor, v tomto případě soubor s příponou .pdf, může obsahovat malware, který může spustit škodlivý kód,
    a. Proto se před stažením nebo otevřením souboru vždy ujistěte, že se nejedná o podvodný e-mail.
3. Legitimní zpráva od personálního oddělení by neobsahovala varování o externím odesílateli; pokud tedy uvidíte externí varování, buďte opatrní, než něco uděláte,
4. Pokud by vám někdo z personálního oddělení poslal e-mail o povýšení, pravděpodobně by zvolil osobnější pozdrav,
5. Využití časového nátlaku k získání rychlé odpovědi,
6. Není příliš pravděpodobné, že by odesílatel nenapsal své jméno,
7. Útočníci mohou ukrást firemní loga, proto přítomnost loga není určující pro legitimitu zprávy.




*Obrázek 25 - Školení zaměstnanců - Office 365 password*

Posledním příkladem byla notifikace ze systému MS Office, se kterou se může setkat každý zaměstnanec firmy. Jednalo se o základní typ útoku, který upozorňuje na vypršení platnosti hesla a zároveň dostává adresáta pod časový tlak, aby byla reakce okamžitá a dotyčný byl méně ostražitý (více o využití nátlaku při útoku např. v kapitole 3.3.3). I v tomto případě byly zaměstnancům představeny a doporučeny kroky, podle kterých by se měli řídit a postupovat. Tato zpráva byla do kvízu umístěna rovněž z důvodu, že byť nebyla označena

za zprávu od externího odesílatele, i tak se jednalo o podvodný e-mail. Je nutné, aby si zaměstnanci uvědomili, že i když zpráva neobsahuje naše interní varování, nemusí to automaticky znamenat, že je e-mail v pořádku.




*Obrázek 26 - Školení zaměstnanců - Přihlašovací stránka*

Poslední otázka byla do kvízu umístěna jako reakce na vysoký počet zaměstnanců, kteří na nelegitimní webové stránce v rámci testování zadali své osobní údaje (viz kapitola 4.3.1.5). Zaměstnancům byla představena konkrétní situace, kdy jsou přesměrováni na webovou stránku, kde mají zadat své osobní údaje (viz Obrázek 26). Následně jim byly představeny kroky, jak si tuto stránku ověřit a identifikovat případné nesrovnalosti:

1. Vždy byste měli zkontrolovat název domény stránky,
    a. [nazevfirmy].regstr.cloud - Není správná adresa,
    b. Pokud si nejste jisti správností adresy, je vždy lepší stránku zavřít a navštívit ji napřímo. Zjistěte si například správnou adresu z našeho firemního Sharepointu a poté použijte oficiální adresu, která je zde uvedena,
2. Pokud jste navštívili některý z našich interních systémů, můžete si všimnout, že se v tomto případě jedná o falešné logo,
3. V naší společnosti nově používáme nástroj Keeper, což je náš správce hesel,
    a. Jednou z jeho výhod je, že Keeper umí automaticky vyplňovat vaše osobní údaje pouze na té stránce, pro kterou jste si je uložili.

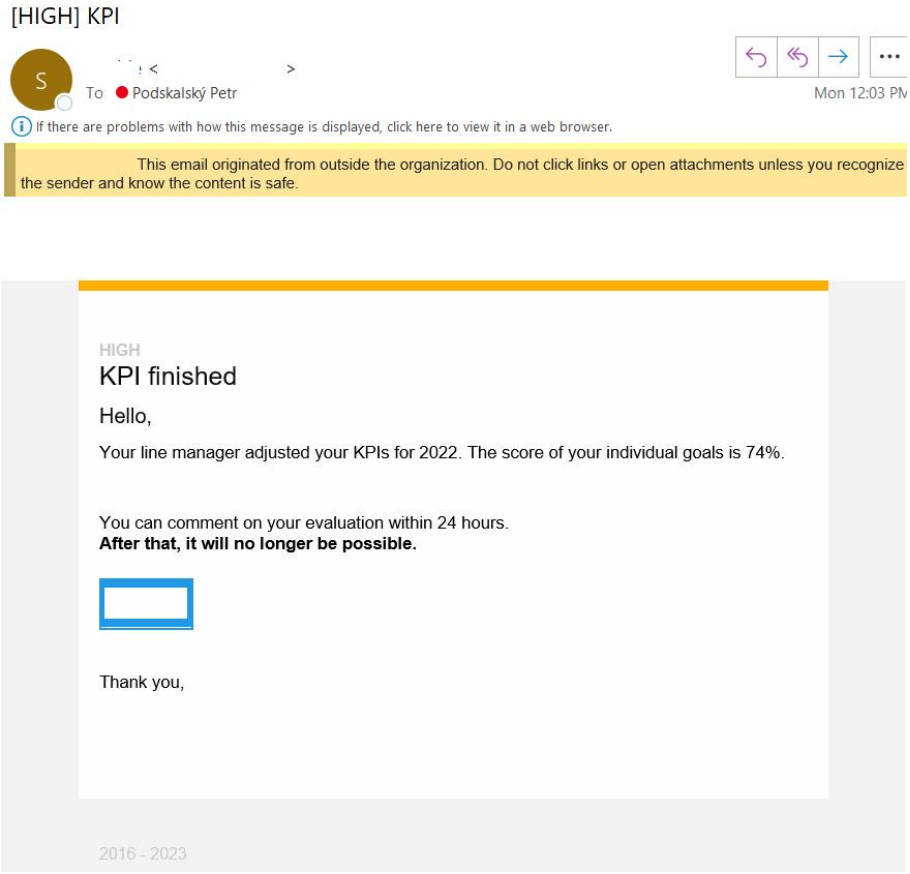
V závěru kvízu byl zaměstnancům předložen krátký přehled všech důležitých informací, které v rámci celého kvízu zazněly a které je nutné brát v potaz při jejich dalších aktivitách. Aby měli zaměstnanci možnost se ke kvízu znovu vrátit, byl tento umístěn na

firemní intranet, kde je možné jej opakovaně absolvovat, čímž se z něj stává pomůcka využitelná při možných reálných útocích.

### 4.3.3 Otestování účinnosti zavedených organizačních opatření

Pro otestování, zda byla zavedené organizační opatření popsaná v této práci účinná, a zda se díky nim povedlo rozšířit povědomí zaměstnanců o phishingových e-mailech a poučit je, jak s nimi zacházet, bylo provedeno náhodné otestování 355 zaměstnanců pomocí phishingové kampaně. Tato kampaň na zaměstnance byla spuštěna po ročním rozestupu od prvotního otestování.

Phishingový e-mail napodoboval notifikaci z interního systému, který využívají zaměstnanci pro zadávání a vyhodnocování svých KPI[12].




*Obrázek 27 - Ukázka útoku - KPI*

V e-mailu byla uvedena informace, která zaměstnance informovala o tom, že jejich hlavní manažer jim nastavil jejich celkové ohodnocení výkonnosti na 74 % a že mají den na

[12] KPI (Key performance indicators neboli klíčové ukazatele výkonnosti, které si každý zaměstnanec na začátku roku nastaví a na konci roku je odměněn dle svých výsledků).

to, aby se k ohodnocení vyjádřili (viz Obrázek 27). Navíc tento e-mail přišel pár týdnů poté, co byly opravdové KPI uzavřeny.

Pro zjištění a vyhodnocení výsledků byl zvolen stejný postup jako v předchozích testování, kdy bylo sledováno, zda si zaměstnanec e-mail zobrazil, smazal, klikl na link či zadal osobní údaje na škodlivé webové stránce (viz příloha 5).

**Základní přehled**

| **Kampaň** | **Celkem otestováno** | **Přečtení e-mailu** |
|---|---|---|
| Informace o KPI | 355 | 270 (76 %) |

*Tabulka 2 - Základní přehled testování zaměstnanců 2. kolo*

Z výsledné tabulky je patrné, že 76 % zaměstnanců si minimálně e-mail zobrazili. Rozbor jednotlivých akcí, které zaměstnanci s e-mailem provedli, je zaměřen pouze na ty zaměstnance, kteří e-mail minimálně viděli. Proto dále bude počítáno pouze s 270 zaměstnanci.

**Detailní přehled kampaně**

| **Kampaň** | **Přečtení e-mailu** | **Včasné nahlášení** | **Ignorování / Smazání zprávy** | **Kompromitovaní zaměstnanci** (minimálně klikli na link) |
|---|---|---|---|---|
| Informace o KPI | 270 | 89 (33 %) | 97 (36 %) | 84 (31 %) |

*Tabulka 3 - Souhrnný přehled testování zaměstnanců 2. kolo*

Oproti prvotnímu testování je vidět lehké snížení kompromitovaných zaměstnanců; jedná se zde o 31 % zaměstnanců, kteří minimálně klikli na link. Velkého zlepšení se dočkalo nahlašování e-mailů; při druhém testování 33 % otestovaných zaměstnanců již správně nahlásilo škodlivý e-mail. U prvotního testování to bylo pouhých 6 % zaměstnanců.

**Druhá pracovní hypotéza tedy byla ověřena částečně. Včasné nahlášení sice bylo provedeno u třetiny zaměstnanců, což potvrzuje předpoklad, že při vhodně zavedených organizačních opatřeních dojde ke zlepšení postupu zaměstnanců, ale počet kompromitovaných zaměstnanců zůstává nadále vysoký.**

Toto lze vysvětlit např. nutností dalšího vzdělávání a pokračování v phishingových kampaních v delších intervalech, aby byli zaměstnanci v rámci prevence neustále připravováni na potenciální skutečný útok. Při omezeném dosahu edukativního kvízu zřejmě odezva nebyla dostatečná.

## 4.4 Technická opatření

Tato kapitola se zaměřuje na technická opatření aplikovaná v podniku. V kapitole je zhodnoceno, zda firma využívá veškeré možné bezpečnostní funkce, které služba Microsoft 365 nabízí, zda je ve firmě správně nastaven DKIM, DMARC a SPF. Dále je v kapitole navržen nový způsob notifikování uživatelů, přičemž tato notifikace zaměstnance upozorní, že příchozí e-mail pochází z prostředí mimo vybraný podnik. Také je zde nastaven nový způsob reportování pro uživatele. Druhá část kapitoly se věnuje odezvě v momentě, kdy e-mail projde přes bezpečnostní opatření do schránky uživatele a nástroje jej tedy včas a správně nezachytí. V závěru této kapitoly budou představena doporučení pravidel, na kterých by měla každá firma lpět v rámci své bezpečnostní politiky. Tato vychází ze zkušeností s vybraným podnikem a jsou extrapolovatelná díky své obecnosti na větší množinu organizací.

### 4.4.1 Prevence

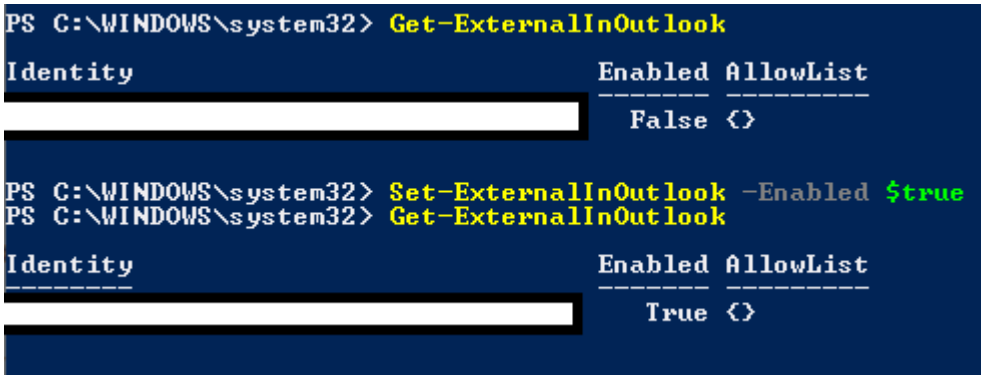
Prevenci lze ve firmě rozdělit na dvě části. První část je věnována zaměstnancům, tedy zajištění dostatečného školení pro zaměstnance (viz kapitola 4.3), jakož i co nejvýraznějšímu usnadnění rozpoznávání interních a externích e-mailů a rozdílů mezi nimi. Druhá část prevence slouží k tomu, aby firma zajistila co nejvyšší procento odchycených škodlivých e-mailů dříve, než se škodlivý e-mail vůbec k zaměstnanci dostane.

#### 4.4.1.1 Označení externích e-mailů

Dle názoru autora je velice důležité, aby uživatelé hned na první pohled dokázali identifikovat, zda se jedná o interní zprávu či externí zprávu (k tomu viz teoretickou část práce). Tohoto lze dosáhnout pomocí dvou způsobů:

1. Upravit globální nastavení pomocí PowerShell a nastavit v něm upozornění na hlavičku e-mailu,
2. Nastavení nového pravidla v Mail Flow pro příchozí zprávy.

### Úprava pomocí PowerShell




*Obrázek 28 - Označení externích e-mailů - PowerShell*

Nejprve bylo pomocí příkazu Get-ExternalInOutlook (viz Obrázek 28) zjištěno, že notifikace nebyla doposud ve firmě aktivována. Následně pomocí příkazu *Set-ExternalInOutlook -Enabled $true* byla tato notifikaci zapnuta (lze vidět taktéž na obrázku č. 28). Pokud by bylo potřeba, lze přidat další domény, pro které by toto pravidlo neplatilo, a tedy zaměstnanci by nebyli upozorněni, že se jedná o externí zprávu. Povolené domény lze přidat pomocí příkazu: *Set-ExternalInOutlook -AllowList @{Add="domain1", "domain2"}.*

### Nastavení pravidel v Mail Flow

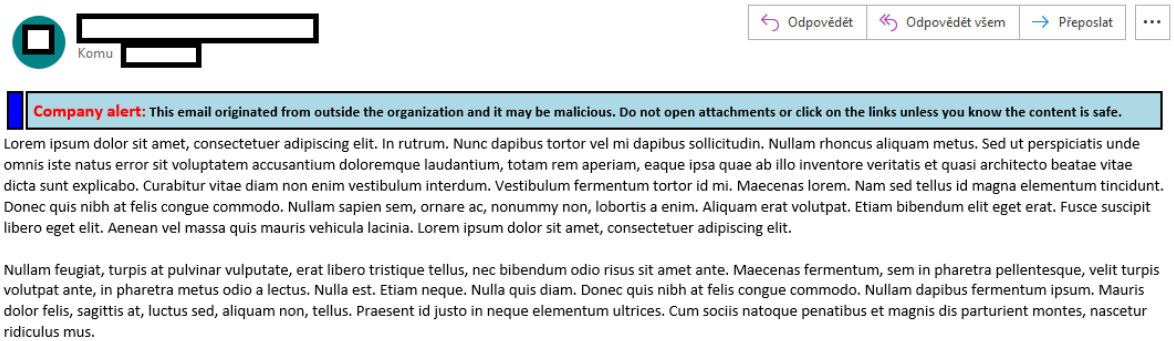
Druhým způsobem, kterým lze uživatele informovat, že e-mail přichází z prostředí mimo organizaci, je nastavení správného pravidla. Toto pravidlo bylo nastaveno v Exchange admin center – Mail Flow – Rules. Tato pravidla neslouží pouze pro nastavení upozornění pro uživatele, ale umožňují další funkce, jako je přeposílání zpráv na zvolený cílový e-mail v případě, kdy je splněna definovaná podmínka, smazání zpráv, zakázání automatického přeposílání atd. Zde již má firma několik svých definovaných pravidel implementovaných.

Pravidlo pro firmu bylo navrženo tak, že se zobrazí upozornění vždy v momentě, kdy e-mail dorazí jakémukoliv zaměstnanci na firemní účet a zároveň odesílatel e-mailu pochází z prostředí mimo organizaci. V momentě splnění této podmínky je na základě pravidla vloženo do těla e-mailu upozornění, které bylo navrženo pomocí html kódu.

```
<style>
  table, th, td {
    border:2px solid black;
    border-spacing: 0pt;
  }
  table {
    padding-bottom:10pt;
    border: none;
  }
  td {
  padding:4pt;
  }
  .alert {
    color:red;
    font-weight: bold;
    font-size: 12pt;
  }
  .notify{
    font-size: 10pt;
    font-weight: bold;
  }
</style>

<body>
  <table cellpadding=0 width="100%">
    <tr>
    <td style="background:blue;"></td>
    <td width="100%" style="background:lightblue;word-wrap:break-word">
      <div class="notify" style="color:black;">
        <span class="alert">Company alert:</span>
        This email originated from outside the organization and it may be malicious.
        Do not open attachments or click on the links unless you know the content is
        safe.
      </div>
    </td>
    </tr>
  </table>
</body>
```

*Kód 1 - Upozornění na příchozí externí e-mail*




*Obrázek 29 - Označení externích e-mailů – pravidla v MailFlow*

Na obrázku (viz Obrázek 29) je již vidět finální výsledek implementovaného řešení. Pro firmu byla zvolena odlišná barva upozornění ve firemních barvách. Pro zachování anonymity byl tento formát upozornění upraven.

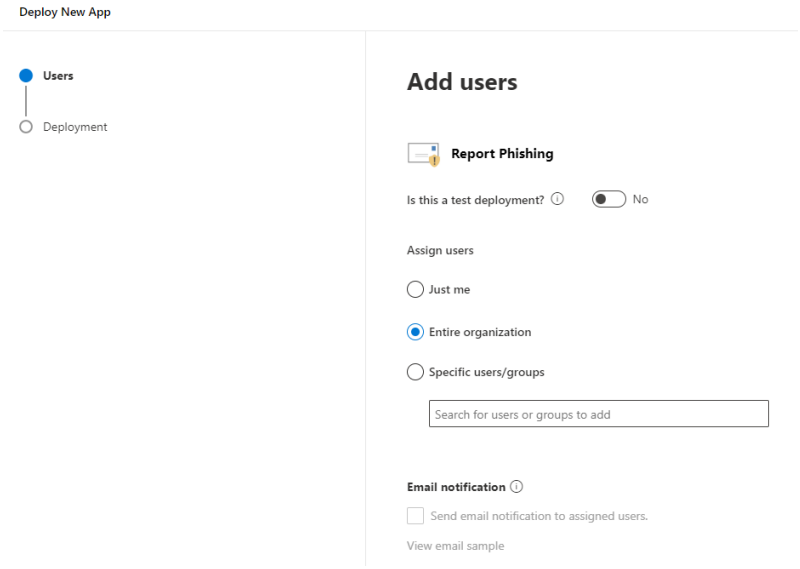
První způsob označení přes PowerShell je velice snadným a rychlým řešením, které se zobrazuje v e-mailovém klientu elegantněji a součástí upozornění je i tag, který v přehledu zobrazí string: External. Nicméně celkové upozornění tímto způsobem nelze nijak graficky editovat, a proto musí zůstat v základní nastavené podobě; uživatel tak může upozornění při nepozornosti přehlédnout. Rovněž zde není možnost nastavení vícero podmínek, pouze lze přidat důvěryhodné domény.

Oproti tomu druhý způsob upozornění přes pravidla umožňuje naprosté přizpůsobení dle potřeb a požadavků firmy. Grafická úprava je vytvořena pomocí html kódu, tedy lze upozornění navrhnout dle představ zaměstnanců zodpovědných za kybernetickou bezpečnost, či managementu. Také jednotlivé podmínky umožní vytvoření rozsáhlejšího souboru pravidel, které umožňují diverzifikovat notifikaci pro zaměstnance. Například by bylo možné připravit specifické upozornění pro e-mail, který v sobě obsahuje nějakou přílohu a důrazněji na ni upozornit. Nevýhodou tohoto způsobu je fakt, že v momentě přeposílání zpráv tento kód v e-mailu již zůstane a následně se vrství, což není vždy žádané.

Pro potřeby firmy byl zvolen druhý způsob upozornění, který je uživatelsky přívětivější a na pohled lehce identifikovatelný.

#### 4.4.1.2 Nastavení tlačítka pro nahlašování phishingu

Jelikož ve firmě existoval poměrně složitý a zdlouhavý postup pro nahlašování potenciálně škodlivého či podezřelého e-mailu, bylo pro zaměstnance navrženo a implementováno jednodušší řešení. Pokud nově zaměstnanci obdrží e-mail, u kterého se domnívají, že je škodlivý, nemusí již vytvářet incident přes Jira systém. Stačí pouze v otevřeném e-mailu kliknout na reportovací tlačítko, které škodlivý e-mail odešle na prozkoumání do bezpečnostního systému vybraného podniku. Tato funkcionalita přinesla zaměstnancům zjednodušení pro nahlašování, jakož i mnohem více informací o konkrétním e-mailu pro IT bezpečnostní exporty.




*Obrázek 30 - Implementace nahlašovacího tlačítka*

Instalace tlačítka od Microsoftu je velice jednoduchá, stačí v prostředí Microsoft 365 admin center jít do nastavení – integrované aplikace – získat novou aplikaci – nainstalovat reportovací tlačítko. Tlačítko bylo nainstalováno pro celou organizaci (viz Obrázek 30).

#### 4.4.1.3 Nastavení filtrů

Jedním z hlavních prostředků obrany proti phishingovým e-mailům je mít správně nastavené filtrové politiky. Firma má tyto filtry již nastavené, ale v rámci revize byla provedena jejich kontrola a následné přenastavení v anti-spamové a anti-phishingové politice.

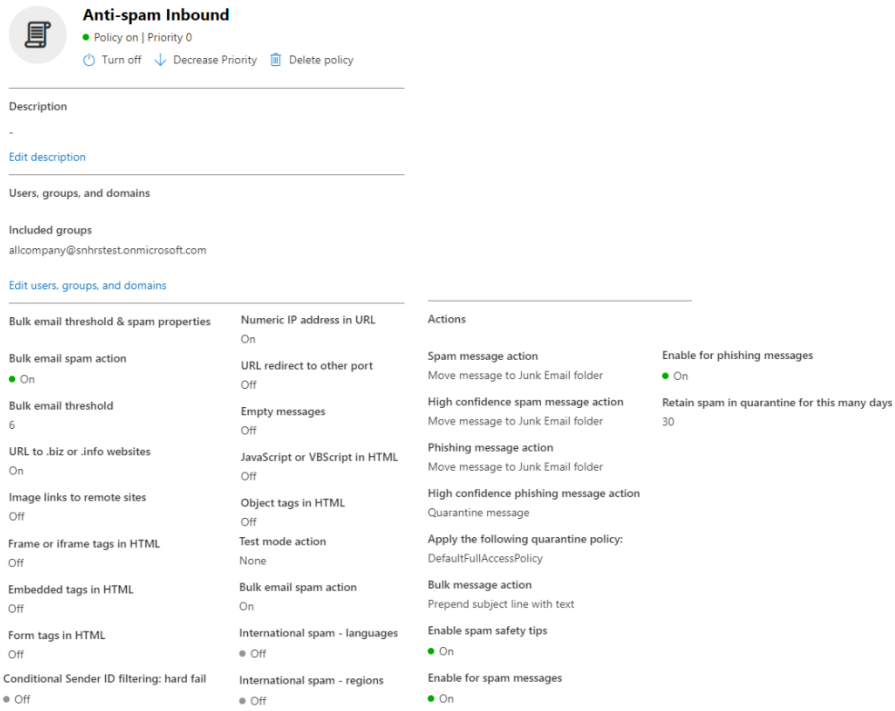
**Anti-SPAM**

Pro nastavení správného SPAM filtru se vycházelo ze základního doporučení Microsoftu (viz teorie) a potřebám firmy. Nastavení se provedlo v systému Microsoft 365 Defender, ve kterém vznikla nová antispamová zásada dle těchto vlastností:

| **Skupina vlastností** | **Hodnoty** |
|---|---|
| Priorita | 0 |
| Zahrnutá skupina | allcompany |
| Bulk Email threshold | 6 |
| URL to .biz or .info websites | On |
| Numeric IP address in URL | On |
| Bulk email spam action | On |
| SpamAction | Move to Junk |
| HighConfidenceSpamAction | Move to Junk |

| | |
|---|---|
| PhishSpamAction | Move to Junk |
| HighConfidencePhishAction | Move to Quarantine |
| BulkSpamAction | Move to Junk |
| QuarantineRetentionPeriod | 30 dnů |
| Zero-hour auto purge | On (phishing, spam) |

*Tabulka 4 - Anti-SPAM politika*




*Obrázek 31 - Nastavení Anti-spam politiky*

## Anti-phishing

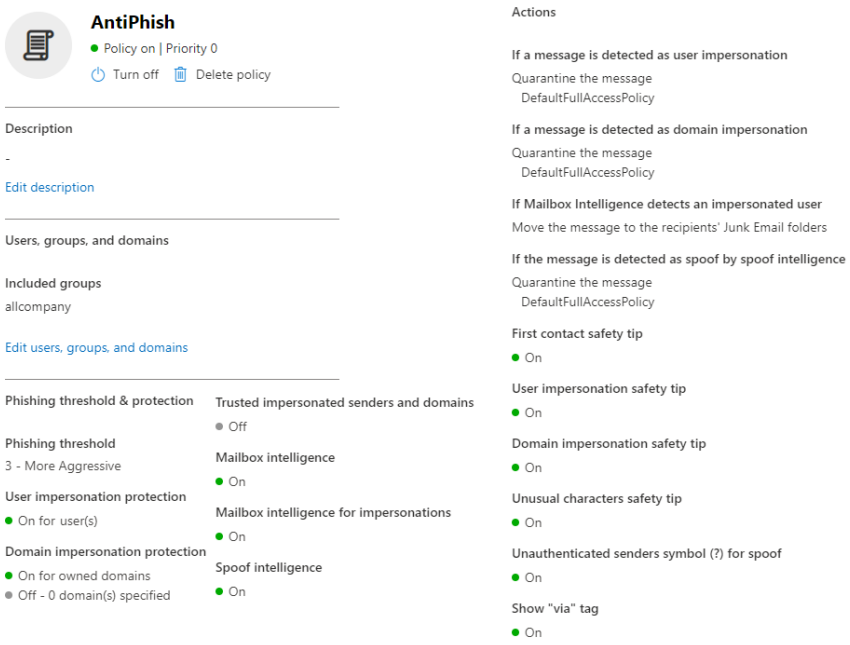
Nastavení Anti-phishingu probíhalo obdobně jako u SPAM filteru. Na základě doporučených hodnot od Microsoftu (viz teorie) a potřebám firmy, bylo optimalizováno již z vytvořené Anti-phishingové zásady.

| **Skupina vlastností** | **Hodnoty** |
|---|---|
| Priorita | 0 |
| Zahrnutá skupina | allcompany |
| Phishing threshold | 2 - Aggressive |
| TargetedUsersToProtect | 62 users (Top management, HR) |
| Domain impersonation | On – for owned domains |
| EnableMailboxIntelligence | On |
| Detected as user impersonation | Move to Quarantine |

| | |
|---|---|
| Detected as domain impersonation | Move to Quarantine |
| Mailbox Intelligence detects an impersonated user | Move to Quarantine |
| detected as spoof by spoof intelligence | Move to Quarantine |

*Tabulka 5 - Anti-phishing politika*

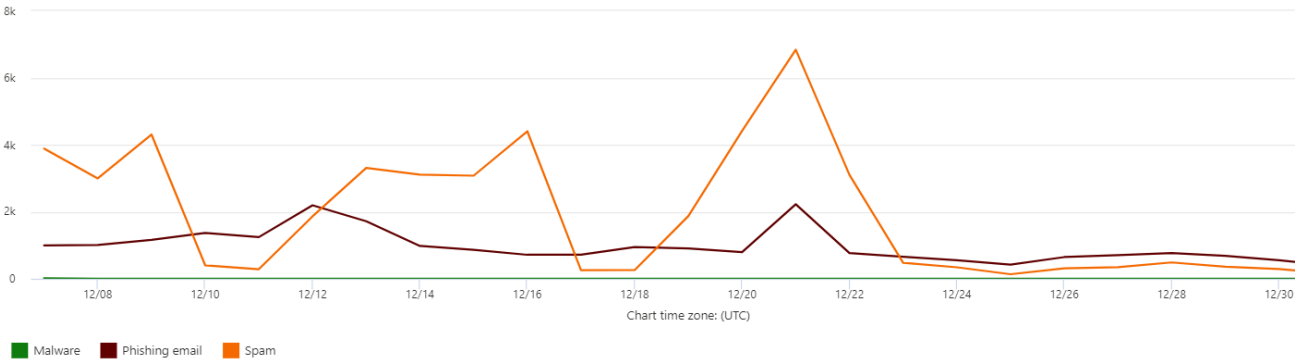
V anti-phishingové zásadě bylo vybráno 62 zaměstnanců, kteří byli zařazeni do ochrany uživatelů, přičemž se jednalo primárně o top management. Tato možnost byla zvolena z toho důvodu, že zprávy od těchto uživatelů podléhají kontrole, zda se nejedná o typ útoku zosobnění; tedy že se pouze útočník nesnaží vydávat za tyto osoby. Stejný přístup byl zvolen pro domény vlastněné firmou.




*Obrázek 32 - Nastavení Anti-phishingové politiky*

## Statistika škodlivých e-mailů

S existujícími pravidly byl sledován stav příchozích e-mailů a bylo tak zkontrolováno, že pravidla vyfiltrují alespoň část škodlivých e-mailů.




*Obrázek 33 - Filtrování škodlivých příchozích e-mailů*

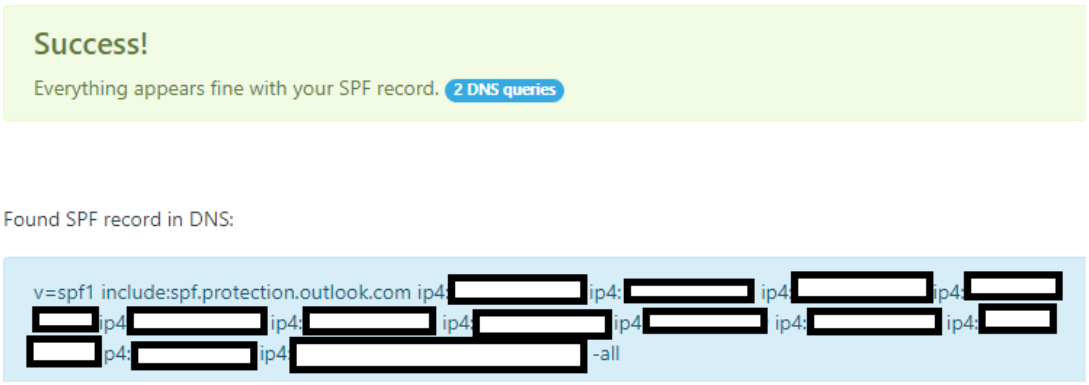
Z grafu (viz Obrázek 33) jsou vidět všechny e-maily které byly zablokované v období od 7. 12. 2022, až do 31. 12. 2022 z důvodu anti-phishingové a anti-spamové politiky. Phishingových e-mailů bylo zablokováno celkem 23986; SPAM e-mailů bylo zablokováno celkem 47286. Z grafu lze vidět značný nárůst celkově škodlivých e-mailů v období před vánočními svátky, což souvisí právě s technikami sociálního inženýrství, stresem a nepozorností zaměstnanců a akcentem na štědrost a chamtivost (viz teoretickou část práce).

#### 4.4.1.4 Kontrola SPF, DKIM, DMARC

Jedním z důležitých technických aspektů při ověřování e-mailů je trojice SPF, DKIM a DMRARC (viz kapitolu 3.5.2). Jelikož ve firmě jsou tato tři opatření již implementována, bylo otestováno, zda jsou správně nastavena a zda nebudou nalezeny nedostatky, které by si vyžádaly změnu technických opatření.

**SPF**

SPF je DNS záznam, který v sobě obsahuje informaci všech serverů, které mají povolené posílat e-maily z konkrétní domény. Pro ověření všech konkrétních domén firmy, zda mají nastavené SPF, byl využit online nástroj dmarcly.com.




*Obrázek 34 - SPF záznam*

Z obrázku (viz Obrázek 34) je vidět, že SPF záznam pro specifickou doménu je v pořádku. Ze záznamu je patrné, že firma využívá službu Outlook, a proto je nutné ho zahrnout mezi povolené odesílatele. V záznamu je dále povoleno několik dalších IP adres, které mají povoleno odesílat zprávy z konkrétní domény. Tyto adresy byly prověřeny a jedná se ve všech případech o validní důvody, nevyžadující další zásah. Z provedeného testu je také vidět, že firma využívá -all, což značí nastavení přísné politiky, tedy když zpráva přijde z neautorizovaného serveru, příjemce by ji měl odmítnout. Tímto způsobem byly otestovány všechny domény i subdomény, které firma využívá, a žádné nesrovnalosti nebyly nalezeny. Je tedy patrné, že firma má tento aspekt kybernetické bezpečnosti v pořádku.


*Obrázek 35 - Nastavení SPF záznamu*

SPF záznam je velice jednoduché nastavit, stačí spravovanou doménu přidat v Microsoft 365 admin centru. V tento moment služba vygeneruje základní DNS záznam pro SPF, přičemž tento DNS záznam pak stačí přidat u poskytovatele domény.

**DKIM**

Pro ověření správného nastavení DKIM záznamu byl využit nástroj dmarcanalyzer.com. Bylo zjištěno, že firma pro své hlavní domény má všude nastavený správný DKIM záznam. Pro své klíče využívá šifru rsda o délce 1024 bitů, což je doporučený standart pro DKIM. Dalo by se zvážit případné zvýšení na délku 2048-bit, nicméně existují případy, kdy tato délka nebyla DNS poskytovatelem podporována a pak byly e-maily označovány jako SPAM. Z tohoto důvodu lze říci, že i v tomto případě má firma tento aspekt dostatečně zabezpečen, přičemž, jak je řečeno, by vyšší bezpečnost při zvětšení délky šifry mohla vést k nežádoucím výsledkům.

Nastavení ve službě Microsoft je opět jednoduché a relativně intuitivní. Ve službě Microsoft 365 Defender je třeba jít do politik a pravidel a zde vybrat nastavení e-mailového ověření. Po vybrání domény, pro kterou je v plánu nastavit DKIM, Microsoft vygeneruje dva veřejné CNAMEs záznamy pro selector1 a selector2. Tyto záznamy je opět nutné nastavit u DNS poskytovatele domény, poté stačí zakliknout podepisování zpráv pomocí DKIM podpisu v Microsoft 365 Defender. Následně je vše správně nastaveno.

**DMARC**

Je velice důležité, aby firma měla správně nastavenou technologii DMARC, která navazuje na předchozí technologie SPF a DKIM. (viz teoretickou část práce, kap. 3.5.2).

Jelikož firma vlastní několik domén a subdomén, byl v rámci diplomové práce vytvořen PowerShell script, který u všech těchto domén zkontroluje, zda mají nastavený DMARC záznam.

Nejprve si pomocí importu skript nahraje známé domény, které jsou uloženy v souboru .csv. Následně pro každou doménu provede dotaz na DNS server, kde hledá záznamy pro typ TXT. Pokud narazí na jakýkoliv TXT záznam, který začíná názvem DMARC1, uloží si ho do proměnné. Pokud žádný záznam neexistuje, zkontroluje, zda se nejedná o subdoménu. V případě subdomén záleží na dvou aspektech – DMARC může nastavení dědit z hlavní domény, nebo může mít nastavené své pravidlo. Pokud se záznam pro subdoménu nenalezne, zkontroluje skript následně DMARC i pro hlavní doménu. Všechny výsledky následně uloží jako .csv soubor.

```
#Nahraje seznam domen u kterych je potreba overit zda je nastaveny DMARC
$domeny = Import-Csv -Path "C:\ export.csv" -Header "Domena" | ForEach-Object { $_.Domena }
$results = foreach ($domen in $domeny) {
    $zaznamDmarc = $null
    $hostDmarc = "_dmarc." + $domen
     try {
#Resolve-DnsName provede dotaz na DNS server se zadanym nazvem _dmarc.domena. Zaznam typu TXT.
        $txtZaznamy = Resolve-DnsName -Name $hostDmarc -Type TXT -ErrorAction Stop
#Pokud se na zacatku zaznamu vyskytuje DMARC1, tak to ulozi do promenne zaznamDmarc
          if ($txtZaznamy.strings -match "^v=DMARC1") {
             $zaznamDmarc = $txtZaznamy.strings
          }}
    catch
    {}
    if ($zaznamDmarc)
    {
       $vysledek="DMARC zaznam nalezen pro ${domen}"
       $string = $zaznamDmarc -replace ";", " "
       @(
           [pscustomobject]@{ Domena = $domen; Result = $vysledek; Pravidlo="$string"}
        )
    }
    else
    {
#Podminka pro subdomeny. Vytvori hlavni domenu tak, ze rozdeli domenu podle tecek. Nasledne z pole
vybere posledni dva prvky a spoji teckou.
       $hlavniDomena = $domen.Split('.')[-2, - 1] -join '.'
       $hostHlavniDomena = "_dmarc." + $hlavniDomena
       $zaznamDmarcHlavni = $null
       try
       {
          $txtZaznamy = Resolve-DnsName -Name $hostHlavniDomena -Type TXT -ErrorAction Stop
             if ($txtZaznamy.strings -match "^v=DMARC1")
             {
                $zaznamDmarcHlavni = $txtZaznamy.strings
             }
       }
       catch
       {
       }
       if ($zaznamDmarcHlavni )
       {
          $string = $zaznamDmarcHlavni -replace ";", " "
          $vysledek="DMARC nenalezen pro subdomenu ${domen}, ale nalezen pro hlavni domenu
${hlavniDomena}"
          @(
             [pscustomobject]@{ Domena = $domen; Result = $vysledek; Pravidlo="$string"}
           )
       }
       else {
          $vysledek="DMARC nenalezen"
           @(
             [pscustomobject]@{ Domena = $hlavniDomena; Result = $vysledek; Pravidlo="null"}
            )
       }}}
$results | Export-Csv -Path C:\OUTPUT.csv’
```

*Kód 2 - Skript pro kontrolu DMARC záznamů*

Celkově pro firmu bylo otestováno 31 domén.

| Vysledek | Pravidlo |
|---|---|
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen | null |
| DMARC nenalezen pro subdomenu [redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=none sp=none rua=mailto:dmarc-rua@[redacted]n ruf=mailto:dmarc-ruf@[redacted]n adkim=r aspf=s |
| DMARC nenalezen pro subdomenu [redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=none rua=mailto:dmarc-r[redacted] ruf=mailto:dmarc-r[redacted] fo=1 pct=100 |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=none rua=mailto:pi1rqn5o[redacted],mailto:dmarc-[redacted] |
| DMARC nenalezen pro subdom[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC nenalezen pro subdom[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=none sp=none rua=mailto:dmarc-r[redacted] ruf=mailto:dmarc-[redacted] adkim=r aspf=s |
| DMARC nenalezen pro subdom[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=none sp=none rua=mailto:dmarc-rua@[redacted]n ruf=mailto:dmarc-ruf@[redacted] adkim=r aspf=s |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=none sp=none rua=mailto:dmarc-rua@[redacted]n ruf=mailto:dmarc-ruf@[redacted]n adkim=r aspf=s |
| DMARC nenalezen pro subdome[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC nenalezen pro subdome[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC nenalezen pro subdomenu ma[redacted] ale nalezen pro hlavni dome[redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC zaznam nalezen pro [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC nenalezen pro subdomen[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |
| DMARC nenalezen pro subdome[redacted] ale nalezen pro hlavni domenu [redacted] | v=DMARC1 p=quarantine adkim=r aspf=r |

*Obrázek 36 - Kontrola DMARC záznamů u firemních domén*

Na základě výše uvedeného průzkumu lze říci, že má podnik zapnutý DMARC pro svou hlavní doménu. Zde má správně nastavený DMARC, SPF i DKIM záznam. V DMARC záznamu má navíc režim p=quarantine, tedy pokud by zpráva kontrolou neprošla, byla by označena za SPAM. Zde by stálo za zvážení nastavit ještě přísnější režim p= reject. Pro dalších 5 hlavních domén má firma sice DMARC zapnutý, ale pouze v režimu p=none, což znamená, že příjemce na výsledek nebere ohledy. Jelikož jsou tato pravidla u domén, které jsou pro firmu důvěrně známé, měla by co nejdříve tento nedostatek napravit a nenechávat domény pouze v režimu testování. Zodpovědné osoby ve společnosti byly informovány i o tom, že 14 domén vůbec DMARC nastaven nemá.

### 4.4.2 Reakce

Ve firmě byl stanoven proces, podle kterého se bude postupovat v momentě, kdy nastane situace, že phishingový e-mail projde skrze filtrovací pravidla (viz kapitola 4.4.1.3 Nastavení filtrů) do e-mailové schránky zaměstnanci:

1. Získání kopie podvodného e-mailu,
2. Shromáždění artefaktů z podvodného e-mailu a jejich prozkoumání,
3. Provedení obranných opatření,
4. Informování příjemců, kteří obdrželi škodlivý e-mail.

**Získání kopie podvodného e-mailu**

Pro získání kopie škodlivého e-mailu byla využita funkce, která souvisí s reportovacím tlačítkem (viz kapitola 4.4.1.2). V rámci nastavení reportovacího tlačítka byla zapnuta možnost, která přepošle veškeré nahlášené e-maily od zaměstnanců do e-mailové schránky SOC týmu.

**Shromáždění artefaktů z podvodného e-mailu a jejich prozkoumání**

Artefakty lze získat přímo z originálního e-mailu, nebo za využití nástroje Threat Explorer ve službě Microsoft 365 Defender. Zde lze dohledat veškeré e-maily, které byly zaměstnancům poslány, a to včetně jejich detailů.

Důležité prvky, které je nutné pro investigaci získat a ověřit, jsou:

1. Jméno odesílatele,
2. Doménové jméno,
3. IP adresa odesílatele,
4. Zpětná adresa, která by byla využita při odpovědi na e-mail,
5. Předmět e-mailu,
6. Datum a čas,
7. Soubory v e-mailu:
    a. Názvy příloh,
    b. HASH hodnoty příloh,
8. URL adresy v e-mailu
9. Zda e-mail prošel z hlediska ověřování:
    a. DKIM, SPF, DMARC
10. Všechny adresy příjemců

**Provedení obranných opatření**

Ve chvíli, kdy se e-mail prokáže jako podezřelý, musí dojít k následujícím krokům:

1. Přidat škodlivou doménu mezi blokované v Threat policies – Tenant Allow/Block lists; pokud se jedná o specifickou doménu, která byla vytvořena pouze k útoku,
2. Pokud je potřeba blokovat pouze konkrétního odesílatele, pak nastavit e-mailové pravidlo v systému Exchange admin center, které bude zprávy od této osoby posílat do karantény,
3. Blokování IP adres; pouze v nezbytně nutném případě;

4. Pokud bude e-mail posílán od různých odesílatelů se stejným předmětem v e-mailu, pak nastavit e-mailové pravidlo v systému Exchange admin center pro blokování zprávy, která bude obsahovat tento předmět,
5. V případě výskytu škodlivého souboru; zablokovat jeho hash kód v Tenant Allow/Block lists,
6. V situaci, kdy bude phishingový e-mail odkazovat na škodlivou stránku; zablokovat její URL adresu v Tenant Allow/Block lists,
7. Pokud škodlivý e-mail bude doručen více zaměstnancům; smazat e-mail všem zaměstnancům z jejich e-mailové schránky, kteří tento e-mail obdrželi přes Microsoft 365 Defender v Threat Exploreru.

# 5 Výsledky a diskuse

## 5.1 Rekapitulace práce

Jak bylo řečeno v kapitole 2 (Metodika a cíle práce), primárním cílem autora byl návrh vhodné formy obrany proti phishingovým e-mailům. K přiblížení tohoto tématu sloužily teoretické části práce, jež měly za úkol představit:

1. Kybernetickou bezpečnost, respektive některé její základní části (související legislativu, zajištění bezpečnosti apod.),
2. Technické aspekty elektronického přenosu zpráv (e-mailová komunikace) a technické prostředky zabezpečení tohoto přenosu (internetové standardy, spam filtry apod.),
3. Microsoft 365 Defender, primární pracovní nástroj pro praktickou část práce,
4. Phishing – pojem, jak je používán, a s ním související techniky tzv. sociálního inženýrství.

Praktická část práce, čerpající z poznatků teoretické části, se zaměřila na dvě hlavní oblasti:

1. Organizační opatření k ochraně před phishingem, zaměřené na prevenci a vzdělávání (cvičné phishingové kampaně, návodný kvíz),
2. Technická opatření, prováděná nastavením správných pravidel a filtrů pro příchozí poštu, a dále implementací tlačítka pro nahlášení podezřelé e-mailové komunikace, kontrolou existujících protokolů SPF, DKIM a DMARC, a stanovením správného reakčního procesu na hrozící kompromitaci společnosti.

U organizačních i technických opatření byl hlavním pracovním nástrojem program Microsoft 365 Defender, jenž je ve vybraném podniku implementován a pro potřeby této práce byly některé jeho funkcionality modifikovány (viz např. kap. 4.3.1.4).

## 5.2 Naplnění cílů práce

Hlavní cíl práce, tedy navržení vhodné formy obrany proti phishingovým e-mailům, byl dle názoru autora naplněn; v rámci vybraného podniku byla provedena kontrolovaná phishingová kampaň pomocí Microsoft 365 Defender (důvodem pro zvolení právě tohoto zabezpečení je implementace této práce a do již funkčního, realistického scénáře, tedy velké nadnárodní firmy, která právě toto řešení používá pro zajištění své bezpečnosti – více k tématu v kapitole 5.3 Diskuse). Na základě vyhodnocených výsledků byla zvolena

organizačně-vzdělávací opatření (konkrétně edukativní kvíz, který výraznou měrou rozšiřuje vstupní informace pro nové zaměstnance) a technická opatření (např. implementace jednoduššího způsobu reakce na potenciální bezpečnostní incident formou jednoduchého tlačítka namísto stávajícího zdlouhavého systému reportování přes Jira ticket a systém reakce na možnou přítomnost phishingu v prostředí vybrané firmy).

Úspěšné naplnění tohoto primárního cíle lze doložit úspěšnou realizací dílčích cílů stanovených v metodické části práce.

### 5.2.1 Zvýšení povědomí zaměstnanců o možnostech phishingových útoků

Tento dílčí cíl byl naplněn provedením simulovaných phishingových kampaní (ve kterých se zaměstnanci prakticky seznámili s vlastní zranitelností v této oblasti a byla jim představena praktická možnost útoku, která může kompromitovat nejen je, ale i celou společnost). Na něj navazovalo rozšíření znalostí formou kvízu s praktickými poznámkami, který je zaměstnancům neustále dostupný i po jeho absolvování.

### 5.2.2 Zvýšení kybernetické bezpečnosti v rámci organizace

Tohoto cíle bylo dosaženo jak kontrolou protokolů SPF, DKIM a DMARC, tak anti-spam a anti-phishing filtrů, aby tyto byly funkční a splňovaly bezpečnostní standardy popsané v kapitole 4.4.1.2 a 4.4.1.3.

### 5.2.3 Zlepšení organizace práce a bezpečnosti ve vybraném podniku obecně

Tento dílčí cíl je jistou kulminací předchozích cílů – vychází ze zvýšení povědomí o možnostech phishingové kampaně, zvýšení kybernetické bezpečnosti, preventivních opatření (kontroly dílčích bezpečnostních opatření v organizaci) i jasném stanovení postupu při zjištění bezpečnostního incidentu (tedy jednoduchého kliknutí na tlačítko, které je zaměstnanci neustále přístupné). Výsledkem je čtyřfázová reaktivní struktura popsaná v kapitole 4.4.2.

## 5.3 Diskuse

Vzhledem k praktickému zaměření této práce v rámci již existující společnosti s rozsáhlou strukturou a informační infrastrukturou musela práce být nutně omezena, např. následujícími faktory:

1. Nutností použít Microsoft Defender 365, který je přítomný ve vybraném podniku (toto limitovalo možnosti jiných řešení kyberbezpečnosti a v práci jim tedy není věnován výrazný prostor),
2. Nutností přizpůsobit praktickou část práce potvrzení vedoucích pracovníků a IT specialistů tak, aby nebyl narušen provoz vybraného podniku.

Jak je řečeno v této kapitole výše, cíle práce včetně dílčích kritérií byly realizovány. Ve vybraném podniku bylo provedeno s pomocí nástroje Microsoft Defender 365 více simulovaných phishingových kampaní s relativně vysokou mírou kompromitace a s nízkým procentem korektně nahlášených podezření na bezpečnostní incident. Po zavedení výše popsaných technických a organizačně-vzdělávacích opatření naopak výrazně vzrostla míra správně reportovaných incidentů a lehce poklesla míra kompromitace zaměstnanců. Toto potvrzuje obecný trend naznačený v teoretické části práce, tedy že i při ne úplně důkladném seznámení s bezpečnostními pravidly a vůbec se základy kyberhygieny bude dosaženo vyšší míry bezpečnosti v rámci (nejen) vybraného podniku. Ačkoliv bylo předpokládáno nižší procento kompromitovaných zaměstnanců, lze pravděpodobně přičíst tento nedostatek ne úplně důkladné vzdělávací kampani – v rámci dalších pozitivních kroků v oblasti kyberbezpečnosti (nejen) vybraného podniku by bylo vhodné se zaměřit právě na rozvoj oblasti vzdělávání, ale takový úkol je v každé větší společnosti třeba koordinovat a autor práce ho nemůže realizovat sám.

Výsledky (včetně kvízu a příloh této práce) lze teoreticky považovat za použitelné i pro jiné podniky. Původní předpoklad, se kterým byla tato práce zahájena, tedy extrapolace výsledků pro potřeby dalších podniků, ale vzhledem k omezením (např. v nemožnosti použít Microsoft Defender 365 ve všech jiných firmách, jiném způsobu reportingu bezpečnostních incidentů, různosti zákonů dopadajících na různé firmy či státní instituce apod.) nebylo plně realizováno.

Závěrem k této části lze ale říci, že základní poučka při ochraně před phishingem, tedy nutnost prevence (realizováno např. edukativním kvízem) a detekce (realizováno v technické části této práce) pro úspěšnou ochranu před phishingem, byla, s výše popsanými omezeními, potvrzena.

# 6 Závěr

Tato práce se věnovala tématu kybernetické bezpečnosti, ochrany před phishingem a edukaci v oblasti kyberhygieny u osob, které mohly a mohou být ve firemním prostředí vystaveny riziku phishingového útoku (jako ostatně každý uživatel moderních technologií, jak ukazuje kapitola o dalších technikách sociálního inženýrství). Za hlavní přínos práce lze označit zlepšení zabezpečení vybraného podniku před budoucími kybernetickými útoky, zlepšení reportování možných pokusů o phishingový útok a zavedení odpovídajícího vzdělávacího modulu pro zaměstnance, který jim může sloužit jako vodítko při bezpečném uživatelském chování.

Teoretická část práce se kromě témat vysloveně spojených s praktickou aplikací získaných poznatků (zvláště v části týkající se phishingu a přidružených technik, popisu nástroj Microsoft 365 Defender či organizačních aspektů kybernetické ochrany) dotýká též některých širších souvislostí spojených s kyberbezpečností. Hlavně jejím přesahem i do činností na první pohled nespojených se světem informačních technologií, např. legislativním uchopení kybernetické bezpečnosti (ačkoliv vybraný podnik přímo nepodléhá většině zákonných požadavků české legislativy, např. ZKB) či historie phishingu, pomáhá teoretická část vidět téma v širších souvislostech.

Praktická část představuje řešení vytyčeného primárního problému v omezeném reálném prostředí, ve kterém se phishingové útoky odehrávají – ve velké společnosti, u které je motivace útočníka jedna z nejvyšších (z důvodu zisku, sběru dat či přípravy na další, rozsáhlejší útok). Základem praktické aplikace poznatků z teoretické části bylo dostatečné obeznámení se s vnitřním fungováním společnosti (které je usnadněné vzhledem k tomu, že autor práce je jejím zaměstnancem), využitím stávajících kapacit a funkčního prostředí společnosti (existujících programů, např. využitím všech možností, které ve stávajícím nastavením tyto programy sice umožňovaly, ale nebyly dostatečně využívány). Následným výzkumem a několika cvičnými phishingovými kampaněmi, uskutečněnými pomocí programu Microsoft Defender, byla prozkoumána stávající úroveň zaměstnanců vybraného podniku, jakož i celých oddělení. Z takto získaných dat byla vytvořena vzdělávací kampaň ve formě kvízu, jež umožnila zaměstnancům jak sebevzdělávání, tak možnost své znalosti konfrontovat s poznatky z praxe. Po této edukativní části bylo přistoupeno k další cvičné phishingové kampani, která zaznamenala slibnější výsledky jak v oblasti správného reportování potenciálních bezpečnostních incidentů, tak bezpečného zacházení s rizikovými

zprávami. Tyto výsledky sice nebyly dramaticky pozitivnější (viz praktickou část práce), ale pozitivní trend byl přesto patrný. Nedostatečné zlepšení lze přičítat například relativně krátké době, ve které si zaměstnanci měli osvojit bezpečné chování. Na tento základ pro zlepšení bezpečnosti ve vybraném podniku lze v budoucnu navázat dalšími vzdělávacími kampaněmi.

V technické části této práce byly detailněji rozebrány protokoly zajišťující ochranu před nevyžádanou poštou (DKIM, DMARC, SPF) a možnosti filtrování příchozích nevyžádaných zpráv (anti-phishing a anti-spam). Přínosem této části práce byla také implementace zjednodušeného procesu reportování rizikové pošty (jednoduchým tlačítkem, které nahradilo předchozí složitější mechanismus reportu přes nástroj Jira).

Úplně na závěr autor doufá, že tato práce přispěje k bezpečnosti a zlepšení ochrany před phishingem a dalšími nebezpečími, se kterými se běžný uživatel i profesionál potkává.

# 7 Seznam použitých zdrojů


1. ABAGNALE, Frank. *Scam Me If You Can: Simple Strategies to Outsmart Today's Rip-off Artists*. Portfolio, 2019. ISBN 9780525538974.
2. BERLIN, Amanda a Lee BROTHERSTON. *Defensive Security Handbook*. O'Reiley Media, 2017. ISBN 9781491960387.
3. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed. Wiley, 2018. ISBN 111943338X.
4. OZKAYA, Erdal. *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*. Packt Edition, 2019. ISBN 111943338X.
5. RAINS, Tim. *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks. Illustrated edition*. Packt Publishing, 2020. ISBN 978-1800206014.
6. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.
7. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
8. ARSHAD, Ayesha, Attique Ur REHMAN, Sabeen Javaid a Tahir Muhammad ALI. *A Systematic Literature Review on Phishing and Anti-Phishing Techniques*. Pakistan Journal of Engineering and Technology, PakJET. 2021(04).
9. BOSSOMAIER, Terry R. J., Steven D'ALESSANDRO a R. H. BRADBURY. *Human dimensions of cybersecurity*. Boca Raton: CRC Press, Taylor & Francis Group, 2020. ISBN 978-1-138-59040-3.
10. JAMPEN, Daniel, Gürkan GÜR, Tahir Muhammad ALI a Bernhard TELLENBACH. *Don't click: towards an effective anti-phishing training. A comparative literature review*. Human-centric Computing and Information Sciences. 2020 (33).
11. STUPKA, Václav. *Kybernetická bezpečnost v České republice*. Brno, 2018. Disertační práce. Masarykova univerzita.
12. SHAHRIAR, Saddat, Arjun MUKHERJEE a Omprakash GNAWALI. *Improving Phishing Detection Via Psychological Trait Scoring*. 2022.

13. OSULA, Anna-Maria, Bríd NÍ GHRÁINNE, Dan Jerker B. SVANTESSON, et al. *Cybersecurity law casebook*. Brno: Masaryk University, 2021. ISBN 978-80-210-9773-5.
14. DRAŠTÍK, Antonín. *Trestní zákoník: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-790-4.
15. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti. Páté doplněné a upravené vydání*. Praha: Centrum kybernetické bezpečnosti, z.ú., 2022. ISBN 978-80-908388-4.
16. HOUSE, Nathan. *The Complete Cyber Security Course* [online]. 2017 [cit. 2023-01-10].
17. SHORT, Donald, Charles J. BROOKS a Christopher GROW. *Cybersecurity Essentials*. Sybex, 2018. ISBN 9781119362395.
18. APANDI, Siti Hawa, Jamaludin SALLIM a Roslina Mohd SIDEK. *Types of anti-phishing solutions for phishing attack*. IOP Conf. Ser.: Mater. Sci. Eng. 769 012072.
19. HARPER, Allen a kol. *Gray Hat Hacking: The Ethical Hacker's Handbook*. 5th ed. McGraw Hill, 2018. ISBN 1260108414.
20. AL-QAHTANI, Ali F. a Stefano CRESCI. *The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID*-19. IET Information Security. 16(5).
21. KOLOUCH, Jan, Tomáš ZAHRADNICKÝ a Adam KUČÍNSKÝ. *Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the Covid-19 Pandemic*. Masaryk University Journal of Law and Technology. 15(2). Dostupné z: doi:DOI 10.5817/MUJLT2021-2-7
22. NOVÁK, Luděk a Josef POŽÁR. *Systém řízení bezpečnosti informací*. [online]. 2011, 1-10 [cit. 2023-01-12]. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf.
23. Deutsche Gesellschaft für Cybersicherheit. Phishing: *The most popular scam of cybercriminals*. [online]. 2023. [cit. 2023-01-15]. Dostupné z: https://dgc.org/en/phishing/.
24. NIGHTINGALE, Stephen. *E-mail Authentication Mechanisms: DMARC, SPF and DKIM*. [online]. 2017. 1-43 [cit. 2023-01-15]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1945.pdf

25. ALSMADI, Izzat. *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics*. San Antonio, TX, USA: Texas A&M University, 2017. ISBN 978-3-030-02359-1.
26. BŘOUSEK, Pavel. *Multi-Factor Authentication in Large Scale*. Brno, 2019. Diplomová práce. Masarykova univerzita.
27. BROOKS, Charles J. a kol. *Cybersecurity Essentials*. Indianopolis, Indiana: John Wiley & Sons, Inc. 2018. ISBN 978-1-119-36239-5.
28. Security Blue Team. *Blue Team Level 1 Certification*. [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://securityblue.team/why-btl1/
29. KnowBe4 Security Awareness Training Blog. *KnowBe4 Top-Clicked Phishing Email Subjects for Q3 2022 [INFOGRAPHIC]*. [online]. 2023 [cit. 2023-01-05]. Dostupné z: https://blog.knowbe4.com/knowbe4-top-clicked-phishing-email-subjects-for-q3-2022-infographic
30. NAGELE, Chris. *DMARC: What is it and why do you need it*? Postmark [online]. 2022 [cit. 2023-01-05]. Dostupné z: https://postmarkapp.com/guides/dmarc
31. Kaspersky. *What is Typosquatting*? [online]. 2023 [cit. 2023-01-15]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting
32. KRČMÁŘ, Petr. *Phishingový útok výměnou IDN znaků v doméně znovu na scéně*. Root.cz [online]. 2017 [cit. 2022-12-26]. Dostupné z: https://www.root.cz/clanky/phishingovy-utok-vymenou-idn-znaku-v-domene-znovu-na-scene/
33. Modrý Blog O2. *Jaký je nejnákladnější typ kyberzločinu? Podvržený e-mail od šéfa*. [online]. 2022 [cit. 2022-12-26]. Dostupné z: https://blog.o2.cz/2022/07/04/jaky-je-nejnakladnejsi-typ-kyberzlocinu-podvrzeny-e-mail-od-sefa/
34. GRÁSGRUBER, Lukáš. *Útočníci se v kyberprostoru snaží lépe mířit a přecházejí od náhodných k cíleným útokům*. [online]. 2023 [cit. 2022-12-26]. Dostupné z: https://www.systemonline.cz/zpravy/utocnici-se-v-kyberprostoru-snazi-lepe-mirit-a-prechazeji-od-nahodnych-k-cilenym-utokum-z.htm
35. ESET. *Trendy a výzvy v kyberbezpečnosti v roce 2023*. [online]. 2023 [cit. 2022-12-26]. Dostupné z: https://digitalsecurityguide.eset.com/cz/trendy-a-vyzvy-v-kyberbezpecnosti-v-roce-2023

36. HOUSER, Pavel. *Průzkum Sophos: Více než polovina manažerů českých firem čelila phishingu*. [online]. 2019 [cit. 2023-01-15]. Dostupné z: https://www.itbiz.cz/tiskove-zpravy/pruzkum-sophos-vice-nez-polovina-manazeru-ceskych-firem-celila-phishingu
37. O2 . *Zastavujeme kyberútoky dříve, než dorazí k vám do firmy*. [online]. [cit. 2023-01-15]. Dostupné z: https://www.o2.cz/podnikatele-a-firmy/o2-cyber-security
38. SPECHT, Bettina. *Everything you need to know about SMTP*. [online]. 2022 [cit. 2023-01-15]. Dostupné z: https://postmarkapp.com/guides/everything-you-need-to-know-about-smtp
39. Microsoft. *What Is Microsoft 365 Defender*? [online]. 2023 [cit. 2023-02-18]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender
40. Microsoft. *Microsoft 365 Defender Portal. Microsoft.* [online]. 2023 [cit. 2023-02-18]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-portal.
41. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání.* Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.
42. CARLSON, Brian. *Top cybersecurity statistics, trends, and facts.* [online]. 2021 [cit. 2023-02-28]. Dostupné z: https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html
43. NÚKIB. *Podvodné e-maily nebo zprávy na sociálních sítích na míru: Spear-phishing a jak se před ním chránit.* [online]. 2020 [cit. 2023-02-15]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Spear-phishing_a_jak_se_pred_nim_chranit.pdf.
44. Proofpoint. *2023 State of the Phish: Europe and the Middle East.* [online]. 2023 [cit. 2023-02-27]. Dostupné z: https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish.
45. ENISA. *What is "Social Engineering"?* [online]. 2022 [cit. 2022-12-25] Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

46. Microsoft. *Get started using Attack simulation training in Defender for Office 365*. [online]. 2023 [cit. 2023-02-28]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started
47. Lewik, s.r.o.. *Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident (zákon o kybernetické bezpečnosti, § 7).* [online]. 2022 [cit. 2022-12-28]. https://www.lewik.org/term/13385/kyberneticka-bezpecnostni-udalost-a-kyberneticky-bezpecnostni-incident-zakon-o-kyberneticke-bezpecnosti-7/
48. Microsoft. *Microsoft 365 Defender Blog.* [online]. 2023 [cit. 2023-02-28]. Dostupné z: https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/bg-p/MicrosoftThreatProtectionBlog.
49. FBI. *Spoofing and Phishing.* [online]. [cit. 2023-03-01]. Dostupné z: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing.
50. ALLISON, George. *Classified Challenger tank specs leaked online for videogame*. [online]. [cit. 2022-12-29]. Dostupné z: https://ukdefencejournal.org.uk/classified-challenger-tank-specs-leaked-online-for-videogame/.
51. Ministerstvo práce a sociálních věcí. *Kybernetická hygiena*. [online]. [cit. 2023-03-10]. Dostupné z: https://portaldigi.cz/digislovnik/kyberneticka-hygiena
52. Microsoft. *Threat Explorer and Real-time detections*. [online]. [cit. 2023-14-03]. Dostupné z: https://learn.microsoft.com/en-gb/microsoft-365/security/office-365-security/threat-explorer
53. Microsoft. *Recommended settings for EOP and Microsoft Defender for Office 365 security*. [online]. [cit. 2023-15-03]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365
54. SentinelOne. *What is Open Source Intelligence (OSINT)?* [online]. 2023 [cit. 2023-15-03]. Dostupné z: https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/
55. TrustedSec. *The Social-Engineer Toolkit (SET).* [online]. 2023 [cit. 2023-15-03]. Dostupné z: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

56. GeeksforGeeks. *ASCII vs UNICODE*. [online]. [cit. 2023-15-03]. Dostupné z: https://www.geeksforgeeks.org/ascii-vs-unicode/
57. Národní úřad pro kybernetickou a informační bezpečnost. *Vzdělávání.* [online]. [cit. 2023-15-03]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/
58. National Cyber Security Centre. *All topics* [online]. [cit. 2023-15-03]. Dostupné z: https://www.ncsc.gov.uk/section/advice-guidance/all-topics

# 8 Seznam obrázků, tabulek, grafů a zkratek

## 8.1 Seznam obrázků



## 8.2 Seznam kódů

## 8.3 Seznam tabulek



## 8.4 Seznam použitých zkratek

| | |
|---|---|
| BYOD | Bring Your Own Device (přineste si své vlastní zařízení) |
| DNS | Domain Name systém (systém doménových jmen) |
| ENISA | The European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací) |
| MTA | Mail Transfer Agent (program pro přepravu elektronické pošty v prostředí internetu) |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| NCSC | National Cyber Security Centre (Národní centrum kybernetické bezpečnosti) |
| VOIP | Voice Over Internet Protocol |
| ZKB | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) |
| SOC | Security Operations Center (bezpečnostní operační centrum) |
| SMTP | Simple Mail Transfer Protocol (jednoduchý mailový transportní protokol) |
| TCP | Transmission Control Protocol (protokol pro řízení přenosu) |
| POP | Post Office Protocol |
| IMAP | Internet Message Access Protocol |
| VPN | Virtual Private Network (virtuální soukromá síť) |

# Přílohy

Příloha č. 1 - Vytvoření základních rad pro zaměstnance, kterých by se měli držet.
Příloha č. 2 - Phishingový testovací e-mail – Confluence
Příloha č. 3 - Phishingový testovací e-mail – Helpdesk
Příloha č. 4 - Školení pro zaměstnance – Nahlašování škodlivých e-mailů
Příloha č. 5 - Škodlivá webová stránka – Phishing KPI

**Příloha 1 – Vytvoření základních rad pro zaměstnance, kterých by se měli držet.**

Těchto 11 rad bylo vytvořeno pro zaměstnance a následně nahráno na firemní SharePoint, kde jsou zaměstnancům kdykoliv k dispozici.

1. **Never click on a link or download attachments immediately,**
    a. It is very important to always check the email first to see if it contains any identifiers that could tell you that it is a malicious email. Because even just clicking on a link can cause certain security risks to the company.
2. **Always check the sender's address,**
    a. Whenever you receive an email, you should check the sender's address carefully. It could be that one letter is omitted from the address, replaced with a very similar one, a third subdomain is used (feg.whatever.eu) or the 1st domain is different (feg.ru). At this point it is a completely different sender than who it claims to be.
3. **It is better to check the authenticity of the person on the other side,**
    a. If you receive an email that looks like it came from someone you know, but the email looks suspicious to you, 101 tis always better to contact the person by another method and verify the authenticity of the email. You can do this using MS Teams for example or just a new email where you select the recipient from your contact list and ask them if they really sent the message,
    b. You may also encounter a situation where you get a call from an unknown number claiming to be user support. If it asks for any personal information or cooperation from you, for example, downloading an app, it is better to hang up the phone at this point and contact our user support directly.
4. **Always report suspicious email using the report button in Outlook,**
    a. It is very important for us to know about threats as soon as possible. Therefore, even if you are unsure, it is always better to report a threat than to just ignore it. We will then investigate it for you and let you know if it was a malicious message or not. Even if it turns out that the message was OK, nothing will happen. It's always better to be more careful.
    b. If the message turns out to be malicious, your reporting will help us protect other colleagues who might not recognize it as phishing.
5. **Report any other incidents using the Jira ticket,**

a. The report button in Outlook is only for reporting a phishing message, but if you encounter another type of incident, there is an option to report the incident using a Jira ticket. For example, an incident could be if you don't recognize a malicious website and enter your personal information on it. Or if strange things start happening on your computer. It's always better to report the situation so we can protect you.

6. **Do not forward suspicious emails,**
    a. If you receive a suspicious email pretending to be from a colleague and you would like to check with them to see if they really sent the email. Never forward the email to him. It is better if you take a screenshot for example and send it to him as a picture. If you forward the email and it contains malicious stuff, you could cause malicious content to spread in the company.
7. **Use keeper password manager,**
    a. When you use the password manager, you can afford to have a unique password for each system. You won't have to remember them all because the password manager remembers them for you. Password manager allows you to generate a very strong and long password that no one can crack. It can also automatically fill in your personal information on the page you have login credentials for in the password manager. Therefore, it will also help you in discovering a malicious site that only mimics a valid site. Because it won't want to fill in the login details for that malicious site.
8. **Don't give in to time pressure,**
    a. You should never take any action just because of fear of missing something. On the contrary, you should be alert if someone is going to use time pressure on you. There may be situations when you really need to do something immediately. However, you should always make sure that it is a valid request and from the right person. If you are going to be pressured for time by someone via email or phone, it is always better to check with someone before you take the requested action that the request is legitimate.
9. **You should not use work email for personal purposes,**
    a. You shouldn't be sending work-related stuff via personal email and not send private things to your work email. You should not post your work email

anywhere for any reason and use it to register on a website for personal purposes or to make any private orders.

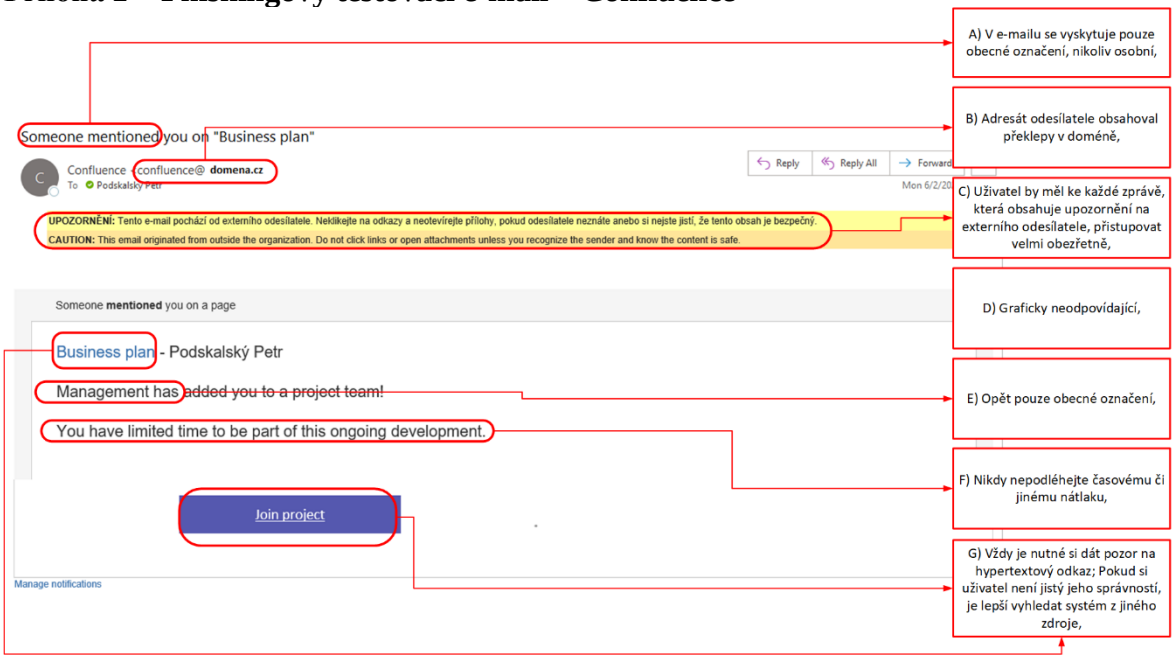
**10. Don't leave your computer unlocked,**

a. You should lock your computer whenever you leave it. You can never be sure that someone with malicious intent did not get access to your computer while you were away. For example, it only takes a very short period of time to send an email under your name with a malicious file and spread it through your company.
b. It only takes a few seconds to lock your computer, and it can keep you safe.
c. You can use keyboard shortcuts to lock your computer quickly:
    i. Win:
        1. win+L
    ii. Linux:
        1. Ctrl+Alt+L
    iii. macOS:
        1. Control-Command-Q

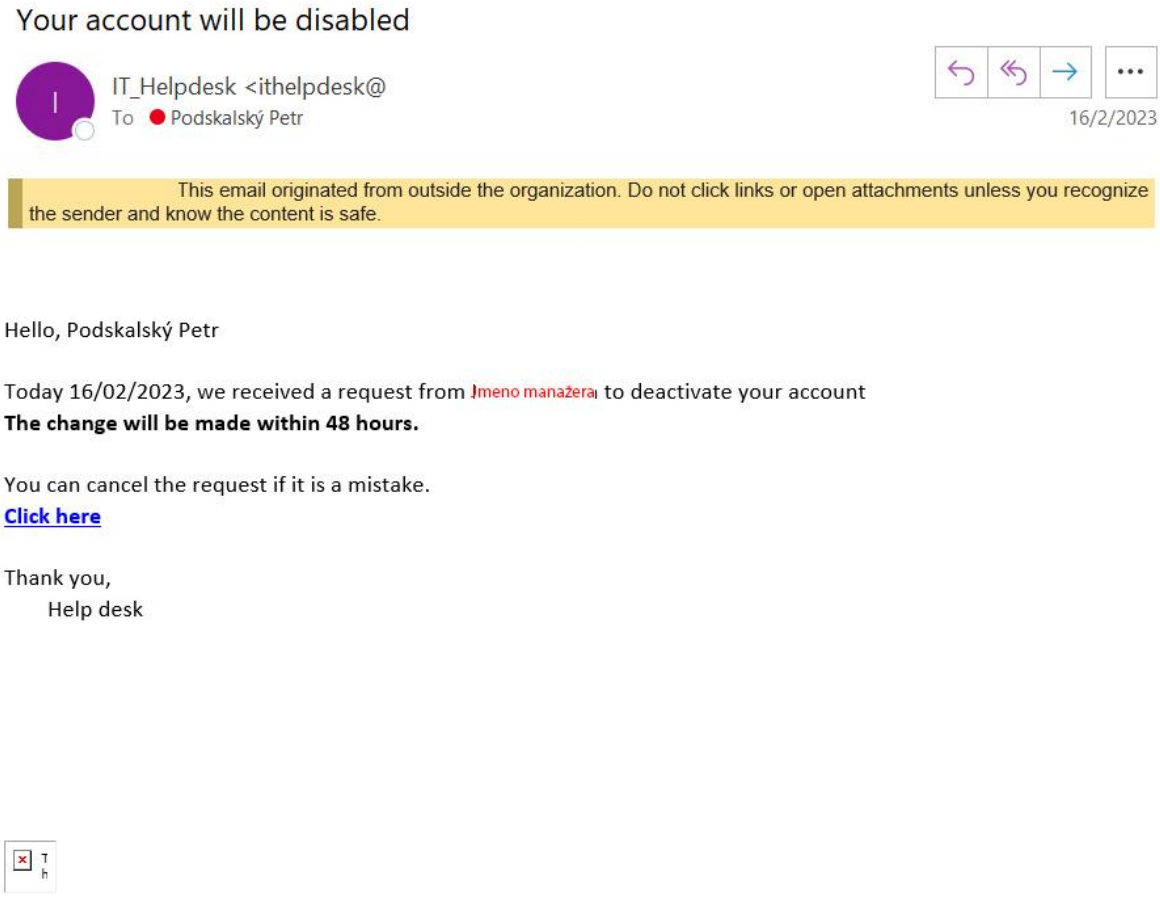
**11. You are always the most important part in the process.**

a. You need to behave responsibly on the computer. Keep your software up to date, download only software that you know is safe and only from trusted sources. It is important that you never share your personal login details. If you need to share any private keys always remember that we have a password manager in the company that allows secure sharing. Please never send passwords in an insecure form, do not share them on confluence, jira, etc. Whenever you have any suspicions, please contact us. We'll be happy to help you.

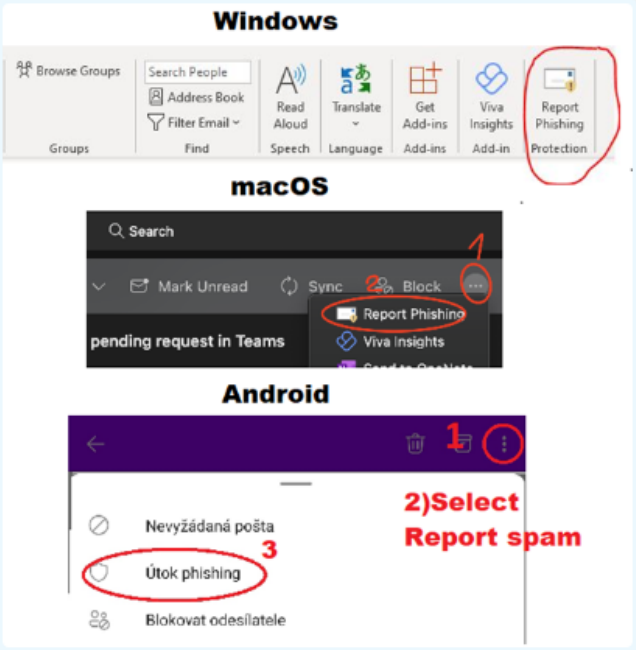
## Příloha 2 – Phishingový testovací e-mail – Confluence




## Příloha 3 - Phishingový testovací e-mail – Helpdesk



**Příloha 4 – Školení pro zaměstnance – Nahlašování škodlivých e-mailů**




**Please do not ignore the email. If you report the email correctly, you can help other colleagues who might not be as cautious as you. So please always report any suspicious e-mails you receive throught the Outlook option.**

Even if you know a colleague has already reported it. This is important to us because once the email is reported, we get the email into our queue for investigation and then we are able to take the necessary steps to protect our employees. Also, when you are not sure if it is phishing, it is always better to report the email. We will investigate it for you and let you know if it was malicious or not.

**How to report:**

1. Select the e-mail you want to report as phishing,
2. The next step depends on what device and operating system you are using.

**For Windows:**

1. From the Home tab on the ribbon, select Report phishing,
2. To confirm, click on the Report button that appears,
3. Done.

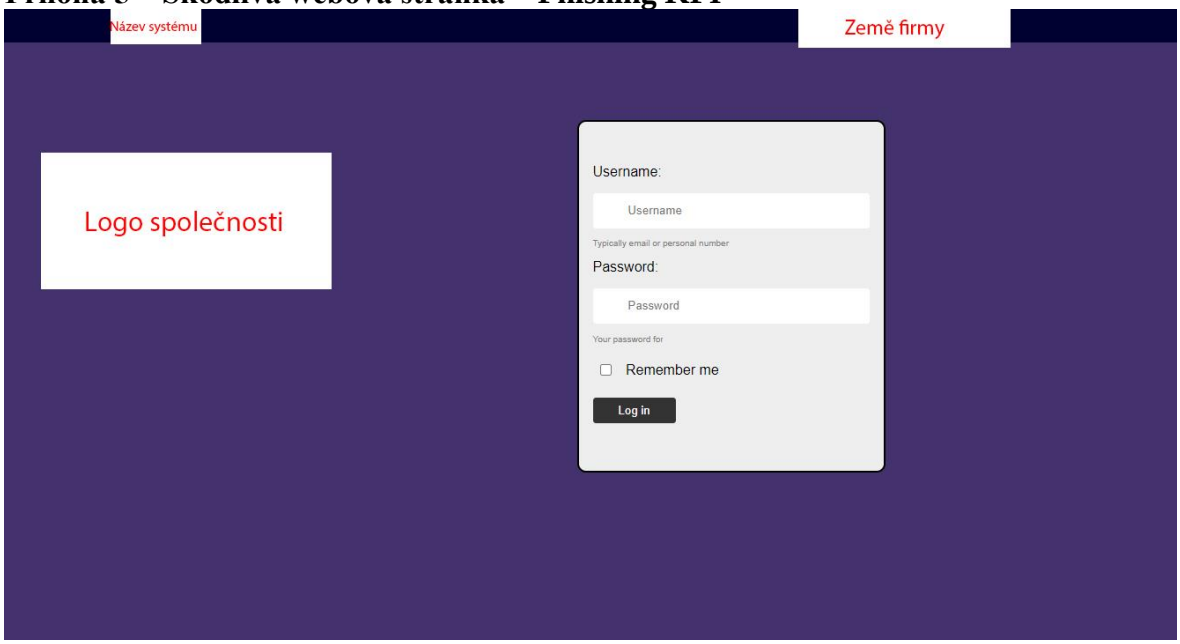
**For macOS**

1. From the Home tab on the ribbon, click on the three upper-right dots,
2. Select Report Phishing,
3. Confirm,
4. Done.

**For Android**

1. From the Home tab on the ribbon, click on the three upper-right dots,
2. Select Report Spam
3. Select Report Phishing,
4. Confirm,
5. Done.

## Příloha 5 – Škodlivá webová stránka – Phishing KPI




Vytvořeno pomocí HTML, CSS