**UNIVERZITA OBRANY**

**FAKULTA VOJENSKÝCH TECHNOLOGIÍ**

**Studijní program: Vojenské technologie**

Studijní obor: Kybernetická bezpečnost

Ev. číslo: xxxx/22



**DIPLOMOVÁ PRÁCE**

Název: Nástroj pro testování a zvyšování odolnosti organizací proti phishingu

Zpracoval: rtm. Tomáš Hujňák

Vedoucí práce: mjr. Ing. Tomáš Šlajs

BRNO 2025

**PODĚKOVÁNÍ**

**ČESTNÉ PROHLÁŠENÍ**

Prohlašuji, že jsem zadanou diplomovou práci na téma „Nástroj pro testování a zvyšování odolnosti organizací proti phishingu“ vypracoval samostatně, pod odborným vedením vedoucího mjr. Ing. Tomáše Šlajse. a použil jsem pouze literární zdroje uvedené v práci.

Dále prohlašuji, že jsem seznámen s tím, že se na moji diplomovou práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména skutečnosti, že Univerzita obrany má právo na uzavření licenční smlouvy o užití této diplomové práce jako školního díla podle § 60 odst. 1 výše uvedeného zákona, a s tím, že pokud dojde k užití této diplomové práce mnou nebo bude poskytnuta licence o užití díla třetímu subjektu, je Univerzita obrany oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladu, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Souhlasím se zpřístupněním své diplomové práce pro prezenční studium v prostorách knihovny Univerzity obrany.

V Brně, dne xx. dubna. 2022

..........................................

Tomáš Hujňák

**ABSTRAKT**

**Klíčová slova:**

**ABSTRACT**

**Key words:**

**OBSAH**

[SEZNAM POUŽITÝCH ZKRATEK 13](#_Toc177658103)

[SEZNAM OBRÁZKŮ 15](#_Toc177658104)

[SEZNAM TABULEK 16](#_Toc177658105)

[ÚVOD 17](#_Toc177658106)

[Teoretická část 18](#_Toc177658107)

[Phishing 18](#_Toc177658108)

[Historie 18](#_Toc177658109)

[Typy phishingu 18](#_Toc177658110)

[Jak phishing funguje 20](#_Toc177658111)

[Technické aspekty 20](#_Toc177658112)

[Dopady phishingu 22](#_Toc177658113)

[Legislativa 22](#_Toc177658114)

[Současné metody ochrany 23](#_Toc177658115)

[Odolnost organizací proti phishingu 23](#_Toc177658116)

[Význam lidského faktoru 24](#_Toc177658117)

[AI 24](#_Toc177658118)

[Cíle a omezení 25](#_Toc177658119)

[Analýza rizik 26](#_Toc177658120)

[ZÁVĚR 27](#_Toc177658121)

[SEZNAM POUŽITÉ LITERATURY 28](#_Toc177658122)

[SEZNAM PŘÍLOH 31](#_Toc177658123)

# SEZNAM POUŽITÝCH ZKRATEK

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# SEZNAM OBRÁZKŮ

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Obrázek 1 | − |  |  |
| Obrázek 2 | − |  |  |
| Obrázek 3 |  |  |  |
| Obrázek 4 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# SEZNAM TABULEK

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Tabulka 1 | − | Popis tabulky | … XX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ÚVOD

V

# Teoretická část

## Phishing

Úvod do phishingu

* definice phishingu
* historie
* typy (spear, whaling, vishing, smishing)

Phishing je forma kybernetického útoku, která využívá techniky sociálního inženýrství k manipulaci uživatelů. Útočník využívá podvodné zprávy nebo hovory k získání citlivých údajů oběti, jako jsou přihlašovací údaje, čísla platebních karet nebo jiné osobní informace. Klíčem úspěšného phishingového útoku je důvěryhodnost zdroje. Vydáváním se za legitimní organizace nebo banky zmanipuluje útočník oběti k odeslání citlivých informací, které mohou být zneužity. [7][9][10]

Historie

Phishingové útoky se začaly objevovat v 90. letech. První zaznamenaný útok byl v roce 1995 veden proti uživatelům služby America Online (AOL), kde se útočníci snažili získat přístupové údaje uživatelů pomocí falešných zpráv.

V roce 1996 se po internetových fórech začal rozšiřovat termín „phishing“. Pochází z anglického slova *fishing*, tedy rybaření, což je analogie na útočníka „lovícího“ informace a osobní údaje a od té doby se tento typ útoku stal celosvětovým problémem. V České republice se objevil v průběhu března 2006, kde šlo o podvrhnuté zprávy od banky Citibank. [7][8][10]

Díky nárůstu internetových služeb a rostoucí digitalizaci se phishing stal nejčastější formou kybernetického útoku, jehož metody jsou útočníky neustále zdokonalovány a upravovány dle aktuálních trendů, což vede k sofistikovanějším formám phishingu. [8]  
---- doublování s odstavcem z typů phishingu? -----

Typy phishingu

Phishing má mnoho různých podob a provedení. Všechny využívají lidskou důvěřivost a nedostatečnou pozornost. Tyto útoky se neustále vyvíjí a přizpůsobují novým technologiím a trendům. Díky tomu je phishing jedna z největších kybernetických hrozeb současnosti.[7][9]

Klasický phishing

Jedná se o nejběžnější typ phishingu, při kterém útočník zašle e-mail nebo zprávu s odkazem na falešnou webovou stránku, která na první pohled působí jako legitimní stránka známe organizace. Cílem je získání citlivých údajů. [7][8]

Spear-phishing

Spear-phishing je cílená forma phishingu na konkrétního uživatele nebo organizaci, kteří jsou vybíráni pomocí předem získaných informací pro důvěryhodnější podvodné zprávy. Hlavním rozdílem mezi klasickým a spear-phishingem je, že klasický je rozesílán hromadně, naproti tomu je spear-phishing personalizovaný, a proto také hůře odhalitelný. [7][8]

Whaling

Speciální forma spear-phishingu, která je zaměřena na vysoce postavené osoby ve firmách a organizacích. Cílem je od těchto osob získat citlivé informace, kterými je pak přimět k provedení finanční transakci. [7][8]

Vishing

Voice phishing nebo zkráceně Vishing je typ phishingu využívající telefonní hovory k získání citlivých údajů od obětí. Útočník se vydává za zaměstnance banky, státního úřadu nebo jiné důvěryhodné instituce, a snaží se získat přístup k přihlašovacím údajům nebo k číslům platebních karet. [7][8]

Smishing

Smishing (SMS phishing) je podobný klasickému phishingu, ale k rozesílání falešných odkazů a žádostí o citlivé údaje využívá SMS zprávy. Oběť obdrží textovou zprávu, která se jeví jako odeslaná z banky nebo jiné legitimní instituce, a je požádána o zadání údajů na podvržené stránce. [7][8]

Clone phishing

Při tomto typu phishingu vytvoří útočník přesnou kopii předchozí legitimní e-mailové zprávy, kde nahradí odkazy a přílohy závadným obsahem. Identicky působící e-mail zvyšuje šanci na úspěšný útok, tedy na kliknutí oběti na nebezpečný odkaz nebo stažení škodlivé přílohy.

Jak phishing funguje

* Psychologické triky a techniky používané útočníky (social engineering, manipulace) (již pokryto v úvodu?)
* Technické aspekty – email, web, spoofing, malware …

Technické aspekty

Kromě sociálního inženýrství se phishingové útoky opírají o technické nástroje a metody, které umožňují zneužívat důvěry obětí a přistupovat k jejich citlivým datům.

E-mailový spoofing

E-mailový spoofing je falšování e-mailové adresy odesílatele tak, aby na první pohled e-mail vypadal z důvěryhodného zdroje, jako je banka, e-shop nebo vládní organizace. Útočník upraví hlavičku e-mailu, čímž vytvoří iluzi legitimity a přiměje oběť k interakci s podvodnými odkazy nebo přílohami. [7][9]

Phishingové webové stránky

Podvržené webové stránky vypadající jako legitimní verze webových stránek bank nebo jiných známých organizací. Jsou navrženy tak, aby uživatel zadal citlivé údaje, jako např. přihlašovací údaje nebo údaje o kreditní kartě. [9]

Technická metoda, která se zde používá se nazývá klonování webových stránek, kdy útočník zkopíruje celý obsah legitimní webové stránky a provede malé úpravy, jako je přesměrování uživatele na podvrženou doménu pro zadání údajů. [7][9]

Zkrácené nebo maskované URL

Pro zamezení jednoduché identifikace škodlivé stránky, používají útočníci zkrácené nebo maskované URL adresy, které mohou vést na podvržené weby nebo severy s malware. [8]

Typosquating

Útočník zaregistruje doménu, která se velmi podobá legitimní stránce, avšak má drobné odchylky, například nahrazení znaku podobným (např. „g00gle.com“, místo „google.com“, nebo „arrny.cz“ místo „army.cz“). Této technice se říká typosquatting a je velice efektivní, protože ji uživatel snadno přehlédne. [7]

Man-in-the-Middle útoky (MITM)

V některých případech se útočník uchyluje k MITM útokům, při kterých zachytávají a modifikují komunikaci oběti s legitimní webovou stránkou nebo službou. Tímto způsobem může útočník shromažďovat přihlašovací údaje a další citlivé informace, aniž by si oběť byla vědoma narušení komunikace.[7]

Malvertising

Phishingové kampaně mohou obsahovat také malvertising, což je technika šíření škodlivých reklam. Tyto reklamy obsahují škodlivé odkazy na phishingové weby nebo přímo distribuují malware, který útočníkovi umožní získat kontrolu nad zařízením. [7]

Šíření škodlivých příloh

Škodlivé přílohy jsou běžným nástrojem phishingových útoků. Přílohy mohou obsahovat malware a jakmile je příloha otevřena (např. soubor PDF, Word nebo Excel), může být zařízení kompromitováno, čímž útočník získá přístup k datům nebo vzdálenou kontrolu nad zařízením.

DNS spoofing

DNS spoofing, je technika, při které útočník manipuluje DNS záznamy, což způsobí přesměrování uživatele na podvodné webové stránky, aniž by si toho byl vědom. Útok spočívá ve změně DNS záznamu u domény za jinou IP adresu, která uživatele přesměruje na podvrhnutou webovou stránku, která distribuuje malware nebo se snaží získat od uživatele citlivé údaje. [7]

Tyto technické aspekty umožňují útočníkům získat přístup k citlivým informacím několika sofistikovanými způsoby a dokazují, že způsobů oklamání oběti je mnoho. Co však číní phishing ještě zrádnějším a nebezpečnějším pro uživatele je skutečnost, že útočníci mohou tyto techniky kombinovat a získat tím vyšší úroveň důvěryhodnosti, a tudíž i účinnosti útoku. [5][7]

Dopady phishingu

* Finance, poškození reputace
* Dopad na jednotlivce – krádež identity, únik os. Dat

Phishingové útoky mohou mít vážné dopady jak na organizace, tak na jednotlivce a zahrnují finanční ztráty, poškození reputace, krádež identity a únik citlivých informací.

Dopady na organizace

Jedním z nejzávažnějších dopadů phishingového útoku je pro organizace finanční ztráta způsobená především únikem citlivých firemních dat a přístupů do interních systémů nebo přesvědčením zaměstnanců k bankovním převodům, při kterých se útočník vydává za vedoucího pracovníka a přikazuje zaměstnancům provést finanční transakce, které se pohybují v řádech milionů dolarů. [5][7]

Úspěšný phishingový útok na známou organizaci může také výrazně poškodit její pověst. Únik osobních údajů zákazníků, jako jsou čísla kreditních karet, hesla a adresy, může vést k narušení důvěry a dlouhodobých obchodních vztahů. Navíc tyto organizace mohou čelit žalobám, vyšetřováním a kompenzaci zákazníků, čímž se značně zvýší náklady na obnovu firmy po takovém útoku. [7][9]

Dopady na jednotlivce

Hlavní riziko pro jednotlivce je u phishingového útoku krádež identity. Získáním údajů, jako jsou jména, rodná čísla, čísla bankovních účtů nebo přihlašovací údaje do online služeb, může útočník otevírat bankovní účty, žádat o úvěry nebo nakupovat na internetu jménem oběti. [5][7]

Phishingové útoky mají zničující dopady jak na jednotlivce, tak i korporáty. Proto je důležitá prevence a povědomí o těchto útocích a jak jim předejít.

Legislativa

* Právní rámec pro boj s phishingem(GDPR, zákony o kyber. bezpečnosti)
* Mezinárodní a národní standarty kyber. bezpečnosti

Phishing je vážnou hrozbou pro soukromí a bezpečnost. Z tohoto důvodu existují právní rámce a standardy jak na národní, tak mezinárodní úrovni, s cílem posílit kybernetickou bezpečnost a ochranu osobních údajů jednotlivců i organizací. Pro cíle této práce se budeme bavit o legislativě ČR a EU.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon zpracovávající předpisy EU (transpozice NIS). Stanovuje pravidla pro ochranu informačních a komunikačních systémů a zavádí opatření proti kybernetickým útokům, včetně phishingu. Vztahuje se na subjekty kritické infrastruktury, provozovatele základních služeb a poskytovatele digitálních služeb. Klíčovým prvkem je povinnost hlášení kybernetických bezpečnostních incidentů.[11]

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Tato vyhláška upravuje podrobné požadavky na bezpečnostní opatření a reakce na kybernetické bezpečnostní incidenty. Doplňuje zákon č. 181/2014 Sb. a definuje konkrétní postupy, jak mají organizace reagovat na incidenty. Po přijetí nové směrnice NIS2 bude nahrazena novými předpisy.[11][12]

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Nařízení stanovující kritéria pro určení kritické infrastruktury, včetně ochrany proti kybernetickým útokům. Toto nařízení je důležité pro provozovatele sítí a systémů, které jsou nezbytné pro fungování státu, aby zajistili jejich odolnost vůči kybernetickým hrozbám.[11]

GDPR (General Data Protection Regulation)

Klíčovou legislativou EU pro ochranu osobních údajů je GDPR. Definuje, která data se považují za osobní a zajišťuje, aby organizace, které je spravují, zaváděly adekvátní bezpečnostní opatření. GDPR vyžaduje ochranu osobních dat před neoprávněným přístupem, čímž přímo souvisí s prevencí phishingu. Jakýkoliv únik osobních údajů musí být hlášen do 72 hodin (od zjištění úniku).[13]

Směrnice NIS (Directive on Security of Network and Information Systems)

Směrnice z roku 2016, která byla prvním krokem ke sjednocení kybernetické bezpečnosti v EU. Po provozovatelích základních služeb a poskytovatelích digitálních služeb požaduje, aby zaváděli opatření proti kybernetickým hrozbám a hlásili významné incidenty.[11]

Směrnice NIS2

Nahrazuje původní směrnici NIS, rozšiřuje oblast působnosti na více sektorů, zvyšuje požadavky na kybernetickou bezpečnost a zpřísňuje sankce za nehlášení kybernetických incidentů. K implementaci do české legislativy mělo dojít do října 2024 a v platnost do 1.1.2025.[14][15][16]

Současné metody ochrany

* Technologické nástroje (antivir, firewall, detekce v mailech)
* Školení zaměstnanců, bezpečnostní osvěta
* Dvoufaktorová autentizace a šifrování

Odolnost organizací proti phishingu

Testování odolnosti organizací

* Simulované kampaně
* Nástroje pro detekci a reakci na phishing
* Metriky a kritéria úspěšnosti (úspěšnost, rychlost reakce)

Zvyšování odolnosti organizací

* Přístupy k vylepšování bezpečnostní kultury
* Pravidelné školení a simulace
* Vyhodnocování účinnosti opatření

Význam lidského faktoru

* Role zaměstnanců v prevenci phishingu
* Proč jsou lidé nejslabším článkem a jak je posilovat

## AI

## Webové aplikace

## Databáze

# Cíle a omezení

# Analýza rizik

# ZÁVĚR

Je nutné věnovat stejnou, ne-li větší pozornost jako úvodu. V závěru musíte podat shrnutí, vyzvednout nejdůležitější postřehy a také vyhodnotit, zdali jste naplnili cíle, které jste si stanovili v úvodu své práce.

# SEZNAM POUŽITÉ LITERATURY

**ELEKTRONICKÉ ZDROJE**

1. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 1st ed. Indianapolis: Wiley Publishing, 2010. ISBN 978-0-470-63953-5.
2. HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed. Indianapolis: Wiley Publishing, 2018. ISBN 978-1-119-43338-5.
3. MITNICK, Kevin D., William L. SIMON a Steve WOZNIAK. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. 1st ed. Indianapolis: Wiley Publishing, 2005. ISBN 0-7645-6959-7.
4. TUNSTALL, Lewis, Leandro VON WERRA a Thomas WOLF. *Natural Language Processing with Transformers*. Sebastopol: O'Reilly Media, 2022. ISBN 978-1-492-04113-8.
5. BENDER, Emily M. a Alexander KOLLER. *Climbing towards NLU: On Meaning, Form, and Understanding in the Age of Data*. In *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*. Online: Association for Computational Linguistics, 2020, s. 5185-5198. ISBN 978-1-950737-66-9.
6. POLČÁK, Radim. *Ochrana osobních údajů podle GDPR v informačních systémech*. Brno: Computer Press, 2018. ISBN 978-80-251-4641-1

(špatné ISBN, Polčák ani nemá takto pojmenovanou publikaci)

1. HADNAGY, Christopher, a Michele FINCHER. *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. 1st ed. Indianapolis: Wiley Publishing, 2015. ISBN 978-1-119-02812-9.
2. CHVÁTALOVÁ, Jana. Phishing. Bakalářská práce. Praha: AMBIS vysoká škola, a.s., Katedra bezpečnosti a práva, 2022. Vedoucí práce: doc. JUDr. Jan Kolouch, Ph.D.
3. ANTI-PHISHING WORKING GROUP. Phishing Activity Trends Report, 2nd Quarter 2024. Publikováno 21. srpna 2024. Dostupné online: <https://apwg.org/resources/apwg-reports/>.
4. ANTIMALWARE.CZ. Co je phishing a jak se proti němu bránit. Publikováno 15. září 2012. Dostupné online: <https://www.antimalware.cz/blog/co-je-phishing/>.
5. NÚKIB. Legislativa v oblasti kybernetické bezpečnosti. Publikováno 19. září 2024. Dostupné online: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>.
6. GDPR.cz. Nařízení o kybernetické bezpečnosti. Publikováno 19. září 2024. Dostupné online: <https://www.gdpr.cz/narizeni/kyberneticka-bezpecnost>.
7. CrowdStrike. Obecné nařízení o ochraně osobních údajů (GDPR). Publikováno 19. září 2024. Dostupné online: <https://www.crowdstrike.com/cybersecurity-101/data-security/general-data-protection-regulation-gdpr/>.
8. NÚKIB. Zákon o kybernetické bezpečnosti. Publikováno 19. září 2024. Dostupné online: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>.
9. EUR-Lex. Směrnice NIS2. Publikováno 19. září 2024. Dostupné online: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32022L2555&qid=1724329129730>.
10. PICH, Jan a PLECHÁČEK, Petr. Nová směrnice společné úrovně kybernetické bezpečnosti v EU NIS2 přichází. EY Česká republika, 13. února 2023 [online]. Dostupné z: <https://www.ey.com/cs_cz/insights/cybersecurity/nova-smernice-nis2-kyberneticke-bezpecnosti>

* Pozn. ČSN ISO 690 Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů

|  |  |
| --- | --- |
|  |  |
|  |  |

# SEZNAM PŘÍLOH

|  |  |  |  |
| --- | --- | --- | --- |
| Příloha č. 1 | − | Popis přílohy (→ styl Odstavec) |  |
| Příloha č. 2 | − | Popis přílohy (→ styl Odstavec) |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

(→ Styl Příloha – číslování) Příloha 1

Popis přílohy (→ styl Příloha – popis)

|  |
| --- |
|  |