**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](#_Toc176449062)

[SEZNAM OBRÁZKŮ 15](#_Toc176449063)

[SEZNAM TABULEK 16](#_Toc176449064)

[ÚVOD 17](#_Toc176449065)

[Teoretická část 18](#_Toc176449066)

[Phishing 18](#_Toc176449067)

[Jak phishing funguje 18](#_Toc176449068)

[Dopady phishingu 18](#_Toc176449069)

[Legislativa 18](#_Toc176449070)

[Současné metody ochrany 18](#_Toc176449071)

[Odolnost organizací proti phishingu 18](#_Toc176449072)

[Testování odolnosti organizací 18](#_Toc176449073)

[Zvyšování odolnosti organizací 19](#_Toc176449074)

[Význam lidského faktoru 19](#_Toc176449075)

[Cíle a omezení 20](#_Toc176449076)

[Analýza rizik 21](#_Toc176449077)

[ZÁVĚR 22](#_Toc176449078)

[SEZNAM POUŽITÉ LITERATURY 23](#_Toc176449079)

[SEZNAM PŘÍLOH 25](#_Toc176449080)

# 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)

Jak phishing funguje

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

Dopady phishingu

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

## Legislativa

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

## 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

# 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*. Published August 21, 2024. Available online: <https://apwg.org/resources/apwg-reports/>. Accessed September 4, 2024. (online resource for phishing and cybercrime trends)

* 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)

|  |
| --- |
|  |