**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.

Při tvorbě diplomové práce byly využity jazykové modely pro generování textu a úpravu kódu, při překládání z cizích jazyků, formulaci myšlenek a optimalizaci řešení.

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 A ZNAČEK 8](#_Toc186882678)

[SEZNAM OBRÁZKŮ 10](#_Toc186882679)

[SEZNAM TABULEK 11](#_Toc186882680)

[ÚVOD 12](#_Toc186882681)

[1 Teoretická část 13](#_Toc186882682)

[1.1 Phishing 13](#_Toc186882683)

[1.1.1 Historie 13](#_Toc186882684)

[1.1.2 Typy phishingu 13](#_Toc186882685)

[1.1.3 Jak phishing funguje 15](#_Toc186882686)

[1.1.4 Technické aspekty 15](#_Toc186882687)

[1.1.5 Dopady phishingu 17](#_Toc186882688)

[1.1.6 Legislativa 17](#_Toc186882689)

[1.1.7 Současné metody ochrany 19](#_Toc186882690)

[1.1.8 Odolnost organizací proti phishingu 19](#_Toc186882691)

[1.1.9 Význam lidského faktoru 19](#_Toc186882692)

[1.2 Umělá inteligence (AI) 19](#_Toc186882693)

[1.2.1 Historie a vývoj 20](#_Toc186882694)

[1.2.2 Typy umělé inteligence 20](#_Toc186882695)

[1.3 Webové aplikace 21](#_Toc186882696)

[1.4 Databáze 21](#_Toc186882697)

[2 Praktická část 22](#_Toc186882698)

[Cíle a omezení 23](#_Toc186882699)

[Analýza rizik 24](#_Toc186882700)

[ZÁVĚR 25](#_Toc186882701)

[SEZNAM POUŽITÝCH ZDROJŮ 26](#_Toc186882702)

[SEZNAM PŘÍLOH 29](#_Toc186882703)

# SEZNAM POUŽITÝCH ZKRATEK A ZNAČEK

|  |  |
| --- | --- |
| OSINT | Zpravodajství otevřených zdrojů (Open Source Intelligence) |
| AOL | America Online |
| APWG | The Anti-Phishing Working Group |
| SMS | Služba krátkých textových zpráv (Short Message Service) |
| URL | Jednotná adresa zdroje (Uniform Resource Locator) |
| DMARC | Domain-based Message Authentication, Reporting and Conformance |
| DKIM | DomainKeys Identified Mail |
| SPF | Sender Policy Framework |
| MITM | Man-in-the-Middle útok |
| DNS | Domain Name System |
| ČR | Česká republika |
| EU | Evropská unie |
| GDPR | General Data Protection Regulation |
| NIS | Network and Information Security |
| NIS2 | Network and Information Security 2 |
| 2FA | Dvoufaktorové ověření (Two-Factor Authentication) |
| AI | Umělá inteligence (Artificial Intelligence) |

|  |  |
| --- | --- |
| ML | strojové učení (Machine Learning) |
| DL | hluboké učení (Deep Learning) |
| ASI | Superinteligence (Artificial SuperInteligence) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 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. [2][7][9][10]

Vzhledem k tomu, že je phishing technika manipulace člověka, často samotnému útoku předchází Zpravodajství otevřených zdrojů, obecně známé pod zkratkou OSINT (Open Source Intelligence). Jedná se o techniku shromažďování informací z veřejně dostupných zdrojů, jako jsou sociální sítě, webové stránky, veřejné databáze, nebo třeba zpravodajské články. Zahrnuje tedy jakékoliv informace, které nejsou chráněné nebo utajované. Díky této technice získá útočník přehled o svém cíli, což mu umožní přizpůsobit strategii konkrétním okolnostem a zvýšit tak efektivitu jeho útoku.

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]

Dynamický rozvoj internetu a neustále rostoucí míra digitalizace, ve spojení s relativní technickou nenáročností při realizaci phishingových útoků, vytvořily ideální podmínky pro to, aby se phishing stal jednou z nejčastějších forem kybernetického útoku. [8]

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

Jako phishing se označuje akt zasílání škodlivých e-mailů nebo zpráv, které se na první pohled tváří, že pocházejí z důvěryhodných zdrojů. Možné cíle lze shrnout následovně:

* Doručení škodlivého softwaru, umožňující vzdálený přístup
* Získání přístupových údajů
* Shromažďování dalších informací pro následné útoky

Obsah, záměr a způsob doručení phishingového e-mailu se odvíjí od konkrétního cíle.[2][7][8]

Spear-phishing

Spear-phishing je personalizovaná forma phishingu na konkrétního uživatele. Tomuto typu útoku zpravidla předchází důkladný OSINT mířený jak na cílovou osobu, tak na její rodinu. Hlavním rozdílem mezi klasickým a spear-phishingem je, že klasický je rozesílán hromadně, naproti tomu je spear-phishing personalizovaný, a proto také hůře odhalitelný. [2][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

Termín Vishing byl v roce 2009 zařazen do Oxfordského anglického slovníku. Jedná se o zkrácený výraz odvozený z pojmu Voice phishing, který označuje specifickou formu phishingu využívající telefonní hovory k manipulaci oběťmi za účelem získání citlivých údajů. Při tomto typu podvodné aktivity se útočník vydává za zaměstnance bankovních institucí, státních úřadů nebo jiných důvěryhodných organizací, aby oklamal oběť a přiměl ji k poskytnutí přihlašovacích údajů, čísel platebních karet nebo jiných osobních dat. Tento typ phishingu se v současné době zaměřuje zejména na starší generaci, která není plně obeznámena s moderními technologiemi, jako jsou aplikace pro mobilní bankovnictví. Pro tyto osoby může telefonát údajného bankovního pracovníka působit důvěryhodně a nepodezřele. [2][7][8]

Mezinárodní konsorcium Anti-Phishing Working Group (APWG) zaznamenalo ve třetím čtvrtletí roku 2024 výrazný nárůst phishingových útoků využívajících metodu vishing. Ve srovnání s druhým čtvrtletím došlo ke zvýšení těchto incidentů o 28 %. Rovněž bylo zjištěno, že se tyto kampaně stále častěji zaměřují na organizace, které bývají terčem útoků méně často, jako jsou místní plynárny, energetické společnosti nebo městské služby, například systémy pro úhradu parkovacích pokut, namísto tradičně cílených bankovních institucí. Tento posun v zaměření se na méně tradiční služby může zároveň naznačovat snahu útočníků zasáhnout širší spektrum populace, včetně mladší generace, která má častější zkušenosti s digitálními a městskými službami.[9][20]

Smishing

Smishing, známý také jako SMS phishing, představuje specifickou formu phishingu, při níž útočníci využívají k rozesílání podvodných zpráv mobilní textovou komunikaci prostřednictvím SMS. Tato metoda podvodu funguje obdobně jako klasický e-mailový phishing, avšak namísto e-mailových zpráv jsou falešné odkazy a požadavky na citlivé údaje distribuovány prostřednictvím krátkých textových zpráv. [2][7]

Typicky oběť obdrží SMS zprávu, která se zdánlivě jeví jako odeslaná z důvěryhodné instituce. Zpráva obsahuje výzvu k akci, například k ověření účtu, potvrzení platby nebo aktualizaci osobních údajů, a často obsahuje odkaz na falešnou webovou stránku. Tato stránka je vizuálně a funkčně přizpůsobena tak, aby působila důvěryhodně a přiměla uživatele k zadání přihlašovacích údajů, platebních informací nebo jiných citlivých dat. Smishing je obzvláště nebezpečný kvůli své nenápadnosti a širokému dosahu, neboť SMS zprávy jsou stále běžným komunikačním kanálem a často jsou uživateli vnímány jako důvěryhodnější než e-maily. [2][7]

Podobně jako u vishingových útoků zaznamenalo APWG ve třetím čtvrtletí roku 2024 také výrazný nárůst smishingových incidentů. Podle dostupných údajů vzrostl mezi druhým a třetím čtvrtletím roku 2024 počet těchto útoků o více než 22 %, což svědčí o jejich rostoucí popularitě mezi kybernetickými útočníky. Stejně jako v případě vishingu byl pozorován odklon od tradičně cílených institucí, jako jsou bankovní domy, směrem k menším organizacím a veřejným službám, které nejsou tak často terčem kybernetických útoků a jejichž uživatelé nejsou na podobné podvody dostatečně připraveni. [20]

Vzhledem k tomu, že vishing i smishing využívají jako hlavní přenosové médium mobilní telefon, lze konstatovat, že tyto dvě formy phishingových útoků jsou úzce provázané a často se vyskytují souběžně. Tato provázanost nespočívá pouze ve sdíleném komunikačním kanálu, ale také v podobných manipulačních technikách, jejichž cílem je oklamat oběť a získat od ní citlivé informace. Oba typy útoků se navíc neustále přizpůsobují technologickým zvyklostem uživatelů a reagují na proměnlivé kybernetické prostředí. Potvrzuje to i současný trend přesunu pozornosti útočníků od bankovních institucí k menším organizacím a veřejným službám, které často disponují nižší úrovní zabezpečení a jejichž uživatelé nemají dostatečné zkušenosti s podobnými hrozbami. Tento vývoj naznačuje, že kyberzločinci systematicky rozšiřují spektrum svých obětí s cílem maximalizovat efektivitu podvodných kampaní a zasáhnout co nejširší okruh uživatelů. [20]

Clone phishing

Clone phishing představuje specifickou formu phishingového útoku, při níž útočník vytvoří přesnou kopii (klon) legitimního e-mailu, který již oběť v minulosti obdržela. Tuto zprávu následně modifikuje tak, aby obsahovala škodlivé odkazy nebo přílohy, a poté ji znovu rozešle s tvrzením, že jde o aktualizovanou či opravenou verzi původní komunikace. Oběť je vyzvána k opětovnému kliknutí na odkaz nebo otevření souboru, čímž se může neúmyslně přesměrovat na podvodnou webovou stránku nebo stáhnout škodlivý software. V důsledku toho dochází ke krádeži přihlašovacích údajů nebo infikování zařízení malwarem, což útočníkovi umožňuje získat neoprávněný přístup k citlivým datům. [22]

Clone phishing je obzvláště nebezpečný, protože využívá důvěru oběti v již dříve obdrženou komunikaci. Oproti běžným phishingovým útokům, které se spoléhají na obecně formulované e-maily s generickými výzvami, clone phishing působí přesvědčivěji, protože imituje autentické zprávy, které oběť rozpoznává a kterým důvěřuje. [22]

Tento typ útoku se často zaměřujena firemní prostředí, kde útočníci kopírují interní e-mailovou komunikaci a vydávají se za kolegy, nadřízené nebo IT oddělení. V důsledku toho mohou být zaměstnanci méně obezřetní a mít vyšší pravděpodobnost, že na podvrženou zprávu zareagují. [22]

Jelikož se clone phishing spoléhá na sociální inženýrství a manipulaci důvěryhodných e-mailů, jeho prevence spočívá v důsledném ověřování odesílatele, kontrole URL adres a implementaci pokročilých e-mailových bezpečnostních opatření. Mezi klíčové ochranné mechanismy patří e-mailová autentizace (DMARC, DKIM, SPF), která ověřuje pravost odesílatelů, a pravidelná školení zaměstnanců v oblasti kybernetické bezpečnosti, která pomáhají minimalizovat riziko úspěšného útoku. [22]

Technické aspekty phishingu

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]

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Tento zákon stanovuje právní rámec pro ochranu osobních údajů v České republice a adaptuje požadavky evropského nařízení GDPR do české legislativy. Zaměřuje se na povinnosti správců a zpracovatelů osobních údajů, kteří musí implementovat technická a organizační opatření k ochraně dat před neoprávněným přístupem. Zákon rovněž klade důraz na povinná školení zaměstnanců v oblasti kybernetické bezpečnosti. V případě porušení těchto pravidel mohou být organizace právně postihovány. [21]

GDPR (General Data Protection Regulation)

GDPR je nařízení Evropské unie, které definuje standardy pro zpracování a ochranu osobních údajů napříč členskými státy. Určuje, která data se považují za osobní, a ukládá organizacím povinnost zavádět adekvátní bezpečnostní opatření pro jejich ochranu. GDPR také stanovuje povinnost hlášení bezpečnostních incidentů souvisejících s únikem dat do 72 hodin od jejich zjištění, což pomáhá minimalizovat dopady kybernetických útoků, jako je phishing. [13]

Směrnice NIS (Network and Information Security)

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 (Network and Information Security 2)

Nahrazuje původní směrnici NIS, rozšiřuje oblast působnosti na více sektorů, zvyšuje požadavky na kybernetickou bezpečnost a zpřísňuje sankce za nehlášení kybernetických incidentů. Česká republika měla implementovat směrnici NIS2 do svého právního řádu do 17. října 2024, což se však nestalo. Následně bylo plánováno, že nový zákon o kybernetické bezpečnosti, zahrnující požadavky NIS2, vstoupí v platnost 1. ledna 2025. Ani k tomu však nedošlo, a proto lze očekávat, že implementace NIS2 do české legislativy proběhne nejdříve v první polovině roku 2025. [14][15][16]

Současné metody ochrany

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

V dnešním digitálním světě, kde kybernetické hrozby, jako je phishing, představují významnou výzvu, jsou metody ochrany klíčové pro zabezpečení dat a systémů. Současné metody zahrnují technologické nástroje, školení zaměstnanců a využití pokročilých bezpečnostních technologií, jako je dvoufaktorová autentizace (2FA – Two-Factor Authentication) a šifrování.

Technologické nástroje

Moderní organizace využívají různé technologické nástroje k ochraně nejen před phishingovými útoky a dalšími kybernetickými hrozbami:

* Antivirové programy: Nástroje skenující soubory a e-maily a snaží se detekovat a odstranit škodlivý software, který by mohl být zneužit k získání přístupu k systémům.
* Firewally: Firewally fungují jako bariéra mezi interní sítí a externími hrozbami. Monitorují příchozí a odchozí provoz a blokují podezřelé aktivity.
* Systémy detekce phishingu v e-mailech: Softwarové nástroje implementované ve firemních e-mailových systémech. Analyzují příchozí zprávy a identifikují podezřelé odkazy nebo přílohy, které mohou obsahovat škodlivý obsah.

Školení zaměstnanců a bezpečnostní osvěta

Jednou z nejúčinnějších metod ochrany proti phishingu je vzdělávání zaměstnanců. Člověk, tedy uživatel, je nejslabším článkem v zabezpečení systémů, a proto by měla být pravidelná školení zaměřena na: [1]

* Rozpoznávání podezřelých e-mailů
* Praktiky, jako je ověřování totožnosti odesílatele
* Používání bezpečnostních postupů: nezadávat citlivé údaje na neznámých webových stránkách

Bezpečnostní osvěta nejen zvyšuje povědomí zaměstnanců o potencionálních hrozbách, ale také posiluje celkovou odolnost organizace vůči útokům.

Dvoufaktorová autentizace a šifrování

Pokročilé bezpečnostní technologie, jako je dvoufaktorová autentizace (2FA) a šifrování, hrají zásadní roli při ochraně dat a systémů:

* 2FA: Tento přístup přidává další vrstvu ochrany nad rámec běžného hesla. Uživatelé musí při přihlašování zadat nejen heslo, ale také další faktor, kterým může být například jednorázový kód zaslaný na mobilní zařízení, e-mail, nebo potvrzení přes aplikaci.
* Šifrování: Data jsou během přenosu šifrována, aby byla chráněna před neoprávněných přístupem. I v případě, že budou data odcizena, šifrování zajistí, že bez odpovídajícího klíče nebudou čitelná.

Současné metody ochrany kombinují technologické a organizační přístupy, aby minimalizovali riziko kybernetických útoků. Pro efektivní ochranu je zásadní implementovat jak technická opatření, tak školení a osvětu mezi uživateli. Tento integrovaný přístup zajišťuje, že organizace jsou lépe připraveny čelit stále sofistikovanějším hrozbám.

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

Phishingové útoky jsou účinné především díky tomu, že je to útok na uživatele. Jak bylo zmíněno v předchozí kapitole, uživatel je nejslabším článkem kybernetické bezpečnosti. Proto většina kybernetických útoků začíná využitím phishingu. [1]

Role zaměstnanců v prevenci phishingu

K prevenci phishingového útoku můžou zaměstnanci přispět pouze v případě, že jsou správně vyškoleni a informováni o potencionálních hrozbách. Mezi klíčové úlohy zaměstnance patří:

* Rozpoznání podezřelých e-mailů a zpráv: Zaměstnanci by měli být schopni identifikovat e-maily od falešných odesílatelů, neobvyklé požadavky na citlivé informace nebo odkazy vedoucí na podezřelé weby.
* Dodržování bezpečnostních protokolů: Všichni zaměstnanci by měli být seznámeni s interními pravidly a postupy, jako je používání bezpečných hesel, dvoufaktorové ověření a hlášení bezpečnostních incidentů.
* Okamžité hlášení podezřelých aktivit: Pokud zaměstnanec identifikuje podezřelou zprávu nebo činnost, je klíčové, aby incident okamžitě nahlásil příslušnému oddělení, například IT nebo bezpečnostnímu týmu.

Proč jsou lidé nejslabším článkem [1]

Jak lidský faktor posilovat

## Umělá inteligence (AI)

Umělá inteligence (AI) je vědní obor, který se zabývá vývojem inteligentních systémů, které jsou schopné provádět úkoly běžně vyžadující lidskou inteligenci. Patří sem například automatizace rutinních činností, rozpoznávání řeči nebo obrazu, rozhodování, učení nebo analýza dat.

Moderní AI zahrnuje různé techniky, z nichž nejvýznamnější jsou strojové učení (Machine Learning, ML) a hluboké učení (Deep Learning, DL). ML umožňuje systémům se automaticky učit a zlepšovat své chování na základě zkušeností a dat, aniž by byly explicitně naprogramovány. DL je specializovanou oblastí ML, která se zaměřuje na trénink vícevrstvých neuronových sítí, inspirovaných strukturou lidského mozku a umožňuje analýzu velkých a komplexních dat. [17][19]

Historie a vývoj

Počátky umělé inteligence sahají do poloviny 20. století, přičemž jako formální disciplína byla poprvé vymezena na Dartmouthské konferenci v roce 1956. Tato konference byla klíčovým momentem v historii AI, neboť položila základy pro výzkum a vývoj v této oblasti.

V raných fázích se zaměřovala především na logické operace, jako jsou šachové programy. AI dokázala efektivně řešit úlohy, které jsou pro člověka intelektuálně obtížné, ale lze je popsat matematickými nebo jinými pravidly. Výzvou pro AI se ukázalo řešení úkolů, které člověk provádí snadno, ale jsou obtížné na popis, jako je rozpoznávání znaků, slov nebo obličejů na obrázcích, tedy problémy, které lidé zvládají intuitivně.

Výrazný rozvoj AI nastal až s nárůstem výpočetních kapacit a větší dostupností datových souborů v 21. století. Dnes má umělá inteligence využití v oblastech, jako je zdravotnictví, autonomní doprava a finanční sektor. [18]

Typy umělé inteligence

Umělou inteligenci lze rozdělit na tři hlavní typy:

Úzká AI (Weak AI)

Tento typ AI je navržen tak, aby se choval, jako by byl inteligentní, ale ve skutečnosti neprovádí žádné vědomé myšlení. Slabá AI je schopna simulovat inteligentní chování bez skutečné „inteligence“. John Searle popsal slabou AI jako schopnou vykonávat konkrétní úkoly bez vědomí a sebeuvědomění. Tato umělá inteligence je to, co v dnešní době vídáme ve většině současných aplikací, jako jsou hlasoví asistenti nebo systémy pro rozpoznávání obrazu.

Silná AI (Strong AI) / Obecná AI (General AI)

Silná AI, také označovaná jako „obecná AI“, odkazuje na stroje, které by nejen simulovaly inteligentní chování, ale také by skutečně vykonávaly vědomé myšlení. Tento typ AI by byl schopen řešit širokou škálu úkolů na úrovni člověka, včetně nových a neznámých situací. V současnosti neexistuje žádný systém, který by tuto úroveň dosáhl, a tak zůstává silná AI pouze teoretickým konceptem.

Superinteligence (Artificial Superintelligence, ASI)

Superinteligence představuje hypotetický stav, kdy by AI překonala lidskou inteligenci ve všech oblastech, včetně kreativity, řešení problémů a rozhodování. Tento typ umělé inteligence je často spojován s obavami z toho, že by mohl převzít kontrolu nad budoucností lidstva, jak varovali například Alan Turing, Jonathan Wiener nebo Nick Bostrom, ale také Stephen Hawking, Bill Gates nebo Elon Musk.[18]

* Gorilla problem – reference na evoluční větev rozdělenou na gorily a homo sapiens – tedy gorily utlačené lidstvem

## Webové aplikace

## Databáze

SQL/NonSQL

PosgreSQL

# Praktická část

# 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 POUŽITÝCH ZDROJŮ

**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.
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>
11. GOODFELLOW, Ian, YOSHUA Bengio a Aaron COURVILLE. *Deep Learning*. MIT Press, 2016. ISBN 978-0-262-03561-3.
12. RUSSELL, Stuart a Peter NORVIG. *Artificial Intelligence: A Modern Approach*. 3rd ed. Pearson, 2009. ISBN 978-0-13-604259-4.
13. MITCHELL, Tom. *Machine Learning*. McGraw Hill, 1997. ISBN 0-07-042807-7.
14. ANTI-PHISHING WORKING GROUP. Phishing Activity Trends Report, 3rd Quarter 2024. Publikováno 21. listopadu 2024. Dostupné online: <https://apwg.org/resources/apwg-reports/>.
15. ČESKO. Zákon č. 110 ze dne 12. března 2019 o zpracování osobních údajů. In: *Sbírka zákonů České republiky* [online]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>.
16. PROOFPOINT. Clone Phishing [online]. Proofpoint,. Dostupné z: <https://www.proofpoint.com/us/threat-reference/clone-phishing>

* 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)

|  |
| --- |
|  |