

Phishing a sociální inženýrství

Sociální inženýrství a phishing představují v oblasti informační bezpečnosti techniky, které se nespolehají primárně na prolomení technických zranitelností (jako jsou softwarové exploity nebo síťové chyby), ale útočí na nejslabší článek každého systému – člověka.

Sociální inženýrství

Sociální inženýrství (*Social Engineering*) je psychologická manipulace s lidmi za účelem přimět je k provedení určité akce nebo k prozrazení důvěrných informací. Útočník pro dosažení svého cíle využívá přirozených lidských emocí a vlastností, jako je důvěřivost, strach, zvědavost, chamtivost nebo ochota pomáhat autoritám.

Běžné techniky sociálního inženýrství

Pretexting: Útočník si vytvoří falešnou identitu a promyšlený scénář. Může se vydávat například za technickou podporu, auditora nebo policii, aby získal citlivé údaje.

Baiting: Využití lidské zvědavosti nebo chamtivosti. Klasickým příkladem je záměrně zanechaný infikovaný flash disk s chytlavým názvem (např. `Mzdy_2026.xlsx`) na parkovišti před firmou.

Quid pro quo: Nabídka služby nebo výhody výměnou za informace. Například falešný IT technik obvolává zaměstnance s tím, že jim „opraví“ pomalý počítač, pokud mu obratem sdělí své přístupové heslo.

Tailgating (Piggybacking): Fyzický průnik do zabezpečeného prostoru. Útočník těsně následuje oprávněnou osobu do budovy, například tím, že předstírá, že nese těžké krabice a požádá o podržení dveří.

Phishing

Phishing je v současnosti nejrozšířenější formou sociálního inženýrství v kyberprostoru. Jedná se o podvodnou techniku rozesílání elektronických zpráv, které se tváří jako oficiální komunikace od důvěryhodné entity (banka, doručovací služba, nadřízený). Cílem je zmanipulovat oběť k instalaci malwaru nebo k zadání přihlašovacích údajů a čísel platebních karet na falešnou webovou stránku.

Typy phishingu

Spear phishing: Cílený útok na konkrétního jednotlivce nebo organizaci. Zpráva je vysoce personalizovaná a často obsahuje informace, které útočník předem shromáždil z veřejných zdrojů, sociálních sítí nebo OSINT (*Open-Source Intelligence*).

Whaling: Specifický druh spear phishingu zaměřený na takzvané „velké ryby“ – vysoce postavené

manažery (CEO, CFO). Cílem bývá často kompromitace e-mailu za účelem autorizace velkých finančních transakcí (známé také jako *CEO fraud*).

Vishing (Voice Phishing): Phishing prováděný telefonicky. Útočník se snaží vyvolat pocit naléhavosti, například volá jménem banky a tvrdí, že došlo k „napadení účtu“ a je nutné okamžitě přesunout prostředky.

Smishing (SMS Phishing): Podvodné zprávy šířené prostřednictvím SMS nebo komunikačních aplikací typu WhatsApp. Často obsahují zkrácené URL adresy a zprávy o zablokovaných balíčcích nebo nezaplacených pokutách.

Obrana a mitigace

Obrana proti sociálnímu inženýrství vyžaduje kombinaci vyspělých technických řešení a budování silné bezpečnostní kultury uvnitř organizace (*Security Awareness*).

Technická opatření

MFA (Multi-Factor Authentication): Vícefázové ověřování je absolutně kritickým prvkem. Pokud uživatel nevědomky odevzdá své heslo útočníkovi, bez druhého faktoru (např. TOTP kódu nebo hardwarového tokenu) se útočník k účtu nepřihlásí.

Zabezpečení e-mailové infrastruktury: Nasazení a striktní konfigurace protokolů pro ověření e-mailů – SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting, and Conformance). Tyto nástroje dramaticky ztěžují podvržení odesílatele (*Email Spoofing*).

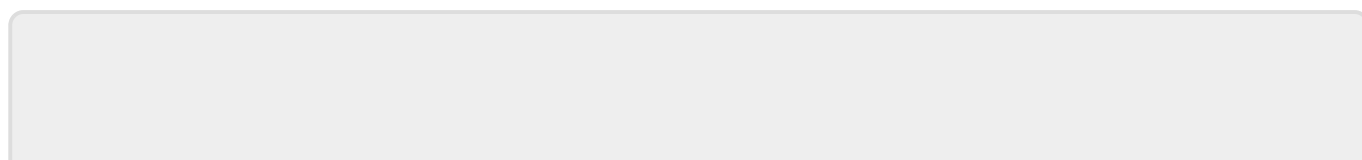
Filtrování a Sandboxing: Pokročilé e-mailové brány s antispamem a izolovaným prostředím pro testování podezřelých příloh (sandbox) a analýzu URL adres v reálném čase.

Organizační opatření

Edukace a školení: Pravidelná, interaktivní školení zaměstnanců spojená s náhodnými simulacemi phishingových kampaní. Zaměstnanci musí umět rozpoznat znaky manipulace (časový nátlak, hrozby, neobvyklé požadavky).

Zero Trust: Přijetí principu „nikdy nedůvěřuj, vždy prověřuj“.

Ověřovací procesy: Zavedení procesů mimo digitální komunikaci. Například požadavek na změnu bankovního účtu dodavatele zaslaný e-mailem musí být vždy ověřen telefonicky kontaktní osobě přes číslo, které již má firma v interním systému.



From:

<http://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

<http://serviceit.cz/doku.php?id=it:sec:phishing>

Last update: **2026/06/06 14:55**

