Nabídka pro Ústav územního rozvoje, o.s.s.
Sociální inženýrství a DarkWeb monitoring

I. Předmět poptávky

Dodavatel realizuje pro organizaci a její zaměstnance a vybrané externí dodavatele (úzce spolupracující) službu testování odolnosti nástroji sociálního inženýrství. Služba bude poskytnuta jako simulace dílčích útoků potenciálních útočníků a s využitím manipulativních technik sociálního inženýrství.

Dodavatel zajistí provedení takto simulovaných útoků na mailové, telefonní účty zaměstnanců a sídlo organizace.

Předmětem poptávané služby je simulace útočných technik na organizaci s využitím nástrojů:

• Mail phishingu;

• Spear phishingu;

• Vishingu;

• Fyzického průniku neautorizovaného datového média do sídla organizace.

Nedílnou součástí poptávky je dále:

1) Návrh a konzultace scénářů technik simulovaných útoků;

2) Detailní monitoring reakcí a přístupů adresátů k podvrženému obsahu;

3) Prověření případných kompromitovaných digitálních identit organizace vybraných zaměstnanců organizace a doménových účtů (DarkWeb monitoring a DarkNet detekce): přístupová hesla, telefonní čísla, přístupy k mailovým schránkám a serverům, přihlašovací údaje do OS, k webovým aplikacím, službám 3. stran a bankovním službám;

4) Zpracování Závěrečné zprávy s detailním přehledem průběhu a vyhodnocení služby v souladu s doporučením NÚKIB dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat;

5) Realizace školení zaměstnanců organizace s prezentací výstupů realizované služby.

II. Časový plán realizace

Dodavatel zajistí výše uvedený rozsah služeb v následujících termínech:
• Testy budou probíhat v době 4 – 6 pracovních týdnů;
• Počátkem této lhůty se rozumí spuštění prvního simulovaného útoku;
• Ukončením této lhůty se rozumí předání Závěrečné zprávy a realizace školení zaměstnanců
• Služba bude realizována v průběhu období září – říjen 2024.

Nabídka společnosti Faster CZ spol. s r.o.

1) Sociální inženýrství vč. školení a certifikace uživatelů

Provádíme koncentrované útoky simulující nástroje sociálního inženýrství, konkrétně mail phishing, spear phishing a fyzickou infiltraci na koncové stanice uživatelů. Na provedené operace navazuje školení s vyhodnocením dopadů námi provedených simulovaných útoků.

Detail služby

- Otestování odolnosti celého prostředí organizací vůči útokům (cílem není identifikace zranitelností konkrétní oblasti, či oddělení)
- Průnik zneužitím zranitelností prostřednictvím sociálního inženýrství s využitím aktuálních hackerských technik integrace sběru informací z otevřených zdrojů s podporou AI / umělé inteligence (př. OSINT, ChatGPT, Chatsonic), darkwebového tržiště digitálních identit a dalších zdrojů
- Nástroje AI využíváme pro prevenci podvržení důvěryhodných identit, scamů webových stránek a unikátní kódy proti detekci škodlivého obsahu
- Detailní monitoring reakcí a přístupů adresátů k podvrženému obsahu
- Ověření znalosti zaměstnanců pomocí technik sociálního inženýrství při využívání neautorizovaných technologií v organizaci, dodržování politik BYOD, ověření úrovně bezpečnosti Mobile Devices Managementu (zablokování přístupových systémů k firemním datům, stav dodržování směrnic, příp. serveru správy mobilních zařízení) a míru součinnosti zaměstnanců v případě identifikace bezpečnostního incidentu
- V případě zájmu lze provést darkweb monitoring emailových účtů a digitálních identit organizace a jejich zaměstnanců. Přibližně v 90% této činnosti úspěšně identifikujeme kompromitované údaje na darkweb tržištích (přístupy k mailovým serverům a schránkám, přihlašovací údaje do OS, do webových aplikací a služeb, apod.).
  V případě pozitivní identifikace kompromitovaných údajů zajistíme nápravu směřující k zabezpečení kompromitovaných účtů a odstranění záznamů z darkweb tržišť

Způsob realizace

Pro simulaci napadení organizace metodami sociálního inženýrstvím využijeme znalosti a postupy našich členů bezpečnostního týmu se zkušeností etického hackingu. Využijeme stejných sofistikovaných prostředků jako reální útočníci podle aktuálních TOP trendů hackerských technik.

Hlavní znaky útoku:

- projekt bude neohlášený a o jeho realizaci bude vědět pouze pověřený zástupce společnosti
- naším cílem nebude identifikace zranitelností konkrétní oblasti, či oddělení, ale otestování odolnosti celého prostředí společnosti vůči útoku
- součástí napadení bude i interaktivní workshop, který proběhne do 14 dní od poslední fáze ze tří etap útoku a jeho obsahem bude i vyhodnocení odolnosti zaměstnanců
- samotný test proběhne v několika vlnách v rozmezí 14ti pracovních dnů
- průnik zneužití zranitelnosti využije v rámci sociálního inženýrství aktuální hackerské techniky integrace sběru informací z otevřených zdrojů s podporou AI /

umělé inteligence (př. OSINT, ChatGPT, Chatsonic), darkweb tržišť digitálních identit a fyzické infiltrace koncových zařízení zaměstnanců

Návrh útoku sociálního inženýrství

Připravíme scénáře penetračního testu s provedením simulovaného útoku nástroji sociálního inženýrství na zaměstnance organizace:

- **Fáze 1: Pokročilý mail phishing** přes falešnou doménu: hromadný mail zaměstnancům od existujícího subjektu vyzve adresáty podvržené zprávy k poskytnutí osobních údajů, k prokliku na podvržené www stránky a stažení přílohy se škodlivým kódem

- **Fáze 2: Spear phishing** směřovaný na konkrétní zaměstnance bude směřovat adresáty k vyplnění formuláře a registrace osobních údajů na podvržených stránkách existující instituce, či využívané služby

- **Fáze 3: Fyzická infiltrace koncových zařízení** prostřednictvím USB: do prostor organizace budou námi různými cestami doručeny např. 3x USB obsahující škodlivý kód (ovládnutí klávesnice, malware) a 3x USB s trackovacím kódem pro monitoring přístupů zaměstnanců, kteří případně USB použijí v PC stanicích

- **Fáze 4**: **Voice phishing:** založený na principu podvodných telefonních hovorů, kdy se volající představí falešnou identitou a bude žádat od zaměstnanců poskytnutí citlivých údajů

Cíle provedené simulace útoků

Provedenými technikami prověříme:

- úroveň dodržovaní standardů bezpečného chování zaměstnanců v online prostředí (ověřování identit, stahování neautorizovaných příloh, poskytování osobních a jiných citlivých údajů)
- odolnost zaměstnanců při využívání neautorizovaných technologií v organizaci
- dodržování politik BYOD (bring your own device)
- ověření úrovně bezpečnosti Mobile Devices Managementu (zablokování přístupových systémů k firemním datům, stav dodržování směrnic, příp. serveru správy mobilních zařízení)
- míru součinnosti zaměstnanců v případě identifikace bezpečnostního incidentu

2) Školení a certifikace zaměstnanců

Vzdělávání zaměstnanců, managementu a majitelů firem v oblasti kybernetické bezpečnosti je jednou z klíčových povinností připravované aktualizace Zákona o kybernetické bezpečnosti v rámci transpozice NIS2**.**

Důvodem je přenesená povinnost dodržování vyhlášek návrhu Zákona o kybernetické bezpečnosti dle § 15 na dodavatelské řetězce subjektů, které pod NIS2 spadají. **Deklarace školení managementu a zaměstnanců prokazující kompetenci v personálním i technologickém zabezpečení před kybernetickými hrozbami tak bude povinnou a vymahatelnou součástí smluvních vztahů již od roku 2025.**

Koncepce školení pro naše zákazníky a obchodní partnery je založena na důrazu na praxi, nikoliv na normách a bude zahrnovat:

- představení aktuálních technik útoků z prostředí hackerských komunit a jejich praktické zneužití dle segmentace zákazníka
- přehled aktuálních kybernetických technik vůči organizacím a institucím
- předcházení kybernetickým útokům v organizaci dle uživatelských rolí zaměstnanců
- interakce posluchačů se simulací útoku na jejich zařízení a síťovou infrastrukturu, tj. vyhodnocení provedených simulovaných kybernetických útoků

3) DarkWeb monitoring

Pro zákazníky realizujeme forenzní činnosti za účelem identifikace kradených dat a kompromitace digitálních identit zaměstnanců a organizace.

Využíváme k této činnosti monitorovací nástroje na bázi OSINT | Open Source Intelligence Framework, nástrojů ChatGPT, WormGPT a individuálních vyšetřovacích aktivit uvnitř komunit a na darknetových fórech dark webu.

Zjištěné nálezy následně vyhodnotíme dle závažnosti a zpracujeme doporučení pro nápravu. Tato nápravná opatření mají charakter:

- Individuálních prvků bezpečnosti: aktualizace hesel, revize digitální stopy, antivir na koncových zařízeních
- Technických prvků bezpečnosti: 2 faktorová autentikace, NextGen firewall, šifrování komunikace
- Systémových prvků bezpečnosti: monitoring zařízení/služeb a síťového provozu, detekce malware a ransomware, inteligentní systém záloh, atd.

Námi využívané techniky získávaní informací z otevřených i uzavřených zdrojů (WWW, Deep web & Dark Web) jsou nedílnou součástí procesu Competitive Intelligence. Na jedné straně se tyto metody staly nedílnou součástí vytěžování informací pro účely bezpečnostních týmů a zpravodajských služeb, na straně druhé je využívají i aktéři hrozeb a hackeři pro realizaci pokročilých útoků na organizace i jednotlivce.

Co hledáme a v případě pozitivního nálezu identifikujeme:

- **Kompromitaci mailových účtů** a identit: přístupy k mailovým účtům a službám, kradená hesla, telefonní čísla, data narození, fyzické adresy, pracovní pozice, primární a sekundární IP adresy
- **Zdroje kompromitace**: původ kradených údajů, aktuální stav z pohledu přístupnosti a prodeje na darknetu
- **Obchodované přístupy** a údaje k doménám k subdoménám mezi provozovateli botnetů a hackery
- **Krádeže digitálních identit** na darknet tržištích: přístupy k sociálním sítím, bankovní údaje, přihlašovací údaje k platebním bránám, osobní a rodinné informace

Ke službě zajišťujeme doporučenou podporu technických a organizačních opatření v souladu se standardy ISO 27000 a požadavků ZoKB & nZoKB| NIS2 i doplňující servis:

- OSINT, DEEP & DARK WEB monitoring & detekce
- Forenzní vyšetření: identifikace rizik a původu hrozeb
- Odstranění hrozby a definice nápravných opatření

Pozn.:

OSINT, DEEP & DARK WEB monitoring & detekce pro 5 mail účtů a 1 organizaci

Forenzní vyšetření: realizováno od 2 pozitivních nálezů níže

Odstranění hrozby zahrnuje výmaz nálezů z deep a dark web databází

Služba nezahrnuje cenu za případný odkup dat z darknetu

CENOVÁ NABÍDKA

Položka	Cena v Kč bez DPH
Sociální inženýrství (fáze 1 – 4)	[redacted]
Školení a certifikace zaměstnanců	[redacted]
Dark web monitoring	[redacted]
Cena celkem bez DPH	**94 800**

Zpracovala:
Ing. Jana Zajíčková
[redacted]
www.faster.cz

V Brně dne 15. 8. 2024. Nabídka je platná 60 dní.