Předmět nabídky:

„Testy sociálního inženýrství“

Nabídka pro:

Správa železnic, státní organizace

Datum publikace:	24.5.2022
Status:	Originál

Nabídka pro:	**Správa železnic, státní organizace** Generální ředitelství Dlážděná 1003/7 110 00, Praha 1
K rukám:	[redacted] Systémový specialista Odbor podpory a servisu [redacted] Tel.: [redacted]
Uchazeč:	**Corpus Solutions, a.s.**
Kontaktní spojení:	[redacted]
Vypracovali:	[redacted]
Schválil:	[redacted]
Dne:	24.5.2022
Počet stránek:	13

Omezující podmínky pro zveřejnění a použití:

Tento dokument obsahuje informace důvěrného charakteru a je určen výhradně pověřeným pracovníkům společnosti SŽDC a osobám pověřeným výkonem zadavatelských činností. Jako takový nesmí být bez předchozího souhlasu Corpus Solutions a.s. kopírován, předán či jinak zpřístupněn třetí fyzické nebo právnické osobě, ani použit pro jiné účely, než je posouzení uchazečů ve výběrovém řízení.

Upozornění:

Všechny známky a názvy produktů uvedené v tomto materiálu jsou nebo mohou být registrované obchodní značky, obchodní známky nebo ochranné známky jejich vlastníků.

Poděkování

Velice si vážíme možnosti, že naše společnost Corpus Solutions a.s. může nabídnout své služby právě společnosti Správa železniční dopravní cesty, státní organizace.

Pevně věříme, že námi navržené řešení a zvolený přístup odpovídají Vašim představám a požadavkům.

S úctou za společnost Corpus Solutions a.s.

……..

Ing. Tomáš Přibyl
CEO
Corpus Solutions a.s.

OBSAH

I Identifikační údaje o uchazeči

Obchodní jméno	Corpus Solutions a.s.
Sídlo společnosti	Štětkova 1638/18, 140 00 Praha 4
Právní forma společnosti	Akciová společnost vedena u Městského soudu v Praze pod spisovou značkou B. 5936
Statutární orgán	Představenstvo: Ing. Tomáš Přibyl, předseda představenstva Ing. Ivo Musil, člen představenstva Ing. Pavel Horák, člen představenstva
Založení společnosti	1992
Bankovní spojení	Raiffeisenbank a.s., číslo účtu 69474001/5500
IČ	25764616
DIČ	CZ25764616
Telefon	(+420) 241 020 333
ID Datové schránky	2xhpac2
Předmět podnikání	Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona Zprostředkování obchodu a služeb Velkoobchod a maloobchod Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály Pronájem a půjčování věcí movitých Poradenská a konzultační činnost, zpracování odborných studií a posudků Příprava a vypracování technických návrhů, grafické a kreslířské práce
Obory činnosti	Testování, měření, analýzy a kontroly Reklamní činnost, marketing, mediální zastoupení Služby v oblasti administrativní správy a služby organizačně hospodářské povahy Mimoškolní výchova a vzdělávání, pořádání kurzů, školení, včetně lektorské činnosti Poskytování technických služeb Výroba, obchod a služby jinde nezařazené
Základní jmění	2,006 mil. Kč
www	www.corpus.cz

Společnost Corpus Solutions a.s. (založena 1992) je předním dodavatelem služeb a technologií v oblasti zabezpečení informačních systémů. V projektech kombinujeme znalosti teoretické základny (doloženo certifikáty pracovníků) s praktickými zkušenostmi získanými při realizaci technologických projektů.

2 Požadavek zadavatele

Zadavatel požaduje provést následující penetrační testy:

- Testování sociálního inženýrství v rozsahu:
  - phishing (forma e-mailová komunikace) – rozsah cca 1100 zaměstnanců
  - vishing (forma telefonická komunikace) – 20 zaměstnanců

2.1 Požadovaný způsob provedení a metodika

Testy budou probíhat z pohledu „gray box“. Útočník – penetrační tester bude bez detailní znalosti prostředí zadavatele. Zadavatel dodá seznam emailu a telefonická čísla pro kampaně. Obsah skriptů a šablon použitých pro phishingové kampaně bude konzultován se zadavatelem – realizátor testu předloží návrh vypracovaný podle požadavků zadavatele.

Realizace bude provedena na projektovém základu s naplánováním testů. Provedení jednotlivých testů podlého schválení společnosti SŽDC s.o.. Předložený plán bude obsahovat:

1. Popis testu
2. Rozsah testu
3. Datum a čas testu
4. Použité nástroje

3 Základní principy při testování

V rámci každého penetračního testování využíváme následující postup:

Plánování a příprava

Tvorba Rules of Engagement (RoE), příprava testovacích scénářů, schvalování, definice scope – záběr a hloubka penetračního testu. KickOff – meeting zahajující penetrační test.

Konfigurace phishingové platformy

Konfigurace a příprava prostředí pro realizaci kampaně.

Tvorba skriptů a šablon

Příprava šablon a skriptů pro kampaně. Jedná se o přípravu šablon pro emaily, které budou odesílány v průběhu kampaně. Dále pak o přípravu telefonní skriptu, který bude využit v pro realizaci telefonické kampaně

Testování

Odeslání testovacích vzorků phishingu na malou skupinu vybraných zasvěcených uživatelů (např. pracovníci odboru bezpečnosti). Cílem této fáze je ověřit, zda emaily prochází, nejsou zachytávány spamovým filtrem a zobrazují se uživatelům očekávaný a plánovaným způsobem. Pro telefonickou kampaň bude proveden testovací hovor s cílem ověřit telefonický skript

Realizace kampaní

Samotná realizace kampaní.

Závěrečná zpráva

Výstupem penetračního testu bude závěrečná zpráva o provedeném testu. Ve zprávě je především obsaženo: popis a shrnutí výsledků testů, identifikace zranitelností a jejich nebezpečnosti, časový harmonogram testování, popis a statistika úspěšnosti jednotlivých kampaní, Získané informace o chování uživatelů (granularita uživatel), doporučení nápravných opatření.

Komunikační protokol

Před začátkem penetračního testu se po vzájemné dohodě nastaví, jak a které stavy budou komunikovány. Toto nastavení komunikace se formálně zpracuje do dokumentu RoE (kapitola notifikační proces), který je schválen zadavatelem testu před začátkem testu. Běžné nastavení je notifikovat začátek a konec testu domluveným způsobem na seznam pověřených osob.

Opatření vedoucí k minimalizaci vzniku provozních a bezpečnostních incidentů

Aby se co nejvíce snížila rizika bezpečnostních testů, bude se jejich provádění řídit následujícími zásadami:

Testy budou prováděny v nedestruktivním režimu. Před zahájením každé sady testů bude se zadavatelem domluvena hloubka a záběr (scope) konkrétních testů ve formě dokumentu „Rules of Engagement“. Tento dokument obsahuje směrnice a omezení, týkající se provedení bezpečnostních testů a uděluje testovacímu týmu formální pověření a oprávnění k provedení činností v něm popsaných.

Dokument „Rules of Engagement“ bude obsahovat následující atributy:

- Časový plán
- Místo testování
- Účel a cíle testování
- Rozsah a hloubka testování

- Plánované nástroje použité pro provedení testu
- Domluvená pravidla a podmínky testování
- Informace poskytnuté zákazníkem
- Notifikační proces a seznam zodpovědných osob s jejich údaji
- Rizika a jejich pokrytí
- Podepsaný souhlas odpovědných osob

3.1 Požadavky na součinnost

- Poskytnutí definovaných informací o cílech. Půjde zejména o emailové adresy a telefonní čísla.
- Poskytnutí informací o možném riziku postižení třetí strany a zajištění jejich informování (např. ISP, hosting, Cloud apod.), resp. zajištění souhlasu třetí strany
- Provedení zvláštních bezpečnostních opatření (pokud bude potřeba), snižujících výpadek nebo ztrátu dat (např. mimořádné zálohování)

4 Předmět plnění

Testované cíle a zvolené metody a rozsah testování je specifikován dále v této kapitole.

4.1 Sociální inženýrství – phishing emailová kampaň

Předmětem testu je phishingová emailová kampaň, která má uživatele zmanipulovat k vyzrazení informace, která by neměla být poskytnuta např. přihlašovací heslo.

Technické parametry testu

Typ testu: gray-box

Rozsah testu: phishing kampaň interní uživatelé, cca 1100 uživatelů

Forma testu: neinvazivní test

Provedení testu: Vzdáleně přes internet a email

Hlavní testovací scénáře:

- Phishing email kampaň

Potenciální rizika:

- Možná diskreditace hesla v případě že bude objeveno/odhaleno

Požadovaná součinnost:

- Seznam emailů

Uvažované nástroje:

- KingPhisher
- In-house používané neveřejné nástroje a interně vyvinuté nástroje

4.2 Sociální inženýrství – vishing kampaň

Předmětem testu je vishing telefonická kampaň, která má uživatele zmanipulovat k vyzrazení informace, která by neměla být poskytnuta např. přihlašovací heslo.

Technické parametry testu

Typ testu: gray-box

Rozsah testu: vishing kampaň vybraní **interní** uživatelé, telefon cca 20 uživatelů

Forma testu: neinvazivní test

Provedení testu: Vzdáleně pomocí telefonu

Hlavní testovací scénáře:

- Telefonická kampaň

Potenciální rizika:

- Možná diskreditace hesla v případě že bude objeveno/odhaleno

Požadovaná součinnost:

- Vybraná telefonní čísla

Uvažované nástroje:

- Telefon

5 Referenční zakázky

Corpus Solutions realizoval v oblasti sociálního inženýrství v uplynulých 5 letech mimo jiné následující zakázky:

Pořadové číslo zakázky	Zákazník	Předmět plnění	Termín realizace
1.	[redacted]	Testy sociálního inženýrství (phishing, vishing)	Q1, 2020
2.	[redacted]	Testy sociálního inženýrství (phishing, vishing)	Q2, 2021
3.	[redacted]	Testy sociálního inženýrství (phishing, vishing)	Q4, 2017
4.	[redacted]	Realizace phishing kampaní	Q1, 2020

6 Cena a pracnost projektu

6.1 Kalkulace projektu

Činnosti v rámci projektu	Pracnost v MD	Cena bez DPH
Sociální inženýrství – phishing emailová kampaň		
Definice „Rules of Engagement“ a projektové řízení	1	14.000,- Kč
- Příprava kampaně (konfigurace prostředí, šablony emailu, testování) - Realizace kampaně - Závěrečná zpráva	5 1 2	112.000,- Kč
Sociální inženýrství – telefonická kampaň		
Definice „Rules of Engagement“ a projektové řízení - Příprava skriptu - Realizace kampaně - Závěrečná zpráva	2 2 1	70.000,-Kč
CELKEM za 1. kolo testů Q3 2022		196.000,- Kč
CELKEM za 2. kolo testů Q4 2022		196.000,- Kč
CELKEM oba testy		**392.000,- Kč**

Celková cena **včetně DPH je 474.320,- Kč.**

7 Platební podmínky

Předpokládáme částečnou fakturaci, vždy po provedení dané kampaně. Faktura bude vystavena na základě předávacího protokolu a bude mít splatnost 30 dnů od data jejího vystavení.

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Doložka číslo: 2776650

Původní datový formát: application/pdf

UUID původní komponenty: f07d9875-b6c2-42db-97de-0932465103c1

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:

Systém ERMS (zpracovatel dokumentu Miriam HEMZOVÁ)

Subjekt, který změnu formátu provedl: Správa železnic, státní organizace

Datum vyhotovení ověřovací doložky: 09.06.2022 13:47:02