**Technické podmínky / Specifikace předmětu plnění**

**Bezpečnostní a penetrační testy**

# Předmět veřejné zakázky

Předmětem veřejné zakázky je dodání služby, pomocí které budou provedeny bezpečnostní a penetrační testy formou sociálního inženýrství a to s cílem ověřit, zda:

* lze získat neoprávněný přístup k službám, datům či informačním systémům zadavatele,
* lze neoprávněně modifikovat nebo zničit data zadavatele,
* lze narušit dostupnost služeb nebo informačních systémů zadavatele,
* lze získat autentizační údaje zaměstnanců zadavatele či jiných osob,
* lze zneužít ICT infrastrukturu zadavatele,

a poskytnout o tom důkazy.

Bezpečnostní a penetrační testy formou sociálního inženýrství musí být provedeny v níže požadovaném rozsahu a musí splňovat veškeré níže uvedené požadavky na formy, metody, režimy, postupy a vyhodnocení.

# Požadavky na režimy testování

Testování bude probíhat v režimu tzv. black-box testu, kdy dodavatel služby nebude mít od zadavatele k dispozici žádné informace o organizační struktuře, interních a externích procesech, personálně organizačních opatření a struktur, architektuře sítě, konfiguraci informačních systémů a poskytovaných služeb, vyjma těch, které budou uvedeny v tomto zadání nebo těch, které budou nezbytné k poskytnutí služby. Takové informace budou předem specifikovány v této zadávací dokumentaci.

Testování by mělo simulovat reálný útok přiměřeně finančně motivovaného externího útočníka, proto všechny testovací scénáře budou v režii dodavatele, zadavatel tedy neposkytne součinnost při vymýšlení scénářů a specifik testovacích útoků.

Zadavatel předpokládá převážně manuální testování s využitím automatických nástrojů a metod v relevantních částech testů.

# Požadavky na metody testování

Zadavatel požaduje provedení všech těchto metod a testů sociálního inženýrství:

## e-mailový test – tzv. phishing

* + test bude dodavatelem proveden prostřednictvím elektronické pošty
  + rozsah testu:
    - minimálně 2 rozdílné podvodné kampaně, kdy každá bude časově rozložena do 4 fází
    - časové fáze budou sloužit rovněž k rozložení útoku mezi uživatele sdílející stejné prostory/kanceláře pro zvýšení důvěryhodnosti útoku
    - celkový počet uživatelů 500 (250 na každou kampaň)
    - uživatelé budou dodavatelem vybráni ze skupin uživatelů, které stanoví zadavatel
  + dodavatel musí alespoň v jedné kampani využít simulovaného podvodného webu, webové či jiné aplikace navržené přímo pro účely podvodné kampaně

## telefonický test – tzv. vishing

* + test bude dodavatelem proveden prostřednictvím telefonického hovoru
  + rozsah testu:
    - minimálně 2 rozdílné podvodné kampaně, kdy každá bude časově rozložena do 4 fází
    - celkový počet uživatelů 30 (15 na každou kampaň)
    - uživatelé budou dodavatelem vybráni ze skupin uživatelů, které stanoví zadavatel
    - u uživatelů s více telefonními kontakty budou preferována mobilní telefonní čísla

## cílený e-mailový test – tzv. spear phishing

* + dodavatel navrhne skupiny uživatelů, kterých se scénáře útoků budou týkat dle vykonávaných agend, přičemž zadavatel bude tyto navržené skupiny uživatelů schvalovat
  + před testem provede dodavatel podrobnou analýza cíle, na jejímž základě bude realizován scénář útoku přesně zacíleného na vybrané uživatele
  + test bude proveden primárně prostřednictvím elektronické pošty, prostřednictvím jiných prostředků (telefonický hovor, sms, sociální sítě, apod.) pouze v případě, pokud to bude vyžadovat scénář testu pro zvýšení důvěryhodnosti útoku
  + rozsah testu:
    - maximálně 10 samostatných cílených útoků vůči 10 vybraným uživatelům
  + cíl této metody musí odpovídat hlavním cílům celého testování specifikovaných v kapitole č. 1 této specifikaci plnění

## sms test – tzv. smshing

* + test bude dodavatelem proveden prostřednictvím krátkých textových zpráv (SMS)
  + rozsah testu:
    - minimálně 2 rozdílné podvodné kampaně, kdy každá bude časově rozložena do 4 fází
    - celkový počet uživatelů 80 (40 na každou kampaň)
    - uživatelé budou dodavatelem vybráni ze skupin uživatelů, které stanoví zadavatel
  + dodavatel musí alespoň v jedné kampani využít simulovaného podvodného webu, webové či jiné aplikace navržené a vytvořené přímo pro účely podvodné kampaně

## aktivní test fyzické bezpečnosti

* + test bude dodavatelem proveden v hlavním sídle zadavatele a bude rozdělen do minimálně 2 časově vzdálených pokusů o fyzický průnik
  + cíl této metody musí odpovídat hlavním cílům celého testování specifikovaných v kapitole č. 1 této specifikaci plnění

## pasivní test fyzické bezpečnosti

* + test bude dodavatelem proveden prostřednictvím vyměnitelných paměťových médií (USB flash disků) s potenciálně nebezpečným obsahem, které dodavatel doručí do 2 lokalit zadavatele, alespoň v celkovém počtu 10 ks
  + testu bude předcházet dodavatelem provedená analýza cílů a metod doručení vyměnitelných paměťových médií za účelem dosažení vysoké důvěryhodnosti útoku
  + lokality určí zadavatel formou adresy a názvu organizační jednotky (oddělení/odbor) po dohodě s dodavatelem a s ohledem na provedenou analýzu cílů

## audit přístupových tokenů

* + dodavatel provede audit možností klonování či jiných úprav přístupových tokenů uživatelů zadavatele (přístupové karty)
  + zadavatel poskytne dodavateli testovací přístupové tokeny v maximálním počtu 3 ks
  + předmětem auditu budou zadavatelem aktuálně používané přístupové karty (Mifare S50 1K)

## test bezdrátových sítí

* + dodavatel provede testování bezdrátových sítí provozovaných zadavatelem a dostupných v sídle zadavatele a jeho okolí v tomto rozsahu:
    - mapování dostupných bezdrátových sítí
    - vytvoření falešného přístupového bodu vhodné sítě za účelem dosažení cílů testování specifikovaných v kapitole č. 1 této specifikace; tento falešný přístupový bod bude umístěn ve 2 lokalitách – v sídle zadavatele a v 1 z detašovaných pracovišť a to na vhodných místech, které vybere dodavatel
      * zadavatel předpokládá využití dodavatelem těchto technologií:
        + captive portál
        + WPA2-Enterprise
        + WPA3-Enterprise
    - pokus o odposlech autentizačních údajů pro 2 sítě provozované dodavatelem (definované zadavatelem pomocí SSID)
    - analýza bezdrátových sítí provozovaných zadavatelem s cílem získání přístupu k aktivům vnitřní sítě

## test sociálních sítí

* + dodavatel provede analýzu používání sociálních sítí s ohledem na
    - oficiální profily na sociálních sítích
    - komunikaci zaměstnanců na sociálních sítích
  + na základě této analýzy dodavatel navrhne možné testovací scénáře vůči zaměstnancům prostřednictvím sociálních sítí za účelem dosažení cílů specifikovaných v kapitole č. 1 této specifikace
  + na základě této analýzy dodavatel navrhne možné testovací scénáře založená na testování odolnosti stávajících používaných profilů na sociálních sítích
  + navržené testovací scénáře před jejich použitím bude schvalovat zadavatel

# Požadavky na realizaci testování

Testování bude provedeno na základě harmonogramu, který zpracuje dodavatel a schválí zadavatel.

V harmonogramu musí být zohledněny požadavky fázování jednotlivých metod.

Dále musí harmonogram zohledňovat rozfázování jednotlivých testů tak, aby testování probíhalo alespoň 6 měsíců za účelem zvýšení důvěryhodnosti testů a snížení podezření ze strany uživatelů.

Zdroje testování budou dodavatelem určeny před zahájením testů a během testování budou neměnné. Změny ve zdrojích bude možné provádět pouze za účelem dosažení stanoveného scénáře, a pokud to bude nezbytné pro provedení konkrétního testu. Taková změna podléhá oznámení odpovědné osobě zadavatele a jejímu schválení. Za zdroje testování zadavatel považuje:

* veřejné IP adresy, ze kterých bude testování prováděno (mail servery, podvodné weby, connect servery pro škodlivý obsah, apod.)
* veřejné domény, ze kterých bude testování prováděno (mail servery, podvodné weby, connect servery pro škodlivý obsah, apod.)
* telefonní čísla, ze kterých bude testování prováděno (pro telefonní hovory i SMS),
* totožnosti osob provádějících test fyzické bezpečnosti (prokazatelná totožnost).

Kontaktní osoby dodavatele včetně telefonického a e-mailového kontaktu budou předem definovány. Tyto kontaktní osoby budou zodpovídat za realizaci a průběh testů.

Dodavatel bude průběžně informovat vždy před započetím každé fáze testu a po ukončení každé fáze testu odpovědné osoby zadavatele specifikované ve smlouvě.

# Požadavky na výstupy testování

Všechny testy musí být provedeny tak, aby bylo možné vyhodnotit a případně sledovat chování testovaných uživatelů v průběhu testů.

Výstupem těchto testů budou:

* Podrobná závěrečná zpráva v elektronické podobě
  + Podrobná závěrečná zpráva musí shrnovat provedené analýzy, výsledky testů dle jednotlivých metod testování až do úrovně výsledků jednotlivých uživatelů. Závěrečná zpráva bude obsahovat kompletní seznam nálezů, jejich klasifikaci dle závažnosti a doporučení na jejich odstranění či zabránění k jejich opakování. Dále bude závěrečná zpráva obsahovat podrobnosti o provedených metodách testování, nástrojích a technických prvcích použitých při testování. Podrobná závěrečná zpráva bude zadavateli předána nejpozději do 3 týdnů po ukončení a vyhodnocení všech metod testování, kampaní a jejich časových fází.
* Průběžné zprávy s výsledky jednotlivých časových fází kampaní v elektronické podobě
  + Průběžné zprávy s výsledky jednotlivých časových fází kampaní musí obsahovat provedené analýzy a výsledky testů jednotlivých metod testování až do úrovně výsledků jednotlivých uživatelů, přičemž tyto zprávy budou vypracovávány a předávány zadavateli průběžně a to vždy po ukončení jednotlivých časových fází, nejpozději však do 2 týdnů od ukončení každé časové fáze.

Dalším výstupem testování bude prezentace výstupů a konzultace u zadavatele po ukončení všech testů a po předání závěrečné zprávy. Termín realizace prezentace a konzultace bude stanoven po vzájemné dohodě zadavatele a dodavatele avšak nejpozději do 1 kalendářního měsíce od předání závěrečné zprávy.

Dodavatel si ponechá všechna zdrojová data potřebná pro analýzy a testování, reprezentaci výsledků testování a sestavení průběžných i závěrečných zpráv po dobu 6 měsíců od provedené prezentace a konzultace u zadavatele pro účely zodpovězení případných dotazů a otázek ze strany zadavatele.