Technická specifikace předmětu plnění

Předmětem smlouvy je poskytování následujících služeb:

Služba číslo 1 - Penetrační testování webových aplikaci
Služba číslo 2 - Penetrační testování interní infrastruktury
Služba číslo 3 - Penetrační testování externí infrastruktury
Služba číslo 4 - Penetrační testování cloud prostředí
Služba číslo 5 - Penetrační testování mobilních aplikací

• Obecné požadavky na testování

Cílem penetračního testování je ověření zabezpečení aplikace nebo infrastrukturních prvků a nalezení slabých míst informačního systému, které by mohly být potenciálně zneužity útočníkem k poškození Objednatele.

Předmětem penetračních testů je nalézt takové zranitelnosti, jejichž pomocí lze prolomit bezpečnostní opatření a narušit dostupnost, integritu nebo důvěrnost systému či aplikace.

Například:

i. získat neautorizovaný nebo neoprávněný přístup k citlivým údajům,
ii. z testovaných systémů a aplikací provést neautorizované nebo neoprávněné kopírování citlivých dat,
iii. provést manipulaci (změnu nebo smazání) citlivých dat uložených v systému, především se zaměřením na manipulaci s informacemi o klientech a transakcích (pozměnění transakce nebo klientských informací, smazání transakce),
iv. zjistit zranitelnost systémů a jejich komponent vůči známým a relevantním typům útoků.

Výsledky testů a měření musí být kvantifikovatelné, opakovatelné a odvozené pouze na základě skutečností zjištěných v testech.

Veškeré reportované zranitelnosti musí obsahovat informaci o potenciálním riziku (závažnosti), konkrétním postupu nápravy a informaci o pravděpodobnosti zneužití v praxi.

Veškeré testy musí být prováděny nedestruktivně a pro ověření zranitelností musí Poskytovatel upřednostňovat především méně invazivní techniky, tak, aby bylo minimalizováno riziko pádu aplikace, systému či narušení chodu společnosti!

V rámci penetračního testování mohou být použity nástroje a technologie uvedené v rámci jednotlivých částí této přílohy s technickými požadavky na provedení testů. Poskytovatel může využít další nástroje, které byly z jeho strany řádně otestovány.

V případě, že Poskytovatel využívá ke své činnosti dle této smlouvy licencovaný software, musí být Poskytovatel schopen prokázat, že disponuje potřebnými licencemi pro použité nástroje a technologie.

V případě zjištění omezené dostupnosti testovaných systémů nebo určité služby v důsledku testů uvědomí testovací tým o situaci neprodleně kontaktní osobu na straně Objednatele. Testování bude probíhat na provozním prostředí.

Poskytovatel musí při provádění penetračních testů vycházet z jedné nebo více v praxi používaných metodik a standardů určených pro provádění bezpečnostního testování, uvedených u jednotlivých služeb.

Poskytovatel také musí neprodleně informovat stanovenou kontaktní osobu na straně Objednatele, pokud při penetračním testování objeví kritické zranitelnosti, které by mohly vést ke

kompromitaci prostředí Objednatele, nebo indikátory o již úspěšné kompromitaci testovaného prostředí. Pokud je to možné, měl by Poskytovatel v rámci oznámení také uvést opatření a doporučení k minimalizaci rizika zneužití těchto zranitelností.

Dále je Poskytovatel povinen dodržovat stanovenou formu a rozsah testování.

Poskytovatel může dle své úvahy zařadit typy útoků na hrozby a zranitelnosti, které považuje na základě svých zkušeností nebo na základě průběžných výsledků penetračního testování za důležité a relevantní pro uvedené komponenty a funkčnosti.

Veškeré testy budou před samotným výkonem konzultovány s Objednatelem. Objednatel poskytne potřebnou součinnost pro provedení testů a Poskytovatel poskytne veškeré IP a MAC adresy, ze kterých bude testování prováděno.

Testování je možné provádět pouze ve dnech a časech stanovených ve schváleném harmonogramu a pouze z IP adres poskytnutých Objednateli. Neohlášené testy z neschválených IP adres budou považované za nelegální.

V rámci penetračního testování je Poskytovatel povinen zajistit bezpečnost dat a výstupů, které vznikají v průběhu testování.

V případě dodávání fyzických kopií výsledků testů musí Poskytovatel zajistit, aby byly k dispozici pouze autorizovaným osobám na straně Objednatele. Při přepravě musí být zabezpečen přenos těchto kopií tak, aby nedošlo k úniku citlivých informací.

Po dokončení testování musí Poskytovatel zajistit likvidaci všech dat a výstupů, které vznikly v průběhu testování do doby stanovené ze strany Objednatele. Toto zahrnuje jak data na systémech Poskytovatele, tak jakékoliv fyzické kopie a záznamy.

Při předávání výsledků z testování musí Poskytovatel použít kryptografické metody šifrování, jako například PGP nebo S/MIME. Alternativou mohou být heslem chráněné soubory, avšak je třeba zajistit, aby heslo bylo bezpečné a nebylo známo neoprávněným osobám. Heslo tedy musí být distribuováno separátním kanálem (například SMS) a musí mít adekvátní složitost.

Úroveň autentizace při testech je závislá na konkrétním scénáři a požadavcích pro jednotlivé oblasti testování. Při testování může být použito kombinace různých úrovní autentizace, aby testy věrně odrážely skutečné možnosti kompromitace testovaného systému.

V rámci poskytnutí služeb č. 1 až č. 5 požaduje Objednatel vytvoření písemné závěrečné zprávy v následující struktuře (závazné náležitosti zprávy):

- Název testovaného systému nebo aplikace;
- Manažerské shrnutí obsahující přehledovou tabulku s nálezy zahrnující:
    - Popis nálezu,
    - Dopad zranitelnosti,
    - Závažnost (severity) nálezu,
    - Doporučení k odstranění nebo zmírnění nálezu,
    - Odkaz na příslušnou kapitolu s detailním popisem nálezu.
- Použitá metodika testování včetně způsobu klasifikace zranitelností:
    - 1.Black box (Zero Knowledge), kdy nebudou testovacímu týmu předány žádné dodatečné informace o testované aplikaci nebo systému.
    - 2 Gray box (Partial Knowledge), která spočívá v testování s částečnou předchozí znalostí testovaného systému a prostředí.

- 3 White Box (Full Knowledge), která spočívá v testování se znalostmi na úrovni interního bezpečnostního týmu Zadavatele.

- Úroveň autentizace při testech je závislá na konkrétním scénáři a požadavcích pro jednotlivé oblasti testování. Při testování může být použito kombinace různých úrovní autentizace, aby testy věrně odrážely skutečné možnosti kompromitace testovaného systému.
- Seznam nalezených zranitelností rozdělený do kategorií dle metodiky CVSS verze 3.0, resp. PTES pro Red Team testy řazených dle závažnosti od nejzávažnější po nejméně závažnou.
- Popis nálezů a všech známých chyb testované aplikace, včetně potenciálního vektoru útoku, popisu rizik, které nález představuje a možných dopadů spojených s těmito riziky.
- Návrh adekvátních řešení k odstranění nebo zmírnění nálezu.
- Konkrétní vzorový příklad úspěšného útoku ke každé nalezené zranitelnosti (pouze u středního a vysokého stupně rizika dle CVSS, resp. PTES).

• Slovník technických pojmů pro účely této přílohy a výstupů z penetračního testování

DoS/DDoS	Útoky na přetížení systému nebo sítě.
PGP	Program pro šifrování a podepisování e-mailů.
S/MIME	Protokol pro zabezpečení elektronické pošty.
PHP	Skriptovací programovací jazyk pro webové aplikace.
MySQL	Relační databázový systém.
React	Knihovna pro vytváření uživatelských rozhraní.
NodeJS	Otevřená běhová prostředí pro serverovou stranu JavaScriptu.
GraphQL	Dotazovací jazyk pro API.
MS SQL	Microsoft SQL Server, relační databázový systém.
.NET	Rámec pro vývoj softwaru od Microsoftu.
OWASP	Open Web Application Security Project, komunita pro zabezpečení webových aplikací.
Burp Suite	Sada nástrojů pro testování zabezpečení webových aplikací.
OWASP ZAP	Nástroj pro testování zabezpečení webových aplikací.
WSTG	Web Security Testing Guide, průvodce testováním zabezpečení webových aplikací.
CWE	Common Weakness Enumeration, seznam běžných bezpečnostních chyb.
CVSS	Common Vulnerability Scoring System, systém pro hodnocení závažnosti zranitelností.
VM	Virtuální stroj.
VLAN	Virtuální lokální síť.
DHCP starvation	Útok na vyčerpání DHCP adres.
VLAN hopping	Neoprávněný přístup mezi VLANy.
ARP/MAC spoofing	Podvrhnutí ARP nebo MAC adresy.
STP manipulation	Manipulace s protokolem STP (Spanning Tree Protocol).
Pass-the-hash	Útok získáním hashové hodnoty hesla
BloodHound	Nástroj pro analýzu oprávnění v síti.
Mimikatz	Nástroj pro získávání hesel v systémech Windows.
PingCastle	Nástroj pro analýzu zabezpečení infrastruktury Active Directory.
Kerberoasting	Útok na získání hesel z protokolu Kerberos.
nmap	Nástroj pro skenování sítě a zjišťování informací o zařízeních.
Kismet	Nástroj pro bezdrátovou síťovou analýzu.
Aircrack-ng	Sada nástrojů pro testování zabezpečení Wi-Fi sítí.

Wireshark	Nástroj pro analýzu síťového provozu.
PTES	Penetration Testing Execution Standard, standard pro provedení penetračního testování.
OSSTMM	Open Source Security Testing Methodology Manual, metodika pro testování zabezpečení.
ISSAF	Information Systems Security Assessment Framework, rámec pro hodnocení zabezpečení informačních systémů.
VPN	Zabezpečený a šifrovaný kanál pro bezpečný přenos dat.
RDP	Remote Desktop Protocol, protokol pro vzdálený přístup na vzdálené počítače.
CIS Benchmark	Bezpečnostní standardy od organizace Center for Internet Security.
Apache Cordova	Platforma pro vývoj mobilních aplikací.
Objective-C	Programovací jazyk.
Java	Programovací jazyk.
Frida	Nástroj pro analýzu a manipulaci s aplikacemi.
Ghidra	Nástroj pro reverzní inženýrství.
Radare	Rámec pro analýzu binárních souborů.
SPF	Mechanismus pro specifikaci oprávněných serverů pro odesílání e-mailů.
DKIM	Mechanismus digitálního podepisování e-mailů.
DMARC	Mechanismus pro ověřování a vyhodnocování SPF a DKIM.

Služba číslo 1 - Penetrační testování webových aplikací

Specifikace

Bude provedeno testování dvou webových aplikací včetně podpůrné infrastruktury:

1. webová prezentace www.ozp.cz
2. webové rozhraní aplikace VITAKARTA (www.ozp.cz/vtk)

Webová prezentace (www.ozp.cz mimo Vitakartu) slouží především k prezentaci statického obsahu a má jen omezenou možnost uživatelského vstupu (hledání, formuláře, chat atd.).

Scénář testování

Testování bude probíhat ve dvou fázích. První fáze bude realizována v roli anonymního (neautentizovaného) uživatele. V druhé fázi bude testovacímu týmu k dispozici účet běžného (autentizovaného) uživatele pro aplikaci VITAKARTA.
Cílem obou fází je s dostupnými prostředky odhalit případné zranitelnosti v aplikacích a službách, které by mohl zneužít potenciální útočník k útokům na jiné uživatele nebo k narušení dostupnosti, integrity nebo důvěrnosti. Účelem testů je nalezené zranitelnosti odstranit a zvýšit tak bezpečnost celého systému. Popsaný scénář předpokládá využití níže zmíněných metodik OWASP.

Test podpůrné infrastruktury bude zahrnovat scany portů, identifikaci běžících služeb/komponent a zjištění známých zranitelností.
Součástí testování bude také re-test případných nalezených kritických a vysoce závažných zranitelností.

Nástroje a technologie testování

Pro testování je možné využít nástroje typu skenerů zranitelností, jejichž nálezy je potřeba manuálně verifikovat pomocí dodatečných technik. Především ale musí být testování zaměřeno na manuální hledání zranitelností, které mohou automatizované nástroje přehlédnout. Testovací tým tak musí vyžívat standardně využívané nástroje jako jsou Burp Suite, OWASP ZAP nebo Metasploit, případně jiné otestované nástroje s obdobnou funkcionalitou.

Metodiky testování

Testovací tým musí používat v praxi využívané metodiky nebo jejich kombinaci, případně vlastní metodiku, která je s nimi v souladu. Aby bylo zajištěno komplexní a efektivní otestování webové aplikace, musí testovací tým využívat osvědčené metodiky a standardy jako jsou:

- Open Web Application Security Project (OWASP) Web Security Testing Guide (WSTG)
- OWASP Top 10
- OWASP API Security Top 10

Předpokládaná časová náročnost

Testování fáze 1 (neautentizovaný uživatel)	3 MD
Testování fáze 2 (autentizovaný uživatel)	6 MD
Vyhodnocování nálezů a tvorba závěrečné zprávy	2 MD
Re-test včetně zprávy	*5 MD*
Celkem	**16 MD**

Výstup testování

Výstupem testování musí být komplexní písemná zpráva s podrobnými zjištěními, doporučeními a kroky k nápravě doplněná o manažerské shrnutí.

Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a zhodnocení potenciálního rizika. Testovací tým musí poskytnout informace o nástrojích a technikách použitých během testování spolu s případnými vytvořenými skripty nebo kódem. Zpráva musí obsahovat hodnocení závažnosti zranitelností pomocí skóre a vektoru Common Vulnerability Scoring System (CVSS) a jejich kategorizaci dle Common Weakness Enumeration (CWE) nebo OWASP Top 10. Pokud byl zranitelnosti přidělen CVE (Common Vulnerabilities and Exposures) identifikátor, musí být rovněž uveden v závěrečné zprávě. Zpráva musí stanovit priority a doporučení k nápravě zranitelností na základě závažnosti zranitelností a potenciálního dopadu na organizaci.
Výstupní zpráva z fáze re-testu musí obsahovat validaci opravy nalezených kritických a vysoce závažných zranitelností.

Parametry úlohy pro službu číslo 1 – Penetrační testování webových aplikací

Parametr	**Hodnota**
Typ testu	Gray-box
Prostředí testu	produkční
Forma testu	Autentizovaný a neautentizovaný penetrační test webových aplikací
Hlavní testovací scénáře	• Neautentizovaný test (anonymní přístup) • Autentizovaný test (účet běžného uživatele) • Standardní scénáře dle OWASP WSTG • Neoprávněné získání vyšších oprávnění • Únik citlivých dat • Útoky na jiné uživatele aplikace
Typ aplikace	Webová (tenký klient)
Počet formulářů k otestování	5<
Průměrný počet vstupních polí na formulář	10
Počet rolí	2 (běžný uživatel, editor)
Počet API k otestování	2, z toho 1 REST API a 1 SOAP API
Průměrný počet metod v API	10
Průměrný počet parametrů při volání API	5
Počet IP adres	16
Poskytnutá součinnost	Předání přihlašovacích údajů k testovacímu účtu v roli běžného uživatele. Identifikace testovaných cílů (URL adresy). Vzorová volání API, API klíče (pokud je relevantní). Předání informací o primární kontaktní osobě. Předání informací o eskalačním kontaktu

Lhůta pro provedení služby (testování) ode dne objednání (doručení výzvy Objednatele):

- **Základní testování** (testování fáze 1 - neautentizovaný uživatel, testování fáze 2 - autentizovaný uživatel, vyhodnocování nálezů vč. závěrečné zprávy)**: 20 pracovních dnů**
- **Re-test** (vč. zprávy): **10 pracovních dnů**

Služba číslo 2 - Penetrační testování interní infrastruktury

Specifikace

Testování proběhne v prostředí, kde je (jsou) přibližně:

- 170 virtuálních strojů (VMs)
- 50 fyzických strojů
- síťové prvky a bezdrátová síť (segmentovaná síť, cca 35 VLAN)

Scénář testování

Testování bude probíhat formou assumed breach scénáře a bude mít za úkol identifikovat slabá místa v rámci vnitřní ochrany informačního prostředí a zlepšit tak úroveň připravenosti na případný útok. Testovací tým bude v roli útočníka s rolí běžného uživatele a bude mít za úkol najít způsoby, jakými by mohl proniknout do informačního systému a získat přístup k citlivým informacím nebo přístup ke kritickým systémům. Dále bude cílem nalézt slabá místa v konfiguraci systémů a nastavení domény a prakticky ověřit možnosti jejich zneužití.
Konkrétně musí testovací tým ověřit odolnost vůči základním útokům na nastavení sítě (VLAN hopping, DHCP starvation, ARP/MAC spoofing, STP manipulation, úroveň zabezpečení bezdrátových sítí …), útokům na doménu (Kerberoasting, Golden/Silver ticket, Pass-the-hash a další) a u bezdrátových sítí útoky na samotné přístupové body a autentizační a šifrovací mechanismy. Dále bude testovací tým ověřovat potenciální zranitelnosti na všech ostatních zařízeních a možnosti jejich potenciálního zneužití v roli běžného interního uživatele sítě. Testování bude omezeno časem alokovaným pro testování.
Součástí testování bude také re-test případných nalezených kritických a vysoce závažných zranitelností.

Nástroje a technologie testování

Pro testování je možné využít nástroje typu skenerů zranitelností, jejichž nálezy je potřeba manuálně verifikovat pomocí dodatečných technik. Pro testování konfigurace sítě musí testovací tým využít nástroje srovnatelné s běžně využívaným softwarem jako je nmap, Kismet, Aircrack-ng, Wireshark a dalšími. Při testování nastavení domény a autentizace pak nástroje jako jsou BloodHound, Mimikatz nebo PingCastle či jiné nástroje, které mají podobnou funkcionalitu a které byly Dodavatelem řádně otestovány.

Metodiky testování

Testovací tým musí používat v praxi využívané metodiky nebo jejich kombinaci, případně vlastní metodiku, která je s nimi v souladu. Aby bylo zajištěno komplexní a efektivní otestování interní infrastruktury musí testovací tým využívat osvědčené metodiky a standardy jako jsou:

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assesment Framework (ISSAF)

Předpokládaná časová náročnost

Zmapování prostředí a zranitelností na službách (dle přístupů definovaného assumed breach scénáře)	2 MD
Zneužití zjištěných informací k prolomení bezpečnosti, dosažení co nejvyšších oprávnění, pivoting a získání přístupu k citlivým datům (v rozsahu „worst case“ scénáře)	časově omezeno na maximálně 10 MD
Skenování bezdrátových sítí a ověření základních útoků vůči bezdrátové infrastruktuře	2 MD / na jednu fyzickou oblast
Vyhodnocování nálezů a tvorba závěrečné zprávy	3 MD
Re-test včetně zprávy	10 MD

Celkem	**27 MD +**

Výstup testování

Výstupem testování musí být komplexní písemná zpráva s podrobnými zjištěními, doporučeními a kroky k nápravě doplněná o manažerské shrnutí.
Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a zhodnocení potenciálního rizika. Testovací tým musí poskytnout informace o nástrojích a technikách použitých během testování spolu s případnými vytvořenými skripty nebo kódem. Zpráva také musí obsahovat hodnocení zranitelností pomocí skóre a vektoru Common Vulnerability Scoring System (CVSS) nebo Common Weakness Enumeration (CWE). Pokud byl zranitelnosti přidělen CVE (Common Vulnerabilities and Exposures) identifikátor, musí být rovněž uveden v závěrečné zprávě. Zpráva musí stanovit priority a doporučení k nápravě zranitelností na základě závažnosti zranitelností a potenciálního dopadu na organizaci.
Výstupní zpráva z fáze re-testu bude obsahovat validaci opravy nalezených kritických a vysoce závažných zranitelností.

Parametry úlohy pro službu číslo 2 - Penetrační testování interní infrastruktury

Parametr	**Hodnota**
Typ testu	Gray-box
Prostředí testu	Produkční
Forma testu	Forma assumed breach s výchozí pozicí běžného uživatele
Testovací scénář	Testování má za úkol ověřit, jaké škody by mohl napáchat útočník v roli běžného uživatele.
Počet server v testovaném prostředí	170 VM, 50 fyzických serverů
Operační systémy v testovaném prostředí	Linux, Microsoft Windows Server <prosím o upřesnění>
Průměrný počet otevřených portů na server / běžících služeb	6
Segmentace prostředí	cca 35 VLAN
Poskytnutá součinnost	Poskytnutí údajů/zařízení potřebných pro zajištění výchozí pozice (běžný uživatel). Dohodnutí termínů pro testování. Předání informací o primární kontaktní osobě. Předání informací o eskalačním kontaktu

Lhůta pro provedení služby (testování) ode dne objednání (doručení výzvy Objednatele)

- **Základní testování** (zmapování prostředí a zranitelností na službách, zneužití zjištěných informací k prolomení bezpečnosti, dosažení co nejvyšších oprávnění, pivoting a získání přístupu k citlivým datům, skenování bezdrátových sítí a ověření základních útoků vůči bezdrátové infrastruktuře, vyhodnocování nálezů vč. závěrečné zprávy): **40 pracovních dnů**
- **Re-test** (vč. zprávy): **10 pracovních dnů**

Služba číslo 3 - Penetrační testování externí infrastruktury

Specifikace

Bude testováno celkem 10 IP adres dostupných z internetu přes cca 20 domén. Na těchto IP adresách je do internetu publikováno přibližně 5 služeb. V rozsahu této služby je veškerá infrastruktura a služby OZP, které jsou dostupné z internetu. Mimo rozsah testování jsou webové a mobilní aplikace definované zvlášť v samostatných sekcích.

Scénář testování

Při testování vnějšího perimetru bude mít testovací tým za úkol simulovat útok externího neautentizovaného škodlivého aktéra, který má za cíl získat neoprávněný přístup do sítě nebo systémů organizace. Jedná se tedy o Black box (Zero-knowledge) test.

Testování bude zahrnovat identifikaci potenciálních zranitelností v obranných prvcích perimetru, jako jsou firewally, systémy IPS, webové firewally, v řešeních pro vzdálený přístup (např. VPN nebo RDP), v interních službách, serverech a využívaných protokolech (SMTP, FTP, databáze a tak dále).

Při testování se testovací tým bude soustředit především na možnosti zneužití známých zranitelností publikovaných služeb přístupných z internetu a možné chyby v nastavení. Cílem bude zmapovat celý perimetr OZP, identifikovat potenciální zranitelné cíle a služby a pokusit se jejich zranitelnosti využít k získání výhodnější pozice k dalšímu postupu.

Součástí testování bude také re-test případných nalezených kritických a vysoce závažných zranitelností.

Nástroje a technologie testování

Pro testování je možné využít nástroje typu skenerů zranitelností, jejichž nálezy je potřeba manuálně verifikovat pomocí dodatečných technik. Dále je vhodné využít nmap pro mapování perimetru a exploitačního frameworku, jako například Metasploit, pro následné zneužití nalezených zranitelností.

Metodiky testování

Testovací tým musí používat v praxi využívané metodiky nebo jejich kombinaci, případně vlastní metodiku, která je s nimi v souladu. Aby bylo zajištěno komplexní a efektivní otestování musí testovací tým využívat osvědčené postupy a zdroje jako jsou:

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assesment Framework (ISSAF)

Předpokládaná časová náročnost

Zmapování externího perimetru a testování publikovaných služeb na IP adresách	cca 4 MD
Vyhodnocování nálezů a tvorba závěrečné zprávy	2 MD
Re-test včetně zprávy	4 MD
Celkem	**cca 10 MD**

Výstup testování

Výstupem testování musí být komplexní písemná zpráva s podrobnými zjištěními, doporučeními a kroky k nápravě doplněná o manažerské shrnutí.

Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a zhodnocení potenciálního rizika. Testovací tým musí poskytnout informace o nástrojích a technikách použitých během testování spolu s případnými vytvořenými skripty nebo kódem. Zpráva také musí obsahovat hodnocení zranitelností pomocí skóre a vektoru Common Vulnerability Scoring System (CVSS) nebo Common Weakness Enumeration (CWE). Pokud byl zranitelnosti přidělen CVE (Common

Vulnerabilities and Exposures) identifikátor, musí být rovněž uveden v závěrečné zprávě. Zpráva musí stanovit priority a doporučení k nápravě zranitelností na základě závažnosti zranitelností a potenciálního dopadu na organizaci.
Výstupní zpráva z fáze re-testu bude obsahovat validaci opravy nalezených kritických a vysoce závažných zranitelností.

Parametry úlohy – Služba číslo 3 - Penetrační testování externí infrastruktury

Parametr	**Hodnota**
Typ testu	Black-box
Prostředí testu	Produkční
Forma testu	Zero-knowledge externí penetrační test.
Testovací scénář	Testování má za úkol otestovat možnosti průniku útočníka do interního prostředí.
Počet externích IP adres	50
Průměrný počet otevřených portů na server / běžících služeb	5
Poskytnutá součinnost	Poskytnutí externích IP rozsahů (volitelné). Dohodnutí termínů pro testování. Předání informací o primární kontaktní osobě. Předání informací o eskalačním kontaktu

Lhůta pro provedení služby (testování) ode dne objednání (doručení výzvy Objednatele)

- **Základní testování** (zmapování externího perimetru a testování publikovaných služeb na IP adresách, vyhodnocování nálezů vč. závěrečné zprávy)**: 12 pracovních dnů**
- **Re-test** (vč. zprávy)**: 8 pracovních dnů**

Služba číslo 4 - Penetrační testování cloud prostředí

Specifikace

Testováno bude cloudové prostředí Office 365, konkrétně bude především zaměřeno na Exchange Online (E3 a E5 licence). Celkový počet uživatelských identit v cloudu je přibližně 600 a využívá se hybridní systém identit doplněný o dvoufaktorovou autentizaci. Kromě Exchange online je využíváno dalších cloudových Microsoft služeb, jako jsou Office aplikace, MS Teams, Yammer a tak dále. Zhodnocení bezpečnosti a konfigurace bude provedeno formou bezpečnostního auditu.

Scénář testování

Testování cloudového prostředí OZP bude provedeno formou bezpečnostního auditu. V současné době má společnost v cloudu poštovní server Exchange Online. Audit bude zahrnovat přezkoumání nastavení zabezpečení a konfigurace v rámci cloudového prostředí s cílem identifikovat případné zranitelnosti nebo chyby v konfiguraci.
V rámci auditu musí být ověřeno nastavení systému identit (heslová politika, typ autentizace, multi-faktorová autentizace a podmíněný přístup). Dále bude provedena kontrola nastavení zabezpečení a blokování škodlivého obsahu (např. konfigurace Exchange Online Protection a Advanced Threat Protection), oprávnění přístupů do e-mailových schránek a bezpečná integrace třetích stran (plug-iny a add-ony). Kontrola správného nastavení mechanismů pro ověřování a zabezpečení elektronické pošty (SPF, DKIM a DMARC). Ověření bezpečného nastavení synchronizace uživatelů (Azure AD Connect a Active Directory Federation Services).

Auditní přístup

Při bezpečnostním auditu bude využito metod řízeného rozhovoru, sbírání auditní evidence a případného testování. V rámci auditu budou shromažďovány informace, které budou vyhodnoceny a budou využity k vypracování závěrečné zprávy. Audit je svou povahou neinvazivní forma ověření bezpečnosti.

Metodiky testování

Testovací tým musí v rámci auditu využívat v praxi využívané metodiky nebo jejich kombinaci, případně vlastní metodiku, která je s nimi v souladu. Aby bylo zajištěno komplexní a efektivní posouzení nastavení cloudového prostředí musí testovací tým využívat osvědčené postupy a zdroje jako jsou:

- Best practices od společnosti Microsoft
- CIS Microsoft 365 Benchmarks

Předpokládaná časová náročnost

Auditní procedury	4 MD
Vyhodnocení získaných informací a testování	8 MD
Tvorba závěrečné zprávy	3 MD
Celkem	**15 MD**

Výstup testování

Závěrečná zpráva z bezpečnostního auditu bude obsahovat shrnutí výsledků, popis prostředí, seznam zjištěných problémů, seznam doporučení pro jejich nápravu. Zpráva musí být výsledkem objektivního hodnocení v souladu s platnými normami a standardy pro bezpečnostní audity daného prostředí. Zpráva bude doplněná o manažerské shrnutí.

Parametry úlohy pro službu číslo 4 – Penetrační testování cloud prostředí

Parametr	**Hodnota**
Typ testu	Audit
Prostředí testu	Produkční
Forma auditu	Bezpečnostní audit O365 prostředí zaměřený na Exchange Online
Scénář auditu	Přezkoumání nastavení zabezpečení a konfigurace v rámci cloudového prostředí s cílem identifikovat případné zranitelnosti nebo chyby v konfiguraci.
Počet entit v cloudu	cca 600 (hybridní systém identit)
Využívané služby v O365	Exchange Online, Office aplikace, Sharepoint, MS Teams, Yammer, MS AZURE
Poskytnutá součinnost	Read-only práva do O365 prostředí pro auditory. Dohodnutí termínů pro audit. Předání informací o primární kontaktní osobě. Předání informací o eskalačním kontaktu

Lhůta pro provedení služby (testování) ode dne objednání (doručení výzvy Objednatele)

30 pracovních dnů (auditní procedury, vyhodnocení získaných informací a testování, závěrečná zpráva)

Služba číslo 5 - Penetrační testování mobilních aplikací

Specifikace

Předmětem testování bude mobilní aplikace mVITAKARTA určená pro platformy Android a iPhone. Testována bude klientská část v prostředí uvedených platforem a serverová část (webové služby). Součástí testů bude i test podpůrné infrastruktury v rozsahu skenu portů, identifikace služeb/ komponent a zjištění známých zranitelností.

Scénář testování

Testování mobilní aplikace bude probíhat formou Gray Box (Partial Knowledge) a testovacímu týmu bude k dispozici účet běžného (autentizovaného) uživatele.
Cílem testování je s dostupnými prostředky odhalit případné zranitelnosti v mobilní aplikaci, které by mohl zneužít potenciální útočník, za účelem jejich odstranění a souvisejícího zvýšení bezpečnosti celého systému.
Pokud testování odhalí kritické zranitelnosti a nálezy, bude poslední částí testování re-test oprav těchto nedostatků.

Nástroje a technologie testování

Testování musí být zaměřeno na manuální hledání zranitelností pomocí standardně využívaných nástrojů jako jsou Burp Suite či OWASP ZAP (pro webové služby aplikace) a exploitační framework Metasploit (pro serverovou část aplikace), případně otestované nástroje s obdobnou funkcionalitou. Dále je možné využít open-source nástroje jako Frida, Ghidra a Radare.

Metodiky testování

Testovací tým musí používat v praxi využívané metodiky nebo jejich kombinaci, případně vlastní metodiku, která je s nimi v souladu. Aby bylo zajištěno komplexní a efektivní otestování mobilní aplikace musí testovací tým využívat osvědčené metodiky a standardy jako jsou:

- OWASP Mobile Security Testing Guide
- OWASP Mobile Top 10

Předpokládaná časová náročnost

Testování mobilní aplikace Partial Knowledge - Android	5 MD
Testování mobilní aplikace Partial Knowledge - iOS	5 MD
Vyhodnocování nálezů a tvorba závěrečné zprávy	2 MD
Re-test včetně zprávy	6 MD
Celkem	**18 MD**

Výstup testování

Výstupem testování musí být komplexní písemná zpráva s podrobnými zjištěními, doporučeními a kroky k nápravě doplněná o manažerské shrnutí.
Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a zhodnocení potenciálního rizika. Testovací tým musí poskytnout informace o nástrojích a technikách použitých během testování spolu s případnými vytvořenými skripty nebo kódem. Zpráva musí také obsahovat hodnocení zranitelností pomocí skóre a vektoru Common Vulnerability Scoring System (CVSS) nebo kategorizaci dle Common Weakness Enumeration (CWE) nebo OWASP Top 10. Pokud byl zranitelnosti přidělen CVE (Common Vulnerabilities and Exposures) identifikátor, musí být rovněž uveden v závěrečné zprávě. Zpráva musí stanovit priority a doporučení k nápravě zranitelností na základě závažnosti zranitelností a potenciálního dopadu na organizaci.
Výstupní zpráva z fáze re-testu bude obsahovat validaci opravy nalezených kritických a vysoce závažných zranitelností.

Parametry úlohy pro službu číslo 5 – Penetrační testování mobilních aplikací

Parametr	**Hodnota**
Typ testu	Gray-box
Prostředí testu	produkční
Forma testu	Autentizovaný test mobilní aplikace (účet běžného uživatele).
Hlavní testovací scénáře	• Autentizovaný test (účet běžného uživatele) • Standardní scénáře dle OWASP MASTG • Neoprávněné získání vyšších oprávnění • Únik citlivých dat • Útoky na jiné uživatele aplikace
Typ aplikace	Mobilní aplikace
Operační systémy	iOS, Android (dvě verze aplikace)
Počet rolí	2 (běžný uživatel, editor)
Počet API k otestování	2, z toho 1 REST API a 1 SOAP API
Průměrný počet metod v API	10
Průměrný počet parametrů při volání API	<5
Počet stránek k otestování	20
Průměrný počet vstupů na testovaných stránkách	50
Poskytnutá součinnost	Předání přihlašovacích údajů k testovacímu účtu v roli běžného uživatele. Vzorová volání API, API klíče (pokud je relevantní). Dohodnutí termínů pro testování. Předání informací o primární kontaktní osobě. Předání informací o eskalačním kontaktu

Lhůta pro provedení služby (testování) ode dne objednání (doručení výzvy Objednatele)

- **Základní testování** (testování mobilní aplikace Partial Knowledge - Android, testování mobilní aplikace Partial Knowledge – iOS, vyhodnocování nálezů vč. závěrečné zprávy)**: 25 pracovních dnů**
- **Re-test** (vč. zprávy)**: 12 pracovních dnů**