**Příloha č. 1 – Podrobná specifikace Služeb**

# specifikace TESTOVání:

Cílem testu je simulace přiměřeně finančně motivovaného útočníka. Jedná se tedy o formu externího testu (z vnějšku), kdy záměrem fiktivního útočníka bude v ideálním případě ovládnout cílovou síť. Za tím účelem bude nejprve získán seznam běžících služeb kombinací skenu portů a dat z veřejně dostupných zdrojů (např. Shodan). Služby budou následně na základě expertní znalosti Poskytovatele seřazeny od těch s největší pravděpodobností úspěšného napadení a dojde k pokusu o zneužití případných zjištěných zranitelností. Při úspěšném získání přístupů bude následovat snaha o „lateral movement“. Paralelně s testováním síťových služeb budou testovány webové služby..

Krom lokálních použitých nástrojů budou použity i webové nástroje, především pro testování webových aplikací.

Testovaný rozsah Objednatelem definovaných IP adres může být testován kdykoliv v průběhu testovacího období od 15. 6. 2025 do 31. 8. 2025, a to i mimo obvyklou pracovní dobu (obvyklou pracovní dobou se rozumí časový rozsah 8 – 16 hodin).

# Plošný scan IP adresy v rozsahu:

# IP adresy, ze kterých bude probíhat Testování:

217.31.192.0/24

217.31.205.1

217.31.205.2

V průběhu testování může být potřeba přidat IP adresu, kterou bude nutné využít k testu. V takovém případě bude zákazník předem informován prostřednictvím uvedených kontaktů, a Poskytovatel novou IP adresu přidá, jakmile Objednatel přijetí informace potvrdí a odsouhlasí.

# termín provádění testování

# Testování bude probíhat v následujících časech:

# Automatizované testy: Dle potřeby

# Ruční testy: Dle potřeby

# Poskytovatel se zavazuje zahájit Testování 15. 6. 2025 a Testování ukončit nejpozději 31. 8. 2025. V případě nutnosti a vyplyne-li tak z okolností, je možné po dohodě smluvních stran dobu Testování prodloužit, maximálně však o čtrnáct (14) pracovních dní.

# O zahájení a ukončení Testování bude Objednatel informován.

# Výčet rizik při testování

Během testování může docházet

* Při provádění automatizovaných testů k odmítnutí služby (zablokování, nedostupnost; Denial of Service) nebo k omezení provozu;
* Při testování autentizace k zablokování uživatelských účtů;
* K nabourání do systémů a k zpřístupnění či získání dat z tohoto systému;
* K nestandardnímu chování aplikace;
* K aktivaci bezpečnostních mechanismů aplikace/firewallu (může dojít k zaslání oznámení administrátorovi);
* K zaplnění logovacího systému;
* K poškození systému/sítě;
* Ke ztrátě dat;
* K tvorbě fiktivních dat;
* K tvorbě fiktivních registrací.

#

**ZÁVĚŘEČNÁ ZPRÁVA**

# Závěrečná zpráva bude vyhotovena a předána Objednateli do 10 pracovních dní od ukončení Testování.

Závěrečná zpráva bude zejména obsahovat:

# Shrnutí výsledků Testování, popis zjištění, včetně zjištěných zranitelností/nedostatků a podobně s uvedením možných technických a bezpečnostních dopadů, včetně hodnocení jejich rizikovosti (a informace o metodice, která byla pro toto hodnocení použita), je-li to vhodné a účelné uvedení konkrétních použitých technik Testování, z nichž zjištění vyplynula, doporučení, jak se zjištěnými informacemi nakládat.