Příloha č. 1 - Technická specifikace

1. Úvod

Tato technická specifikace definuje požadavky na realizaci penetračního testování infrastruktury před implementací opatření na zvýšení úrovně kybernetické bezpečnosti a po jejich realizaci. Cílem je identifikace zranitelností a posouzení účinnosti navržených bezpečnostních opatření s důrazem na jejich dlouhodobou udržitelnost.

2. Rozsah penetračního testování

Penetrační testování bude realizováno ve dvou fázích:
- Před implementací bezpečnostních opatření (stav před navýšením kybernetické bezpečnosti).
- Po implementaci bezpečnostních opatření (stav po navýšení kybernetické bezpečnosti).

Rozsah zahrnuje následující oblasti:
- Externí perimeter (např. veřejně dostupné IP adresy, servery a služby).
- Interní síťová infrastruktura (servery, pracovní stanice, síťové segmenty).
- Webové a aplikační služby (včetně autentizace, autorizace, přenosu dat, API rozhraní).
- Bezdrátová infrastruktura (pokud je přítomna).
- Sociálně inženýrské útoky (phishing, pretexting) – pouze simulované formou kampaně.
- Zabezpečení fyzického přístupu (základní kontrola přístupových bodů, pokud je to relevantní).

3. Předmět penetračního testování

Testování se zaměří na detekci zranitelností, testování odolnosti proti útokům a ověření nastavení bezpečnostních prvků. Předmětem testování jsou:
- Servery (OS, služby, porty, aktualizace, konfigurace).
- Koncové stanice a pracovní stanice.
- Síťová zařízení (firewally, směrovače, switche).
- Aplikační vrstvy (webové aplikace, autentizační mechanismy, datové toky).
- Uživatelské účty a oprávnění.
- Mechanismy zálohování a obnovy.
- Detekční a monitorovací systémy (např. IDS/IPS, SIEM, logování).

4. Nástroje pro penetrační testování

Použité nástroje pro penetrační testování musí splňovat následující charakteristiky:
- Open-source i komerční nástroje pro síťové skenování, zjišťování zranitelností a testování aplikací.

- Nástroje schopné provádět simulace útoků na základě databází známých zranitelností.
- Automatizované testovací frameworky s možností vytváření vlastních exploitů a skriptů.
- Nástroje s podporou CI/CD integrace pro kontinuální testování.
- Produkty s dlouhodobou podporou výrobce (min. do roku 2031).
- Schopnost generovat podrobné reporty a výstupy pro auditní účely.
- Možnost nasazení on-premise i v prostředí cloudu.
- Pravidelná aktualizace signatur a exploit databází.

5. Odpovídající standardy a normy

- ISO/IEC 27001 (Systémy managementu bezpečnosti informací): Mezinárodní standard specifikující požadavky na vytvoření, implementaci, udržování a neustálé zlepšování systému řízení bezpečnosti informací.
- ISO/IEC 27002 (Kód postupů pro řízení bezpečnosti informací): Doplňující normativní dokument k ISO/IEC 27001 poskytující detailní doporučení pro řízení bezpečnostních opatření.
- OWASP (Open Worldwide Application Security Project): Nezávislá komunita zaměřená na zlepšování bezpečnosti softwaru, zejména webových aplikací. Poskytuje metodiky pro testování a seznamy zranitelností.
- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment): Praktická příručka publikovaná americkým Národním institutem pro standardy a technologie, zaměřená na techniky testování informační bezpečnosti.
- ETSI EN 303 645 (Cyber Security for Consumer Internet of Things): Standard popisující minimální bezpečnostní požadavky pro zařízení IoT.
- MITRE ATT&CK Framework: Otevřená databáze reálných taktik a technik používaných útočníky, využitelná při simulaci útoků a testování odolnosti.

- CVE (Common Vulnerabilities and Exposures): Mezinárodní systém pro standardizovanou identifikaci známých zranitelností v softwaru a hardwaru. Databáze CVE poskytuje jedinečné identifikátory pro každou zranitelnost, což umožňuje efektivní sledování, řízení a reportování v oblasti kybernetické bezpečnosti.

6. Udržitelnost a dostupnost nástrojů

Nástroje pro penetrační testování musí být dostupné a licencované nejen pro potřeby testování v průběhu realizace bezpečnostních opatření, ale i po dobu udržitelnosti projektu, tj. nejméně do 31. 5. 2031. Důraz je kladen na:
- Pravidelnou aktualizaci a podporu nástrojů.
- Možnost přizpůsobení testovacích scénářů měnícím se podmínkám infrastruktury.
- Kompatibilitu s nově zavedenými technologiemi a systémy.
- Možnost napojení na systém správy zranitelností a reporting.