Příloha č. 3

Implementace nástrojů pro penetrační testy a jejich realizace

1 Požadavky na dodávky

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.1	Je požadována dodávka nástroje/nástrojů pro periodické testování bezpečnostních zranitelností interních systémů i systémů, které komunikují s externími subjekty i jako součást penetračních testů.
P.2	Minimální rozsah: externí testy, interní testy a testy zranitelností operačních systémů, databází a informačních systémů (aplikací). Jedná se minimálně o: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací;
P.3	Je požadováno, aby nástroj/nástroje umožňoval: 1. Vzdálené privilegované a neprivilegované skeny 2. Neomezené množství koncových IP adres 3. Pravidelné aktualizace signatur/detekčních metod (cca 1x týdně)
P.4	Předmětem dodávky není periodické provádění testů zranitelností (nad rámec testů v rámci vedlejších aktivit), ale zajištění nástrojů pro provádění a vyhodnocování uvedených testů.
P.5	S ohledem na vysokou citlivost zpracovávaných dat musí být dodaný nástroj možné kompletně instalovat na server/počítač umístěný v lokální síti, která je pod správou Zadavatele. Výstupy z testů/skenů musí být rovněž zpracovávány lokálně, bez zasílání do cloudu. Dodaný nástroj musí umožňovat ovládání s pomocí webového GUI.
P.6	Instalaci skeneru musí být možné realizovat na prvky s operačními systémy Microsoft Windows 10 a vyšší, Microsoft Windows Server 2012 a vyšší, macOS i Linux. Součástí dodávky nebude HW, OS ani další aplikační vybavení nutné pro provoz nástroje. Předpokládá se instalaci na prostředky Zadavatele (virtuální server nebo testovací PC/notebook).
P.7	Dodané řešení musí podporovat realizaci vzdálených bezagentských privilegovaných i neprivilegovaných skenů neomezeného počtu zařízení/IP adres a musí být schopné realizovat bezpečnostní skeny webových aplikací.
P.8	Řešení musí být schopné identifikovat chybějící záplaty/zranitelné služby a aplikace běžící na skenovaných systémech.

#	Požadavek
P.9	Součástí dodávky bude licence relevantního nástroje s podporou a funkčností po dobu 5 let, instalace a aktivace jednoho skeneru v prostředí Zadavatele a úvodní zaškolení administrátorů a uživatelů.
P.10	Provedení penetračních testů a testů zranitelnosti: 1. Provedení penetračních testů a testů zranitelnosti pro zabezpečované IS – 12-15 serverů. 2. Pro zabezpečované systémy budou provedeny závěrečné testy zranitelnosti z externí sítě. 3. Provedení penetračních testů a testů zranitelnosti bezdrátové sítě. V zájmu ověření korektního fungování zabezpečení komunikační sítě a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů.
P.11	Závěrečné testy zranitelnosti budou provedeny z externí sítě na zabezpečované. Jedná se tedy o testy zranitelnosti realizované přes bezpečnostní prvky – perimetry (FireWall). Tyto testy musí obsahovat min.: 1. Host Discovery – vyhledávání aktivních strojů; 2. Port Scanning – skenování portů; 3. Service Discovery – vyhledání běžící služby; 4. Web Applications – skenování webových aplikací; Účelem těchto testů je ověření konfigurace perimetrů a nalezení zranitelností publikovaných služeb/systémů.
P.12	V zájmu ověření a zajištění vysoké úrovně bezpečnosti provozovaných aplikací je požadováno provedení jednorázových penetračních testů. Penetrační testy musí splňovat minimálně: 1. Penetrační testy se budou týkat uvedených aplikací provozovaných zadavatelem a jejich účelem bude identifikovat případné nedostatky v nastavení nasazeného WAF a odhalit případné zranitelnosti ve výše uvedených aplikacích, které jsou jím chráněny, a zajistit tak jejich bezpečnost v rámci plnění požadavků §25 vyhlášky 82/2018 Sb. V souladu s bezpečnostní strategií a dalšími dokumenty zadavatele. 2. Testy budou provedeny jak při využití WAF, tak přímo vůči serveru, který aplikaci poskytuje. Testy budou provedeny jak autentizovanou (s právy běžného uživatele), tak neautentizovanou formou (anonymní přístup). 3. Součástí testů nebude vyhledávání zranitelností v síťové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů provozujících uvedené aplikace, které s provozem daných aplikací přímo nesouvisí. Před vlastními penetračními testy bude proveden test zranitelností. Testy budou realizovány dle aktuální verze OWASP Web Security Testing Guide (WSTG) a v souladu s metodikou OSSTMM a budou primárně zaměřeny na odhalování zranitelností dle platné verze OWASP Top 10. Využito při tom bude automatizovaných nástrojů i manuálního testování.
P.13	Výstupem testů zranitelnosti a penetračních testů musí být: 1. Závěrečná zpráva, která bude obsahovat soupis provedených testů a jejich výsledků, detailní popis odhalených zranitelností, ohodnocení jejich nebezpečnosti včetně konkrétního postupu umožňujícího jejich odstranění. 2. Doporučení řešení odhalených zranitelností – konkrétní postupy umožňující jejich odstranění u oblastí/technologií, které nejsou součástí dodávky.

#	Požadavek
	3. Realizace opatření k odstranění odhalených zranitelností ve formě nastavení a implementace u oblastí, které jsou součástí dodávky.
P.14	Realizace min. 2 komplexních testování / kalendářní rok, tj. 10 testování / 5 let.
P.15	Dodávka permanentních licencí včetně maintenance min. na 5 let nebo předplatné min. na 5 let.

Tabulka 1: Požadavky na dodávky

2 Doba plnění

Poskytnutí licencí a služeb na 5 let od účinnosti smlouvy.

3 Smlouva

Vybraný dodavatel poskytne návrh smlouvy.