**Príloha č. 1**

**Opis predmetu zákazky**

1 Predmet zákazky

Názov predmetu zákazky: **Bezpečnostné testovanie LaaS**

2 Opis predmetu zákazky

2.1 **Informácie potrebné pre ocenenie prác:**

2.1.1 Lokalita, v ktorej bude testovanie prebiehať: ústredie NBS (ul. Imricha Karvaša 1, Bratislava).

2.1.2 LaaS (Login as a Service) je služba určená na autentifikáciu používateľov pristupujúcich cez webové rozhranie a aplikácií pristupujúcich cez API rozhranie k vybraným informačným systémom (aplikáciám)

2.1.3 Používatelia: interní zamestnanci NBS a externí používatelia

2.1.4 Pripojené systémy:

* RBUZ – autentifikácia používateľov aj aplikácie cez API
* Registre – autentifikácia používateľov aj aplikácie cez API

2.1.5 Počet rolí v systéme:

* z hľadiska LaaS: 3 (administrátor LaaS, interný používateľ, externý používateľ), API rozhranie
* pri testovaní budú poskytnuté aj vybrané role v pripojených systémoch

2.1.6 Web rozhranie pre používateľov

* TLS komunikačný kanál
* Podporované prehliadače: Chrome, Firefox

2.1.7 Autentifikácia a autorizácia používateľov

* Heslá (uložené v DB alebo overenie v Active Directory)
* U2F tokeny (Universal 2nd Factor) pre autentifikáciu používateľov a pre digitálne podpisy
* SMS (alternatívny druhý faktor)
* API token (Django TokenAuthentication)
* JWT token podpísaný X.509 certifikátom pre API pre aplikácie aj používateľov

2.1.8 Sieťová infraštruktúra (umiestnenie/dostupnosť serverov):

* Intranet (LAN)
* Univerzal-net (DMZ)
* Internet (DMZ)

2.1.9 Aplikačné servre:

* Aplikačný a externý webový server pre LaaS (DMZ – Univerzal-net; Ubuntu, UFW, Docker);
Docker kontajner: Nginx, Gunicorn, Python image
* Aplikačný a externý webový server pre LaaS (DMZ – Internet; Ubuntu, UFW, Docker);
Docker kontajner: Nginx, Gunicorn, Python image
* Aplikačný a interný webový server pre RBUZ (LAN; Ubuntu, UFW, Nginx, Python)
* Aplikačný a externý webový server pre RBUZ (DMZ – Univerzal-net; Ubuntu, UFW, Nginx, Python)
* Aplikačný a interný webový server pre Registre (DMZ – Internet; Ubuntu, UFW, Nginx, Python)

2.1.10 Testované funkčné oblasti aplikácie LaaS (priemerný počet vstupov na 1 stránke je cca. 1-2 pre autentifikačnú službu, cca. 3-5 pre integrované aplikácie, priemerný počet argumentov v 1 API view je cca. 4-6):

* autentifikácia používateľa vrátane druhého faktora (SMS, U2F) (4 stránky)
* autentifikácia používateľa pri používaní API (token + X.509 podpis) (1 api view)
* správa integrovaných aplikácií (admin – 1 stránka)
* správa používateľov cez ADMIN rozhranie, správa certifikátov (cca 10 stránok)
* autentifikácia na DB a Active Directory
* overenie JWT aplikácie (1 API view)
* webové služby (REST API, JSON) pre správu používateľov (cca 15 API views)
* integrácia LaaSu do RBUZ, Registre – prihlásenie, správa používateľov, správa U2F tokenov, zmena hesla, API, podpisovanie požiadaviek (cca 10 stránok a 2 API views)

2.2 **Cieľ bezpečnostného testovania:**

2.2.1 Cieľom testovania je otestovať bezpečnosť aplikácie a bezpečnostných riešení, identifikovať zraniteľnosti, vrátane návrhu opatrení na nápravu. Testovanie má zhodnotiť či bezpečnostné mechanizmy v aplikácii a spôsoby využívania jej autentifikačných služieb nemajú bezpečnostné nedostatky.

2.2.2 Úspešný uchádzač vyhotoví požadovanú dokumentáciu v slovenskom, českom alebo anglickom jazyku v elektronickej forme vo formátoch aplikačných programov Microsoft Word, Excel, resp. vo formáte PDF.

2.3 **Požiadavky na rozsah prác – fáza A (časový rozsah max. 3 kalendárne týždne, predpoklad realizácie fázy A v Q1/2020):**

2.3.1 posúdenie implementovaných bezpečnostných riešení v oblastiach:

* autentifikácia používateľov (v oboch pripojených aplikáciách)
* využitie všetkých implementovaných autentifikačných metód
* autentifikácia cez API rozhranie
* riadenie prístupu k funkciám aplikácie a údajom
* správa používateľov
* správa kľúčov, certifikátov a ďalších autentifikačných faktorov
* správa integrovaných aplikácií
* integrácia LaaS do pripojených aplikácií

2.3.2 vykonanie bezpečnostného testovania aplikácie, vrátane jej rozhraní a všetkých komponentov, na ktorých je aplikácia prevádzkovaná:

* testovanie zraniteľností: minimálne v rozsahu OWASP Testing Guide v4, v akom sú príslušné sekcie relevantné pre infraštruktúru a funkcie testovaného systému
* penetračné testovanie: bez pridelených oprávnení aj s pridelenými používateľskými oprávneniami
* testovanie bude vykonané z pohľadu všetkých rolí v aplikácii
* testovanie pokryje všetky funkcie aplikácie
* manuálne overenie všetkých identifikovaných zraniteľností (nielen výstup automatizovaného skenovania)

2.3.3 vypracovanie dokumentácie obsahujúcej (štruktúra a rozsah dokumentácie musí zodpovedať, resp. pokrývať štruktúru odporučenú v OWASP Testing Guide v4) najmä:

* zhodnotenie bezpečnosti aplikácie, vrátane zhodnotenia naplnenia bezpečnostných cieľov
* zhodnotenie úrovne bezpečnosti implementovaných autentifikačných metód
* vyhodnotenie jednotlivých oblastí testovania (na úrovní sekcií OWASP Testing Guide v4) a všetkých ostatných realizovaných testov v súlade s požiadavkami a ponukou na rozsah a spôsob testovania
* popis vykonaných testov a ich výsledkov, vrátane získaných podkladov pre jednotlivé zistenia a časových údajov (kedy test prebiehal)
* zhodnotenie jednotlivých zistení (s použitím škály Critical/High/Medium/Low/Informative, zohľadňujúcej potenciálne dopady zneužitia, potrebné schopností útočníka a pod.)
* konkrétne odporúčania na nápravu

2.3.4 prezentácia výsledkov testovania v priestoroch obstarávateľa

2.4 **Požiadavky na rozsah prác – fáza B (časový rozsah max. 1 kalendárny týždeň):**

2.4.1 preverenie upraveného systému z hľadiska (predtým) identifikovaných nedostatkov

2.4.2 vypracovanie záverečného zhodnotenia bezpečnosti IS, vrátane zhodnotenia naplnenia bezpečnostných cieľov

2.5 **Požiadavky na rozsah prác – voliteľne čerpané konzultačné hodiny (max. 15 hodín):**

2.5.1 poskytnutie požadovaného počtu konzultačných hodín k posúdeniu, návrhu a implementácie bezpečnostných opatrení podľa požiadaviek obstarávateľa

2.6 **Spôsob realizácie:**

2.6.1 Technické detaily testovania – testovacie prostredie, čas, rozsah a spôsob vykonania konkrétnych testov – budú dohodnuté pred alebo počas realizácie projektu.

2.6.2 Uchádzač a verejný obstarávateľ spoločne preveria pripravenosť prostredia na bezpečnostné testovanie, po vzájomnej dohode obvykle týždeň pred začatím fázy A.

2.6.3 Verejný obstarávateľ poskytne úspešnému uchádzačovi:

* používateľskú dokumentáciu ako aj potrebnú technickú dokumentáciu aplikácie (vrátane dokumentácie k REST API rozhraniam)
* U2F tokeny potrebné pri testovaní.

2.6.4 Úspešný uchádzač použije na testovanie s použitím nástrojov potrebných pre výkon bezpečnostného testovania vlastné prenosné počítače.

2.6.5 Úspešný uchádzač vykoná bezpečnostné testovanie v priestoroch verejného obstarávateľa.