Príloha č. 1

Opis predmetu zákazky

1 Predmet zákazky

Názov predmetu zákazky: „**Bezpečnostné testovanie Exchange**“

2 Opis predmetu zákazky

2.1 **Informácie o infraštruktúre obstarávateľa potrebné pre ocenenie prác:**

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

2.1.2 Testovaný systém: Exchange (mailový systém)

2.1.3 Infraštruktúra mailového systému (OS všetkých serverov Windows Server 2016):

* 2 lokality
* 4 x fyzické Exchange 2016 Mailbox servery v jednej Database Availability Groupe (DAG)
* 2 x virtuálne WAP (Web application proxy) servery
* 2 x virtuálne ADFS servery
* Antivírusová a antispamová ochrana: Eset Mail Security for Exchange 7.0 (EMSX) na Exchange serveroch, v cluster móde; správa 1x Eset Security Management Center (ESMC)

2.1.4 Použitie Hybrid Modern Authentication (HMA)

2.1.5 Publikované služby cez WAP a ADFS: Offline Address Book, Outlook MAPI over HTTPS, Exchange Web Services, Autodiscovery

2.1.6 Interný prístup používateľov k mailovému systému z LAN:

* Outlook (Office 365), single-sign on autentifikácia v AD (Active Directory)

2.1.7 Externý prístup používateľov k mailovému systému – PC:

* Outlook prostredníctvom Outlook MAPI/HTTPS služby, dvojfaktorová autentifikácia s využitím certifikátov (SW alebo HW), prípadne s využitím RSA SecurID tokenov alebo metódami podporovanými v HMA

2.1.8 Externý prístup používateľov k mailovému systému – mobilné telefóny:

* aplikácia MobileIron Email+, Exchange ActiveSync riadený cez MDM (Mobile Device Management) riešenie MobileIron
* aplikácia Outlook for Android, v rámci Android Enterprise riadenom MDM MobileIron

2.1.9 Podľa potreby podpisovanie a šifrovanie mailov: S/MIME (s využitím X.509 certifikátov)

2.1.10 Individuálne aj spoločné mailové schránky

2.2 **Cieľ bezpečnostného testovania:**

2.2.1 Cieľom testovania je zhodnotiť ochranu údajov a bezpečnosť poskytovaných IT služieb, posúdiť účinnosť a adekvátnosť bezpečnostných mechanizmov a ich konfigurácie v infraštruktúre obstarávateľa, identifikovať a demonštrovať zraniteľnosti, navrhnúť opatrenia na nápravu zistených nedostatkov.

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

2.3 Požiadavky na rozsah prác **– fáza A (časový rozsah max. 3 týždne):**

2.3.1 Vykonanie bezpečnostného testovania minimálne v rozsahu uvedenom v ďalších bodoch. Rozširovanie rozsahu testovania nad rámec ponuky je možné len po predchádzajúcej dohode s NBS.

2.3.2 Manuálne overenie všetkých identifikovaných zraniteľností (nielen výstup automatizovaného skenovania).

2.3.4 Identifikácia zraniteľností, týkajúcich sa týchto oblastí:

* všeobecné zraniteľnosti mailových systémov
* autentifikácia a autorizácia používateľov pri internom prístupe aj externom prístupe k mailovému systému (preveriť všetky možnosti prístupu, vrátane použitia viacfaktorovej autentifikácie)
* neoprávnený prístup k mailom, kalendáru, úlohám a adresnej knihe (uložených na serveroch alebo zariadeniach)
* neoprávnené odosielania mailov
* účinnosť antivírusovej a antispamovej kontroly
* vzdialený prístup k mailovému systému len z autorizovaných zariadení NBS (notebooky, mobilné telefóny)
* kryptografická ochrana dôvernosti a autentickosti mailov (S/MIME), vrátane automatického overovania platnosti certifikátov
* kryptografická ochrana komunikácie autorizovaných zariadení s mailovým systémom

2.3.5 Penetračný test a bezpečnostný audit konfigurácie vybraných serverov z hľadiska bezpečnosti samotných prvkov aj nimi poskytovaných služieb v rozsahu: 1 x Exchange server, 1 x ADFS, 1 x WAP. Pri realizácii obstarávateľ na požiadanie poskytne konkrétne relevantné konfiguračné parametre.

2.3.6 Vypracovanie dokumentácie obsahujúcej najmä:

* stručný popis použitej metodiky a oblastí testovania, vrátane odkazov na best-practice, bezpečnostné benchmarky alebo odporučenia
* zhodnotenie bezpečnosti všetkých služieb, ktoré sú predmetom testovania
* vyhodnotenie jednotlivých oblastí testovania a všetkých 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 schopnosti 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 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. 30 hodín)**

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

2.6 **Spôsob realizácie testovania:**

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 potrebnú technickú dokumentáciu systému.

2.6.4 Verejný obstarávateľ poskytne pre potreby testovania 1 používateľský počítač, 1 mobilný telefón s OS Android a 1 mobilný telefón s iOS so štandardnými konfiguráciami používanými verejným obstarávateľom. Úspešný uchádzač použije na testovanie s použitím nástrojov potrebných pre výkon bezpečnostného testovania aj vlastné prenosné počítače, prípadne ďalšie zariadenia.

2.6.5 Pre získanie relevantných konfiguračných parametrov v rámci bezpečnostného auditu konfigurácie vybraných HW a SW komponentov poskytne úspešný uchádzač verejnému obstarávateľovi skripty na automatizovaný zber týchto parametrov na začiatku fázy A.

2.6.6 Úspešný uchádzač vykoná bezpečnostné testovanie v priestoroch verejného obstarávateľa.