**Odpoveď na žiadosť záujemcu o vysvetlenie informácií potrebných**

**na vypracovanie ponuky**
V súvislosti s výzvou na predloženie ponuky k zákazke s nízkou hodnotou podľa § 117 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“) na predmet zákazky **Bezpečnostné testovanie Exchange** bola verejnému obstarávateľovi dňa 14.02.2019 doručená žiadosť záujemcu o vysvetlenie informácií potrebných

na vypracovanie ponuky.

Verejný obstarávateľ, v súlade so zákonom o verejnom obstarávaní a s bodom 13.5. výzvy na predloženie ponuky poskytuje nižšie uvedené vysvetlenie všetkým záujemcom.

**Všeobecne k položeným otázkam:**

Časť 2.1 poskytuje bližšie informácie o infraštruktúre, v ktorej sa bezpečnostné testovanie uskutoční. NBS nepožaduje testovanie nových zraniteľností samotných SW komponentov, ktoré sú štandardnými produktami spol. Microsoft (alebo štandardných produktov tretích strán), ako sú Outlook alebo Exchange server. Hlavným cieľom je overiť, že architektúra a realizovaná implementácia a konfigurácia Exchange (v rozsahu popísanom v časti 2.1) poskytujú účinné a adekvátne bezpečnostné mechanizmy pre ochranu dát a poskytovaných služieb. To znamená identifikáciu známych zraniteľností, zraniteľností súvisiacich s nevhodne zvolenou architektúrou, konfiguráciou jednotlivých komponentov, nastavením politík, resp. spôsobom používania týchto komponentov v NBS. V časti 2.1 sú preto uvedené základné informácie, z čoho prostredie Exchange pozostáva.

Zároveň pripomíname, že návrh spôsobu vykonania a rozsahu bezpečnostného testovania je súčasťou ponuky uchádzača.

**Otázka č. 1:**

Otázka k bodu 2.1.4 – Můžete poslat přesnější definici scope testu “Použitie Hybrid Modern Authentication (HMA)”

**Odpoveď na otázku č. 1:**

HMA je použitá pre dvojfaktorovú autentifikáciu používateľov. Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s konfiguráciou a spôsobom používania HMA.

**Otázka č. 2:**

Otázka k bodu 2.1.5 – Zde je myšlen test webových aplikací nebo samostatných API zprostředkovávacích dané funkcionality?

**Odpoveď na otázku č. 2:**

NBS nepožaduje test API ani testovanie štandardných SW komponentov spol. Microsoft. Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s konfiguráciou a spôsobom používania týchto služieb.

**Otázka č. 3:**

Otázka k bodu 2.1.6 – Zde by byl ve scope celý Outlook 365 (webová aplikace) nebo pouze vybrané části, případně jaké?

**Odpoveď na otázku č. 3:**

Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s konfiguráciou a spôsobom používania Outlook 365. NBS nepožaduje identifikáciu zraniteľností samotnej aplikácie.

**Otázka č. 4:**

Оtázka k bodu 2.1.7 – Zde by se jednalo o test Outlooku, jakožto desktopové aplikace? Byl by scope nějakým způsobem omezen?

**Odpoveď na otázku č. 4:**

NBS nepožaduje testovanie samotnej desktopovej aplikácie Outlook. Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s konfiguráciou a spôsobom používania Outlook v prostredí NBS.

**Otázka č. 5:**

Оtázka k bodu 2.1.8 – Je požadován kompletní test uvedených mobilních aplikací, či pouze jejich částí?

**Odpoveď na otázku č. 5:**

NBS nepožaduje testovanie samotných mobilných aplikácií tretích strán. Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s ich konfiguráciou a spôsobom používania v prostredí NBS.

**Otázka č. 6:**

Оtázka k bodu 2.1.9 – Je možné upřesnit scope a cíle testu v rámci toho bodu?

**Odpoveď na otázku č. 6:**

Scope testu zahŕňa identifikáciu zraniteľností súvisiacich s ich konfiguráciou a spôsobom používania S/MIME v prostredí NBS, teda napr. identifikácia zraniteľností vyplývajúcich zo spôsobu ukladania súkromných kľúčov, distribúcie certifikátov verejných kľúčov, konfigurácie mailových klientov a pod.