Opis predmetu zákazky verejného obstarávania pre **projekt NFP311070BLC5** s názvom
„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“.

Analýza informačnej a kybernetickej bezpečnosti prevádzky Informačných Technológii sieťových služieb a systémov Banskobystrického samosprávneho kraja (ďalej BBSK).

Manažérske zhrnutie:

BBSK aktuálne nemá implementované riešenia a opatrenia pre ***zabezpečenie kybernetickej bezpečnosti*** povinné podľa Zákona o kybernetickej bezpečnosti č.69/2018 Z.z. a Zákona o informačných technológiách vo verejnej správe č.95/2019 Z.z. Z externého pohľadu sa zvyšuje frekvencia a závažnosť kybernetických útokov, z interného pohľadu sa zase neustále zvyšuje závislosť na informačných aktívach a IT systémoch. Pribúdajú hrozby, zraniteľnosti a následne aj dopady bezpečnostných incidentov na prevádzku a preto je potrebné zvýšiť kybernetickú bezpečnosť a dostupnosť prevádzkovaných informačných systémov a informačných aktív. BBSK chce preto zaviesť **procesy governance kybernetickej bezpečnosti** a realizovať **analýzu rizík** a to aj s pomocou finančných prostriedkov z dopytovej výzvy ***OPII-2021/7/16-DOP „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“.*** Hlavným výsledkom realizácie projektu bude zavedenie procesov governance IT bezpečnosti a riadenia rizík BBSK. Vedľajším produktom je inventarizácia informačných aktív, analýza rizík a výkonné podklady pre bezpečnostné opatrenia na splnenie požiadaviek podľa zákonov č.69/2018 Z.z. a č.95/2019 Z.z., ako aj vyhlášky NBÚ č.362/2018 Z.z.

Opis predmetu zákazky - zadanie:

Predmetom zákazky v rámci projektu Rozvoja governance a úrovne informačnej a kybernetickej bezpečnosti BBSK je dodanie služby komplexnej Analýzy informačnej a kybernetickej bezpečnosti prevádzky IT sieťových služieb a systémov BBSK (ďalej len *analýza*) a customizácia, programovanie komunikačného interfejsu a implementácia klientskeho modulu CMRKB- MIRRI určeného pre monitorovanie a riadenie bezpečnostných incidentov, t.j. dodanie služieb súvisiacich s plnením projektu č. NFP311070BLC5 podľa výzvy OPII-2021/7/16-DOP, v rozsahu prevedenia komplexnej analýzy a jej výstupov, návrhu dizajnu, implementácie, testovania a nasadenia modulu projektu.

Výstupom služby analýzy dodávateľa bude:

1) **Overenie plnenia bezpečnostných opatrení podľa vyhlášky NBÚ č.362/2018 Z.z, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a plnenie ustanovení zákona**.

2) **Klasifikácia informačných aktív a kategorizácie informačných systémov a sietí podľa vyhlášky NBÚ č.362/2018 Z.z § 4, ktorá bude slúžiť ako podklad v vypracovaniu zoznamu nápravných opatrení.**

3) **Návrh nápravných opatrení v kontexte plnenia povinnosti vyplývajúcich zo zákona č.95/2019 Z.z. o informačných technológiách vo verejnej správe a zákona č.69/2018 Z.z. o kybernetickej bezpečnosti.**

4) **Komplexné ohodnotenie zraniteľností organizácie s transferom znalostí na zamestnancov BBSK. Poskytnutá služba musí obsahovať:**

Ohodnotenie zraniteľností z externého prostredia:

a) Identifikácia informácií zistiteľná prostredníctvom techník OSINT.
b) Automatizovaný test sieťových a webových služieb.
c) Manuálne overenie zistených zraniteľností.
d) Exploitácia zistených zraniteľností.

e) Pre dostupné webové portály aj overenie webových služieb v zmysle metodiky OWASP 4.2.
f) Klasifikáciu zraniteľností a návrh bezpečnostných opatrení.

Ohodnotenie zraniteľností z interného prostredia:

g) Mapovanie aktív.
h) Automatizované overenie zraniteľností v interných infraštruktúrach.
i) Manuálna verifikácia zistených zraniteľností.
j) Overenie možností lateral movement v organizácií.
k) Exploitácia zraniteľností.
l) Klasifikácia zraniteľností a návrh bezpečnostných opatrení.

Výsledkom služby musí byť správa z ohodnotenia zraniteľností, ktorá obsahuje minimálne:

- Použité metodiky.
- Použité nástroje a spôsob ich použitia.
- Podrobný zoznam nájdených bezpečnostných zraniteľností a vektorov útoku pre každú zraniteľnosť.
- Popis zraniteľnosti.
- CVSS maticu a ohodnotenie.
- Dôkaz existencie zraniteľnosti.
- Návrh bezpečnostných opatrení.

5) Komplexné interné posúdenie stavu kybernetickej bezpečnosti na procesnej, organizačnej a technickej úrovni.

a) Analýza bezpečnostnej architektúry organizácie.
   i) Best practices z hľadiska odolnosti voči štandardným kybernetickým útokom.
   ii) Best practices z hľadiska odolnosti voči relevantným kybernetickým útokom.
b) Analýza konfigurácie sieťových prvkov z hľadiska kybernetickej bezpečnosti:
   i) Sieťové firewally,
   ii) Access a Core Switche,
   iii) Edge routery.
c) Analýza konfigurácie bezpečnostných prvkov:
   i) Antimalware,
   ii) Network Behavior Analytics riešenie,
   iii) Intrusion Prevention System.
d) Analýza konfigurácie domény AD:
   i) Súlad s best practices,
   ii) Súlad s CIS lvl 1.
   iii) V rámci služby je potrebné dodať aj implementačné politiky na implementáciu CIS lvl1.
e) Analýza spôsobilostí zachytávania digitálnych stôp v prípade kybernetického útoku.
f) Posúdenie pripravenosti organizácie na kybernetický útok:
   i) Komplexné posúdenie pripravenosti na zvládnutie útoku typu ransomware.
   ii) Posúdenie vykonávaných záloh v prípade ransomware útoku.
   iii) Vypracovanie plánu na riešenie kybernetického útoku typu ransomware.

A. Pod IT sieťovými službami a systémami v tomto dokumente sa posudzujú nasledovné oblasti:

1. Elektronická pošta (email) a súvisiace systémy (ich SW a HW) zabezpečujúce tok emailovej komunikácie v rámci BBSK, ktoré poskytuje úradu, jeho aktívam a zamestnancom bezpečné prostredie na odosielanie a prijímanie e-mailov.
2. WEB služby, hlavne WEB brána (Proxy), ako aj súvisiace systémy (SW a HW), ktoré zabezpečujú bezpečnú komunikáciu koncových užívateľov do Internetu.
3. Autentifikačné služby, slúžiace na autentifikáciu koncových užívateľov alebo systémov pristupujúcich na sieťové služby (Email, proxy, fileserver...), príklad AD/LDAP.
4. Firewall systémy zabezpečujúce bezpečné kontrolované oddelenie pripojenia k internetu, DMZ, interná sieť LAN, prípadne iné siete – v závislosti od topológie siete to môže byť jedna, dve alebo viac sieti a Firewallov.
5. Ochranné sieťové systémy a systémy pre detekciu alebo zabránenie úniku dát (IPS, IDS, DLP...).
6. Ochranné systémy - pre koncové stanice a servery - Antivírus, anti-malvér alebo EDR.
7. LAN a WIFI systémy tvoriace internú alebo hosťovskú sieť a zabezpečujúce kontrolované pripojenia koncových užívateľov k ďalším službám.
8. WAN systémy tvoriace prepojenie na externé lokácie.
9. VPN systémy zabezpečujúce pripojenie koncových užívateľov zvonku do internej siete.
10. Doplnkové sieťové služby ako DHCP, NTP, SYSLOG, SIEM.
11. Softvéry a aplikácie, ktoré akýmkoľvek spôsobom monitorujú, alebo manažujú komponenty horeuvedených služieb a systémov (napríklad LAN manager).
12. Špecializované sieťové sondy alebo analyzéry, ktoré monitorujú komunikáciu (napr. NetFlow, TAP monitor), alebo aktívne zasahujú do komunikácie (napr. IPS, aktívne forenzné systémy, a pod.).

B. Pod súvisiacimi systémami sa rozumejú systémy, ktoré nie sú nevyhnutne neoddeliteľnou súčasťou danej služby, ale ktoré slúžia ako:

1. doplnková služba/systém danej služby/systému (príklad – antispamový filter pre Elektronickú poštu, pokiaľ je umiestnený na inom serveri ako emailový server, alebo je dodávaný formou externej služby - napr. cloud),
2. doplnok, ktorého nefunkčnosť by službu obmedzila, alebo zmenila úroveň jej bezpečnosti (príklad autentifikácia pre emailových klientov, email brána v DMZ perimetri, autentifikačný server druhej úrovne).

C. Technickými krokmi pre realizáciu analýzy informačnej bezpečnosti služieb a systémov budú:

1. Analýza fyzickej bezpečnosti.
2. Analýza hardvérových komponentov – Servery, Dátové úložiská, Pracovné stanice.
3. Analýza softvérových komponentov – Serverové OS, OS pracovných staníc a aplikácie.
4. Analýza riadenia zraniteľností – Audit procesov aktualizácie OS, aplikácií.
5. Analýza komunikačných kanálov - prístupy do sieťových služieb a systémov cez softvér na pracovný staniciach, mobilných zariadeniach, web alebo iné spôsoby pripojenia.
6. Analýza administrátorských ako aj užívateľských účtov sieťových služieb a systémov.
7. Analýza prevádzkových záznamov (log, syslog).
8. Analýza procesov pre obnovenie dát v prípade ich straty.

D. Metodiky zisťovania pre realizáciu analýzy informačnej bezpečnosti sieťových služieb a systémov budú:

1. Fyzicky – návštevou datacentier kde sú sieťové služby a systémy prevádzkované.
2. Pomocou aplikácie pre zisťovanie existencie zariadenia v sieti a v doméne.
3. Analýzou procesov týkajúcich sa prevádzky sieťových služieb a systémov.
4. Auditovaným prístupom na konfiguračné rozhrania sieťových služieb a systémov.
5. Rozhovorom s poverenými zamestnancami objednávateľa – administrátormi sieťových služieb a systémov.
6. Auditovaným prístupom slúžiacim na otestovanie využitia zraniteľností sieťových služieb a systémov.

E. Komplexná správa musí obsahovať výsledky analýz všetkých systémov a podsystémov BBSK z bodov A. a B. Výstupom analýzy informačnej a kybernetickej bezpečnosti prevádzky sieťových služieb a systémov bude aj kontrola plnenia prevádzkovateľa informačných systémov podľa Vyhlášky č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy vo vzťahu k jednotlivým kategóriám informačných aktív predovšetkým z pohľadu:

- organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- personálnej bezpečnosti,
- riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- technických zraniteľností systémov a zariadení,
- riadenia bezpečnosti sietí a informačných systémov,
- riadenia prevádzky,
- riadenia prístupov,
- kryptografických opatrení,
- riešenia kybernetických bezpečnostných incidentov,
- monitorovania, testovania bezpečnosti a bezpečnostných auditov,
- fyzickej bezpečnosti a bezpečnosti prostredia,
- kontinuity prevádzky,

F. **Požadovaná výstupná dokumentácia z projektu**

Výstupná dokumentácia z projektu bude dodaná vo forme dokumentácie MS Word, MS Excel, MS Access a pod, pričom časť údajov bude pripravená vo formáte na prenos údajov do Klientského modulu evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.

Správa musí obsahovať spôsob uskutočnenia analýzy, kroky prevedené na získanie informácií, výstup získaných informácií, zistené riziká a odporúčania na elimináciu rizík.
Tieto výstupy umožnia overiť skutkový stav, či prevádzkovateľ spĺňa povinnosti vyplývajúcich zo zákona č.95/2019 Z.z. o informačných technológiách vo verejnej správe a zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, pričom výstupy analýzy navrhnú nápravné opatrenia.