Opis predmetu zákazky: Implementácia technických opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

V rámci analýzy technických opatrení v súlade so zákonom č.69/2018 Z.z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia analytických výstupov a súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu v priebehu 6 mesiacov:

Názov aktivity: Analýza stavu a príprava pre log management + mapovanie zdrojov
Zadanie:
Analýza stavu správy logov a auditných záznamov. Príprava pre log management a mapovanie zdrojov.
Popis:
Zaznamenávanie a uchovávanie auditných záznamov vytvára údajovú bázu pre aplikovanie požiadaviek na bezpečnostný monitoring.
Pre naplnenie procesných a technologických požiadaviek definovaných legislatívou je nutné realizovať niekoľko na seba nadväzujúcich krokov. V rámci projektu musia byť realizované nasledujúce aktivity:

- Identifikácie relevantných legislatívnych a normatívnych požiadaviek,
- vypracovanie jednotnej politiky zaznamenávania a uchovávania auditných záznamov (logov) týkajúcich sa:
    - prevádzky IS,
    - prvkov infraštruktúry,
    - aktivít príslušných používateľov týchto systémov,
    - aktivít pracovníkov zabezpečujúcich správu a prevádzky týchto systémov (administrátorov interných aj externých),
    - prevádzky pracovných staníc úradu,
- analýza existujúceho stavu logov, ich väzieb a súlad s navrhovanou politikou,
- vypracovanie návrhu na realizáciu úprav rozsahu a obsahu logov,

V rámci politiky zaznamenávania a uchovávania auditných záznamov predpokladáme definovať najmä nasledovné oblasti:

- rozsah systémov a komponentov z ktorých sa musia vytvárať auditné záznamy,
- typy udalostí a činností, ktoré sa majú zaznamenávať do auditných záznamov z jednotlivých systémov a komponentov,
- informácie zaznamenávane z jednotlivých udalostí,
- spôsob uchovávania auditných záznamov,
- spôsob a periodicita sledovania a vyhodnocovania auditných záznamov,
- spôsob zálohovania, archivovania a vymazávania auditných záznamov.
- Pravidlá logovania pre dodávateľov.
- Správa a konsolidácia logov, mapovanie zdrojov z troch lokalít (úrad, Datacentrum, vládny cloud) a do budúcnosti s možných ďalších.

Výstupy:

1. Politika zaznamenávania a uchovávania auditných záznamov.
2. Pravidlá logovania pre dodávateľov IT systémov na úrad.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

V rámci analýzy musí byť zhodnotený súlad aktuálneho stavu s politikou vytárania auditných záznamov. Výstupom analýzy bude prehľad formátov, obsahu a rozsahu logov pre jednotlivé systémy a prvky infraštruktúry. Pre implementáciu úprav budú navrhnuté priority na základe určenia dôležitosti konkrétneho systému, rozsahu a náročnosti úprav.

Názov aktivity: Príprava zadaní a mapovanie zdrojov pre implementáciu SIEM, kontrola kvality
Zadanie:
Identifikácia parametrov pre implementáciu bezpečnostného monitoringu SIEM (Security Information and Event Management)
Popis:
Údajovú bázu pre identifikáciu a vyhodnocovanie bezpečnostných udalostí tvoria prevádzkové logy a auditné záznamy. V tomto zmysle nadväzuje príprava implementácie SIEM riešenia na aktivitu mapujúcu stav spracovania logov a auditných záznamov v rámci ktorej budú zmapované zdroje a vypracovaná politika uchovávania auditných záznamov. Implementácia SIEM nástroja zabezpečí naplnenie požiadaviek na bezpečnostný monitoring prevádzky IT

Návrh implementácie musí byť zameraný na definovanie kvantitatívnych a kvalitatívnych parametrov.
Primárnym kvantitatívnym parametrom pre implementáciu SIEM riešenia je :

- počet spracovaných udalostí za sekundu – EPS (events per second),
- distribúcia zberu dát v závislosti na architektúre prevádzkového prostredia.

Z hľadiska získavania logov pre vyhodnocovanie udalostí v SIEM je nutné predovšetkým definovať:

- zdroj logov a auditných záznamov, mapovanie zdrojov
- spôsob zberu – možnosti integrácie do centralizovaného zberu (syslog, log súboru, event logy),
- spôsob zberu – topológia architektúry prevádzkového prostredia,
- početnosť a objem dát pre definovanú časovú periódu.

Z hľadiska kvalitatívnych parametrov je to predovšetkým:

- požadovaná dostupnosť,
- úroveň zabezpečenia riešenia,
- podporované rozhrania a šablóny pre efektívnu integráciu,
- úroveň automatizácie pri vyhodnocovaní udalostí,
- podporné funkcie pre detekciu a analýzu bezpečnostných incidentov.

Výstupy:

1. Politika prevádzky SIEM.
2. Pravidlá logovania - integrácie do SIEM pre dodávateľov IT systémov na úrad.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

V rámci návrhu sa očakáva identifikácia a vyčíslené parametrov pre implementáciu riešenia. Zároveň sa očakáva návrh referenčnej architektúry pre nasadenie do existujúcej prevádzkovej infraštruktúry.

Názov aktivity: Analytická príprava a technické možnosti na dvojfaktorovú autentifikáciu pre vzdialene prístupy

Zadanie:

Analýza a identifikácia technických parametrov pre zabezpečenie kontroly a riadenia prístupov

Popis:

Pre zabezpečenie požadovanej úrovne integrity a bezpečnosti prístupov je nevyhnutné identifikovať kľúčové procesy správy prístupov a definovať politiky – požiadavky na ich zabezpečenie. Analýza a návrh musí zabezpečiť definovanie prístupových politík a zodpovednosti za procesy ktoré zahŕňajú celý životný cyklus jednotlivých typov prístupových účtov. Pre jednotlivé typy prístupových účtov sa predpokladá aplikovanie odlišnej úrovne zabezpečenia z pohľadu komplexnosti a časovej platnosti hesla.

Špecifikované parametre musia vychádzať z minimálnych požiadaviek definovaných vo všeobecných zásadách pre manažment prístupov IKT a pokryť procesy:

- Inicializácia hesla,
- Notifikácie a upozornenia,
- Exspirácia hesla,
- Revalidácia – prehodnotenie prístupov,
- Použitie generických privilegovaných prístupov.

Zároveň musia špecifikovať požiadavky a parametre technických riešení pre nasadenie:

- Dvojfaktorovej autentifikácie pre vzdialené prístupy
- Správy, riadenia a monitorovania privilegovaných prístupov,
- Segregovania privilegovaných prístup (viac-vrstvový model administrácie serverov a pracovných staníc).

Výstupy:

1. Smernica riadenia prístupov a prideľovania prístupových práv.
2. Zakreslenie procesov v Camunde.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Analýza a implementácia procesov riadenia zraniteľností - vulnerability manažment

Zadanie:

Analýza a návrh procesov riadenia zraniteľností

Popis:

Pre zabezpečenie efektívnej a promptnej reakcie na relevantné bezpečnostné hrozby je nutné v prvom rade definovať:

- vstupy na základe ktorých sa vyhodnocuje miera rizika (bezpečnostné varovania, pravidelné skenovanie, penetračné testovanie),
- proces hodnotenia miery rizika v nadväznosti na klasifikáciu aktív,
- zodpovednosti za spôsob schvaľovania eliminácie rizika.

Definované procesy pre riadenie zraniteľnosti sa predovšetkým musia zamerať na :

- pravidlá a procesy pre bezpečný vývoj a aplikovanie bezpečnostných mechanizmov,
- začlenenie testovania zraniteľnosti do procesu riadenia zmien,
- nasadenie nástroja pre pravidelné skenovanie, hodnotenie a manažment známych zraniteľností.

V rámci návrhu sa očakáva identifikácia a vyčíslené parametrov pre implementáciu riešenia nástroja pre pravidelné skenovanie, hodnotenie a manažment známych zraniteľností.

Výstupy:

1. Smernica hodnotenie zraniteľností a prevencia ich odhaľovania.
2. Zakreslenie procesov v Camunde.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Analytická príprava a možnosti pre mobile device management

Zadanie:

Analýza a identifikácia technických parametrov pre zabezpečenie a správu mobilných zariadení.

Popis:

Efektívna ochrana mobilných zariadení (notebook, smartphone) je kľúčová pri eliminácií hrozieb a bezpečnostných rizík. Súčasťou zabezpečenia mobilných zariadení musí byť správa a ochrana zariadení:

- Správa zariadení musí zabezpečiť zvýšenie efektivity prevádzky a technickej podpory koncových používateľov.
- Ochrana mobilných zariadení pôsobí ako funkčný prvok a prevencia úniku dát a proti prípadným útokom uskutočneným prostredníctvom mobilného zariadenia.

Analýza využitia mobile device managementu musí byť zameraná na spôsob implementácie, využiteľnosť a identifikáciu technických parametrov pre oblasti :

- centralizovaná bezpečná správa, evidencia a konfigurácia mobilných zariadení,
- oddelenie pracovných a súkromných dát, aplikácií (prostredí - kontajnerizácia),
- zabezpečenie vzdialených prístupov z mobilných zariadení k IKT zdrojom,
- zabezpečenie ochrany dát nachádzajúcich sa na mobilných zariadeniach,
- zabezpečenie prípadného bezpečného zmazania mobilného zariadenia na diaľku,
- spracovanie auditných záznamov o činnosti administrátora aj používateľov.

Výstupy:

1. Politika zabezpečenia mobilných zariadení.

2. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Plánovanie kontinuity činností, vypracovanie návrhu Stratégie kontinuity a vytvorenie plánov kontinuity, Havarijné plánovanie, DRP – disaster recovery plány

Zadanie:

Zabezpečenie vypracovania stratégie kontinuity činností a návrhu vzoru plánov kontinuity a obnovy.

Popis:

Cieľom stratégie kontinuity činností je definovať a dokumentovať základný rámec na zaistenie kontinuity činností metódou „Worst Case Scenario“. V rámci stratégie kontinuity činností musia byť navrhnuté možné stratégie obnovy jednotlivých kritických procesov pre zvolené krízové udalosti a vybraná najoptimálnejšia stratégia.

Stratégia kontinuity činností musí vychádzať zo záverov už vypracovanej analýzy dopadov a analýzy rizík.

Stratégia kontinuity činností sa musí sústreďovať najmä na:

- výber alternatívnych metód, ktoré budú použité v prípade narušenia alebo neočakávanej udalosti na zabezpečenie kontinuity kritických procesov v súlade so stanovenou prioritou počas analýzy dopadov,
- zraniteľnosti a kritické prvky zlyhania (single points of failure) v kritických procesoch, ktoré boli identifikované počas analýzy rizík.

Stratégia kontinuity činností musí obsahovať:

- sumarizáciu výstupov z analýzy dopadov a analýzy rizík, vrátane požiadaviek na obnovu,
- definíciu havárie, predpoklady vymedzujúce haváriu,
- definíciu princípov, podľa ktorých budú realizované činnosti v havarijnom stave,
- identifikáciu zdrojov, ktoré budú použité v havarijnom stave,
- popis riadenia aktivít v havarijnom stave.

Stratégia kontinuity činností môže pozostávať z viacerých dokumentov vo viacúrovňovej architektúre (organizačná, procesná, technologická).

Súčasne je potrebné vypracovať vzorové dokumenty pre plánovanie prvotnej reakcie na neočakávanú udalosť, ktorá nastala, ako aj na určenie náhradných postupov pri vzniku neočakávanej udalosti (plánov kontinuity činností), resp. určenie postupov oživenia pri výpadku IKT komponentov (DRP). Tieto dokumenty poskytnú organizácii jednotný rámec pre vypracovávanie plánov.

Výstupy:

1. Návrh procesov a postupov pre Riadenie kontinuity prevádzky – vypracovanie smernice Riadenie kontinuity prevádzky. Zakreslenie procesov v Camunde.
2. Dokument: Analýza funkčných dopadov (BIA), určenie cieľovej doby obnovy a cieľového bodu obnovy
3. Dokument: Stratégia kontinuity činností.
4. Dokument: Vzorové dokumenty pre plánovanie prvotnej reakcie a plánov kontinuity činností
5. Dokumenty DRP pre:

a. Systém registratúry
b. Systémy LS Telcom, CRC Data Radiolab
c. Dochádzkový systém
d. Účtovníctvo a pohľadávky, softvérové riešenia Štátnej pokladnice

Názov aktivity: Integrácia na VISKB
Zadanie:
Integrácia na Vládny informačný systém kybernetickej bezpečnosti (VISKB).