PRÍSTUP K PROJEKTU

(Verzia dokumentu v1.01/07_2021)

Identifikovanie požiadaviek **na technickú časť riešenia**

Identifikácia projektu

Povinná osoba	*Ministerstvo vnútra Slovenskej republiky*
Názov projektu	*Bezpečnostné, monitorovacie a certifikačné centrum - projekt PFA*
Zodpovedná osoba za projekt	*RNDr. Branislav Baláž*
Realizátor projektu	*Ministerstvo vnútra SR, Odbor počítačovej kriminality PPZ, Kriminálno expertízny ústav PPZ*
Vlastník projektu	*RNDr. Branislav Baláž*

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	**Podpis** (alebo elektronický súhlas)
Vypracoval	Branislav Baláž	MVSR	Riaditeľ OB SITB	11.5.2023	
Upravil	Branislav Baláž	MVSR	Riaditeľ OB SITB	14.6.2023	
Upravil	Branislav Baláž	MVSR	Riaditeľ OB SITB	5.7.2023	
Schválil	Igor Sibert	MVSR	GR SITB MVSR	6.7.2023	

OBSAH

1. POPIS ZMIEN DOKUMENTU

1.1 História zmien

Verzia	Dátum	Zmeny	Meno
1a	14.6.2023	Aktualizácia technických popisov	OB SITB
2	5.7.2023	Doplnenie architektúry riešenia	OB SITB

2. ÚČEL DOKUMENTU

*V súlade s **Vyhláškou 85/2020 Z.z. o riadení projektov -** je dokument **Projektový zámer** pre iniciačnú fázu určený na rozpracovanie detailných informácií prípravy projektu Bezpečnostné, monitorovacie a certifikačné centrum - projekt PFA. Ide o projekt „Služby preventívnej a forenznej bezpečnosti" v rámci ktorého budú vytvorené forenzné laboratória pre OČTK na zaisťovanie stôp kybernetických trestných činov a pre potreby policajnej spravodajskej činnosti v rámci odhaľovania páchateľov týchto trestných činov.*

2.1 Konvencie používané v dokumentoch – označovanie požiadaviek

Požiadavky koncových používateľov

číslo požiadavky	Požiadavky užívateľov
1	Forenzné získavanie, extrakcia digitálnych dôkazov uložených v mobilných zariadeniach.
2	Prekonanie zabezpečenia mobilných telefónov s operačným systémom iOS: iPhone X iPhone XR, XS, XS Max iPhone 11, 11 Pro, 11 Pro Max iPhone 12, 12 Pro, 12 Pro Max
3	Vykonanie extrakcie na úrovni súborového systému z mobilných telefónov s operačným systémom iOS: iPhone X iPhone XR, XS, XS Max iPhone 11, 11 Pro, 11 Pro Max iPhone 12, 12 Pro, 12 Pro Max
4	nájsť a identifikovať viac než stovky artefaktov z rôznych počítačov, mobilných telefónov a tabletov a prehľadne ich usporiadať do jedného konkrétneho prípadu
5	možnosť skúmania min 750 typov artefaktov vo operačných systémoch Windows, MAC, iOSa Android, alebo ich ekvivalentov
6	dešifrovanie hesiel a diskov
7	možnosť vytvoriť si vlastné definície artefaktov, podpora PhotoDNA a jej ekvivalentov, integrovaný dešifrovací modul
8	modul na automat. rozpoznávanie obsahu chatovej komunikácie, analýza a obnova viac ako 1000 artefaktov, možnosť vytvárania a zdieľania prenosných prípadov, ktoré obsahujú databázu nájdených artefaktov
9	Forenzné získavanie, lokalizácia, extrakcia a analýza digitálnych dôkazov uložených vo vnútri počítačov. Umožňuje vyhľadávať v ťažko dostupných, poškodených, vymazaných, skrytých a šifrovaných informáciách. Založený na winhexovom hexadecimálnom a diskovom editore
10	detekcia čiernobielych alebo šedých obrázkov, farby kože osôb na obrázku, PDF OCR súborov, zašifrovaných súborov, chránených oblastí
11	rozhranie pre PhotoDNA a jej ekvivalentov, automatická detekcia pornografického materiálu vo fotkách
12	automatické sfarbenie pozadia buniek založené na podmienkach definovaných používateľom, integrovaný prehliadač súborov, ktorý podporuje min. 270 súborových typov
13	možnosť vytvorenia grafických náhľadov z videosúborov v užívateľom definovanom časovom intervale
14	podpora pre súborové systémy FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF
15	Forenzné získavanie, lokalizácia, dešifrovanie, lámanie hesiel, extrakcia a analýza digitálnych dôkazov uložených vo vnútri mobilných zariadení
16	Prelomenie ochrany najnovších zariadení s operačným systémom iOS a high-endových Android zariadení
17	virtuálny analyzátor, ktorý umožňuje zobraziť androidové aplikácie v ich natívnej forme
18	Podpora cloud analýzy dát,
19	Bruteforce prelamovanie hesiel použitím akcelerácie čipom grafickej karty (GPU)

20	Podpora tvorby sociálneho grafu a zobrazenie interakcie viacerých zariadení v sociálnom grafe a diagrame
21	Manažment riešených prípadov
22	Ukladanie, porovnávanie a zaraďovanie-indexovanie získaných stôp a informácií
23	Automatizovanú koreláciu informácií na základe vybraných atribútov s rozširovateľnou dátovou schémou a korelačnými pravidlami na základe meta-informácií a získaných stôp
24	Automatizované úložisko na ukladanie dát dostupných na darkwebe, clearwebe a v špecializovaných zdrojoch
25	Obohacovanie skúmania o informácie zistené pri predchádzajúcich prípadoch
26	Databáza udalostí
27	Databáza škodlivého kódu uložená bezpečným spôsobom obohatená o výsledky analýz
28	Vedomostná base pre analytikov, forenzných špecialistov a tretie strany.

3. POPIS NAVRHOVANÉHO RIEŠENIA

MODUL PFA
Služby preventívnej a forenznej bezpečnosti

Služby preventívnej a forenznej bezpečnosti budú poskytované jednotlivými pracoviskami, vybavenými zodpovedajúcimi technológiami a poskytujúce tieto služby podľa potreby a na základe požiadaviek.

Tieto služby sú čiastočne využívané ako vnútorný zdroj pre monitorovaciu časť BMCC.

Jednotlivé pracoviská budú vybavené nástrojmi, ktoré umožňujú danú činnosť vykonávať. Jedná sa o softwarové a hardwarové nástroje, ktoré sú pre danú činnosť nosné, ale je ich treba považovať za nevyhnutné vybavenie. V čase implementácie a aj v priebehu práce sa tieto nástroje musia a budú doplňovať ďalšími nástrojmi podľa toho, aký charakter, prípadne aj rozsah daná činnosť bude mať.

Pracoviská preventívnej a forenznej bezpečnosti sú určené pre OPK – odbor počítačovej kriminality, KEU-kriminalisticky a expertízny ústav, OB-SITB – Odbor bezpečnosti MV SR.

Pracovisko analýz hrozieb

Pracovisko analýz hrozieb a rizík bude slúžiť ako centrálny bod analýzy a vyhodnocovania bezpečnostne relevantných informácií a hrozieb v nasledujúcich 3 základných oblastiach:

Taktická threat intelligence

Základné technické informácie ako napríklad IOC so zameraním na proaktívne vyhľadávanie a obranu pred útočníkmi.

Operačná threat intelligence

Detailné informácie o útočníkoch zamerané napríklad na nimi použité nástroje, techniky, postupy, motiváciu, schopnosti a podobne.

Strategická threat intelligence

Bezpečnostne relevantné informácie ako sú riziká a dopady spojené s hrozbami pre potreby riadenia stratégie subjektu vo vzťahu na kybernetickú bezpečnosť, ako je napríklad financovanie a podobne.

Pracovisko forenzných analýz

V spolupráci so službami Pracoviska analýzy malware bude Pracovisko forenzných analýz poskytovať služby zamerané na detailné porozumenie schopností a zámerov artefaktov, mechanizmov ich doručovania, šírenia, odhalenia, ohraničenie dopadu a neutralizácie útokov.

Všetky forenzné dôkazy musia byť získavané a analyzované bez akýchkoľvek úprav a po nutnú dobu uchovávané v izolácii. Vzhľadom na to, že niektoré forenzné dôkazy môžu byť použité v rámci trestného konania je potrebné dbať na osobitné nariadenia alebo požiadavky.

Získavanie dôkazov plní v procese forenznej analýzy primárnu a nenahraditeľnú úlohu. Z globálneho pohľadu na proces forenznej analýzy, predstavuje dostatočné a správne zabezpečenie dôkazov elementárny funkčný krok, od ktorého závisia všetky následné kroky procesu.

Pri akvizícii forenzných dôkazov v mnohých prípadoch dochádza k situáciám, kedy nie je možné extrahovať dôkazy „štandardným" spôsobom. Takýmito situáciami je napríklad extrakcia dôkazov zo zariadenia, ktoré má prístup chránený autentifikačnými údajmi, alebo sa jedná o poškodené zariadenie, resp. o zariadenie, kde nie je z rozličných príčin možná logická extrakcia dôkazov. Pre možnosť extrakcie forenzných dôkazov musí v takýchto prípadoch forenzný analytik disponovať špecializovaným hardvérovým a softvérovým vybavením.

Fyzická extrakcia dôkazov prostredníctvom komunikačného portu alebo proprietárneho vstupu je založená na predpokladoch, že výrobca zariadenia umožnil, resp. využíva takúto komunikáciu a forenzný analytik správne interpretuje použitý protokol a využije túto komunikáciu. Zväčša je takáto komunikácia povolená či už priamo cez štandardný dátový kábel, resp. rozhranie,
alebo cez špecializované dátové káble a rozhrania.

Pracovisko analýzy malware

Pracovisko analýzy malware bude predstavovať základné fyzické a logické rozhranie pre riadenú interakciu so škodlivým kódom.

Analýza malware je neoddeliteľnou súčasťou procesu riešenia incidentov, v ktorých úlohu zohráva škodlivý kód a teda softvérové i hardvérové vybavenie pracoviska analýzy malware musí podporovať vykonávanie statickej, dynamickej a behaviorálnej analýzy identifikovaných škodlivých kódov.

Oblasti pôsobenia „Laboratória analýzy malware" možno na základe realizovaných stretnutí rozdeliť do dvoch nasledujúcich základných kategórií:

Digital Forensics and Incident Response (DFIR)

Z pohľadu DFIR bude Pracovisko analýzy malware zabezpečovať podporu forenznej analýzy v procese riešenia kybernetických bezpečnostných incidentov s cieľom rýchlej reakcie (takmer v reálnom čase) na bezprostrednú hrozbu s výstupom základných IOC/IOA („Taktická Threat Intelligence").

Forenzná analýza malware

Z pohľadu analýzy malware bude Pracovisko analýzy malware zabezpečovať podrobnejšiu (hĺbkovejšiu) analýzu malware a iných potenciálne nebezpečných zdrojových kódov.

Pracovisko penetračného testovania

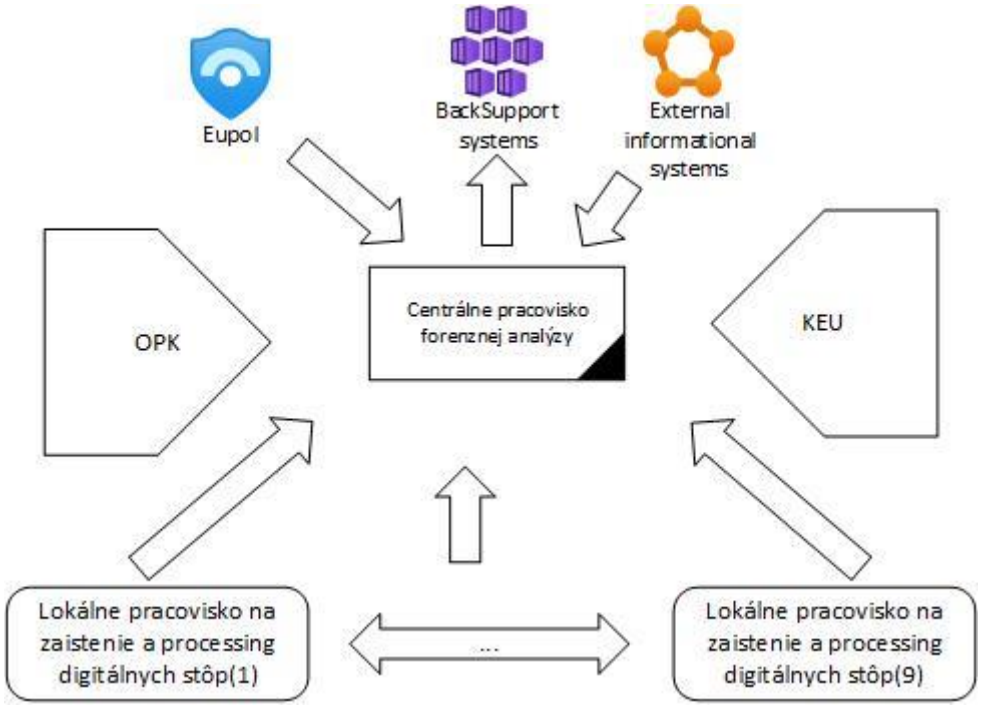
Toto pracovisko bude poskytovať služby interných aj externých penetračných testov.

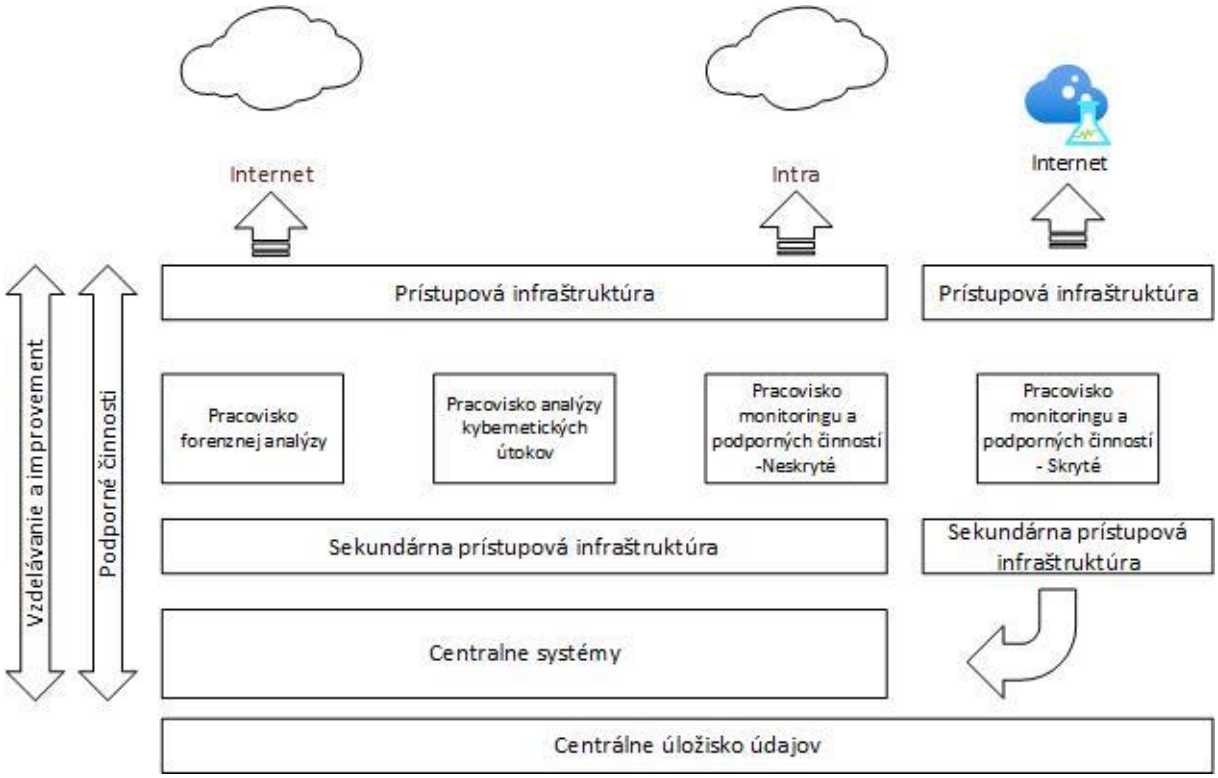
Pre zabezpečenie plnenia úloh služieb bude pracovisko vybavené systémami:

- Systém pre riadenie zraniteľností a rizík, umožňujúci určovať zraniteľnosti aktív (v operačných systémoch, aplikáciách i sieťových zariadeniach.
- Exploatáciu zraniteľností na cieľovom systéme. Primárnu výhodu predstavuje modularita a možnosť vytvárať kampane zamerané na využitie metód sociálneho inžinierstva.
- softvérový nástroj určený pre penetračné testy webových aplikácií.
- Nástroj určený na testovanie a emuláciu API rozhraní viacerých typov
- Nástroj pre testovanie útokov na WiFi siete.
- Systém pre simuláciu hrozieb a bezpečnostného testovania.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

4.1 Biznis vrstva





Obrázok č.2 Model biznis architektúry – príklad

4.2 Aplikačná vrstva

Nezverejňuje sa

4.2.1 Rozsah informačných systémov

Nezverejňuje sa

4.2.2 Využívanie nadrezortných centrálnych blokov a podporných spoločných blokov (SaaS)

Nezverejňuje sa

4.2.3 Prehľad plánovaného využívania podporných spoločných blokov (SaaS)

Nezverejňuje sa

4.2.4 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky – spoločné moduly

Integrácia nebude realizovaná

4.2.5 Prehľad plánovaných integrácií ISVS na nadrezortné centrálne bloky - modul procesnej integrácie a integrácie údajov (IS CSRÚ)

Integrácia nebude realizovaná

4.2.6 Poskytovanie údajov z ISVS do IS CSRÚ

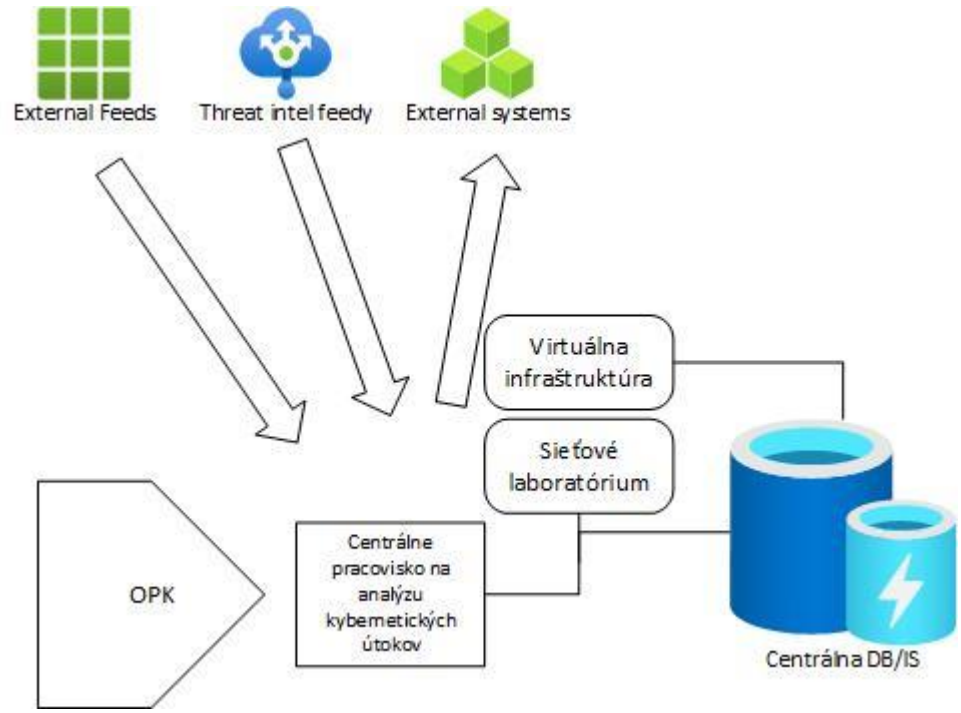
Údaje sa nebudú poskytovať do IS CSRU

4.2.7 Konzumovanie údajov z IS CSRU

Údaje z IS CSRU sa nebudú konzumovať.

4.3 Dátova vrstva

Centrálne pracovisko na analýzu kybernetických útokov a vytváranie vyšetrovacích plánov



4.3.1 Údaje v správe organizácie

Všetky údaje budú v správe MV SR . Všetky údaje budú v režime utajovaných skutočností .

4.3.2 Dátový rozsah projektu

Nezverejňuje sa

4.4 Referenčné údaje

V národnej koncepcii informatizácie verejnej správy bol zadefinovaný princíp „jedenkrát a dosť", ku ktorému boli ďalej detailnejšie rozpracované úlohy v dokumente Strategická priorita Manažment údajov. Cieľom je dosiahnutie stavu, kedy orgány verejnej moci pri poskytovaní svojich služieb odstránia povinnosti občanov alebo podnikateľských subjektov predkladať údaje vo forme rôznych výpisov, odpisov, potvrdení, atď., ktorými už disponuje verejná správa v rámci svojich registrov.
Projekt nepočíta s povinnosťou občanov alebo podnikateľských subjektov predkladať údaje vo forme rôznych výpisov, odpisov, potvrdení, atď

4.4.1 Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné

Projekt nepočíta s vytváraním ani využívaním referenčných údajov.

4.5 Otvorené údaje

Neaplikuje sa

4.6 Analytické údaje

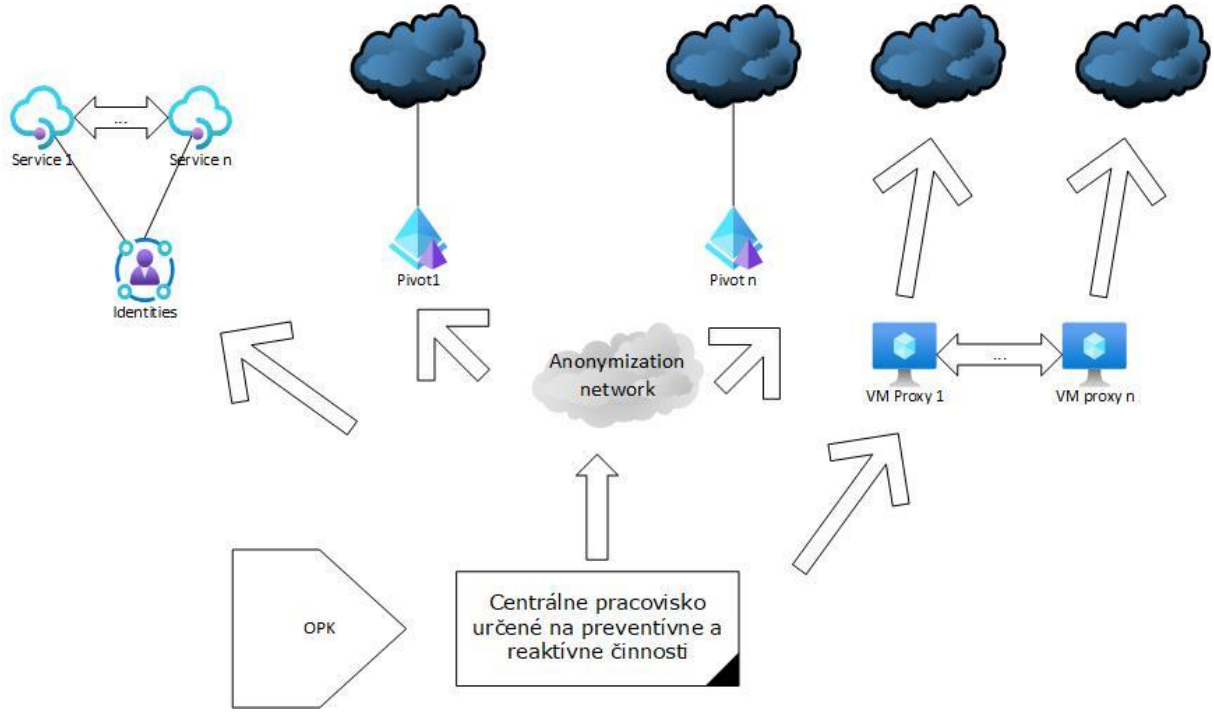
Nezverejňuje sa

4.7 Moje údaje

Neaplikuje sa

4.8 Technologická vrstva

4.8.1 Prehľad technologického stavu



4.9 Bezpečnostná architektúra

Nezverejňuje sa

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Nepočíta sa so žiadnou závislosťou na iných ISVS

6. ZDROJOVÉ KÓDY

Nezverejňuje sa

7. PREVÁDZKA A ÚDRŽBA

7.1 Prevádzkové požiadavky

- *PFA bude prevádzkovaný 7 x 24 x 365*

7.1.1 Úrovne podpory používateľov:

BMCC PFA bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- ***L1 podpory*** *(Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod*
- ***L2 podpory*** *(Level 2, postúpenie požiadaviek od L1) - vybraná skupina analytikov so znalosťou KB*
- ***L3 podpory*** *(Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore (zabezpečuje dodávateľ systému)*

Definícia:

- ***Podpora L1 (podpora 1. stupňa)*** *- začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy, overovanie nastavení SW a HW atď.*

- ***Podpora L2 (podpora 2. stupňa)*** *– riešiteľské tímy s hlbšou technologickou znalosťou oblasti KB. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.*

- ***Podpora L3 (podpora 3. stupňa)*** *- Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobťažnejších Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.*

7.2 Požadovaná dostupnosť IS:

Popis	***Parameter***	***Poznámka***
Prevádzkové hodiny	24x7	nepretržite
Servisné okno	Do 12 hodín	Podľa prevádzkových požiadaviek
Dostupnosť produkčného prostredia IS	99,5	Produkčné prostredie pre modul PFA

- ***99,5% dostupnosť*** *znamená výpadok 1,83 dňa ročne.*

8. POŽIADAVKY NA PERSONÁL

Nezverejňuje sa

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

- Fáza I. – Analýza a dizajn:
  - konzultačné a analytické práce,
  - identifikácia možností realizácie, potrebných zdrojov a riešení,
  - identifikácia a analýza rolí, procesov a integrácií,
  - funkčná a nefunkčná špecifikácia celého riešenia,
  - definícia všetkých bezpečnostných a špecializovaných produktov spolu s akceptačnými kritériami,
- Fáza II. – Nákup HW, SW a ostatných technických prostriedkov:
  - nákup hardvéru a softvéru pre systém BMCC PFA,
  - nákup hardvéru a softvéru pre zabezpečenie ochrany dát, dátových prenosov a komunikácie a ochrany proti pokročilým a externým hrozbám na úrovni sieťovej komunikácie, monitoringu incidentov, rozšírenú detekciu a odozvu na vniknuté incidenty korelujúcu naprieč komunikačnými vrstvami celkovej IKT infraštruktúry,
- Fáza III. – Implementácia:
  - zavedenie a konfigurácia modulov systému PFA,,
  - inštalácia technického vybavenia centra PFA,
  - inštalácia technického vybavenia pre zabezpečenie ochrany dát, dátových prenosov a komunikácie a ochrany proti pokročilým a externým hrozbám na úrovni sieťovej komunikácie, monitoringu incidentov, rozšírenú detekciu a odozvu na vniknuté incidenty korelujúcu naprieč komunikačnými vrstvami celkovej IKT infraštruktúry,
  - obvyklé testovanie a ladenie riešení popri ich implementácii,
- Fáza IV. – Testovanie:
  - testovanie funkcionality riešenia,
  - testovanie zraniteľností,
  - testovanie pilotnej prevádzky,
  - akceptačné testovanie,
- Fáza V. – Nasadenie:
  - nasadenie riešenia do produkčného prostredia,
  - prechod na plnú prevádzku.
- Podporná aktivita – Riadenie projektu:

10. PRÍLOHY

- *Projektový tím – Utajovaný zoznam osôb*
- *Konkrétne pracovné náplne členov projektového tímu – Utajované*
- *Štúdia uskutočniteľnosti – Utajované stupeň „Dôverné"*
- *Tabuľka rizík a závislostí P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI_BMCC_PFA*

Koniec dokumentu