**Výsledky projektu a cieľový stav (manažérske produkty) a katalóg požiadaviek**

**Čiastková aktivita a) Organizácia KB,**

Na základe zistených nedostatkov v oblasti riadenia kybernetickej a informačnej bezpečnosti v organizácii sa určuje nasledovný cieľový stav:

Komplexná bezpečnostná dokumentácia bude novo vypracovaná, pričom zohľadňuje predchádzajúcu dokumentáciu a jej aktualizácie vrátane rozsahu a metód dodržiavania všeobecných bezpečnostných opatrení.

Budú novo sa vyvinuté a implementované špecifické interné riadiace akty pre vybrané oblasti kybernetickej a informačnej bezpečnosti.

Bude aktualizovaný stav bezpečnostného výboru organizácie.

Bude vypracovaný bezpečnostný projekt komplexnej ochrany informačného systému verejnej správy.

**Čiastková činnosť b) Riadenie rizík KB,**

Na základe zistených nedostatkov v oblasti riadenia rizík kybernetickej a informačnej bezpečnosti v organizácii sa určuje nasledovný cieľový stav:

Všetky aktíva súvisiace so spracovaním informácií a centrálnym inventárnym záznamovým zariadením budú identifikované ich hodnotou a s označením ich vlastníka, ktorý definuje ich požiadavky na dôvernosť, dostupnosť a integritu (EAM).

Riadenie rizík bude automatizované pomocou nástroja, pozostávajúce z identifikácie zraniteľnosti, identifikácie hrozieb, identifikácie rizík a analýzy rizík s ohľadom na aktíva, určenia vlastníka rizika a implementácie organizačných a technických bezpečnostných opatrení, funkčnej analýzy dopadov a pravidelného prehodnocovania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení.

Bude implementovaný automatizovaný systém správy a registrácie pre inventarizáciu majetku (EAM/).

Bude implementovaný automatizovaný systém riadenia a registrácie pre katalogizáciu hrozieb.

Bude zavedený sa automatizovaný systém riadenia a registrácie pre katalogizáciu rizík a opatrení.

**Čiastková činnosť c) Personálna bezpečnosť,**

Na základe zistených nedostatkov v oblasti personálnej bezpečnosti v organizácii je stanovený nasledovný cieľový stav:

Bude vyvinutý postup na priradenie osoby k jednej z rolí zabezpečenia

Bude zavedený plán na rozvoj bezpečnostného povedomia a vzdelávania

Bude vyvinutá metóda hodnotenia účinnosti rozvojového plánu bezpečnostného povedomia

Budú určené pravidlá a postupy pri riešení porušení bezpečnostnej politiky

Budú zavedené postupy na ukončenie pracovného pomeru

Budú zavedené postupy pre prípady porušenia bezpečnostných politík

Bude vypracovaný a aktualizovaný akt vnútorného riadenia s bezpečnostnými zásadami pre koncových používateľov

Postupy a procesy, ktorými sa riadi personálna bezpečnosť organizácie, budú vypracované a implementované prostredníctvom interného riadiaceho aktu.

Bude vyhotovený automatizovaný systém riadenia a evidencie pre prácu s organizačnou štruktúrou je implementovaný s prepojením na technické získavanie existujúcich informácií z dostupných technických zdrojov – najmä MS AD.

**Čiastková aktivita k) Zaznamenávanie udalostí a monitoring sietí a IS,**

Na základe zistených nedostatkov v oblasti zaznamenávania a monitorovania udalostí je stanovený nasledovný cieľový stav:

Implementovaný bude centrálny log management systém pre zber a ukladanie logov z jednotlivých informačných systémov s podporou napojenia na riadiace systémy a poskytovania potrebných podporných dát.

Bude vypracovaná dokumentácia metód monitorovania a fungovania systému správy log a centrálneho nástroja na monitorovanie bezpečnosti a bude definovaný spôsob evidencie prevádzkových záznamov, ich vyhodnocovanie, spôsoby hlásenia podozrivej činnosti, zodpovedné osoby a ďalšie povinnosti.

Vytvorí sa špecifikácia všetkých udalostí, ktoré sa musia zaznamenávať, a súvisiaca konfigurácia prvkov informačných technológií verejnej správy vrátane dokumentácie rozsahu údajov zaznamenaných v protokolových súboroch.

Bude vypracovaný sa vnútorný zákon o riadení, ktorý obsahuje a upravuje povinnosti stanovené platnou legislatívou.

Zdôvodnenie nevyhnutnosti aktivít projektu:

Vo štvrtom štvrťroku 2024 nadobudne účinnosť nová legislatívna úprava premietajúca smernicu EÚ NIS2.

Nová povinnosť riadiť riziká dopadne na oveľa širší okruh subjektov, než tomu bolo doteraz. Pre tieto subjekty je určený systém zberu a riadenia logov s online vyhodnocovaním a napojením na systém riadenia rizík. Tým sa zabezpečí neustály prehľad o možných hrozbách, ich včasná identifikácia a zhodnotenie, ako aj návrh riešení pri riadení rizík. Toto riešenie popisuje možnosti pre vybudovanie centrálnej platformy, ktorá bude v prvej fáze zameraná na zber logov pomocou sofistikovaného nástroja, ich parsovanie a vyhodnocovanie na základe jednotlivých scenárov podľa nariadenia NIS2, aby sa zabezpečil bezpečný chod a včasná detekcia hrozieb všetkých organizácií. Systém bude obsahovať aj samotné riadenie aktív a rizík, aby detekované problémy boli automaticky zachytené v samostatnom systéme, kde prebehne ich vyhodnotenie. Riešenie bude realizované na výkonnom serveri tzv. „ALL in one box“. Dôležitou časťou inštalácie je konfigurácia technických aktív, aby zasielali relevantné záznamy.

Jednotlivé organizačné jednotky (OZ), teda regionálne úrady verejného zdravotníctva (ktorých je 36) využívajú centrálny informačný systém (IS ÚVZ), tzn. že každá OZ, ak sa stane terčom kybernetického útoku, ohrozuje fungovanie IS ÚVZ ako celku a môže spôsobiť odstavenie celého systému. V dúsledku toho je nevyhnutné, aby navrhovaným systémov disponovalo nie len ÚVZ, ale aj všetky RÚVZ.

Zasielané udalosti sú v jednotlivých organizáciách na vstupe prijaté, označkované a parsované podľa technológie. Následne sú buď vhodnými základnými pravidlami produktu a implementačnými pravidlami na mieru spracované, aby bolo možné s nimi vytvárať potrebné navrhnuté scenáre. Ďalej sú uložené a vizualizované buď prostredníctvom základných nástrojov, alebo v budúcnosti vyššou formou pomocou integračnej platformy. Implementácia zahŕňa vytvorenie prístupových oprávnení v súlade s požiadavkami na viditeľnosť a spracovanie dát a následnú vizualizáciu.

Prevádzkové informácie budú zobrazovať aktuálne informácie o stave logovaných ICT systémov jednotlivých organizácií. Nad týmito logmi bude vykonané parsovanie a následne sa uložia do centrálneho dátového skladu, kde bude možné s týmito dátami ďalej pracovať. Primárne sa jedná o nepretržitý zber logov a monitorovanie prevádzky ICT technológií, systémov, aplikácií, stavu kybernetického a fyzického zabezpečenia a poskytovanie dát a informácií pre riešenie odchýlok a nápravných opatrení. Všetky údaje uložené v dátovom sklade budú podrobené procesu sledovania a vyhodnocovania podľa nižšie uvedených scenárov. Tým bude zabezpečené sledovanie jednotlivých systémov podľa nariadenia NIS2. Jednotlivé zistenia budú automaticky evidované v systéme na riadenie bezpečnosti, ktorý riadi všetky zistené riziká a navrhuje vhodné opatrenia. Takto evidované a riadené sledovanie logov povedie k včasnej detekcii rizík a ich okamžitej náprave.

Z pohľadu kompletného zberu logov bude vyhodnocované:

- prihlasovanie a odhlasovanie ku všetkým účtom, vrátane neúspešných pokusov

- vykonanie a neúspešný pokus o vykonanie privilegovanej činnosti

- manipulácia a neúspešný pokus o manipuláciu s účtami, oprávneniami a právami

- neuskutočnenie činností v dôsledku nedostatku prístupových práv alebo oprávnení

- začatie a ukončenie činností technických aktív

- kritické a chybové hlásenia technických aktív

- prístup a neúspešný pokus o prístup k záznamom udalostí

- manipulácia a neúspešný pokus o manipuláciu so záznamami udalostí

- zmenu a neúspešný pokus o zmenu nastavení nástrojov na zaznamenávanie udalostí

- ďalšie činnosti používateľov, ktoré môžu mať vplyv na bezpečnosť regulovanej služby.

**Čiastková činnosť o) Audítorská a kontrolná činnosť**

Na základe zistených nedostatkov v oblasti audítorských a kontrolných činností sa stanovuje nasledovný cieľový stav:

Bude vypracovaný program hodnotenia bezpečnosti pre definované informačné technológie verejnej správy, hodnotenie zraniteľnosti a penetračné testy.

Bude realizovaný audit kybernetickej bezpečnosti, ktorý sa vykonáva v súlade so zákonom o kybernetickej bezpečnosti a smernicou NIS2.

Budú vykonávané pravidelné externé testy zraniteľnosti, penetračné testy v nevyhnutnom rozsahu.

Automatizované nástroje budú implementované a používané na technickú podporu riadenia bezpečnosti a audítorských činností.

Podporné nástroje pre správu budú naplnené údajmi o existencii a stave technických a aplikačných aktív automatizovaným a technickým spôsobom.

Základ pre audítorské a kontrolné činnosti bude vytvorený technicky na základe skutočného prevádzkového stavu majetku s prípustným oneskorením do 10 minút.

Dokumenty pre audítorské a kontrolné činnosti budú vždy obsahovať technické diferenčné správy s presným vyznačením zmien vstupov z predchádzajúceho obdobia.

Podporné nástroje pre správu minimalizujú ľudské chyby a maximálne využívajú napojenie existujúcich informácií o aktívach a používateľoch na technické zdroje – najmä MS Active Directory, API prístup do systému Log Management a importy výstupov zraniteľnosti.

**Súčasne žiadateľ deklaruje že v rámci navrhovaného projektu realizuje nasledovné povinné aktivity:**

- vytvára stratégiu kybernetickej bezpečnosti,

- vytvára bezpečnostné politiky kybernetickej bezpečnosti,

- vykoná inventarizáciu aktív, klasifikáciu informácií a kategorizáciu sietí a informačných systémov,

- bude realizovať analýzu rizík a analýzu dopadov spolu, vrátane riadenia rizík.

**Všetky ostatné informácie definované v Tabuľka č.1a - Zoznam povinných kapitol sú uvedené v rámci ŽoNFP v časti 7.**