Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.4 | cyber_projekty@mirri.gov.sk | júl 2023

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Usmernenie k výzvam Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti

Projekty v rámci dopytových výziev „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore verejnej správy“ a „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v zdravotníckych zariadeniach“ sú financované z Operačného programu Integrovaná infraštruktúra. V rámci projektov je potrebné dodržať merateľné ukazovatele definované v tomto Operačnom programe. Konkrétne ide o merateľné ukazovatele pre Prioritnú os 7, resp. Špecifický cieľ 7.9: „Zvýšenie kybernetickej bezpečnosti v spoločnosti“.

Vzhľadom na skutočnosť, že tieto merateľné ukazovatele OPII (zadefinované v minulosti) nie je možné naplniť len „analytickými“ projektami, ktoré napr. realizujú len počiatočné a nutné kroky riadenia informačnej a kybernetickej bezpečnosti, ako sú napr. inventarizácia aktív, ich klasifikácia, kategorizácia IS a najmä analýza rizík a analýza dopadov (AR/BIA), bolo zo strany SKB MIRRI SR navrhnuté odporúčanie (ako jedno z možných riešení), využiť pripravovaný klientsky modul vládneho informačného systému kybernetickej bezpečnosti (ďalej len „VISKB“), ktorým je možné naplniť merateľný ukazovateľ P0193 „Počet nasadených nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov“.

Vývoj VISKB beží paralelne a v podstate nezávisle od vyššie uvedených projektov dopytovej výzvy. Je primárne určený pre vládnu jednotku CSIRT.SK, ktorá prostredníctvom tohto systému potrebuje zbierať rôzne informácie od jednotlivých OVM pre efektívnejšie a adresnejšie riadenie informačnej a kybernetickej bezpečnosti a najmä riadenie kybernetických incidentov v podsektore verejnej správy. Nakoľko má tento projekt na záver dodať aj klientsky modul, ktorý prepája spomínané projektové aktivity a napĺňa uvedený merateľný ukazovateľ, odporúčali sme využiť tento klientsky modul pre projekty uvedenej dopytovej výzvy. V konečnom dôsledku budú OVM tento modul v budúcnosti využívať bez ohľadu na to, či realizujú projekt z uvedenej výzvy alebo nie.

Za týmto účelom bol dodávateľ VISKB požiadaný o prednostný vývoj off-line klientskeho modulu VISKB, ktorý by bolo možné použiť aj v projektoch dopytovej výzvy. Pre projekty, ktoré končia v priebehu roka 2023 bola už začiatkom tohto roku uvoľnená „beta“ verzia modulu, ktorá je práve v týchto dňoch nahradzovaná finálnou verziou. Už na základe uvoľnenej „beta“ verzie, ktorá nemala plnú funkčnosť z pohľadu cieľov projektu VISKB, bolo možné túto verziu použiť na ukončenie projektov z dopytovej výzvy, nakoľko už aj táto verzia obsahovala funkčný model evidencie a riadenia bezpečnostných incidentov, čo postačuje na deklarovanie naplnenia merateľného ukazovateľa P0193.

Ako uvádzame vyššie, vývoj klientskeho modulu je zabezpečený v rámci samostatného projektu VISKB na MIRRI SR, takže od OVM sa v súvislosti s týmto modulom nepožaduje (a ani to zo strany OVM nie je možné) realizovať prakticky žiadne aktivity v rámci realizačnej fázy, ako sú napr. analýza a dizajn, implementácia a testovanie, post-implementačná podpora a podobne. Rovnako sa nepredpokladá a neočakáva žiadna integrácia na žiadne IS OVM.

Z pohľadu OVM ide len o využitie licencie na použitie tohto produktu, t. j. jeho inštalácie v prostredí OVM a následne používanie v súlade s licenčnými podmienkami. V rámci projektov z dopytovej výzvy je potrebné vo fáze nasadenia tento modul nainštalovať v súlade s používateľskou príručkou a prakticky len otestovať úspešnosť tejto inštalácie a základnej konfigurácie modulu. Žiadne iné testovanie (bezpečnostné, funkčné, záťažové a pod.) sa od OVM nevyžaduje, nakoľko je testovanie zabezpečené samotným projektom VISKB na MIRRI SR.

Aj vzhľadom na vyššie uvedené je zrejmé, že OVM rovnako nemusia (nie je na to dôvod),

v súvislosti s týmto modulom, vypracúvať žiadne príručky ani inú dokumentáciu.

Pre úspešnú implementáciu (zúženú len na inštaláciu a základnú konfiguráciu) klientskeho modulu je potrebné si stiahnuť distribuovaný balíček z nasledovného linku: https://viskb.csirt.sk/download/km/.

Jednotlivé OVM sú zároveň priebežne kontaktované z adresy cyber_projekty@mirri.gov.sk a sú distribuované používateľské príručky, číselníky a súbor s údajmi o organizácii.

Následne je potrebné podľa používateľskej príručky modul nainštalovať a zabezpečiť úvodnú konfiguráciu (vytvorenie administrátorského a používateľského účtu) a zrealizovať import dodaných číselníkov (taktiež súčasť inštalačného balíka). Po vykonaní tejto úvodnej konfigurácie je možné pristúpiť priamo k vyplneniu zberných údajov (ako sú aktíva, audity, evidencia kybernetických incidentov, katalóg rizík atď.) za dané OVM. Detailný postup je popísaný v používateľskej príručke. Pre účely ukončenia projektov z dopytovej výzvy postačuje zatiaľ vyplniť len údaje o bezpečnostných incidentoch za uplynulé obdobie (odporúča sa aspoň za posledný rok, prípadne aj viac).

Po ukončení projektu VISKB si bude môcť OVM vybrať v akom móde (on-line alebo off-line) bude klientsky modul používať. Základné rozdiely sú nasledovné:

Off-line klientsky modul je možné nainštalovať na akýkoľvek PC, ktorý nemusí mať žiadnu konektivitu do siete Internet alebo Govnet a prakticky ani do internej siete OVM. Pre účely zasielania dát do VISKB bude musieť OVM manuálne realizovať pravidelný export povinných údajov do zašifrovaného súboru (funkcionalita modulu), a tento súbor následne manuálne nahrať prostredníctvom webového rozhrania centrálneho portálu VISKB.

V prípade, že sa OVM rozhodne používať on-line verziu klientskeho modulu, bude na strane OVM potrebné zabezpečiť sieťovú konektivitu z PC, kde bude prevádzkovaný klientsky modul VISKB, smerom na centrálny portál VISKB (prostredníctvom siete Internet alebo Govnet).

Ak dnes OVM použije off-line mód, bude samozrejme možné, po dokončení projektu VISKB (teda prakticky kedykoľvek v budúcnosti), prejsť na on-line verziu klientskeho modulu.

Aktuálne funkčnosť vyššie uvedenej funkcionality on-line zasielania zberných údajov do VISKB nie je podmienkou úspešného ukončenia projektov z dopytovej výzvy, týka sa len projektu VISKB, ktorý realizuje MIRRI SR, ako celku.

Ako bolo uvedené vyššie, pre ukončovanie projektov z dopytovej výzvy u ktorých využitie VISKB je viazané na naplnenie merateľného ukazovateľa, zatiaľ postačuje funkčná off-line evidencia bezpečnostných incidentov. V tejto fáze odporúčame OVM pracovať s off-line verziou klientskeho modulu, aj z dôvodu stále prebiehajúcich prác nasadenia centrálneho portálu VISKB do produkčnej prevádzky na strane MIRRI SR.

Pre aktuálne informácie sledujte web CSIRT.SK.

V prípade akýchkoľvek ďalších otázok nás prosím kontaktuje na cyber_projekty@mirri.gov.sk.