Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

CSIRT.SK

Všeobecné informácie o systéme Achilles od VJ CSIRT

Verzia 1.0

Výhody registrácie do systému Achilles

Vládna jednotka CSIRT („VJ CSIRT“) ako súčasť Ministerstva investícií regionálneho rozvoja a informatizácie SR („MIRRI“) je v súlade so zákonom č. 95/2019 Z.z. o informačných technológiách verejnej správy v platnom znení, oprávnená vykonávať pravidelné neinvazívne hodnotenie zraniteľností služieb verejnej správy poskytovaných cez internet alebo prostredníctvom Govnetu**.** Výsledky sú následne vyhodnocované a oznamované správcovi. VJ CSIRT môže vykonať detailné hodnotenie zistených zraniteľností so súhlasom správcu.

Registráciou do systému Achilles získate:

1. Každý mesiac Vám odošleme **report zraniteľností**, ktoré sa nachádzajú na Vašich verejných IP adresách. Tento report z kapacitných dôvodov vykonávame automatizovaným skenerom zraniteľností (vykonáva sa plošne) a jeho cieľom je odhaliť najznámejšie druhy zraniteľností. V prípade záujmu o kompletné penetračné testovanie aplikácií je možné požiadať o službu Ares. Manuálne overovanie (validácia) kritických zraniteľností sa vykonáva len v prípade dostatočných kapacít VJ CSIRT alebo na základe konkrétnej žiadosti. VJ CSIRT má právo rozhodnúť, akým spôsobom, v akom rozsahu a v akom poradí bude poskytovať služby.[1]
2. Získate informácie o **aktívne zneužívaných zraniteľnostiach**; pokiaľ VJ CSIRT deteguje zraniteľné služby na Vašich verejných IP adresách, pošleme Vám varovanie alebo odporúčanie.
3. **Odporúčania** pre zabezpečenie Vašej siete vyplývajúce z identifikovaných nálezov, ak sa na Vašich verejných IP adresách nachádzajú potenciálne zneužiteľné služby.
4. **Monitoring** dostupnosti Vašich webových služieb cez modul **Domino**. O túto službu je potrebné požiadať zvlášť.

[1] VJ CSIRT môže určovať spôsob, rozsah a prioritizáciu prostriedkov a zdrojov pri poskytovaní preventívnych služieb a reaktívnych služieb prostredníctvom objektívnych kritérií založených na analýze rizík zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov (§ 15 ods. 5 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti v platnom znení).

Systém Achilles ako služba vyhľadávania zraniteľností

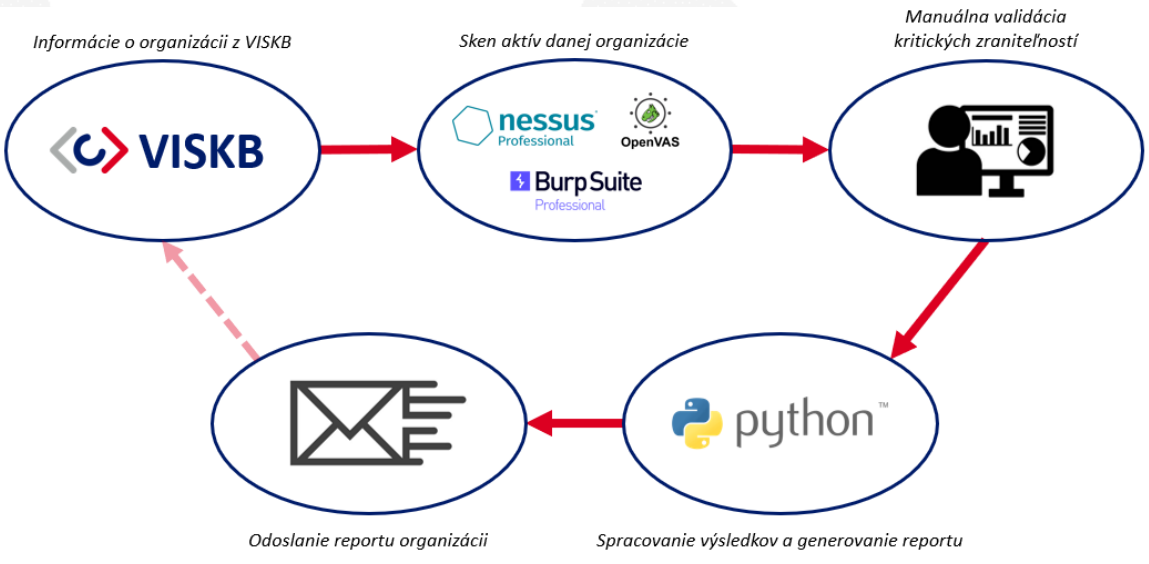
VJ CSIRT prevádzkuje systém **Achilles**, ktorý bol vybudovaný na centralizovanú správu zraniteľností z pohľadu aktéra hrozieb útočiaceho z prostredia verejného internetu. V systéme Achilles VJ CSIRT získava a spracováva informácie o zraniteľnostiach, informuje inštitúcie o zraniteľnostiach, ktoré sú detegovateľné z verejného internetu. Bližšie informácie nájdete v článku na oficiálnej webovej stránke VJ CSIRT. Súčasťou je modul **Domino**, ktorý slúži pre monitoring dostupnosti verejne dostupných webových služieb, teda ako systém včasného odhaľovania útokov typu DoS/DDoS alebo technických výpadkov.

Ciele systému Achilles

Systém Achilles má za úlohu znížiť riziko zneužitia potenciálnych vektorov útokov na infraštruktúry organizácií/subjektov verejnej správy a tým cielene znižovať pravdepodobnosť vzniku závažných kybernetických bezpečnostných incidentov. Ďalšou úlohou systému je včasne informovať o nedostupnosti webových služieb, či už z technických príčin alebo dôsledkom útokov typu DoS/DDoS. To má na starosti modul **Domino**.

Prvky systému Achilles

Systém Achilles sa skladá z proprietárneho programového vybavenia aj programového vybavenia s otvoreným zdrojovým kódom, skenerov zraniteľností či analytickej/kolaboračnej platformy nad ktorými pracuje vlastná aplikácia VJ CSIRT pre ukladanie, filtrovanie a



Obrázok 1 - Jednotlivé prvky systému Achilles

spracovávanie dát subjektov štátnej a verejnej správy. Základný mesačný cyklus fungovania systému Achilles je zobrazený na Obrázku 1.

Modul Domino na kontrolu dostupnosti webových služieb

Modul **Domino** má v systéme Achilles na starosti pravidelné overovanie dostupnosti webových služieb, ktoré si organizácia definuje. Dostupnosť sledovanej webovej lokality je overovaná cez odosielanie **GET požiadaviek** na porty 80 (HTTP) a 443 (HTTPS). Frekvencia týchto požiadaviek je max. každých 15 minút (ak je aktívum nedostupné), min. každých 30 minút (ak je aktívum dostupné). Zaručuje sa tak kontinuálne overovanie dostupnosti určených aktív bez ohľadu na ich aktuálny stav.

V prípade nedostupnosti kontaktujú vlastníka pracovníci VJ CSIRT cez kontakty uvedené v systéme VISKB so zámerom overiť aktuálny stav daného aktíva, resp. či konštituent vie o aktuálnom stave daného aktíva.
O službu je aktuálne potrebné požiadať **samostatne**, a to tak, že v registračnom e-maili vyjadrí vlastník webovej stránky záujem aj o služby modulu Domino a explicitne uvedie, ktoré služby majú takto byť monitorované.

Pripomíname, že na poskytovanie služieb modulu Domino je nutné, aby si správca nastavil svoju infraštruktúru tak, aby nedošlo k automatickému blokovaniu požiadaviek z modulu Domino, resp. z verejnej IP adresy, odkiaľ Domino posiela požiadavky. Bližšie informácie k tejto požiadavke vieme poskytnúť v procese registrácie do systému Achilles.

Požiadavky na registráciu do systému Achilles

Systém Achilles je poskytovaný konštituencii VJ CSIRT, resp. organizáciám, ktoré spadajú do verejnej správy, čo je aktuálne jedinou podmienkou na prijatie požiadavky o registráciu do systému Achilles.

V rámci registrácie nás treba kontaktovať na e-mailovej adrese achilles@csirt.sk s nasledujúcim textom:

> ***Máme záujem o registráciu do systému Achilles.***
>
> - ***Názov organizácie/subjektu (verejnej správy)***
> - ***Kontakt (e-mail, telefónne číslo)***

Ak máte záujem aj o služby modulu Domino, do e-mailu pridajte aj nasledujúci text s uvedenými aktívami[2]:

> ***Máme záujem aj o modul Domino, kde žiadame o monitoring nasledujúcich aktív:***
>
> - ***Aktívum 1***
> - ***Aktívum 2***
> - ***Aktívum 3***
> - ***...***

Po úspešnom prijatí e-mailovej žiadosti Vám vytvoríme prístup k systému VISKB pre registráciu informácií o Vašej organizácii. V systéme Vás požiadame o zaznamenanie informácií o Vašej infraštruktúre, ktorá bude predmetom pravidelného monitoringu zraniteľností a dostupnosti z verejného internetu.

[2] *Aktíva nemusia byť určené samostatne, môže ísť aj o skupinu aktív, ako napr. celý subnet.*

Kontaktné údaje

V prípade otázok na systém Achilles a jeho poskytovanie môžete kontaktovať VJ CSIRT na e-mailovej adrese achilles@csirt.sk.