Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

CSIRT.SK

Všeobecné informácie o službe penetračného testovania „Ares“ od VJ CSIRT

ARES
by CSIRT.SK
ATTACK TO PROTECT

Verzia 1.8

Ako mi (mojej inštitúcii) Ares pomôže?

Ministerstvo investícií, regionálneho rozvoja informatizácie Slovenskej republiky (MIRRI) prostredníctvom Vládnej jednotky CSIRT (VJ CSIRT) poskytuje svojej konštituencii službu hodnotenia zraniteľností formou **penetračného testu**. Výsledkom penetračného testovania je ucelená správa (report), ktorej obsahom je zoznam objavených zraniteľností testovaného systému. Tieto zraniteľnosti sú kategorizované podľa ich závažnosti (nízka, stredná, vysoká alebo kritická) a pravdepodobnosti ich zneužitia (nízka, stredná alebo vysoká). Ku každej zraniteľnosti náleží popis, špecifikácia miesta výskytu, príklad možného zneužitia a **odporúčané opatrenia** na jej odstránenie alebo zníženie rizika jej zneužitia. S touto správou ďalej pracujú vývojári systému a jednotlivé zraniteľnosti odstraňujú. Je možné vykonať aj opätovné testovanie. V takom prípade kontrolujeme, či sú už nájdené zraniteľnosti opravené, a či pri ich odstraňovaní neboli zavedené nové. Pre optimálny výsledok treba **odporúčania VJ CSIRT vždy implementovať bezodkladne.**

Rozdiel medzi penetračným testovaním a vyhľadávaním zraniteľností (skenovaním)

Veľmi často sa môžete stretnúť so zámenou týchto pojmov.

Vyhľadávanie zraniteľností (skenovaním) trvá od niekoľkých hodín do niekoľkých dní a je vykonávané automatizovane nástrojom na to určeným (napr. Nessus, OpenVAS, Artemis alebo tzv. Vulnerability Assesment modul v rámci XDR riešenia). Odhalí vybrané zraniteľnosti systému, pričom sa opiera o hlavičky stránok, verzie softvéru alebo prednastavené odpovede softvéru. Nedokáže identifikovať chyby v biznis logike, ani neodhalí slabé, ale ľahko zneužiteľné miesta v aplikácii. Takúto formu testovanie ponúka VJ CSIRT v rámci svojej konštituencie bezplatne v rámci služby **Achilles**.

Penetračné testovanie trvá v závislosti od dohodnutého rozsahu od niekoľkých týždňov po niekoľko mesiacov a jeho úlohou je prekonávať bezpečnostné mechanizmy na odhalenie zraniteľných miest v rámci infraštruktúry a aplikácií. Identifikuje aj také zraniteľnosti, ktoré nie je možné identifikovať automatizovaným nástrojom v rámci vyhľadávania zraniteľností. Je to teda dlhší, ale precíznejší proces.

Penetračné testovanie ako služba od VJ CSIRT

VJ CSIRT poskytuje bezodplatne svojej konštituencii službu hodnotenia zraniteľností formou penetračného testu podľa dostupných kapacít. Na vyjadrenie záujmu o túto službu je potrebné zaslať dopyt na podmienky poskytnutia penetračného testovania oficiálne na adresu **ares@csirt.sk** (kvôli kapacitným obmedzeniam) aspoň 4 mesiace pred Vami plánovaným termínom penetračného testovania.

Podmienkou vykonania penetračného testovania je uzatvorenie písomnej dohody o penetračnom testovaní medzi MIRRI a Vašou organizáciou, v ktorej sa bližšie dohodne najmä predmet testovania a podmienky výkonu testovania, a následne podanie záväznej žiadosti o výkon penetračného testovania. Zapojením sa do služby **Ares** a výkonom penetračného testovania získavate podklad pre zabezpečenie súladu s vybranými požiadavkami, najmä v oblasti hodnotenia zraniteľností, bezpečnostných aktualizácií a auditu/kontrolných činností, vyplývajúci predovšetkým zo Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe v platnom znení a jeho vykonávajúcich predpisov a Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

VJ CSIRT sa v rámci služby Ares zameriava najmä na penetračné testovanie webových aplikácií metódou **white-box**. Pri tomto druhu penetračného testu sa jedná o testovanie zraniteľností s prístupom ku zdrojovému kódu. Zdrojový kód spolu s používateľskými účtami so všetkými rolami, ktorých oprávnenia sú súčasťou testov, je nutné poskytnúť pred vykonaním samotného penetračného testu. Po doručení zdrojových kódov tieto prejdú procesom revízie z hľadiska bezpečnosti, tzv. **code review.**

Okrem white-box testovania VJ CSIRT ponúka aj testovanie metódami **gray-box** a **black-box**, v závislosti od dostupnosti informácií a požiadaviek zákazníka. Pri gray-box testovaní má testovací tím k dispozícii len **čiastočné informácie o systéme**, ako napríklad obmedzenú dokumentáciu alebo testovacie používateľské účty, bez prístupu ku zdrojovému kódu. Black-box testovanie prebieha **bez akejkoľvek predchádzajúcej znalosti interného fungovania aplikácie** – zákazník neposkytuje zdrojové kódy, dokumentáciu ani technické detaily. Testovanie sa realizuje výlučne na základe dostupnosti samotnej aplikácie a poskytnutých prístupových údajov, čím simuluje reálny útok z pohľadu externého útočníka.

Súčasťou služby Ares je taktiež **penetračné testovanie externej infraštruktúry**, zamerané na identifikáciu a vyhodnotenie zraniteľností vo verejne dostupných systémoch, ako sú servery, sieťové zariadenia alebo iné exponované služby.

V rámci služby Ares poskytuje takisto tzv. proces **CIS Benchmark Review.** Ten označuje proces hodnotenia konfigurácie systému podľa bezpečnostných odporúčaní publikovaných organizáciou Center for Internet Security (CIS). Cieľom je identifikovať nesúlad s osvedčenými bezpečnostnými praktikami a zhodnotiť celkový stav zabezpečenia. Výsledkom je **prehľad rizík a odporúčaní**, ktorý slúži ako podklad pre posilnenie bezpečnosti a zabezpečenie súladu s bezpečnostnými štandardmi.

Technické podmienky realizácie penetračného testovania

Pred samotným vykonaním penetračného testovania je zo strany objednávateľa potrebné pripraviť prostredie na výkon penetračného testovania. Táto sekcia obsahuje zoznam podkladov a úkonov, ktoré je potrebné zabezpečiť (platné pre testovanie vo forme white-box):

1. Finálna verzia dokumentácie riešenia (napríklad vo forme Detailného návrhu riešenia, DNR) so zoznamom implementovaných prípadov použitia.
2. Architektúra riešenia (prostredie aplikácie a využívané technológie).
3. Používateľská príručka.
4. Technická alebo integračná príručka.
5. Zdrojový kód testovaného riešenia, ak je k dispozícii.
6. Počas dohodnutej doby testovania je potrebné nastaviť výnimky pre bezpečnostné riešenia zamedzujúce dopytovaniu sa na aplikáciu, napr. Web Application Firewall (WAF) alebo Intrusion Prevention System (IPS). Zdrojové IP adresy, pre ktoré je potrebné WAF alebo IPS vypnúť sú určené členmi VJ CSIRT.
7. V prípade nálezov počas testovania alebo analýzy zdrojového kódu môže byť potrebná súčinnosť dodávateľa, ak sa objavia otázky zo strany VJ CSIRT.

8. Biznis logiku aplikácie je potrebné predviesť používateľom aplikácie pre členov VJ CSIRT, aby sme vedeli určiť, ako sa s aplikáciou pracuje a určiť, kde môžu nastať chyby v jej logike.
9. Penetračné testovanie sa vykonáva **na testovacom prostredí** a **na dokončenej verzii aplikácie** alebo systému.
10. Je nevyhnutné zriadiť požadované prístupy a roly (odporúča sa po 2 prístupy z každej používateľskej roly) v rámci aplikácie a prístup do testovacieho prostredia pre členov VJ CSIRT (pre požadovaný počet bezpečnostných analytikov). Ak je prístup k testovaciemu prostrediu realizovaný formou VPN, je potrebné vytvoriť aj tieto prístupy.