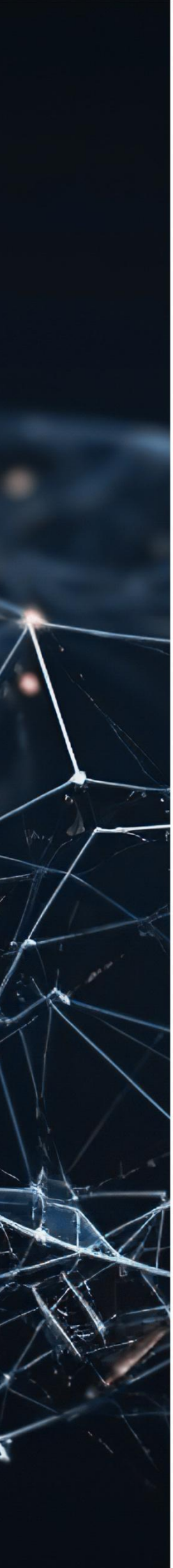

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

CSIRT.SK

Všeobecné informácie o systéme

ARES

od **VJ CSIRT**

ARES
by CSIRT.SK
ATTACK TO PROTECT

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 (skenovanie) trvá od niekoľkých hodín do niekoľkých dní a je vykonávané automatizovane nástrojom na to určeným (napr. Nessus, OpenVAS, Artemis alebo modul na hodnotenie zraniteľností 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:

1. **Penetračné testovanie webových aplikácií** predstavuje testovanie zraniteľností webových aplikácií. Pred vykonaním testovania je potrebné poskytnúť všetky podklady potrebné pre testovanie, a to najmä prístup k aplikácii (napr. prostredníctvom VPN), testovacie účty so všetkými rolami, ktoré sa v systéme nachádzajú, a v prípade, že ide o white-box metódu testovania aj zdrojové kódy aplikácie.
2. **Penetračné testovanie internej infraštruktúry** predstavuje testovanie zraniteľností vnútornej sieťovej infraštruktúry organizácie z pohľadu útočníka s prístupom do internej siete. Testovanie zahŕňa identifikáciu slabých miest v prostredí Active Directory, interných systémoch, serveroch, sieťových

zariadeniach a službách. Pred vykonaním testu je nutné poskytnúť sieťovú dokumentáciu, rozsah IP adries a prístupové údaje do internej siete.

3. **Penetračné testovanie externej infraštruktúry** predstavuje testovanie zraniteľností z pohľadu externého útočníka bez predchádzajúceho prístupu do internej siete. Testovanie sa zameriava na verejne dostupné systémy, služby a rozhrania organizácie, ako sú webové servery, e-mailové servery, VPN brány a iné komponenty dostupné z internetu. Pred vykonaním testu je nutné poskytnúť zoznam verejných IP adries a domén patriacich do rozsahu testovania.

4. **Bezpečnostný audit zariadení** predstavuje komplexné posúdenie bezpečnostnej konfigurácie a stavu koncových zariadení, sieťových prvkov alebo iných hardvérových komponentov. Audit zahŕňa kontrolu konfigurácie, aktualizácií, prístupových práv a dodržiavania bezpečnostných politík. Pred vykonaním auditu je nutné poskytnúť prístup k auditovaným zariadeniam spolu s ich technickou dokumentáciou a platnými bezpečnostnými politikami organizácie.