ALISON

Vystresovaný a bohatý. Taký je život špičkového hackera

White hat hackers, bug bounty hackers, penetrační testeri či lovci zraniteľností. Odmeny pre lovcov zraniteľnosti či certifikovaných hackerov sa blížia honorárom hviezd.

Peniaze však nie sú jedinou motiváciou hackerskej komunity. Zaujímajú ich aj rebríčky lídrov, ktoré hackerom pripisujú zásluhy za objavy a pomáhajú im tak budovať si uznanie.

Bug bounty sú na odbornej úrovni skvelým doplnkom štandardných penetračných testov. Líšia sa motiváciou, pravidlami, priebehom, no jedno majú spoločné – profesionáli hľadajú chyby. V práci alebo ako dobrodružstvo. Hľadanie zraniteľností je súboj, ktorý sa nikdy nekončí, a biznis, ktorý nikdy nespí.

Odmena za chybu

Program bug bounty je verejnou výzvou spoločností, ktoré ponúkajú etickým hackerom finančnú odmenu za nahlásenie zistených bezpečnostných zraniteľností ich internetových stránok, programov či mobilných aplikácií. Odmenu získajú títo výskumníci po objavení chyby, ktorá nie je verejne známa.

V súčasnosti sú bug bounty programy čoraz bežnejšou metódou na nájdenie a opravu rôznych zraniteľností. Skutočné obrátky však tieto programy nabrali vo chvíli, keď sa do nich začali začiatkom minulej dekády zapájať technologické giganty.

Najlepšie ceny, najviac odvahy a nelimitované odmeny!

Bug bounty program pre webové aplikácie spustil Google v roku 2010 a desať rokov nato už rozdelil na odmenách 6,7 milióna amerických dolárov medzi 682 výskumníkov v 62 krajinách.

Facebook na seba nenechal dlho čakať a spustil program Whitehat s odmenou začínajúcou sa na päťsto dolároch. No už v marci 2011 zaplatil 15-tisíc dolárov 22-ročnému odborníkovi za jednu nájdenú chybu a do roku 2015 vyplatili výskumníkom vo svete viac ako 4,3 milióna dolárov. Dnes patrí do klubu nelimitovaných odmien, čo znamená, že suma najvyššej odmeny za nájdenie zraniteľnosti nie je ohraničená.

V roku 2015 vstúpil do hry aj Microsoft. S jednorazovou odmenou 250-tisíc dolárov patrí medzi najveľkorysejších motivátorov s podmienkou, že zraniteľnosť musí byť kritická a dôležitá. Sekunduje mu Apple s limitom 200-tisíc dolárov za „security issues“ na firemnom hardvéri.

Všetci proti všetkým

Najpopulárnejšími vyhlasovateľmi bug bounty však stále zostávajú úložiská, prehliadače, online platformy, dodávatelia bezpečnostného hardvéru a softvéru, platobné systémy a operátori. Pre

zaujímavosť – v klube nelimitovaných odmien sú aj Word Press (ak používate, tak plne chápete), AT&T, ale aj sieť klubov a reštaurácií Zomato.

Medzi známe rýchloobrátkové značky, ktoré vyhlasujú bug bounty, sa zaradili aj Uber či Starbucks. Obe spoločnosti deklarujú, že im záleží na bezpečnosti ich zákazníkov, a Starbucks povzbudzuje výskumníkov, aby záškodnícke aktivity uplatňovali aj na ich web, infraštruktúru aj webové aplikácie. A svoje bug bounty vyhlasujú aj platformy, ktoré bug bounty ponúkajú, čiže Hackerone a Bugcrowd.

Potichu, ale isto

Zatiaľ čo hľadanie zraniteľnosti a nálezy v bud bounty sú predmetom prestíže a slávy minimálne v hackerskej komunite, výsledkami penetračných testov sa málokto chváli. Pen testy simulujú profesionálny kybernetický útok, zatiaľ čo bug bounty programy priťahujú širokú škálu hackerov s rôznymi schopnosťami a odbornými znalosťami – a aj motiváciou.

Pen testy musia prebiehať v súlade s reguláciami a stanovenými štandardmi. Na penetračné testy a ich výkon tak dohliadla Všeobecné nariadenie o ochrane údajov (GDPR) či súbor medzinárodných bezpečnostných štandardov PCI DSS (Payment Card Industry Data Security Standard) a séria štandardov ISO27k.

Vykonávanie penetračných testov má zmysel, iba ak ich firmy vykonávajú na pravidelnej báze, minimálne aspoň raz ročne. Preto report firmy Positive Technologies za minulý rok šokoval výsledkami.

Toto manažment nerád počuje

Pen testerom sa až v 93 percentách spoločností podarilo prelomiť prístup do siete počas penetračných testov. V šestine testovaných spoločností našli dokonca aj stopy po predchádzajúcich útokoch. Alarmujúcim zistením bolo, že pri 71 percentách testovaných spoločností by dokázal preniknúť do ich vnútornej siete aj nekvalifikovaný hacker.

Priemerný čas na preniknutie do lokálnej siete bol štyri dni. V jednom prípade dokonca stačilo hackerovi iba 30 minút na preniknutie do lokálnej siete. Zložitosť útoku bola vo väčšine prípadov nízka, čo znamená, že aj hacker so základnými schopnosťami by mohol pri útoku uspieť.

Pri 77 percentách prípadov bola základným penetračným vektorom nedostatočná ochrana webových aplikácií. Najmenej jeden takýto vektor bol prítomný v 86 percentách spoločností.

Najčastejším nálezom pri pen testoch bolo hneď niekoľko spôsobov narušenia. Jedna spoločnosť mala v priemere identifikované dva penetračné vektory. Maximálny počet penetračných vektorov detegovaných v jednej spoločnosti bol trinásť.

ALISON

Raz do roka a aj stále

Penetračné testy sú dôležité pre veľké spoločnosti s geograficky rozmanitými infraštruktúrami kvôli úplnej náročnosti zabezpečenia systémov. Najčastejšími objednávateľmi penetračných testov sú podľa správy od Positive Technologies spoločnosti z odvetvia financií a IT. Za nimi nasledujú odvetvia palivového a energetického priemyslu a vládny sektor.

Penetračné testy však treba vykonávať pravidelne a aj vtedy, keď pribudne nová sieťová infraštruktúra alebo aplikácia, pri výrazných upgradoch alebo zmenách na infraštruktúre alebo aplikáciách. Odborníci sa zhodujú na potrebe penetračných testov aj po aplikovaní bezpečnostných záplat a pri akvizícii nových pobočiek.