ALISON

# Bug Bounty. Alebo dohodnime sa radšej po dobrom

Výzva švajčiarskej vlády pre hekerskú komunitu viacej prekvapila vládny sektor ako hekerskú obec. Elektronický volebný systém prevádzkuje Švajčiarska pošta a na súčasný experiment testov zraniteľnosti vyčlenila vláda 250-tisíc švajčiarskych frankov, pričom väčšia časť je určená na odmeny úspešným účastníkom a časť pre špecializovanú bezpečnostnú firmu.

Do poslednej februárovej nedele sa na špecializovanej webovej stránke prihlásilo 2 902 subjektov – etických hekerov a počas mesiaca sa bude pokúšať infiltrovať, znefunkčniť, zmanipulovať alebo ovplyvniť švajčiarsky volebný systém. Vyhodnotenie bude po mesiaci a pre tých, ktorým sa podarí prelomiť bezpečnostný systém, sú odmeny od sto do päťdesiattisíc švajčiarskych frankov.

Zverejnenie výzvy pre hekerov nie je nič neobvyklé a verejnému testu prelomenia sú vystavované napríklad aj riešenia pre šifrovanie údajov a podobne. Vystavenie nejakého systému verejnému otestovaniu, skôr ako sa použije v ostrej prevádzke, svedčí o zodpovednosti toho, kto je vlastníkom tohto riešenia, voči konečným používateľom. Koniec koncov, nechcenému testovaniu zo strany hekerov sú dennodenne vystavené všetky systémy pripojené do internetu. Rozdiel je len v tom, kto má z toho prospech.

Výzva Bug Bounty je vo svete populárna, o čom svedčí aj rebríček Top 30 Bug Bounty programov na rok 2019. Nikoho neprekvapí , že medzi vyhlasovateľmi sú spoločnosti ako Facebook, Google, Apple, PayPal, LinkedIn, Starbucks, Uber a mnohé ďalšie.

Kapacita ľudských a technických zdrojov, ktoré útočia na systém, môže a nemusí závisieť vždy len od komplexnosti testovaného riešenia. Niekedy stačí na prelomenie len mobilný telefón a šikovný tester, ktorý odhalí slabé miesto. Inokedy to môže byť tím ľudí, ktorí budú využívať rôzne techniky vrátane sociálneho inžinierstva. Testovacie útoky môžu prebiehať podľa dopredu pripravených scenárov, ale môže to byť aj „voľný štýl“, ktorý sa bude prispôsobovať podľa toho, ako bude pokus o narušenie postupovať dopredu.

Čo sa týka zneužitia dát alebo vydierania za odblokovanie, je to delikátna téma. Dohody s vydieračmi nie sú práve tá najlepšia cesta a skôr je tendencia neplatiť, ako platiť. Zaplatením výkupného totiž nie je nijak zaručené, že sa postihnuté firmy aj dostanú k nedostupným údajom alebo sa vyhnú ďalšiemu napr. DDoS útoku. Skôr firmy ticho požiadajú o pomoc a spoluprácu orgány činné v trestnom konaní alebo expertov na počítačovú bezpečnosť.

Aby sa predišlo špirále čoraz väčších súm za vydieranie a strate dobrého mena, napadnuté subjekty často kybernetický útok tajili. V súčasnosti však aktuálna legislatíva a regulačné orgány vyžadujú hlásiť kybernetické bezpečnostné incidenty alebo úniky údajov pre pomerne široké spektrum organizácií. Dá predpokladať, že minimálne 60 percent identifikovaných napadnutí by dnes už malo byť ohlásených. Koľko z nich je, ale je aj zverejnených v médiách, je už ťažké povedať.