ALISON

Zabudnite na maklérov a influencerov. Táto dekáda bude patriť hekerom, šifrovaniu a steganografii

Najväčšie svetové podujatia v kybernetickej bezpečnosti od začiatku roka a opatrenia proti pandémii priniesli spoločný záver: buďte opatrní. Ľudský faktor je najslabší článok bezpečnosti.

Sláva a bohatstvo, občas aj väzenie

Odmeny za hľadanie zraniteľnosti (bug bounty) vytvorili samostatný a prudko rastúci ekosystém, ku ktorému sa pridalo viac ako pol milióna hackerov. Tradičný **Hacker Report** hodnotí stav trhu a trendy ako dramaticky rastúce. V skratke? Trh sa profesionalizuje, rastú odmeny a najčastejšou motiváciou, prečo sa učiť hackerským zručnostiam, býva osobná motivácia „ja to dám!“.

Na odmenách za report zraniteľností firmy vyplatili ročne 82 miliónov USD, pričom odmenu milión dolárov v roku 2019 dosiahlo sedem hackerov. Podľa domicilu peniaze putovali pre hackerské (oficiálne) komunity v USA (19 percent objemu), Indii (10 %), Rusku (8 %), Číne (7 %), Nemecku (5 %) a Kanade (4 %).

Hacker Report mapuje 3 150 hackerov zo 120 krajín, ktorí do jedného z bug bounty systémov úspešne nahlásili aspoň jednu zraniteľnosť. Tu je pár stručných faktov.

Medzi pracovné vybavenie patrí najlepšie pripojenie na internet a ambícia stále sa učiť nové veci. A kde hackeri bývajú? To by chceli vedieť všetci. Neexistuje totiž žiadna relevantná lokácia, ale Hacker Report uvádza ako významné krajiny Panamu, Nový Zéland, Maďarsko, Senegal, Kubu, Vietnam a Venezuelu.

Prečo je lukratívne študovať matematiku

Obrat trhu so šifrovacím softvérom sa v priebehu piatich rokov zdvojnásobí. Toľko triezvy odhad odborníkov, ktorí vidia rast z minuloročnej hodnoty trhu 7,5 miliardy amerických dolárov až na 16,6 miliardy do konca roka 2024. Znamená to dvojciferný rast ročne a obrovské príležitosti v celej oblasti prostriedkov šifrovej ochrany.

Nespochybniteľnými drajvermi rastu budú čoraz prísnejšie nároky regulátorov na ochranu dát a súkromia, exponenciálny rast cloudových a virtuálnych technológií a hrozba úniku dát. Rozvoj mobility, fenoménu IoT vo všetkých segmentoch a požiadavky zamestnancov pracovať kdekoľvek a na čomkoľvek tak prispeli k rozvoju špecializovaných matematických odborov, kde sa znalosti vyvažujú zlatom (alebo kryptomenami).

Vládne agentúry a regulátori vo svete za ostatné roky sprísňujú pravidlá a požiadavky na kybernetickú bezpečnosť na inštitúcie a firmy v záujme ochrany občianskych aj spotrebiteľských

práv. Platí to pre dáta, siete, koncové zariadenia, aplikácie aj cloudové úložiská v každej fáze, počínajúc architektúrou, používaním a končiac vymazaním. A odmeny? Atraktívne.

Delikatesa pre kybernetickú bezpečnosť: Steganografia

Na temnom aj bežnom webe patria medzi populárne aplikácie audiokonvertory, ktoré dokážu ukryť dáta do audiozáznamov. Ak sú šifrované, je to bonus, ale samotná forma utajenej komunikácie má svoje pomenovanie – steganografia.

Ak by ste si chceli tento odbor prakticky predstaviť, tak to je to písmo, ktoré sa kedysi v listoch objavilo až nad plameňom, skryté symboly na obraze zašité v ornamentoch alebo čítanie podľa dohodnutého kľúča – napríklad vždy druhé písmeno v každom druhom slove. Proste dorozumievanie sa tajných služieb, zakázaných sektárov, vojska a milencov.

V dnešnej dobe sa dáta dajú takto posielať v utajených pixeloch v obrázkoch alebo vnorené v audiosúboroch.

Steganografia je predmetom záujmu v prípade kybernetického útoku, kde sa súbory skúmajú, či neobsahujú skryté kódy, ktoré napadajú nechránené zariadenia a využívajú ich napríklad na ťažbu kryptomien. Jej primárne využitie však zostáva v treťom tisícročí rovnaké – dorozumievanie sa medzi militantnými zložkami, preto sú odborníci v hľadáčiku tých najlepších firiem a vládnych inštitúcií.