Bezpečnostný report 04/2019

Technologickí producenti, akademický sektor a bezpečnostné zložky vo svete hodnotia s odstupom rok 2018, aby vedeli, čo čakať v tomto. Aspoň približne.

V tejto štatistike by ste naozaj byť nechceli! Najmä preto, že ide o veľa peňazí.

Keďže konektivita biznisovej infraštruktúry sa stále zvyšuje, odhaduje sa, že v priebehu roku 2019 spôsobí kybernetický zločin škody vyše **dvoch biliónov dolárov** (necelých 1,8 bilióna eur). Na porovnanie, za rok 2018 sa rozsah globálnych škôd napáchaných kyberzločincami odhaduje na bilión dolárov (do 900 miliónov eur).

Priemerná škoda pri jednom úniku dát, respektíve prelomení ochrany dát (data breach) v roku 2020 tak dosiahne približne 150 miliónov dolárov (133 miliónov eur).

Jeden z najväčších, vlaňajší útok na americké mesto Atlanta a jeho inštitúcie si vyžiadal náklady 9,5 milióna dolárov (8,5 milióna eur) na likvidáciu spôsobených škôd. Hackerská skupina zaútočila ransomvérom na päť z 13 mestských inštitúcií, pričom žiadala „výkupné“ vo výške 50-tisíc dolárov v podobe bitcoinov. Radnica odmietla zaplatiť a dodnes vedú technologickí lídri a politickí predstavitelia diskusiu o tom, **ako a koľko o takejto udalosti diskutovať** s verejnosťou a na verejnosti.

Prevažná väčšina, až 95 percent únikov dát, sa odohráva v niektorom z nasledujúcich troch odvetví: **verejná správa, maloobchod a technológie**. Dôvodom určite nie je fakt, že práve tieto odvetvia sú menej obozretné pri ochrane dát svojich zákazníkov. Podstatné je, že predstavujú veľmi populárne terče, a to predovšetkým vďaka vysokej koncentrácii osobných dát, ktoré uchovávajú. Práve tieto osobné dáta predstavujú pre hackerov obchodný artikel, ktorý sa dá výhodne speňažiť.

Odborníci preskúmali 700 zdravotníckych organizácií vrátane zariadení lekárskej starostlivosti, zdravotných poisťovní a spoločností, ktoré vyrábajú produkty pre zdravotníctvo. **75 % zdravotníckych inštitúcií** rôznej veľkosti vo svete bolo infikovaných malvérovými vírusmi.

Akokoľvek dokonalá je ochrana infraštruktúry a databáz, predsa len má jednu nekonečnú slabinu – a tou je **ľudský faktor**. V 95 percentách úspešných kybernetických útokov a hackerských prienikov bolo dôvodom zlyhanie ľudí, a nie technológií.

Poslaním roku 2019 bude rozhodne spochybniť aj ďalší mýtus, a to že **hackeri kradnú peniaze len od veľkých** korporácií, bánk alebo od bohatých celebrít. Nie je to pravda, hoci obrovské útoky na korporácie, ako bola sieť hotelov Marriot, by nás mohli utvrdiť v tomto mylnom presvedčení. Terčom môže byť aj malý podnik a vlastne ktorýkoľvek používateľ – pokiaľ ste pripojený na internet, môžete sa kedykoľvek stať obeťou kyberútoku.

Druhy kyberútokov sa líšia a z roka na rok sa menia. Mimoriadne perspektívnou zločineckou oblasťou sú v súčasnosti **kryptomeny a ich ťažba**. Ťaženie kryptomien reprezentuje najprudšie rastúcu oblasť kyberzločinu. Miera útokov detegovaných antivírusovými programami stúpla medziročne o 8 500 percent. Mimoriadne expanzívne narástla v posledných mesiacoch roku 2017 aj samotná ťažba kryptomien – celkovo sa zvýšila o 34 000 percent. Ťažba kryptomien si vyžaduje obrovskú počítačovú kapacitu a hackeri môžu na to použiť priamo váš počítač bez toho, aby si od vás pýtali povolenie.

Zdroj: Symentec, Cyber Centers, Ponemon Institute, Juniper Research, Reuters