ALISON

Máj naozaj nebol v kybernetickej bezpečnosti romantický

- **Spojené kráľovstvo dokazuje pozíciu lídra v kybernetickej bezpečnosti precedentnými opatreniami**
- **Veľký počet kritických bezpečnostných zraniteľností a záplat**
- **Zlý mesiac pre Huawei**
- **Podvody pri kryptomenách**

Britská armáda dostane nové operačné centrum na boj proti kybernetickej kriminalite, ktoré jej má pomáhať v internetovej ofenzíve proti „nepriateľovi“.

Investíciu vo výške 22 miliónov GBP ohlásila ministerka obrany Penny Mordaunt, ktorá zároveň povedala, *„je načase venovať sieťovému prostrediu väčšiu pozornosť. Všetci si uvedomujeme riziká. Či prídu útoky z Ruska, Číny alebo Severnej Kórey, či ich spáchajú hektivisti, zločinci alebo extrémisti, či ide o malvér alebo falošné správy. Kybernetická kriminalita môže narušiť fungovanie našej národnej infraštruktúry a demokracie.“*

Kybernetické operačné centrum armády začne fungovať na budúci rok a malo by pokryť medzeru medzi operáciami britských spravodajských služieb a vojenských útvarov. Pozoruhodné je rozhodnutie z roku 2018, keď vznikla špecializovaná škola na vzdelávanie „odborníkov na kybernetickú bezpečnosť budúcej generácie“.

V máji vynikla kritická bezpečnostná aktualizácia Windows od Microsoftu, ktorá dosiahla na škále CVSS stupeň 9,8 z 10. Táto aktualizácia napráva zraniteľnosť CVE-2019-0708, známu ako BlueKeep. Ide o bezpečnostnú dieru, ktorá potenciálne umožňuje rýchle šírenie malvéru (t. j. červov) na zariadeniach v sieti. Podobná situácia sa vyskytla v roku 2017, keď počítače napadol vydierací softvér (ransomvér) WannaCry. Microsoft považuje situáciu za takú vážnu, že veľmi výnimočne vydal záplaty na BlueKeep aj pre nepodporované verzie Windows (napr. XP, Vista, Server 2003). Výskumníci z Errata Security uvádzajú, že odhalili takmer milión systémov pripojených na internet, ktoré sú postihnuté chybou BlueKeep.

Kritické bezpečnostné zraniteľnosti a súvisiace záplaty boli tiež ohlásené pre Adobe, Drupal, zariadenia Cisco, WhatsApp a procesory Intel. Zraniteľnosť WhatsApp (CVE-2019-3568) zaujala aj svetové médiá, pretože postihla aplikáciu, ktorá má zabezpečovať šifrovanú komunikáciu na zariadeniach iPhone aj Android. Izraelská firma NSO vytvorila súbor nástrojov na využívanie tejto zraniteľnosti a predala ho viacerým vládam. Súbor nástrojov nesie názov Pegasus a dáva prístup k zoznamu hovorov v telefóne a textovým správam. Umožňuje tiež potajomky snímať kamerou a

mikrofónom. Na AppStore sú k dispozícii nové, opravené verzie aplikácie WhatsApp, ktoré odporúčame nainštalovať.

V máji naplno prepukla politická a mediálna búrka okolo bezpečnostného rizika zariadení Huawei po tom, ako spoločnosť Google oznámila, že obmedzí prístup čínskeho telekomunikačného giganta k svojmu operačnému systému Android.

Máj bol z hľadiska nových únikov údajov relatívne pokojný. Do médií sa ani nedostali správy o britskom reťazci pohostinstiev Greene King. Ten zaslal zákazníkom svojho webu, ktorý ponúka darčekové poukazy, informáciu, že pri hekerskom útoku na web boli odcudzené ich osobné údaje. O prelome informoval blog, ktorému sa sťažovali zákazníci Greene King.

Krádež osobných údajov bola odhalená 14. mája 2019 a potvrdená o deň neskôr. Spoločnosť prevádzkujúca pohostinstvá, reštaurácie a hotely informovala postihnutých zákazníkov e-mailom dňa 28. mája 2019.

Podľa Greene King sa hekeri dostali k údajom v štruktúre meno, e-mailová adresa, identifikačné číslo používateľa, zašifrované heslo, adresa a poštové smerové číslo. Reťazec neinformoval, akým spôsobom sú heslá šifrované, len vo svojom e-maile oznámil, že „heslá boli zašifrované, ale napriek tomu mohlo dôjsť k ich odcudzeniu“.

Potešujúce informácie o únikoch dát kompenzuje správa o raste podvodov s kryptomenami.

Britské národné centrum na boj proti podvodom (Action Fraud) a Úrad pre dohľad nad trhom s finančnými službami (FCA) uviedli, že v roku 2018 prišli ľudia prostredníctvom podvodov s kryptomenami a zahraničnými investíciami o 27 miliónov GBP, čo je trojnásobok oproti predchádzajúcemu roku.

Zdroje: uvedené cez hyperlink