

Diplomatické depeše a deravé sociálne siete v decembri a oblasti, kde asi „žijú tisíce bezpečnostných expertov“

Najväčšou **bezpečnostnou udalosťou** decembra 2018 v médiách v Európskej únii už pravdepodobne zostane únik diplomatických depeší, ktoré dosiaľ neznámi hackeri odchytili minimálne tri roky. Kalifornská bezpečnostná spoločnosť Area 1 tento incident objavila a poskytla [1 100 depeší](#) americkému denníku The New York Times. Hackeri získali cez phishing smerovaný na cyperských diplomatov prístupové heslá k databáze menej dôležitých diplomatických depeší EÚ a korešpondenciu zo zabezpečených sietí publikovali na webových stránkach, ktoré na tento účel zriadili. Podľa bývalých pracovníkov americkej NSA, ktorí pracujú v spoločnosti Area 1, technika je obdobná, ako používa elitná skupina v Čínskej ľudovej armáde.

Silná hackerská skupina stála aj za [únikom údajov](#) o 500 miliónoch **hostí hotelovej siete** Marriott. Tá pod tlakom médií priznala, že mohlo dôjsť okrem krádeže osobných údajov aj k získaniu čísel kreditných kariet klientov. Hotelová sieť tak v decembri utrpela jeden z najväčších útokov kybernetických zločinu a zároveň čelí hnevu európskych aj amerických bezpečnostných autorít.

Spoločnosť Google priznala v novembri **odhalenie údajov** o 52,5 milióna používateľov svojej sociálnej siete Google+. Dostupné boli profily používateľov vrátane mien, zamestnania, e-mailových adries, dátumu narodenia, veku a vzťahového statusu. Kým ešte pri prvom útoku bolo zasiahnutých „iba“ vyše pol milióna dát, pri druhom útoku to bolo spomínaných vyše 50 miliónov. Oba incidenty prispeli k rozhodnutiu spoločnosti [zrušiť sieť Google+](#) v roku 2019.

Jednou z príčin podobných útokov je iste aj skutočnosť, že už piaty rok po sebe sa v zoznamoch **najčastejšie používaných hesiel** objavuje na prvom mieste *123456*, nasleduje invenčné *password*, potom jednoduché kombinácie po sebe idúcich číslíc alebo znakov na klávesnici *qwerty*. Keďže analýza hesiel sa robí na množine uniknutých dát, rebríček týchto hesiel neznamena najčastejšie používané heslá, ale dá sa interpretovať ako varovanie pre používateľov, ktorým určite skôr či neskôr nabúrajú účty. Rebríček 100 najhorších hesiel, ktorý už ôsmy rok spravuje [SplashData](#), má hlavný cieľ – motivovať všetkých na silnejšie heslá a ochranu.

V rámci programu [bug bounty](#) – odmien za **nájdenie bezpečnostných chýb** v systéme vyplatil Facebook v decembri vôbec najväčšiu odmenu vo výške 50-tisíc USD. V roku 2018 spoločnosť „lovcom chýb“ vyplatila už celkovo 1,1 milióna USD.

Ku koncu roka 2018 ponúka na základe svojich bežných dostupných Google nástrojov spoločnosť štatistiku, odkiaľ prichádza **najviac vyhľadávaní** pre výraz *cyber security*. Teoreticky by to znamenalo, že v krajinách a mestách, odkiaľ je najviac vyhľadávaní, sa to priam hemží záujmom a odborníkmi na kybernetickú bezpečnosť. © V tom prípade by boli Singapur, Svätá Helena (ostrov na polceste z Južnej Afriky do Brazílie), Zimbabwe, Etiópia a Ghana svetovými lídrami. Prvá päťka miest s najvyšším počtom IT bezpečnostných vyhľadávaní je Washington, Singapur, New York, Gurgaon v Indii a San Antonio. Slovensko sa v rebríčku vôbec neobjavuje, keďže vzhľadom na objem dát neprekročilo na relatívnej škále ani nulu.

Hodnota 100 predstavuje najvyššiu popularitu príslušného výrazu – v tomto prípade „cyber security“, ktorú dosiahol v ročnom hodnotení. Skóre 50 znamená polovičnú popularitu.

	OBLASŤ	MESTO
1	Singapur – 100	Washington D.C. – 100
2	Svätá Helena – 95	Singapur – 70
3	Zimbabwe – 94	New York – 62
4	Etiópia – 75	Gurgaon – 58
5	Ghana – 55	San Antonio – 53