Vážené čtenářky, vážení čtenáři,

před měsícem vstoupily v platnost směrnice GDPR a zatím se dá říci, že se až tak nic nestalo – podle všeho se čeká na nějaký precedens, kdy se zneužijí něčí osobní data a přijde odpovídající exemplární trest. Do této doby totiž mnohé firmy berou GDPR na lehkou váhu – poslední globální průzkumy renomovaných agentur mluví až o 40 procentech organizací, které se na GDPR zatím nepřipravily. K tomu, aby se rozhýbaly, musejí podle všeho vidět následky takového nekonání. Uvidíme, co přinesou nejbližší měsíce.

Uzákonit přísnou ochranu osobních dat ve stylu GDPR ale podle všeho chystá ještě na tento rok i Čína. Připravované opatření přitom podle Sammy Sacks z think-tanku CSIS jde ještě dále než evropské obecné nařízení o ochraně osobních údajů a samozřejmě překoná i příslušné americké normy.

Po řadě skandálů na konci loňského roku Čína vydala svůj první standard ochrany dat, který má velmi podrobná pravidla ohledně toho, co společnosti mohou shromažďovat, zpracovávat, uchovávat, sdílet nebo předávat. Uvidíme, jak se to celé dá do souladu s různými tamějšími vládními regulacemi.

Také výrobci mobilního hardwaru se vydali na cestu daleko bezpečnějších osobních dat. Apple a Google totiž představily řešení, které umožní uchovávat kritická data – čísla kreditních karet, vzorky otisků prstů – ve speciálních úložištích, která budou velmi významně chráněna před neoprávněným přístupem, a to včetně jejich možné hardwarové extrakce.

U Googlu to nabízí zatím jen Pixel 2, ale Android P to dovolí kterémukoliv výrobci. Apple, který systém označuje jako Secure Enclave, jej už má na všech nových přístrojích.

Apple zároveň ohlásil, že v přístrojích s iOS už nebude možné legálně spouštět software pro těžbu kryptoměn. Zdůvodnil to snahou o vyšší ochranu uživatelů. Konkrétně učinil opatření, která neumožní žádné aplikaci včetně reklam třetích stran, které se v nich zobrazují, spouštět nesouvisející procesy na pozadí, jako je například ono dolování kryptoměn.

Samozřejmě že výkon jednoho iPadu na dolování měn je velmi nedostatečný, ale pokud se propojí třeba tisíce těchto zařízení, což tento malware zpravidla dělá, může si hacker přijít k zajímavým sumám. A to by už teď jít u Applu nemělo.

Jak funguje nelegální těžba kryptoměn v oblasti počítačů a jak se tomu bránit, vysvětluje jeden z hlavních příspěvků tohoto vydání.

S přáním příjemně stráveného léta třeba i nad stránkami nejnovějšího SecurityWorldu přeje

Pavel Louda
vedoucí projektu

Obsah