ALISON

Máte Apple? Toto by ste mali vedieť. Alebo máte Android? Aj pre vás je to dôležité.

Technologický škandál alebo zlomyseľnosť * Problém sa dotkne miliardy používateľov *** Čo vysvetľoval Tim na stretnutí s Margrethou *** Antijablčný zákon**

Tima Cooka si predvolala prvá dáma Európskej únie pre informačné technológie. Nebol ani prvý, ani posledný predstaviteľ technologického gigantu, ktorý išiel vysvetľovať princípy svojho podnikania.

Keď nám všetci chcú dobre

Cookov tím prišiel vyzbrojený štúdiou o raste mobilného malvéru v Európe s dôrazom na to, ako si predstavuje ochranu používateľov zariadení Apple. O ochrane spotrebiteľov totiž chcela hovoriť aj Únia. Pre nás, majiteľov mobilných zariadení, samé dobré správy.

Chválitebné úmysly oboch strán a napriek tomu zrážka v protismere. Je to riešiteľné?

Začalo sa to bruselskou politickou úvahou, že niektoré IT firmy sú prirodzenými monopolmi a treba s tým niečo spraviť. Dôvodenie, prečo vznikli IT monopoly, teraz nechajme bokom. Podstatné je, že podnikanie v IT oblasti je niekedy naozaj viazané na použitie technologických platforiem, ktoré nemajú reálnu konkurenciu.

Na digitálnych trhoch sa tomuto postaveniu platforiem hovorí *strážcovia* (gatekeepers), pretože sú pre ostatných účastníkov vstupnou bránou na tieto trhy. Príklady – Facebook, Google, Apple, Amazon, Microsoft, IBM. A mnohé iné. Tieto súkromné podniky majú silnú sprostredkovateľskú pozíciu, keďže prepájajú veľké množstvo používateľov s veľkým počtom iných podnikov.

Ďalším problémom pre európskeho úradníka je najmä fakt, že deväťdesiat percent takýchto firiem nie je v európskom vlastníctve. Vytvoriť podmienky na vznik nových, čisto európskych firiem by bol beh na dlhé trate. Čo teda urobí typický úradník? Zreguluje existujúci trh. A nazve to „vytvorenie spravodlivých podmienok“ s oficiálnym označením zákon o digitálnych trhoch (DMA).

Komisia chce „prešetrovať“

Toto nové nariadenie má úprimnú a oneskorenú snahu priniesť spravodlivejšie podnikateľské prostredie pre komerčných používateľov vstupných brán. Používatelia sú proste od týchto brán závislí, ak chcú ponúknuť svoje služby na jednotnom trhu. Všetko smeruje k ochrane koncových spotrebiteľov, aby si mohli vyberať z lepších služieb a získať k nim prístup za spravodlivejšie ceny.

Tu niekde to však začína narážať na otázku zachovania bezpečnosti informácií.

Jedna z požiadaviek DMA je, že strážcovia nesmú brániť spotrebiteľom v prístupe k podnikom mimo ich platforiem. Na prvý pohľad to znie logicky. Avšak pri extenzívnom výklade tejto požiadavky z toho napríklad vyplynie, že platforma by už nesmela obmedzovať inštaláciu neotestovaného softvéru z nedôveryhodných zdrojov.

Tento bezpečnostný problém má názov

Nazýva sa *sideloading*.

Ak teda nejaký strážca mal doteraz štandardný proces posudzovania a testovania bezpečnosti nových aplikácií, bude povinný povoliť sideloading, t. j. inštaláciu akéhokoľvek softvéru. Dôraz je na slove *akéhokoľvek*.

Každý slušný prevádzkovateľ systémov má už dávno v rámci manažmentu IT služieb zavedené dva procesy zásadné pre kybernetickú bezpečnosť: riadenie konfigurácií a riadenie vydaní softvéru. Tu sa do životného cyklu softvéru napevno zabudujú princípy bezpečnostného testovania a princípy riadenia verzií softvéru, ktoré zaručia, že sa do systému „zboku“ nedostane žiadna skrytá háveď.

Zraniteľnosť systémov vychádza z ľudskej podstaty. Omylní sú architekti aj programátori systémov, administrátori aj projektoví špecialisti. Žiaden systém, ktorý kedy človek navrhol a postavil, nebol nikdy bezchybný.

Sme preto povinní urobiť všetko, aby sme odhalili maximum možných zraniteľností ešte skôr, než sa softvérová aplikácia začne používať. Ale bez otestovania nikdy nezistíme, či je naozaj bezpečná.

Ak sa legislatívny proces naštartuje v tejto podobe, trh a vnímanie bezpečnosti sa navždy zmenia. Povolenie *sideloading* sa totiž dotkne odhadom miliardy používateľov.

Protijablčný zákon

Povedzme si otvorene – problém sa síce týka viacerých platforiem, ale najviac proti kontroverznému návrhu bojuje firma Apple Inc. K problematike sideloadingu vydala samostatnú štúdiu.

Dokument zhromažďuje aktuálne čísla od európskych agentúr, ktoré uvádzajú 230-tisíc vzoriek malvéru denne. Rozhodne najpopulárnejším sa stalo porovnanie Apple – Android, ktoré uvádza, že za ostatné štyri roky zaznamenali zariadenia na platforme Android 15- až 47-krát viacej škodlivého softvéru ako iOS.

Argumenty proti *sideloadingu* sa začínajú ochranou používateľov pred ransomvérom či kradnutím hesiel a prístupov. A končia sa vyčíslením miliardových strát súvisiacich s ochranou duševného vlastníctva a podnikania na technologickom a reklamnom trhu.

ALISON

***

Building a Trusted Ecosystem for Millions of Apps

A threat analysis of sideloading, October 2021

***

Podľa predstaviteľov firmy by umožnenie inštalácie mobilných aplikácií z nedôveryhodných zdrojov mimo App Store mohlo zásadne ohroziť bezpečnosť zariadení Apple.

Európska komisia, ktorá návrh DMA predkladá, tvrdí, že orgány budú mať lepšie prostriedky na ochranu občanov, keďže budú na platformy dohliadať a spoločne presadzovať pravidlá v celej Únii.

Aká môže byť realita

Tá najhoršia? Prevádzkovatelia vstupných brán stratia väčšinu možností, ako overiť bezpečnosť aplikácií inštalovaných do ich platforiem.

Regulácia totiž v sebe obsahuje aj sankcie. V tomto prípade pri nedodržaní pravidiel DMA budú hroziť pokuty do výšky desať percent celkového celosvetového ročného obratu spoločnosti alebo penále do výšky päť percent priemerného denného obratu.

Či sa šéfovi Applu podarí citlivo vysvetliť európskym politikom, že spolu s vaničkou vylievajú aj dieťa, to si zatiaľ odborníci netrúfajú ani odhadnúť.