http://www.blesk.cz/clanek/zpravy-live-zpravy/500484/vedci-z-brna-nasli-slabinu-pri-generovani-kryptografickych-klicu.html

Vědci z Brna našli slabinu při generování kryptografických klíčů

17. října 2017 ● 16:28

Brněnským vědcům se podařilo odhalit vážné bezpečnostní riziko spojené s čipy německého výrobce Infineon Technologies. Jde o způsob, jakým se generovaly kryptografické klíče pro široké spektrum zabezpečených zařízení. "Z veřejné klíče části bylo možné získat jeho tajnou hodnotu," řekl dnes ČTK Petr Švenda z Masarykovy univerzity. Problém se týká i Slovenska.

Vědci už výrobce o problému informovali na začátku roku a nyní, s dohodnutým časovým odstupem, výzkumníci z fakulty informatiky o svém zjištění informovali veřejnost.

Společnost Infineon Technologies dnes ČTK sdělila, že ji na problém spojený se softwarem vědci upozornili letos v únoru. Potíže podle ní mohou vzniknout jen při kombinaci několika faktorů a týkají se jen malé části produktů. O záležitosti firma podle svého vyjádření okamžitě informovala klienty, příslušný software aktualizovala. Aktualizovaný software nyní prochází certifikací a je zaváděn do výroby.

Čipy z Infineonu se používají v mnoha různých zařízeních, třeba v elektronických dokladech v Estonsku, což je pionýrská země v oblasti digitální komunikace. Výzkumníci podle Švendy nemají informace, že by slabinu objevil také někdo jiný a stihl ji zneužít.

Přesto jde prý o poměrně závažné zjištění. "Díra v zabezpečení" existovala několik let a potenciálně se dotkla velkého množství různých zařízení. Brněnští výzkumníci vytvořili a dali veřejnosti k dispozici nástroj, jehož prostřednictvím mohou lidé zjistit, zda rizikový čip mají také oni. V českých elektronických dokladech se ale používají jiné, zdůraznil Švenda.

Občanské průkazy se zmiňovaným čipem se naproti tomu vydávají na Slovensku, kde letos v létě začaly úřady komunikovat s firmami až na výjimky elektronicky. Zástupci podniků se do datových schránek dostanou právě například s využitím občanského průkazu s čipem. Elektronický podpis si na pětimilionovém Slovensku aktivovalo asi 300.000 lidí.

Slovenské ministerstvo vnitra v reakci na informace vědců uvedlo, že k plošné výměně občanských průkazů s čipem v zemi nedojde, úřad ale připravuje změny, aby odstranil hrozbu zneužití zmiňovaného bezpečnostního rizika.

"Ministerstvo vnitra upozorňuje, že když si držitel elektronického občanského průkazu důsledně chrání svůj bezpečnostní osobní kód BOK, není důvod k panice. Elektronická komunikace v prostředí slovenského e-Governmentu si totiž vyžaduje opakované přihlašování přes BOK při používaní elektronického podpisu, což je jindy terčem kritiky," sdělilo dnes ČTK ministerstvo, podle kterého při dodržení zásad bezpečnosti není používání elektronického podpisu ohroženo.

Ministerstvo uvedlo, že podle dosavadních informací je možnost rizika vzniku bezpečnostního problému pouze teoretická a vyžadovala by nasazení 640 serverů během jednoho roku. Navzdory tomu úřad hodlá v krátké době zvětšit vytvářený kryptografický klíč a ve střednědobém výhledu zamýšlí změnit celý algoritmus jeho vytváření.

Patřičné kroky podnikly také estonské autority nebo společnost Microsoft.

Autor: ČTK

Více na http://www.blesk.cz/clanek/zpravy-live-zpravy/500484/vedci-z-brna-nasli-slabinu-pri-generovani-kryptografickych-klicu.html?utm_source=blesk.cz&utm_medium=copy