http://www.dnes24.sk/elektronicke-obcianske-preukazy-maju-bezpecnostnu-chybu-utocnik-moze-sfalsovat-podpis-282061

Elektronické občianske preukazy majú bezpečnostnú chybu: Útočník môže sfalšovať podpis

Tím expertov odhalil vážne bezpečnostné nedostatky elektronických občianskych preukazov. O citlivé dáta môžu prísť aj Slováci.

Aktualizované 17. október 2017 2017 15:46 Lucia Šútorová

Zdroj: Policajný zbor SR

Na mimoriadne vážny bezpečnostný problém prišiel vedecký tím z Masarykovej univerzity v Brne s tromi slovenskými bezpečnostnými expertmi Matúšom Nemcom, Marekom Sýsom a Dušanom Klincom, ďalej sú v ňom Petr Švenda a Vašek Matyáš. Informoval o tom web dsl.sk. ***„Útočník môže za splnenia predpokladov a zainvestovania do útoku sfalšovať***

dokonca kvalifikovaný elektronický podpis občana, ktorý je ekvivalentom vlastnoručného podpisu,“ uvádza sa na stránke dsl.sk.

V čom je problém?

Problémom sú podľa portálu dsl.sk populárne hardvérové kryptografické čipy od popredného výrobcu Infineon, ktoré generujú slabé kľúče pre asymetrický šifrovací algoritmus RSA. Útočníci môžu získať privátne kľúče, ktoré umožňujú napríklad falšovať elektronické podpisy či prihlasovať sa.

Zraniteľné čipy sú podľa dsl.sk použité aj na slovenských elektronických občianskych, tzv. eID kartách. ***„Znamená to, že ktokoľvek kto sa dostane k verejnému kľúču občana napríklad z jeho kvalifikovaného podpisu ľubovoľného dokumentu si vie po zainvestovaní zatiaľ potrebných 20 až 40 tisíc dolárov vypočítať privátny kľúč kvalifikovaného certifikátu obyvateľa,“*** píše sa na webe dsl.sk.

Ministerstvo o probléme vie

Ako dodáva dsl.sk útočník tak zrejme vie vytvoriť technicky platný kvalifikovaný podpis tohto obyvateľa pod ľubovoľným dokumentom. Dobrou správou podľa dsl.sk je, že ani verejné kľúče sa zrejme nedajú aspoň podľa avíza vlastností eID získať z občianskych bez zadania šesťciferného kódu BOK. Získaním fyzického prístupu k eID tak verejné kľúče obyvateľa nie je možné získať.

Podľa portálu dsl.sk ministerstvo vnútra SR, ktoré má na starosti vydávania eID, o probléme vie a robí opatrenia na jeho elimináciu.

PREČÍTAJTE SI AJ

Policajná akcia Shark: NAKA obvinila 63 osôb z ekonomickej trestnej činnosti

Polícia obvinila Bulhara: Na Slovensko sa mal pokúsiť previezť piatich Afgancov

Stanovisko ministerstva vnútra

Svoje stanovisko nám zaslalo aj Ministerstvo vnútra SR, ktoré upozornilo, že ak si držiteľ elektronického OP dôsledne chráni svoj bezpečnostný osobný kód BOK, nie je dôvod na paniku. ***„Elektronická komunikácia v prostredí slovenského e-Governmentu si totiž vyžaduje opakované prihlasovanie cez BOK pri používaní elektronického podpisu, čo je***

inokedy terčom kritiky. Pri dodržaní zásad bezpečnosti nie je používanie elektronického podpisu ohrozené,“ uvádza ministerstvo vnútra.

„Možnosť vzniku bezpečnostného problému je podľa dosiaľ zverejnených informácií len teoretická a vyžadovala by si dlhodobé nasadenie 640 serverov počas obdobia 1 roka. Okrem toho, dosiaľ všetky bezpečnostné certifikáty vydané certifikačnými autoritami BSI /Bundesamt fur Sicherheit in der Informationstechnik/ a NBÚ SR sú platné,“ dodáva ministerstvo vnútra.

Pracujú na riešení

Ministerstvo vnútra zároveň potvrdilo, že sa pracuje na riešení na eliminácii možností zneužitia. ***„Držitelia elektronických OP si svoje doklady nebudú musieť meniť. Ak však považujú riziko za vysoké, môžu certifikáty pre tvorbu kvalifikovaného elektronického podpisu zneplatniť využitím buď využitím elektronickej služby alebo na oddelení dokladov,“*** uvádza Ministerstvo vnútra SR.

„V krátkodobom horizonte eliminujeme riziko zväčšením generovaného kľúča a v strednodobom horizonte zmeníme celý algoritmus jeho generovania. Pri obnove a generovaní nových komponentov pre tvorbu kvalifikovaného elektronického podpisu v maximálnej miere využijeme elektronické služby,“ píše sa v závere stanoviska MV SR k ohrozenej bezpečnosti certifikátov pre elektronický podpis na občianskych preukazoch s čipom.

Foto: ilustračné