Víkend HN, 8. 10. 2010

Strážce klíče

Na první pohled by to do něj člověk neřekl, ale Ondřej Surý je jednou z klíčových postav internetu: patří mezi sedm "důvěryhodných zástupců internetové komunity" na světě. Díky tomu dostal od organizace ICANN, která dohlíží na bezpečnost internetu, čipový klíč umožňující v případě potřeby obnovu jeho zabezpečení.

Kam jste uložil startovací klíč?

Do bezpečnostní schránky v bance.

Ve které bance?

To nemůžu říct. Můžu vás jen ujistit, že jsem vybral takovou, kde měli volné bezpečnostní schránky. V tomto procesu figuruji jako zástupce CZ.NIC, ale zodpovědnost za ochranu klíče leží jenom na mně.

Můžete mi přiblížit, o jaký druh ochrany internetu, jíž se zabýváte, se vlastně jedná?

Systém DNS, kterým se dlouhodobě zabýváme, je jedna z hodně důležitých součástí internetu, která běží jakoby na jeho pozadí. Když do počítače napíšete jakékoliv doménové jméno, tak se převede na číselnou adresu, které počítače rozumějí. Překlad doménových jmen na číselné adresy je hlavní princip DNS. Protokol DNS je hierarchický. Když si vezmete známé domény jako ".cz", ".com", ".eu" nebo ".org", tak nad nimi je jakási neviditelná tečka, která se nikde nepíše, říká se jí kořenová zóna. Kdyby došlo k nějakému problému při poskytování služby kořenové zóny, tak by přestal fungovat jmenný překlad.

A co by to konkrétně znamenalo?

Kdybyste napsal do prohlížeče požadovanou adresu, tak by se vám nezobrazily požadované webové stránky, nedostal byste se na žádnou z nich. Veškeré překlady jmen na čísla by přestaly fungovat. DNSSEC - zabezpečení DNS, kterému se hodně věnujeme a u jehož zavedení do kořenové zóny jsem měl možnost být, brání podvržení údajů uložených v DNS.

Jaké potíže by hrozily, kdyby bylo DNS nezabezpečené?

Systém DNS funguje na volnější bázi, takže do něj teoreticky může dobře vybavený útočník vstoupit a změnit to, co jde po drátě do serveru, který poskytuje služby. Představte si například stránky s burzovními informacemi, na které se jdete podívat. Útočník vás přesměruje na vlastní, falešné stránky, kde zveřejní zavádějící informace, aby vyvolal reakci, kterou očekává. Začnete prodávat nebo nakupovat na základě nepravdivých informací. Klasickým cílem útoku je pochopitelně vysát někomu konto. Nevím, do jaké míry je mezi uživateli jasné, že když jdou něco nakupovat přes internet, tak při zadávání citlivých informací, jako je například číslo kreditní karty, by měli dbát na zabezpečení a důvěryhodnost stránek. Řekl bych, že velká část lidí, když vyběhne nějaký dialog o tom, že certifikát stránky je neplatný, ho přesto odkliknou a jdou klidně dál.

Klíč, který jste získal, má sloužit k nastartování ochrany internetu v případě živelní pohromy nebo útoku. Jaká živelní pohroma by mohla internet ohrozit?

Hlavní klíč ke kořenové zóně je uložený v zařízení, které se jmenuje HSM, to je zkratka z Hardware Security Module. Toto zařízení má certifikaci FIPS 140-2 Level 4, což například znamená, že se nesmí přehřívat natolik, aby bylo zvenčí poznat, že se něco uvnitř děje. Mezi další sledované parametry ohrožení patří například příliš vysoká nebo nízká teplota prostředí nebo extrémní otřesy. V případě, že nastanou takto nestandardní podmínky, tak se obsah zařízení vymaže.

Kolik lidí na světě je podle vás schopno masivně zaútočit na celý systém internetu?

Kdyby tady takový člověk byl, tak už by to nejspíš udělal. Na kořenové servery se čas od času útočí, ale když jich je třináct a jsou duplikované, běžná veřejnost to ani nezaznamená.

Jak se člověk stane důvěryhodnou osobou, která může dostat "obnovovací" klíč?

Beru to jako významné ocenění pro celý CZ.NIC za práci, kterou na poli zabezpečení domén děláme. Česká republika byla teprve pátou zemí na světě, která zabezpečila DNSSECem svou národní doménu, tedy .CZ. Můžu říct, že v současné době jsme, co se týče DNSSECu, velmoc, protože jím máme zabezpečeno více než sto tisíc domén s koncovkou .CZ. To je přibližně jedna sedmina všech domén v

našem registru. Mimochodem, Economia byla jednou z prvních firem, jejíž internetové stránky, tedy například respekt.cz, ihned.cz nebo ekonom.cz byly "podepsány" DNSSECem. Dnes máme víc zabezpečených domén než zbytek světa dohromady.

Ochranu internetu má na starosti ICANN, soukromá společnost. Proč to není třeba pod OSN?

Je to dáno historicky. Internet vznikl na amerických univerzitách, a protože se o něj ve Státech starají tak, jak mají, není důvod, aby se jeho správa stěhovala. V posledních několika letech se ICANN čím dál více otevírá světu, je na něj v tomto směru vyvíjen pochopitelný tlak. U podpisu kořenové zóny figurovalo celkem jednadvacet zástupců komunity, kteří byli vybráni z celého světa, aby se ukázalo, že se jedná o otevřený proces, v němž má zbytek světa také svoje slovo. Samozřejmě by ten podpis zvládli sami, ale díky tomu, jak to nakonec udělali, ukázali všem, že nejsou žádná uzavřená a autoritářská organizace. Ani z technického hlediska nebylo nutné, aby ICANNu někdo asistoval; mohli mít vše důležité zamčené v trezoru, na bezpečnosti celé té věci by se v zásadě nic nezměnilo. Mimochodem, organizace ICANN byla původně řízena americkou vládou. Až minulý rok došlo ke změně smlouvy upravující vztahy mezi úřady Spojených států a světem v souvislosti se správou internetu.

Co je k tomu najednou vede?

Směrování k větší otevřenosti plyne z rozšiřování internetu na celém světě a snahy zapojit do procesu správy internetu všechny zúčastněné hráče. Nejedná se o proces, který by se udál z ničeho nic, jde o záležitost, která trvá již delší dobu a která pouze vyvrcholila v poslední době. Cílem všech uživatelů internetu je mít jednotný internet, a jednou z nejhorších věcí, která by se mohla stát, by bylo rozštěpení internetu na menší národní sítě, které by nebyly vzájemně propojeny.

To je možné?

Kupříkladu technologie, která se používá pro digitální podpisy, vychází převážně z americké šifry. Rusko si ale prosadilo, že v systému bude mít svoji vlastní šifru. To ale samozřejmě nevadí, protože se jedná o veřejné standardy, které spolu můžou komunikovat. Kořenová zóna má servery, které ji obsluhují. Těch je z důvodů stability více. Rusové jsou ale podle mě schopni říct: "Teď používejte jen naše servery, a ne ty, které

vám dávají Spojené státy." V tu chvíli by mohlo dojít k rozštěpení internetu, čímž by se vytratila jedna z jeho výhod - jeho globálnost.

Co si představíte, když se řekne internet? To slovo je staré třiadvacet let.

Vybaví se mi informace. Pro mě je to externí paměť. Když potřebuji najít informaci, tak jdu na internet. Internet jsou ale i špatné, zkreslené a nepravdivé údaje. To už je ale jiná diskuse.

Jistě. Na jednom diskusním fóru, které proběhlo poté, co byla uveřejněna informace, že jste se stal držitelem klíče, se psalo, že jste estébák. Jak jste na to reagoval?

To mě pobavilo. Vyloženě jsem se smál. Když byla sametová revoluce, chodil jsem do sedmé třídy. Jak jsem to mohl stihnout? Taky jsem se dozvěděl, že jsem konfident BIS a školím bezpečnostní služby v informatice. Tyhle debaty s anonymy se nedají vyhrát, ve chvíli, kdy přejdou do osobního útoku, potom přestávám diskutovat. Já svoje názory zásadně podepisuji. Jako chybu vidím, že jsem se na tu diskusi vůbec podíval.

Zkvalitňuje podle vás internet obecně život?

Ve studiu určitě. K dispozici je neuvěřitelné množství informací, které můžete využít, ale na druhou stranu to vede k tomu, že lidé zpohodlňují a nemusí si toho tolik pamatovat. U sociálních sítí je těžké určit, do jaké míry zkvalitňují život... v mém případě jsem si jist, že mi ho nezhoršují. Je potřeba si jen dávat pozor, co člověk pouští ven, protože jsou informace, které na Facebook určitě nepatří. Některé věci se dají říct u piva kamarádům, ale neměly by se už dávat na Facebook. Pravdou také je, že sociální sítě jsou zneužitelné represivním režimem, ale na druhou stranu se informace o zločinném režimu můžou díky nim dostat ven, jako se to povedlo v Íránu.

Autor rozhovoru:
Petr Volf, Hospodářské noviny