Metro, 27. 9. 2010

V krizi se síť řešit nebude

Patří mezi sedm vyvolených, kteří v případě nouze opět zprovozní internet Alespoň tak se o Ondřeji Surém psalo v tisku. Zeptali jsme se ho, jaká je ve skutečnosti jeho role a v čem spočívá.

Bezpečnost internetu od léta střeží sedm pečlivě vybraných odborníků z celého světa. Před časem v USA převzali „klíče k internetu“, jak těmto kartám začala světová média přezdívat. Jedním z vyvolených se stal i Ondřej Surý. „Je to spíš jako zašifrovaná záloha,“ upřesňuje v rozhovoru pro deník Metro.

Lze vůbec tu situaci kolem klíčů nějak laicky vysvětlit?

Když na internetu napíšete třeba www.metro.cz, takzvaný DNS protokol přeloží nějaké číslo, kterým počítače rozumí. A ten váš pak ví, ke kterému serveru se má vlastně připojit. Tenhle protokol je jeden z těch nejdůležitějších, který na pozadí internetu běží, aniž o tom běžní uživatelé vědí. Dodnes ale nebyl zabezpečený. Pokud by nějaký útočník chtěl, tak může uživateli podvrhnout cizí adresu, a vy se tak připojíte na cizí server. Třeba v případě Metra to pak může zneužít například k vyvolání nějaké paniky skrze smyšlenou zprávu - například, že prezident zemřel. K tomuto protokolu se tedy přidala nová technologie s bezpečnostními podpisy. DNS je jako stromeček. Úplně na vrcholu je něco, co se jmenuje kořenová zóna - jakýsi centrální bod, kde jsou všechny ty informace uložené. Právě tato zóna se podepsala a její důležitost spočívá v tom, že zde začíná zabezpečení veškerých ostatních domén.

A v čem spočívá vaše role?

To, co držím já a těch zbylých šest lidí, je část klíče, kterým je zašifrovaná záloha toho hlavního klíče kořenové zóny. My sami tedy doslova žádný klíč nemáme. Je to, jako by si člověk zálohoval data na počítači a ta pak nějak zašifroval.

Společně pak můžete obnovit běh internetu...

K tomu, aby se tato záloha obnovila, je potřeba, aby se sešlo v USA alespoň pět ze sedmi lidí, kteří ten klíč, jak vy říkáte, dostali. Tak se obnoví provoz ve chvíli, kdy dojde k selhání základních bezpečnostních zařízení, jež běžně existují.

Máte klíč fyzicky u sebe?

Je to v podstatě bezpečnostní karta o velikosti kreditky, která má na sobě čip. Já osobně ji mám uloženou v bezpečnostní schránce v bance.

Jsou na to nějaká pravidla, kde mít klíč uložený?

Bylo nám doporučeno, abychom jej měli na nějakém bezpečném místě. Bezpečnostní schránka je především moje pojistka. Kdyby mi kartu někdo ukradl, byla by to moje ostuda.

Kdyby je někdo ukradl všechny, stane se něco?

Věcí, které by potenciální zloděj musel udělat, je opravdu strašně moc. A možný zisk je oproti vynaloženým nákladům a riziku minimální. Mnohem jednodušší je dnes napadnout koncové stanice uživatelů.

Proč se držitelé klíčů musejí setkat osobně?

Praxe ukazuje, že zabezpečení funguje nejlépe, když se ti lidé musejí fyzicky někam dostavit. Navíc potřebujete ještě to bezpečnostní zařízení, do kterého se záloha nahraje a rozšifruje právě našimi klíči.

Proč jste byl vybrán právě vy jako jeden z držitelů?

Šlo především o to, aby byly geograficky zastoupeny určité regiony, a dalším vodítkem bylo, že klíč dostali zástupci organizací, jež se o technologii DNS dlouhodobě zajímají. My třeba máme v Česku nejvíc zabezpečených domén na světě v poměru k nezabezpečeným.

Zkoušeli jste si to obnovení třeba nanečisto?

Organizace ICAAN, která jej má na svědomí, celou ceremonii zkoušela dvanáctkrát. My jsme se účastnili až ostré verze. Ale když jsme třeba k procesu měli nějaké připomínky, tak je často zohlednili.

Co se musí stát, abyste se ujal své role?

Já osobně si myslím, že k tomu vlastně nikdy nedojde. Ta pravděpodobnost je totiž velmi nízká. Stávající klíč je uložen celkem ve čtyřech zařízeních. Kdyby došlo k jejich poškození, tak by to asi nebylo teroristickým útokem, ale spíš chybou softwaru. Teprve kdyby byla vymazána všechna, museli bychom se sletět my.

Kdyby se někdo snažil napadnout bezpečnost kořenové zóny, jak by to vypadalo?

Nemělo by to vážnější následky. Znamenalo by to nutnost výměny klíče pro kořenovou zónu a komplikace pro správce.

Klíč máte doživotně, nebo se musí obnovit?

Zálohu bych měl držet po dobu platnosti klíče, tedy dva až pět let. Pokud se něco nezmění, někdo třeba šifru neprolomí. Každoročně ale bude fungovat nějaká procedura, aby se ověřilo, že ten klíč mám v držení. Třeba se budu muset vyfotografovat s dnešními novinami nebo s nějakým heslem, které dostanu.

Vy osobně se tedy nebojíte, že budete muset někdy tu svou kartu využít?

Já se domnívám, že kdyby skutečně došlo ke zničení těch současných klíčů a došlo k nějaké opravdu krizové situaci, asi bychom řešili úplně něco jiného, než je fungování internetu.

Kdo to je

Ondřej Surý je jako vedoucí Laboratoří CZ. NIC odpovědný za desetičlenný tým, jehož hlavním úkolem je hledat možné problémy spojené s bezpečností a stabilitou internetu. Studoval Informatiku na Matematicko-fyzikální fakultě Univerzity Karlovy v Praze. Rád plave a jezdí na kole a také se věnuje charitativním projektům. V dubnu 2009 byl zvolen do kontrolní a revizní komise Amnesty International v Česku. Je rovněž zakladatelem českého lokálního týmu Ubuntu Linux.

Autor rozhovoru:
Jiří Bigas, Metro