Bezpečné domény pro bezpečné elektronické služby veřejné správy

Mgr. Jiří Průša, sdružení CZ.NIC

Začátkem letošního roku se v médiích čím dál tím více začala skloňovat kybernetická bezpečnost, ať již se jednalo o připravovaný zákon nebo útoky, které na několik hodin významně omezily dostupnost předních zpravodajských serverů. Ve stínu stále častějších DDoS útoků však malinko zapadá do pozadí **ochrana koncových uživatelů**, kteří mohou být vystaveni novým sofistikovaným útokům. Jejich následkem pak může dojít např. ke zneužití přihlašovacích údajů včetně e-mailu či platebních karet. Jak ukázaly první březnové dny, nikdy nevíme, kdy jaký útok může přijít. Podobně jako v jiných oblastech však náskok mají Ti, kteří jsou připraveni.

DNSSEC a ochrana na straně uživatelů

Mezi široké veřejnosti méně známé typy útoků patří ty, při nichž se útočník dostane mezi dva vzájemně komunikující počítače (tzv. man-in-the-middle), Může tuto komunikaci odposlouchávat a případně pozměnit. S takovýmto typem útoku se můžeme setkat rovněž v případě, kdy chceme zobrazit vybranou internetovou stránku (např. www.mojedatovaschranka.cz) a do série dotazů, při kterých je vyhledávána IP adresa daného serveru, se dostane neznámý útočník. Uživateli sedícímu u počítače se pak zobrazí jiná stránka, než kterou požadoval, ale se stejnou adresou (viz schéma).

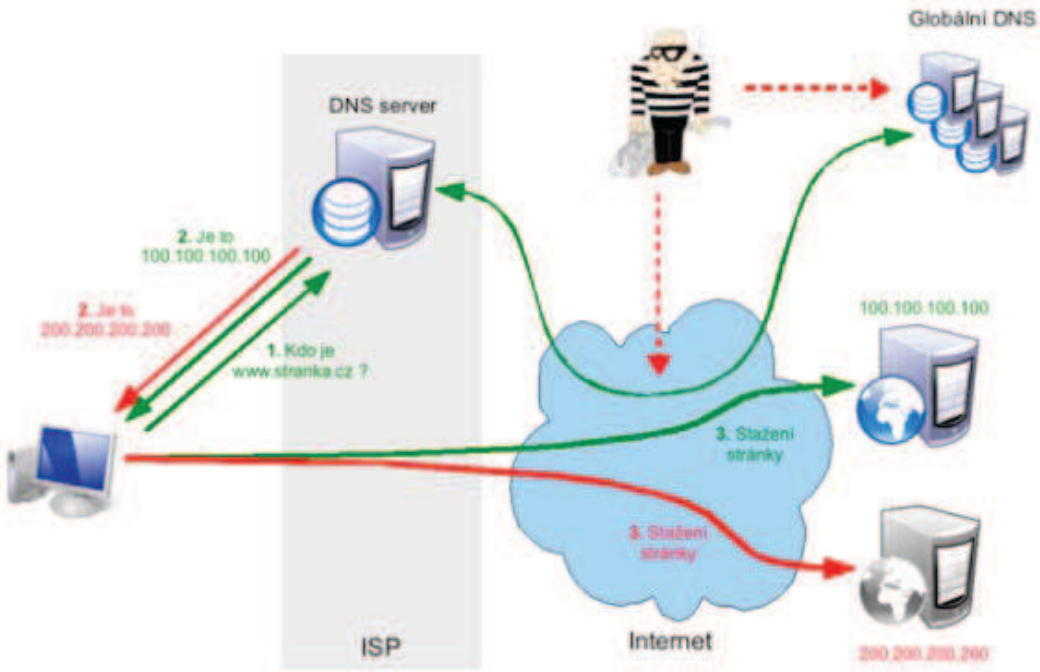


Schéma: sdružení CZ.NIC; www.dnssec.cz

Vzdáleně lze tento typ útoku **přirovnat** k tzv. **phishingu**, při kterém je však uživatel přesměrován na graficky stejný nebo obdobný web, avšak s jinou adresou. Nebezpečí při podvržení dotazů v rámci systému doménových jmen (DNS) je o to závažnější, že uživatel má jen omezené možnosti poznat, že byl přesměrován na jinou stránku.

Jednou ze spolehlivých možností, jak získat jistotu, že se mi zobrazila skutečně ta stránka, kterou požaduji je využití **technologie DNSSEC.** DNSSEC představuje rozšíření systému doménových jmen, které zvyšuje jeho bezpečnost a poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC rovněž reaguje na vývoj v oblasti Internetu, kdy původní architektura DNS vznikala v době, kdy k této počítačové síti bylo připojeno poměrně malé množství uživatelů, jednotliví poskytovatelé se vzájemně znali a mezi uživateli panovala vzájemná důvěra a zájem o spolupráci, nikoliv narušování

vzájemných vztahů. To již nelze říci v dnešní době, kdy se Internet bohužel stává účinným nástrojem pro zviditelnění vybraných zájmových či politických skupin, které neváhají k prosazení svých zájmů využít i kybernetických útoků.

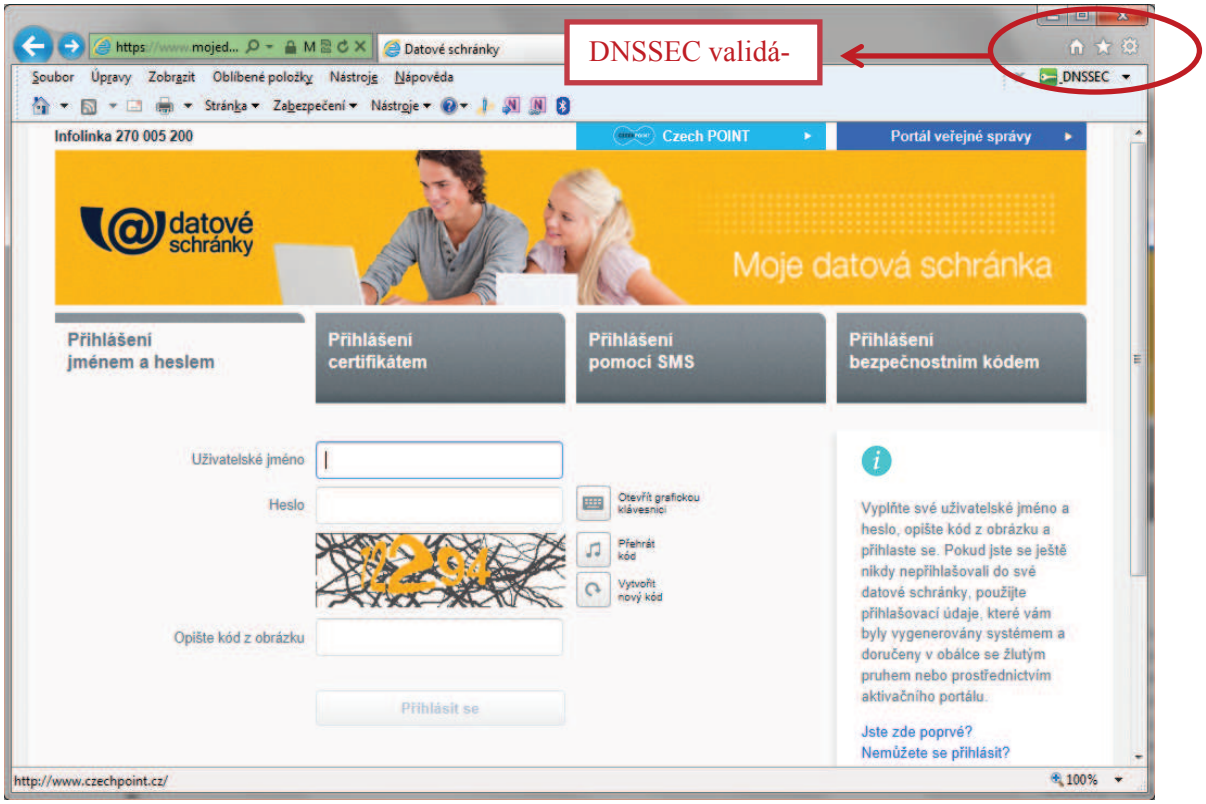
Implementace technologie DNSSEC a její nasazení tak, aby uživatel měl skutečnou jistotu, že se mu zobrazila webová stránka, kterou požadoval, je podmíněna zapojením celé řady subjektů. Vedle správce národní domény (případně jiné domény nejvyššího řádu jako je .com či .info) vyžaduje rovněž zapojení poskytovatelů připojení k Internetu, poskytovatelů obsahu a v neposlední řadě koncových uživatelů, kteří musí mít jednoduchou a uživatelsky přívětivou možnost zjistit, zda je daná stránka prostřednictvím této technologie zabezpečena.

DNSSEC a koncový uživatel

Pro koncového uživatele je důležité ověření zda jeho poskytovatel připojení k Internetu (ISP) tuto technologii podporuje, tj. zda ověřuje příslušné podpisy, a zda je zabezpečena i stránka, resp. doména, kterou právě vidí ve svém prohlížeči. Pro zjištění obou informací je možné použít jednoduchých nástrojů vyvinutých sdružením CZ.NIC, správcem národní domény.

Pro test **zabezpečení internetového připojení** stačí zobrazit stránku www.dnssec.cz s tím, že pokud se v pravé horní části zobrazí ikonka zeleného klíče, daný poskytovatel (např. Telefonica O2) danou technologii podporuje.

Pro kontrolu **zabezpečení** (podepsání) konkrétní **domény** je nejvhodnějším způsobem jednoduchá instalace tzv. plug-inu (rozšíření pro Váš prohlížeč) v podobě **DNSSEC validátoru**. Ten je možné si bezplatně získat na stránkách Laboratoří CZ.NIC[9]. V současné době je plug-in dostupný pro všechny nejpoužívanější prohlížeče, tj. Internet Explorer, Mozilla Firefox i Google Chrome. Po instalaci příslušného doplňku se pak uživateli při procházení stránek přímo v prohlížeči zobrazuje informace, zda je daná stránka zabezpečena DNSSEC (ikona zeleného klíčku) či ne (červený klíček).



Obr. 1: Ukázka domény zabezpečené prostřednictvím DNSSEC

[9] https://labs.nic.cz/page/1253/dnssec-validator-2.0-pro-webove-prohlizece/

DNSSEC pro provozovatele elektronických služeb

Pro provozovatele elektronických služeb jakými jsou např. jednotlivá ministerstva či městské a obecní úřady je důležité, aby svoji doménu podepsali pomocí technologie DNSSEC a uživatelům se tak prostřednictvím DNSSEC validátoru zobrazovala jako zabezpečená.

U DNSSEC hraje hlavní roli registrátor jeho domény. V současné době DNSSEC podporuje celkem 11 registrátorů (Web4U; IGNUM; Kraxnet; Zoner software, Active 24; General Registry, Banan; OneSolution; TELE3; ONE.CZ a AERO Trip Pro) s tím, že pravidelně aktualizovaný seznam registrátorů včetně toho, zda podporují i další technologie jako IPv6 či mojeID je možné nalézt na stránkách[10] správce národní domény, sdružení CZ.NIC.

Vlastní proces zabezpečení domény se pak skládá ze tří kroků:

- **Vygenerování klíčů**, kdy pro zvýšení bezpečnosti a zvýšení výkonu DNSSEC používá dva druhy klíčů: Klíč podepisující zóny (ZSK) používaný k podpisu dat v zóně. Vzhledem ke kratší délce klíče je nutné jej častěji měnit tak, aby nemohlo dojít k jeho prolomení zejm. za pomoci automatických nástrojů. Klíč podepisující klíče (KSK) se používá k podpisu klíče podepisujícího zóny. Tento klíč je delší a není nutné jej proto tak často měnit.
- **Podepsání záznamů** v zóně Vaší domény, kdy vytvořené podpisy budou uloženy přímo vedle podepisovaných záznamů do zónového souboru (jako další typ DNS záznamu). To samozřejmě není nutné dělat ručně, ale je možné provést automaticky nástroji na podepisování zón.
- **Vypublikování DS záznamů** do registru domén .cz za pomoci Vašeho registrátora.

V případě, že Váš registrátor je rovněž správcem Vašich DNS serverů (zejm. v případě, že Vám zajišťuje rovněž web-hosting) by nemělo být problém, aby výše uvedené kroky zvládl on sám s minimální součinností z Vaší strany.

Jak jsou zabezpečeny elektronické služby veřejné správy?

V rámci podpory nových technologií provedlo sdružení CZ.NIC unikátní průzkum zaměřený na to, zda mají jednotlivé orgány veřejné správy své webové stránky (a na nich dostupné elektronické) služby zabezpečené prostřednictvím DNSSEC.

V rámci průzkumu, během kterého jsme ověřovali podporu této technologie u celkem 250 domén orgánů veřejné správy, jsme se zaměřili jak na ministerstva a ústřední orgány státní správy, případně další instituce jako je Poslanecká sněmovna, Senát, ČNB či NBÚ, tak krajské úřady a nejvýznamnější města a obce.

Výsledky tohoto průzkumu ukázaly, že svoji doménu má za pomoci technologie DNSSEC zabezpečeno pouze 28 %, což je o téměř 10 % méně, než činí průměr všech domén .cz[11]. V přehledu pak uvádíme příklady těch úřadů, které pro ochranu svých návštěvníků DNSSEC využívají:

Ministerstva:

- Ministerstvo financí (www.mfcr.cz)
- Ministerstvo kultury (www.mkcr.cz)
- Ministerstvo pro místní rozvoj (www.mmr.cz)
- Ministerstvo školství mládeže a tělovýchovy (www.msmt.cz)

Ústřední orgány státní správy

- Český telekomunikační úřad (www.ctu.cz)
- Státní úřad pro jadernou bezpečnost (www.sujb.cz)
- Úřad pro ochranu hospodářské soutěže (www.compet.cz)

[10] http://www.nic.cz/whois/registrars/list/1/
[11] https://stats.labs.nic.cz/stats/domains_by_dnssec/

Krajské úřady

- Ústecký kraj (www.kr-ustecky.cz)
- Královéhradecký kraj (www.kr-kralovehradecky.cz)
- Kraj Vysočina (www.kr-vysocina.cz)
- Moravskoslezský kraj (www.kr-moravskoslezsky.cz)

Města a obce s rozšířenou působností

- Beroun (www.mesto-beroun.cz)
- Kladno (www.mestokladno.cz)
- Neratovice (www.neratovice.cz)
- Vimperk (www.vimperk.cz)
- Děčín (www.mmdecin.cz)
- Trutnov (www.trutnov.cz)
- Konice (www.konice.cz)
- Holešov (www.holesov.cz)
- Opava (www.opava-city.cz)
- Mariánské lázně (www.marianskelazne.cz)

K většímu rozšíření DNSSEC v rámci veřejné správy včetně služeb eGovernmentu by měly přispět i dvě připravované vládní strategie: Digitální Česko 2.0 z dílny Ministerstva průmyslu a obchodu a Strategický rámec rozvoje veřejné správy a e-Governmentu 2014+ vznikající na půdě Ministerstva vnitra. Pokud by vláda následovala např. příklad při zavádění IPv6, má česká veřejná správa opět možnost dokázat své vedoucí postavení v Evropě. Naše národní doména .cz totiž patří k evropským i světovým lídrům v podpoře této technologie již dnes!