Webové stránky obce mají být bezpečné, i kvůli uživatelům

Dnes jsou čtyři z každých deseti webových stránek obcí s rozšířenou působností zabezpečeny prostřednictvím DNSSEC. Také rozšíření této technologie ve veřejné správě je dnes vyšší, než ve zbytku české domény.

Termín kybernetická bezpečnost se poslední dobou objevuje v médiích stále častěji, ať se jedná o zákon o kybernetické bezpečnosti nebo útoky nejrůznějších hackerských skupin. Metody útočníků jsou čím sofistikovanější, a podobně jako v jiných oblastech, náskok mají ti, kteří jsou připraveni. Ve stínu přibývajících DDoS (Distributed Denial of Service - útok vedený více počítači najednou) útoků je pak **ochrana koncových uživatelů**, kteří mohou být vystaveni novým sofistikovaným útokům.

Mezi méně známé typy útoků patří ty, při nichž se útočník dostane mezi dva vzájemně komunikující počítače. S tímto typem útoku se lze setkat i v případě, kdy chceme zobrazit vybranou internetovou stránku (např. www.tisa.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). Vzdáleně lze tento typ útoku přirovnat k tzv. phishingu, při kterém je 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.

Jistotu, že se zobrazila požadovaná stránka, zvyšuje technologie DNSSEC (Domain Name System Security Extensions). Ta představuje rozšíření systému doménových jmen (DNS), které poskytuje uživatelům jistotu, že informace, které z DNS získal, jsou úplné a jejich integrita nebyla při přenosu narušena.

DNSSEC PRONIKÁ DO VEŘEJNÉ SPRÁVY

Zatímco ministerstva a státní instituce mají povinnost zabezpečení svých domén nejpozději od 1. července 2015 danou usnesením vlády (Usnesením č. 982 ze dne 18. prosince 2013), na města a obce se toto usnesení ze své povahy nevztahuje. Vedle snahy poskytovat důvěryhodné informace může být pro část měst a obcí motivací snaha uspět v soutěžích o nejlepší web, kdy právě zabezpečení domény prostřednictvím DNSSEC je spolu s podporou nového internetového protokolu IPv6 již několik let součástí hodnotících kritérií v soutěži Zlatý Erb a od loňska též soutěže Parádní web.

Zabezpečení stránek prostřednictvím DNSSEC je ze strany samosprávy věnována stále větší pozornost - dnes již 4 z 10 obcí s rozšířenou působností mají své stránky zabezpečeny touto technologií. Rovněž její rozšíření ve veřejné správě je dnes vyšší, než ve zbytku české domény, přestože před asi dvěma lety tomu bylo naopak.

Ukázka domény zabezpečené prostřednictvím DNSSEC

JAK ROZPOZNAT ZABEZPEČENOU STRÁNKU?

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 kontrolu zabezpečení (podepsání) konkrétní domény je nejvhodnějším způsobem jednoduchá instalace tzv. plug-inu (rozšíření pro váš prohlížeč) v podobě DNSSEC validátoru (www.dnssec-validator.cz). 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).

DNSSEC PRO PROVOZOVATELE ELEKTRONICKÝCH SLUŽEB

Pro provozovatele elektronických služeb, jakými jsou např. jednotlivé městské a obecní úřady nebo ministerstva, 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 12 registrátorů (Web4U; IGNUM; Stable.cz; 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 správce národní domény, sdružení CZ.NIC.

Vlastní proces zabezpečení domény se pak skládá ze tří kroků:

- **Vygenerování klíčů**, pro zvýšení bezpečnosti a zvýšení výkonu DNSSEC se používají dva druhy klíčů: klíč podepisující zóny (ZSK) a klíč používaný k podpisu dat v zóně.
- **Podepsání záznamů** v zóně vaší domény, 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.
- **Publikace DS záznamů** do registru domén.cz za pomoci vašeho registrátora.

V případě, že je váš registrátor rovněž správcem vašich DNS serverů (zejm. v případě, že vám zajišťuje rovněž webhosting) by nemělo být problém, aby výše uvedené kroky zvládl sám s minimální součinností z vaší strany.

JIŘÍ PRŮŠA
sdružení CZ.NIC, správce české národní domény