vádění této technologie. Běžný uživatel zavedení DNSSEC v podstatě nepozná a mělo by pro něj být tedy daleko méně bolestivé, než byl třeba přechod z analogového na digitální televizní vysílání.

Jak se chránit pomocí DNSSECu?

Existuje několik typických situací, ve kterých se může běžný uživatel ocitnout, a ve kterých volí různý postup:

1 Jsem držitelem domény, provozuji na ní internetové služby a chci udělat maximum pro zabezpečení své domény. V tomto případě většinou platí, že zároveň nerozumím systému DNS, natož DNSSEC, a ani tomu moc rozumět nechci. Pokud chci svoji doménu zabezpečit, je to velmi jednoduché. Stačí se obrátit na svého registrátora a požádat ho, aby mi moji doménu pomocí DNSSEC zabezpečil, pokud to již sám neudělal. Jestliže při této otázce narazím na neochotu u svého registrátora, pak není nic jednoduššího, než ho změnit a přejít k takovému, kterému zabezpečení domén nebude dělat problém. Změna registrátora i zabezpečení domény je totiž otázkou několika minut. Volbu správného registrátora lze provést díky jejich veřejně dostupnému seznamu (s uvedením jimi podporovaných technologií a úrovní certifikace) na stránkách správce české národní domény **www.nic.cz**.

2 Jsem zaměstnancem nebo manažerem ve firmě, která provozuje svoje DNS servery (a já je využívám při přístupu k internetovým službám). Podle velikosti firmy, ve které pracuji, a samozřejmě také podle pozice, je tento případ jednoduchý či složitější. V každém případě zatlačte na své IT oddělení, aby vaše DNS servery naučilo DNSSEC používat a aby to samé požadovalo od vašeho poskytovatele připojení k internetu. Zavedení podpory DNSSEC na nameservery je poměrně jednoduché a existuje k tomu spousta návodů, například na **www.dnssec.cz** lze najít dostatek informací dokonce v češtině.

3 Jsem uživatel internetu doma a využívám DNS servery poskytovatele připojení. Možná nejsložitější situace, ale i ta je řešitelná. Buď sami, viz níže, nebo dotazem na svého ISP zjistěte, zda DNSSEC podporuje. Pokud ne, změňte poskytovatele připojení, a pokud to není možné, sdělte mu co nejoficiálnější formou, že o DNSSEC stojíte. Každá firma, která to se svým podnikáním myslí vážně, požadavkům svých zákazníků naslouchá a plní je, je tedy šance, že i vy pomůžete svého ISP přesvědčit, aby šel s dobou. Pokud se tak nestane, hrozí mu, že nakonec o své zákazníky přijde a jako bonus navíc bude muset řešit závažné bezpečnostní incidenty ve své síti.

Pro všechny uvedené situace lze hodně informací ohledně své bezpečnosti získat, aniž byste kohokoliv kontaktovali. Tak předně na stránkách www.dnssec.cz najdete, zda máte zabezpečen přístup k internetovým službám pomocí DNSSEC, a zda se tedy máte věnovat uvedenému postupu ad 2) nebo 3). Dále můžete několika způsoby ověřit, zda jsou vámi navštěvované domény pomocí DNSSEC chráněny. Jedním z uživatelsky velmi přívětivých způsobů je instalace Firefox plug-inu DNSSEC Validator, který vám poté bude okamžitě oznamovat, jestli jsou navštěvované domény chráněny, či nikoliv. Od toho je pak již jen krůček, abyste své bance nebo státnímu úřadu napsali, že i oni by měli o zabezpečení svých domén uvažovat.

DNSSEC v ČR a ve světě

Správce české národní domény, sdružení CZ.NIC, začalo se zaváděním technologie DNSSEC v roce 2008 a je ve své snaze velmi úspěšné. Mezi prvními, kdo zavedl jeho podporu, je ACTIVE 24, jeden z největších českých registrátorů domén. Ještě do konce roku 2009 tak byly zabezpečeny první stovky .cz domén. V roce 2009 pokračoval postupný, ale stále ještě pomalý růst počtu zabezpečených domén, roky 2010 a zejména 2011 pak znamenaly výrazné zvýšení dostupnosti této technologie u registrátorů. V roce 2012 bude tato technologie u registrátorů již běžný standard. Vývoj počtu zabezpečených .cz domén lze dobře vidět na grafu.

Z uvedených faktů vyplývá, že na straně registrátorů je situace ohledně podpory DNSSEC již velmi dobrá. Aspoň částečnou podporu této technologie mají zavedenu všichni významní hráči na trhu, další ji zavádějí nebo o ní vážně uvažují. Kvalitní registrátoři domény zabezpečují automaticky a zdarma. Co se týče poskytovatelů připojení, ISP (Internet Service Provider), je situace obecně hůře měřitelná nebo zcela neměřitelná. Nicméně podporu již zavedli takoví hráči jako Telefónica, Vodafone nebo GTS a spousta menších, tedy i zde je situace poměrně dobrá a dá se očekávat, že se bude dále lepšit.

Ve srovnání se světem v zavádění DNSSECu rozhodně Česká republika nekulhá, naopak je v tomto trendu lídrem. Neexistuje více zabezpečených domén pomocí DNSSECu od jedné TLD (a to počtem i penetrací), než je tomu v případě .cz domény. Srovnání s .cz v tomto ohledu snese snad pouze .se doména, která ale začala s podporou DNSSECu dříve než .cz. Zbytek světa rozhodně nespí, z celkového počtu dnes dostupných 304 TLD DNSSEC podporuje 76 z nich, tedy každá čtvrtá. DNSSEC zavedla taková TLD jako .com, .net, .org, .eu nebo z okolních zemí .de, .at a .pl. Podpora DNSSEC poskytovateli připojení ve světě pak více méně kopíruje podporu registrátorů. Výraznou aktivitu v této oblasti tedy najdeme například ve Švédsku nebo v USA.

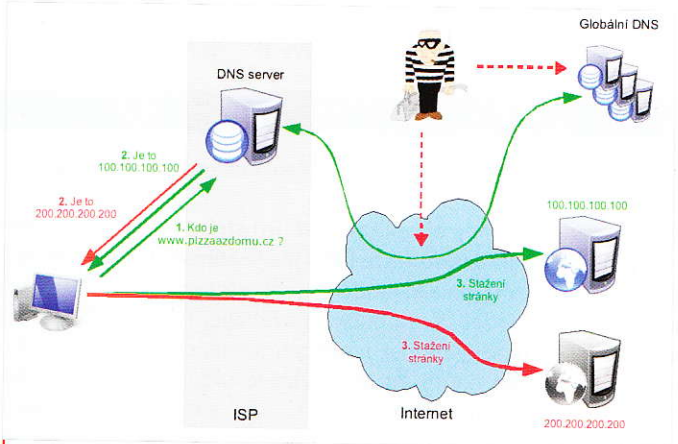
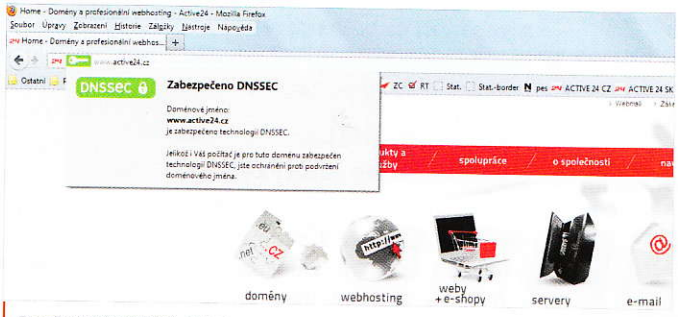


Schéma komunikace přes DNS server, nezabezpečený technologií DNSSEC



Použití DNSSEC Validatoru

Co dál?

Samotným zabezpečením DNS ale přínos DNSSEC nekončí. V současné době je například poměrně živá diskuse kolem projektu DANE (DNS-based Authentication of Named Entities). Toto uvažované rozšíření DNS by přineslo možnost daleko rychlejšího a levnějšího přidání TLS nebo SSL certifikátů k internetovým stránkám. A to pouze díky využití důvěryhodného komunikačního kanálu DNSSEC.

DNSSEC tedy zřejmě nebude sloužit pouze k ochraně systému DNS, ale využije se jako základní stavební kámen pro další užitečné aplikace. ■