Informační technologie

IPv6 a DNSSEC: povinná součást vašeho webu!

Na konci loňského roku přijala vláda Usnesení č. 982, které zavádí povinnost zabezpečení domén držených státní správou prostřednictvím DNSSEC.

Jiří Průša

Technologie DNSSEC představuje rozšíření stávajícího systému doménových jmen (DNS), které zvyšuje jeho bezpečnost a reaguje rovněž na stále častější kybernetické útoky či snahy podvodného vylákání uživatelských informací. Díky DNSSEC má návštěvník vaší stránky jistotu, že se nachází skutečně na těch webových stránkách, jejichž adresu zadal do prohlížeče a informace, které získal, jsou úplné a nebyly podvrženy. Usnesení vlády se zaměřuje rovněž na podporu internetového protokolu verze 6 (IPv6), který reaguje na nedostatek adresních bloků IP adres verze 4. Ve srovnání s usnesením z roku 2009 došlo jak na rozšíření okruhu subjektů, tak služeb, které musí novou verzi internetového protokolu podporovat. V rámci služeb se povinnost podpory IPv6 nově vztahuje rovněž na elektronické podatelny, respektive e-mailové servery, v jejichž případě bývá často implementace této technologie opomíjena.

U povinných subjektů pak Usnesení vlády ustanovuje povinnost podpory IPv6 u všech projektů podpořených ze strukturálních fondů, to jest rovněž poměrně širokého okruhu webových prezentací samosprávy, ať již se jedná o elektronické služby přímo podpořené ze strukturálních fondů nebo informační stránky sloužící pro publicitu projektu například v oblasti vzdělávání či zefektivnění činnosti úřadu.

Za poslední rok udělaly velký pokrok rovněž města a obce, pro které sice není Usnesení vlády závazné, podpora těchto technologií, je však například jedním z hodnotících kritérií v soutěži Zlatý erb.

Zejména pro ministerstva a kraje vláda stanovila povinnost zahrnout DNSSEC a IPv6 jako nedílnou součást výběrových řízení na všechny relevantní služby, mezi které vedle webhostingu patří rovněž zajištění internetové konektivity. Na podporu IPv6 by mělo být pamatováno rovněž u veřejných zakázek na dodávku informačních systémů, ke kterým dnes uživatelé často přistupují přes

webové rozhraní. V této souvislosti je třeba upozornit na to, že opomenutí tohoto požadavku se může poměrně dobře stát důvodem pro odvolání na Úřadu pro ochranu hospodářské soutěže a může vést až k zrušení dané veřejné zakázky. V této souvislosti usnesení vlády reaguje rovněž na nutnost zahrnutí požadavku na podporu IPv6 v rámci výběrových řízeních na *Komunikační infrastrukturu veřejné správy* (KIVS) či chybějící podporu nové verze internetového protokolu u základních registrů, konkrétně u Informačního systému základních registrů (ISZR), kde pro komunikaci mezi takzvanými agendovými informačními systémy (AIS) a ISZR je možné používat pouze adresy IPv4 a IPv6 není podporována.

Přesto, že minimálně u webových a jmenných (DNS) serverů mají orgány státní správy povinnost podpory IPv6 již od 1. ledna 2011, průzkum sdružení CZ.NIC v rámci evropského projektu GEN6 **www.gen6-project.eu** upozornil na to, že tuto povinnost ne všechny úřady dodržují. Mezi úřady, jejichž stránky jsou přes IPv6 nepřístupné, patří především Ministerstvo pro místní rozvoj, Ministerstvo zemědělství a Ministerstvo vnitra. Podporu nové verze internetového protokolu pak neposkytuje ani jedna z komor našeho Parlamentu. Naopak potěšitelné zlepšení bylo v poslední době zaznamenáno u Ministerstva obrany. Za poslední rok udělaly velký pokrok rovněž města a obce, pro které sice není Usnesení vlády závazné, podpora těchto technologií je však například jedním z hodnotících kritérií v soutěži *Zlatý erb*.

Ve snaze podpořit jednotlivé úřady včetně měst a obcí při implementaci těchto technologií připravila Akademie CZ.NIC, vzdělávací středisko správce české národní domény, sérii kurzů s názvem IPv6 a DNSSEC ve veřejné správě a veřejných zakázkách. Ty jsou určené všem, kteří se chtějí s IPv6 a DNSSEC seznámit blíže, dozvědět se obecné postupy implementace těchto technologií a to, jak je zohlednit ve veřejných zakázkách. Pro zástupce veřejné správy je kurz bezplatný! Další kurzy jsou pak zaměřeny na praktické aspekty implementace obou technologií včetně nastavení serverů. Více informací k jednotlivým kurzům včetně termínů a možnosti přihlášení najdete na stránkách **akademie.nic.cz**. ■

Jak zabezpečit doménu prostřednictvím DNSSEC?

U zabezpečení domény prostřednictvím DNSSEC hraje hlavní roli registrátor vaší domény. V současné době DNSSEC podporuje třináct registrátorů (Active 24; AERO Trip Pro; Banan; Český server.cz; General Registry; Gransy; IGNUM; Kraxnet; ONE.CZ; OneSolution; TELE3; Web4U a Zoner software). Pravidelně aktualizovaný seznam registrátorů včetně toho, zda podporují i další technologie jako IPv6 či mojeID, je možné nalézt na stránkách sdružení CZ.NIC (**www.nic.cz**, záložka *Registrátoři*).

Vlastní proces zabezpečení domény se pak skládá ze tří kroků:

- Vygenerování klíčů – Pro zvýšení bezpečnosti 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 zejména za pomoci automatických nástrojů) a klíč podepisující klíče (KSK). Ten 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 – 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 – tento krok učiňte za pomoci vašeho registrátora.

V případě, že váš registrátor je rovněž správcem vašich DNS serverů (zejména v případě, že vám zajišťuje rovněž webhosting), neměl by být problém, aby výše uvedené kroky zvládl on sám s minimální součinností z vaší strany. V případě, že si jmenné servery provozujete sami, je možné využít návod *DNSSEC za 5 minut* volně dostupný na **www.dnssec.cz**. Pokud máte zájem dozvědět se o DNSSEC po teoretické i praktické stránce více, navštivte kurz DNSSEC – zabezpečení DNS, který nabízí Akademie CZ.NIC.

Implementace IPv6 v orgánech veřejné správy

	WWW		DNS		Mail	
	30. 6. 12	31. 1. 14	30. 6. 12	31. 1. 14	30. 6. 12	31. 1. 14
Ministerstva	35,7 %	57,1 %	64,3 %	71,4 %	35,7 %	64,3 %
Ústřední orgány státní správy	50,0 %	81,8 %	58,3 %	72,7 %	33,3 %	27,3 %
Krajské úřady	14,3 %	14,3 %	64,3 %	71,4 %	14,3 %	21,4 %
Města a obce s rozšířenou působností	7,3 %	29,8 %	43,9 %	58,6 %	2,9 %	4,9 %

Zdroj: Sdružení CZ.NIC a projekt GEN6

Jiří Průša se dlouhodobě zabývá především problematikou evropského eGovernmentu. Ve sdružení CZ.NIC má na starosti projekt GEN6, v rámci kterého vede evropské srovnání připravenosti veřejné správy na IPv6.