DNS, NEBO DNSSEC?

Zabezpečený DNS

Představte si idylický večer s rodinou: práci máte za sebou, právě jste e-mailem poslali představenstvu firmy strategický plán, na webu si objednali a přes platební bránu rovnou i zaplatili pizzu. Ve skutečnosti jste během deseti minut předali útočníkovi strategii firmy, peníze i údaje ke své platební kartě. Stali jste se totiž obětí nechráněného DNS systému.

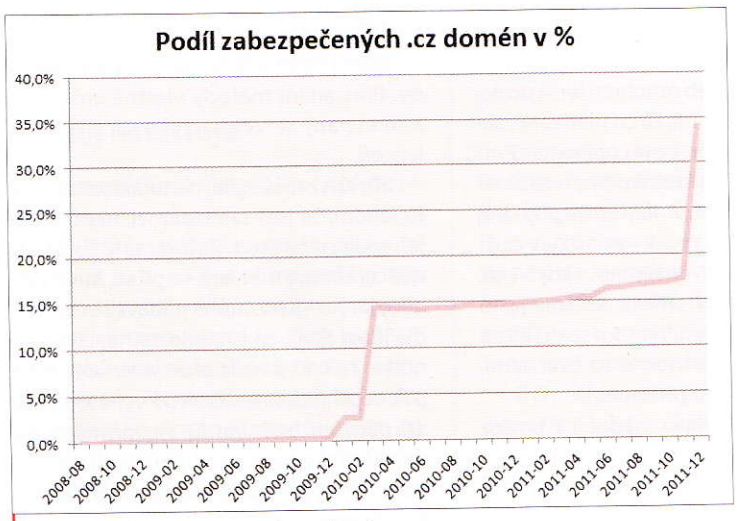
Proč DNS nestačí?

Pro odpověď na tuto otázku musíme jít k jedné ze základních a také nejstarších služeb internetu, tedy k systému doménových jmen, DNS (Domain Name System). Tento systém překládá člověku dobře pochopitelné jmenné internetové adresy, tedy například představenstvo@nasifirmy.cz nebo **www.pizzaazdomu.cz**, na adresy číselné, kterým zase rozumějí počítače a dokážou pomocí nich zobrazit webové stránky nebo odeslat e-mail.

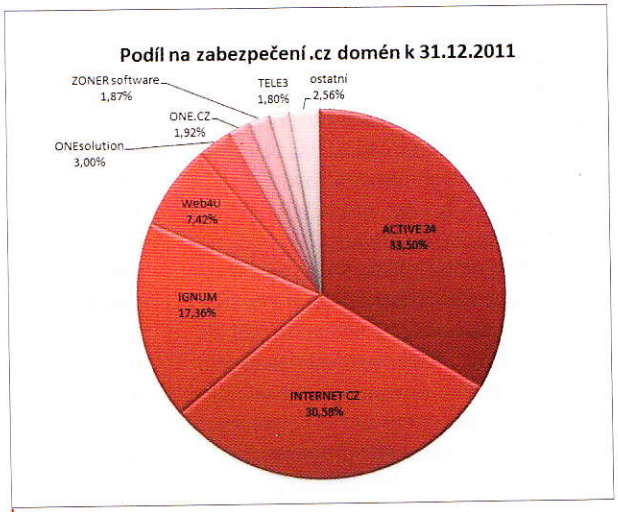
V době, kdy systém DNS vznikl, byl internet tvořen tak malým množstvím subjektů, že se všichni navzájem znali, a neřešili tak příliš otázku bezpečnosti. Ta doba je však dávno pryč. Přes systém DNS není těžké zaútočit na některý z nameserverů, narušit standardní DNS komunikaci a podvrhnout jí své falešné údaje. Snadno lze zaměnit číselnou adresu internetové služby s tím, že ta jmenná zůstane zachována. Poměrně snadno se tak docílí, že přesměruje e-maily nebo zobrazí návštěvníkovi stránek jiný obsah, než tam umístil jejich provozovatel. A to vše v podstatě v neviditelné formě pro běžného uživatele, protože ten používá svoje důvěrně známé adresy.

O tom, že strategie firmy odeslaná do mailboxu útočníka či odcizené peníze nebo osobní údaje jsou závažné problémy, není sporu. Ale představte si, že útočník napadne weby veřejné správy nebo zpravodajských serverů a rozšíří mezi lidi zprávy, které způsobí paniku, pády měn nebo kurzů akcií. Představte si, že ovlivní fungování tisíců internetových služeb v takovém rozsahu, že si to ani představit nelze. Služba DNS, není-li zabezpečena pomocí DNSSEC, poskytuje totiž potenciálnímu útočníkovi několik míst, na kterých je možné komunikaci narušit a zfalšovat údaje.

AUTOR
Zdeněk Brůna
technický ředitel ACTIVE 24



Vývoj podílu zabezpečených .cz domén na celkovém počtu



Podíly jednotlivých registrátorů na celkovém počtu zabezpečených domén (k 31. 12. 2011)

DNSSEC (Domain Name System Security Extensions) je bezpečnostní rozšíření systému doménových jmen, tedy jednoho ze základních stavebních kamenů internetu. Tato technologie výrazně snižuje riziko, že se vám někdo naboural do e-mailové schránky, změní obsah zobrazovaný vaším internetovým prohlížečem nebo odcizí údaje o platební kartě či heslo do důležitého systému.

DNSSEC zavádí do systému doménových jmen asymetrickou kryptografii, tedy princip, který známe například z šifrování zpráv pomocí PGP nebo podepisování e-mailů elektronickým podpisem. Také v případě DNSSEC pracujeme se dvěma klíči, jedním šifrujeme, druhým dešifrujeme – v našem případě DNS záznamy. Konkrétně se provádí tak, že si držitel domény (případně důvěryhodný technický správce domény – správce autoritativního nameserveru pro doménu) vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče je možné ověřit pravost tohoto podpisu, proto je nutné, aby byl veřejný klíč dostupný všem; publikuje se tedy ve veřejné části klíče u nadřazené autority. V případě .cz domény jí je registr domén .cz. Na úrovni registru domén řetěz důvěry nekončí, pokračuje obdobným způsobem k nadřazené autoritě, jak vyplývá z hierarchického uspořádání DNS. Všechna technická data v DNS jsou tak podepsána a důvěryhodnost údajů, které tento systém poskytuje, je na diametrálně vyšší úrovni v porovnání se stavem bez DNSSEC.

Co to je DNSSEC?

Řešením těchto problémů je zavedení DNSSEC, díky kterému získávají uživatelé internetu jistotu, že informace, které z DNS získali, pocházejí ze správného zdroje a nebyly po cestě k nim změněny – že jsou důvěryhodné.

DNSSEC je navíc zpětně kompatibilní se stávajícím DNS a obě varianty fungují současně, což pomáhá při postupném za-