Stručná historie bezpečnosti doménových jmen

Systém pojmenování počítačů textovými názvy vznikl velmi záhy poté, co vznikla síť ARPANET, což byla síť, která se později stala základem toho, čemu dnes říkáme internet. Adresace počítačů pomocí číselných adres byla velmi nepraktická a proto se tento systém velmi rychle ujal.

V úplných počátcích nebyl tento systém centralizovaný a každý počítač si udržoval vlastní kopii souboru pro překlad jména na číselnou adresu. Tento soubor byl spravovaný ručně a záznamy do něj přidával lidský operátor. Záhy bylo jasné, že je potřeba tento systém nějakým způsobem centralizovat. První formální návrh lze najít v dokumentu RFC 606 z prosince 1973; tento centralizovaný systém fungoval celou dekádu až do roku 1983.

S nárůstem připojených počítačů na počátkem osmdesátých let začal být centralizovaný systém pro správu většího množství záznamů nevhodný. Probíhající diskuze vyústila v sérií dokumentů RFC 881 až 883, kde John Postel a Paul Mockapetris vytyčili základy současného systému DNS.

O tři roky později sepisuje Paul Mockapetris dokumenty RFC 1034 a 1035, které shrnují dosavadní vývoj na poli DNS. Tyto dva dokumenty stále obsahují základní definice systému DNS a ač byly mnohokrát aktualizovány, jsou stále platné.

V roce 1990 byl internet stále poklidné místo, kde jeho uživatelé žili v poklidu a vzájemné harmonii. Nebo ne? V tom samém roce přichází Steven M. Bellovin na zásadní chybu při používání DNS. Vzájemná důvěra mezi počítači byla v té době většinou řešena pouze na základě správného doménového jména v DNS. V zásadě se nejedná o chybu samotného DNS, ale chybu přílišné důvěry v systém DNS.

Po zveřejnění tohoto nedostatku se na půdě IETF, což je organizace, která stojí za většinou internetových standardů RFC, začíná uvažovat nad zabezpečením systému DNS. Mezitím Eugene Kashpureff objevuje další zranitelnost v současných implementacích DNS serverů, která mu do DNS umožňuje podvrhnout libovolný záznam. V roce 1997 pak používá tuto chybu k celosvětovému přesměrování stránek registrátora InterNIC na stránky své firmy AlterNIC. Ještě v témže roce vzniká první dokument popisující kryptografické zabezpečení systému DNS – RFC 2065. Tento dokument je pak během dvou dalších let rozpracován a v roce 1999 je v RFC 2535 publikována první verze systému DNSSEC, v roce 2005 pak v RFC 4033 až 4035

následuje verze druhá.

V roce 2008 objevuje v systému DNS další závažnou bezpečnostní chybu Dan Kaminsky. Tato chyba umožňuje v řádu sekund až minut podvrhnout libovolný záznam do DNS, a takto přesměrovat např. libovolné webové stránky na server útočníka.

A co to ten DNSSEC vlastně je? Systém DNSSEC kryptograficky zajišťuje integritu dat poskytovaných DNS servery. Pokud je DNSSEC používán oběma stranami, není již možné podvrhnout a změnit obsah DNS a bez vědomí uživatele přesměrovat webové stránky nebo e-mailovou komunikaci na server útočníka. A nejedná se jen o stránky internetových bankovnictví, vzhledem k velkému dopadu útoku může být pro útočníka zajímavé napadnout zpravodajské servery nebo jiné zdroje důležitých informací (např. burzovní zpravodajství). Situaci bych přirovnal k nedávnému zobrazení atomového výbuchu v televizním vysílání, nicméně internetoví útočníci jsou dnes často součástí organizovaného zločinu a útok na DNS bude spíše motivován finančním ziskem, ať už ve formě přístupů do internetového bankovnictví či průmyslové špionáže.

Dnes se píše rok 2009 a pomocí systému DNSSEC je chráněno pouze několik domén nejvyšší úrovně včetně naší národní .cz. Bezpečnostní chyba objevená Danem Kaminskym naštěstí rozhýbala stojaté vody a o implementaci DNSSEC se začala mimo jiné zabývat i americká administrativa.

Běžný uživatel internetu se do styku s DNSSEC pravděpodobně přímo nedostane, úkol zabezpečit systém DNS leží na jejich poskytovateli připojení, kteří musí nakonfigurovat DNSSEC na svých DNS serverech tak, aby tyto servery ověřovaly integritu DNS dat. Koncoví uživatelé si mohou vyzkoušet, zda-li jejich poskytovatel připojení podporuje DNSSEC na stránkách www.dnssec.cz. Z opačné strany, tedy na straně poskytovatelů obsahu (např. www.vesmir.cz), pak musí dojít k zabezpečení pomocí DNSSEC tak, aby uživatelé mohli ověřit pravost informací z DNS.

Autor:
Ondřej Surý, vedoucí Laboratoří CZ.NIC