DNSSEC

přináší účinnou ochranu proti podvodníkům

Jan Kadlec

Většina internetových služeb, jako je e-mail, web či internetové volání, využívá systém doménových jmen (DNS – Domain Name System). DNS umožňuje těmto službám používat k adresaci doménová jména, která se snadno pamatují a jsou nezávislá na změnách IP adres. V DNS existují dva druhy serverů: rekurzivní a autoritativní. Autoritativní servery jsou v podstatě databáze, které provozují držitelé domén, a do kterých se ukládají DNS data. Rekurzivní servery naopak provozují například poskytovatelé internetového připojení (ISP). Úkolem rekurzivních serverů je řešit DNS dotazy, které přicházejí od uživatelů v dané síti (například v síti daného ISP).

Právě na rekurzivní servery je možno provést útok, který pak ohrožuje všechny uživatele dané sítě. Rekurzivní servery se totiž musí kvůli vyřešení DNS požadavků dotazovat autoritativních serverů. Odpovědi od autoritativních serverů se ukládají do vyrovnávací paměti – tato paměť je zásadní součástí DNS. Právě na vyrovnávací paměti se provádí útoky, při nichž je cílem útočníka dostat do vyrovnávací paměti nepravá data. Pokud se útok povede, může útočník přesměrovat uživatele na své servery, které budou imitovat servery skutečné. Cílem útočníků je samozřejmě získat citlivá uživatelská data, jako jsou přístupové údaje ,nebo čísla kreditních karet.

Na rozdíl od klasických phishingových útoků, při kterých uživatelé musí použít odkaz, jenž jim podvodník pošle například elektronickou poštou, hrozí tento druh útoku i poučeným uživatelům, kteří vědí, že nemají používat tyto odkazy, ale k webovým službám přistupovat buď přímo zadáním doménového jména do prohlížeče, nebo skrz uloženou záložku. Pokud se totiž útočníkovi podaří podvrhnout data na některém z DNS serverů, koncový uživatel nemá jak zjistit, že data, která pomocí DNS získal, nejsou pravá. Když navíc útočník disponuje certifikátem, který vydala jedna z důvěryhodných certifikačních autorit, nemusí pomoci ani protokol HTTPS. Závažnost tohoto útoku navíc zvyšuje fakt, že nepostihuje jen web, ale všechny služby, které DNS využívají – útočník tak může například přesměrovat veškerou elektronickou poštu na své servery.

Řešením problému je rozšíření DNS zvané DNSSEC. DNSSEC používá asymetrickou kryptografii při tomto přístupu se pracuje s dvěma druhy klíčů: soukromým klíčem se data podepíší a veřejným klíčem se pak ověří platnost podpisu.

Držitel domény, která používá DNSSEC, podepíše svá DNS data soukromými klíči. Vzniklé podpisy spolu s veřejnými klíči vystaví v DNS a podá nadřazené doméně informace o svých veřejných klíčích. Rekurzivní servery pak mohou ověřit platnost dat z takto podepsaných domén. Pokud by byl na podepsané domény prováděn útok, bude neúčinný, protože útočník nedisponuje soukromými klíči k daným doménám a nemá tedy svá podvržená data jak podepsat. Kromě toho, že DNSSEC řeší problém s nesprávnými DNS daty, je také prerekvizitou pro protokol DANE (DNS-Based Authentication of Named Entities). Ten zvyšuje bezpečnost protokolu TLS. Protokol TLS používá mimo jiné už zmíněné HTTPS.

Doména .CZ spravovaná sdružením CZ.NIC umožňuje použití DNSSEC pro ochranu záznamů v DNS. Pokud chcete svou doménu ochránit, musíte vygenerovat DNSSEC klíče, své záznamy podepsat a prostřednictvím svého registrátora podat informace o vašich klíčích nadřazené doméně. Sdružení CZ.NIC pak publikuje informace o klíčích v doméně .CZ. Kompletní popis postupu naleznete v průvodci Jak zavést DNSSEC pro .CZ domény, který je dostupný na adrese www.dnssec.cz.

Pro správné fungování ověřování DNSSEC podpisů je nutná speciální konfigurace rekurzivního serveru. Ta spočívá v nakonfigurování důvěryhodného klíče pro kořenovou doménu (kořenová doména stojí na vrcholu DNS hierarchie), který pak server použije jako výchozí body pro ověření DNS dat. Konkrétní postup, jak rekurzivní servery nastavit, najdete opět na www.dnssec.cz, v dnešní době však manuální nastavení často není potřeba, rekurzivní servery získají požadované informace automaticky. ■

Autor článku, Jan Kadlec, je programátorem (sdružení CZ.NIC) a lektorem výukového centra Akademie CZ.NIC