Správné nastavení DNS serverů

Nastavení DNS serverů většina administrátorů dělá automaticky a podle zažitých scénářů. Podobně jako u jiných bezpečnostních pravidel ani u DNS neuškodí si čas od času zopakovat, zda na nějaké pravidlo nezapomínáme.

PETR ČERNOHOUZ, JIŘÍ PRŮŠA

V následujícím textu přinášíme přehled požadavků, které se často podceňují, jejich nedodržení však může ve svém důsledku vést k omezení dostupnosti poskytovaných služeb nebo způsobit zranitelnost umožňující uskutečnit kybernetický útok včetně podvržení poskytovaných dat. Článek vznikl v rámci projektu Zabezpečení DNS serverů v ČR realizovaného Ministerstvem vnitra ČR.

Podle prvních výsledků mezi nejčastější prohřešky patří nekonzistence jmenných serverů, které by v nadřazené zóně měly odpovídat zóně samotné, a dále blokování odpovědí na DNS dotazy přes TCP port 53.

Pro snadné ověření níže uvedených požadavků lze využít i webovou aplikaci Zonemaster na *https://zonemaster.labs.nic.cz/*. Jejím prostřednictvím lze mj. zkontrolovat správnost delegace reverzních DNS záznamů spravovaných organizací RIPE NCC.

Jelikož jde o open source projekt, který nabízí kromě webového rozhraní také API, lze jej snadno zabudovat přímo do svých systémů pro případnou opakovanou kontrolu. Aktuálně Zonemaster dělá celkem 60 testů. Tento počet však není konečný.

Konektivita

Servery by měly naslouchat na portu 53 pro TCP i UDP provoz. Speciálně port TCP 53 je stále v mnoha sítích omezován, což má za důsledek nedostupnost některých služeb a zároveň způsobuje větší náchylnost DNS serverů k útokům, zvláště DDoS útokům technikou zvanou DNS Amplification.

- **Všechny jmenné servery musí odpovídat na DNS dotazy přes protokol UDP na portu 53.** Typický DNS dotaz se posílá prostřednictvím UDP na port 53. Jmenný server musí odpovědět na DNS dotaz zaslaný tímto protokolem na jeho IP adresu/adresy.
- **Všechny jmenné servery musí odpovídat na DNS dotazy přes protokol TCP na portu 53.** V některých případech se DNS dotazy posílají prostřednictvím protokolu TCP na port 53. Dotazy zaslané pomocí TCP jsou rovnocenné s dotazy přes UDP protokol a musí se odbavovat stejně.

Jmenné servery

Jmenný server pro doménu musí implementovat všechny platné DNS standardy, aby byl schopný poskytovat úplné a správné informace a zároveň byl zabezpečen proti útokům. Zároveň je dobrým principem nekombinovat funkci autoritativního a rekurzivního DNS serveru, aby se předešlo vzájemnému ovlivnění.

- **Autoritativní servery by neměly podporovat rekurzivní dotazy.** Pro zajištění konzistence v DNS by autoritativní DNS servery neměly dělat rekurzivní dotazování. Toto chování se vyžaduje od root serverů a pro ostatní autoritativní servery se silně doporučuje. Omezí se tak možnosti útoku na tento server například pomocí tzv. otrávení cache.
- **Jmenné servery musí podporovat EDNS0.** EDNS0 představuje mechanismus pro oznamování schopnosti jednotlivých implementací DNS protokolu a využívá se novými rozšířeními jako například DNSSEC. Mechanismus je detailně popsán ve standardu RFC 6891.
- **Jmenné servery musí zpracovávat QNAME bez ohledu na velikost písmen** (case insensitive). Také musí přistupovat stejně ke všem dotazům bez ohledu na velikost použitých písmen, záznamy example.com a EXAMPLE.COM se musí přeložit na stejnou hodnotu a se shodným návratovým kódem.

Rozdílná velikost písmen se používá pro zvýšení entropie v DNS paketu, čímž se sníží možnost podvržení odpovědi.

Konzistence

Pro stabilitu zóny je potřeba, aby všechny jmenné servery poskytovaly stejné údaje, a nedocházelo tak k nesprávnému vyhodnocování dotazů.

- **Všechny jmenné servery by měly vracet shodné sériové číslo v SOA záznamu.** Stejná sériová čísla v SOA záznamech (tzv. start ofauthority záznam je definován *RFC 1035*) na všech jmenných serverech jsou indikátorem, že zónová data jsou konzistentní a klient dostane stejnou odpověď bez ohledu na jmenný server, kterého se ptá.

Toto pravidlo nemusí být splněno u vysoce dynamických zón, kde rychlost změn je vyšší než doba potřebná k propagaci záznamů na všechny slave servery. U běžných zón je však frekvence změn nízká a nesoulad sériových čísel na jednotlivých serverech může značit problém s propagací zóny.

- **Všechny jmenné servery by měly vracet shodnou hodnotu RNAME v SOA záznamu.** Pole RNAME v SOA záznamu odkazuje na e-mailovou adresu správce odpovědného za danou doménu. Pokud se hodnoty na jednotlivých serverech liší, jde o průvodní jev nekonzistence domény a ztěžuje možnost kontaktovat zodpovědného správce pro zjednání nápravy.
- **Všechny jmenné servery by měly odpovídat se stejnými parametry SOA záznamu.** Parametry REFRESH, RETRY,