Ajánlás DNS szerver üzemeltetőknek

Pásztor Miklós

2011. július

Tartalom

Alapbeállítások

Mivel a DNS az internetes infrastruktúra kritikus eleme, a DNS szerverek üzemeltetésénél különös gonddal kell eljárni. Ajánlatos többek között:

- DNS szervert (nem feltétlenül nagy teljesítményű, de) megbízható gépen üzemeltetni
- DNS szervereket jó paraméterekkel rendelkező hálózaton elhelyezni
- DNS szerveren csak a legszükségesebb szolgáltatásokat működtetni (pl. ssh), a lehető legkevesebb programot telepíteni
- DNS szerveren az operációs rendszert, a rendszerprogramokat rendszeresen frissíteni
- DNS szerverhez lehetőleg minél kevesebb felhasználói azonosítót létrehozni
- Ha a forgalom és/vagy a biztonság megköveteli, akkor egy-egy zónára kettőnél több autoritatív név szervert is üzemeltetni
- A DNS szerverek rendszerfelügyeletét folyamatosan biztosítani

DNS biztonság

Gyakran lehet hallani a DNS gyengeségeiről, támadhatóságáról, az ezekkel való visszaélésről és az ilyen visszaélés elleni védekezésről. Különösen Dan Kaminsky 2008 tavaszán tett felfedezése, és augusztusi előadása váltott ki sok eszmecserét, és lázas tevékenységet is: a DNS szoftver gyártók a „Kaminsky bug” nyilvánosságra kerülése előtt már elkészítették programjaik javított változatát, és a DNS szerver üzemeltetők túlnyomó többsége frissítette a DNS szerver programját, áttért az új változatra. Ez igen örvendetes, de vannak rossz tapasztalatok is: sok üzemeltető olyan módon konfigurálja DNS szerverét, ami veszélyt jelent saját rendszereire, partnereinek, üzletfeleinek rendszereire és a tág internet közösségre.

DNS szerverek régen

A név szervereknek két funkciója van: **autoritatív**, (mutató) és **rekurzív** (látó) funkció. Az internet kezdeti időszakában:

1. Az autoritatív név szerverek általában rekurzív név szerverek is voltak.
2. Bármely IP címről érkező rekurzív kérésekre feleltek, rekurzióba kezdtek.
3. Nem csak az egyes DNS rekordokhoz, hanem teljes zónákhoz hozzáférést engedtek bárkinek: megengedték a zóna transzfert.

Azonban megbízhatóbb és biztonságosabb, ha az autoritatív név szerverek senkinek nem nyújtanak rekurzív szolgáltatást, a rekurzív név szerverek csak saját hálózati környeztük számára szolgáltatnak és a zóna transzfert csak a szükséges IP címekre és védett módon (tipikusan a zóna másodlagos autoritatív szerverei felé) engedélyezik.

Az autoritatív és a rekurzív funkció szétválasztása

A rekurzív név szerverek ki vannak téve cache poisoning támadásnak. A „Kaminsky bug" is ezzel kapcsolatos, de már évtizedekkel ezelőtt is voltak példák ilyen támadásra. Valójában a „Kaminsky bug" ellen hozott intézkedések is csak csökkentik, de nem szüntetik meg a veszélyét annak, hogy a rekurzív név szerverek cache-ét hamis adatokkal mérgezzék.

Veszélybe hozza az autoritatív szolgáltatást nem csak a cache mérgezés, hanem minden más támadás is, ami egy rekurzív név szervert érhet (pl. bénító, DoS támadás).

A .hu alatti domain-oknál tapasztalt hibák

A .hu alatti domain-ok számára gyakran olyan regisztrátorok nyújtanak autoritatív szolgáltatást, akik egyúttal internet szolgáltatók, és így rekurzív név szerver szolgáltatást is adnak ügyfeleiknek. Ismételten előfordultak a következő hibák:

- 1. hiba: átregisztrálás után nem mindenhonnan érhető el a domain
  Az ISP1 név autoritatív szerver egyik ügyfele az Csakegypelda Kft. A Kft. számára az ISP1 név szerver szolgáltatást nyújtott, az `ns.isp1.hu` szerveren. Tehát az `ns.isp1.hu` autoritatív választ adott a csakegypelda.hu zónára vonatkozóan. Az ISP1 nem választotta szét a rekurzív és az autoritatív funkciót, a rekurzív név szerver, amit ügyfelei használtak szintén az `ns.isp1.hu`. Valamilyen okból a `csakegypelda.hu` autoritatív név szerverei átkerültek ISP2 szolgáltatóhoz. Egy adott pillanattól kezdve tehát a `csakegypelda.hu` név szerverei `ns.isp2.hu` és `ns2.isp2.hu` lett. Az átregisztrálás rendben lezajlott, de az ISP1 munkatársai elfelejtették az autoritatív név szervereiken kivenni a konfigurációból a `csakegypelda.hu`-ra vonatkozó részt. Ennek az a következménye, hogy az ISP1 ügyfelei, akik rekurzív név szerverként használják az `ns.isp1.hu`-t, az átregisztrálást nem érzékelik, például nem érik el a `csakegypelda.hu` web lapját, nem tudnak levelet küldeni a `valaki@csakegypelda.hu` címekre! Sőt, lehet, hogy hibás, elavult web lapot látnak, rossz helyre küldik a leveleket stb. A Csakegypelda Kft. számára az ilyen hiba katasztrófális következményekkel járhat.

- 2. hiba: a domain regisztrációja megszűnt, de az ügyfél ezt észre se vette
  A Csakegypelda Kft. az ISP1 hálózata mögött volt. Számára autoritatív és egyben rekurzív név szerver is volt az `ns.isp1.hu.` A domain .hu alatti regisztrációja - pl. fizetési határidő lejárta miatt - megszűnt, a .hu zónában már nem szerepelt a `csakegypelda.hu`, de az ISP1 munkatársai elfelejtették kivenni az autoritatív név szervereikben a `csakegypelda.hu`-ra vonatkozó részt. Ebben az esetben a Csakegypelda Kft. sokáig észre se vette, hogy megszűnt a regisztráció, hiszen az ő hálózatából fel lehetett oldani a `csakegypelda.hu` neveket!

  A konfigurálásnál elkövetett feledékenység nem vezetett volna ilyen hibákhoz, ha az autoritatív és rekurzív funkciók szét lettek volna választva.

Hogyan lehet szétválasztani a rekurzív és autoritatív funkciót?

A legtöbb manapság használatos DNS szoftverben más program valósítja meg a rekurzív és az autoritatív funkciót. A legnépszerűbb szerver program, a Bind azonban lehetővé teszi a régi működést is. Ha autoritatív név szervert üzemeltetünk Bind 9. név szerverrel, akkor a konfigurációjában az opciók között adjuk meg ezt az egy sort:

```
recursion no;
```

Források a szétválasztás szükségességéről

A Bind kézikönyvben ezt olvashatjuk (1.4.6):

The BIND name server can simultaneously act as a master for some zones, a slave for other zones, and as a caching (recursive) server for a set of local clients.

However, since the functions of authoritative name service and caching/recursive name service are logically separate, it is often advantageous to run them on separate server machines. A server that only provides authoritative name service (an authoritative-only server) can run with recursion disabled, improving reliability and security. A server that is not authoritative for any zones and only provides recursive service to local clients (a caching-only server) does not need to be reachable from the Internet at large and can be placed inside a firewall.

Az 1996-ban kiadott RFC2010 így ír:

Recursion is a major source of cache pollution, and can be a major drain on name server performance. An organization's recursive DNS needs should be served by some other host than its root name server(s).

A 2008-ban kiadott RFC5358:

In general, it is a good idea to keep recursive and authoritative services separate as much as practical.

D.J. Bernstein, akinek népszerű DNS szerver implementációja nem szorult javításra a „Kaminsky bug" felfedezésekor, külön oldalt szentel a szétválasztás szükségességének. Ebben idézi a „DNS and Bind" című könyvet, ahol az autoritatív szerverekről ezt olvashatjuk:

You should make sure that these servers don't receive any recursive queries.

A rekurzív név szerverek ne legyenek nyílt rekurzív névszerverek

Ha egy rendszergazda nyílt rekurzív név szervert (Open Recursive Nameserver, ORN) üzemeltet, akkor akaratlanul szolgáltatásokat nyújthat távoli számítógépek részére, és pazarolhatja saját erőforrásait. Nagyvonalúságának következtében azonban a szolgáltatás bénításának veszélye elsősorban nem is nála, hanem az internet bármely más pontján fennáll.

- A nyílt rekurzív név szervereket DoS támadások erősítőjeként lehet használni. Erről szól a már fent idézett RFC5358
- A nyílt rekurzív név szerverek különösen ki vannak téve cache poisoning támadásnak.

A nyílt rekurzív névszervereket könnyű felfedezni: elég egy autoritatív név szerver naplófájlját figyelni, és százezer számra lehet rekurzív név szervereket találni. Ha egy-egy hálózatban keresünk rekurzív név szervert, akkor elég a hálózat valamely gépét arra késztetni, hogy oldjon fel nevet az általunk felügyelt domain-ból, amire sok egyszerű és hatásos eszköz van.

Ha egy támadó el akarja téríteni egy gép forgalmát, akkor elég, ha rezolverét átállítja egy nyílt rekurzív névszerverre, és ezt a nyílt rekurzív névszervert megfertőzi. Fertőzött gépeken a rosszindulatú kód gyakran írja át a rezolvert. Ha ez sok gépen megtörténik, akkor egyetlen fertőzött nyílt rekurzív névszerver hatalmas károkat okozhat akár gépek, felhasználók millióinak.

Hogyan akadályozhatjuk meg, hogy rekurzív névszerverünk ORN legyen?

A látó (caching, rekurzív) név szerverekben definiáljunk egy IP cím halmazt, és csak ezek számára nyújtsunk rekurzív feloldást. Ez Bind-ban ehhez hasonló módon tehető meg:

```
#Felsoroljuk a hálóztokat CIDR formában, ahonnan megengedünk rekurzív kérdéseket:
acl "itt" {
127.0.0.0/8;
10.11.12.0/24;
};

#Az opciók közt megszorítást teszünk arra, hogy kiknek is akarjuk rekurzív kéréseit kiszolgálni:
options {
        allow-recursion {itt;};
};
```

Hol ellenőrizhetjük, hogy névszerverünk nyílt rekurzív névszerver-e?

Sok eszköz rendelkezésre áll. Például az ISZT-nél a http://deneb.iszt.hu/~pasztor/cgi-bin/recursive.cgi lapon ellenőrizhetjük, hogy egy IP címen nyílt rekurzív név szerver működik-e.

Források a nyílt rekurzív név szerverek veszélyeiről

Az US-CERT anyaga jó magyarázatot, és bőséges forrásanyagot tartalmaz: http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

Korlátozzuk és TSIG-gel védjük a zóna transzfert!

Zóna transzfert célszerű csak az autoritatív másodlagos (slave) szerverek fele megengedni. A következő Bind konfigurációs fájl részlet csak a `11.22.33.44` és a `11.22.33.45` címre engedi meg a zóna transzfert:

```
allow-transfer {
               11.22.33.44;
               11.22.33.45;
        };
```

Az `allow-transfer` opciót megadhatjuk a teljes konfigurációra, vagy egy-egy zónára vonatkozóan. Figyelemmel kell lenni az esetleges rejtett (stealth) autoritatív név szerverekre.

A zóna transzfer biztonságát és megbízhatóságát érdemes növelni TSIG (RFC2845) segítségével. A TSIG egy egyszerű szimmetrikus kulcsú technológia, melynek segítségével a zóna transzfernél a partnerek kölcsönösen autentikálják egymást, és biztosítják az adatátvitel sértetlenségét és hitelességét. Az adatátvitel digitális aláírással védett, és a „replay attack" elleni védekezésül az aláírás a pillanatnyi időtől is függ. Ezért fontos, hogy a szerverek órái szinkronban legyenek. Ha TSIG-et akarunk használni a zóna transzferhez, akkor mindkét oldalon be kell vezetni a közös kulcsot a konfigurációba Bind esetén ilyesféleképpen:

```
key z_key {
 algorithm hmac-md5;
 secret "U2FsdmEgbWUgZm9ucyBwaWV0YXRpc1whCg==";
};
```

Az elsődleges (master) oldalon az `allow_transfer` utasításban nem IP címet vagy ACL-t, hanem kulcsot kell megadni:

```
allow-transfer { key z_key; };
```

A másodlagos (slave) oldalon pedig a meg kell adni, hogy a master-t milyen kulcs használatával kell elérni:

```
server 11.11.11.11 {
    keys z-key;
};
```

Ebben a példában `11.11.11.11` a zóna elsődleges (master) szerverének a címe, amit a zone utasításban használunk.

DNS rekordok változtatása

Ha meg akarunk változtatni egy DNS rekordot, akkor figyelembe kell vennünk azt az időt, ameddig rekurzív név szerverek emlékeznek a megtanult értékre, azaz ameddig cache-elik ezt az információt. Szerencsére ezt az időt - a rekordhoz tartozó TTL-t -, maga a rekord **gazdája** tudja eldönteni, és beállítani akár minden egyes rekordra különbözőképpen. Ha például a `www.csakegypelda.hu` web szerver egy napon déli 12 órakor átköltözik az `11.11.11.11` címről a `22.22.22.22` címre, vagyis 12:00-kor megváltoztatják `csakegypelda.hu A` rekordját, és a rekordhoz tartozó TTL 24 óra, akkor azok a kliensek akiknek rekurzív név szervere 11:30-kor tudta meg az IP címet, még majdnem másnap délig a régi címen fogják keresni a `www.csakegypelda.hu` web lapot!

Ezért DNS rekordok változtatásánál előrelátóan először is a rekord TTL-jét kell levenni mondjuk 60 másodpercre, még a **régi** rekord értékkel:

```
www.csakegypelda.hu.          60      A       11.11.11.11
```

Ezek után várni a **régi TTL** ideig, a példában 24 óráig, azaz másnap délig, és csak ekkor írni át az új értékre a rekordot:

```
www.csakegypelda.hu.                  A       22.22.22.22
```

(Ebben a példában nem adtunk meg TTL-t, ezért a zóna alapértelmezése lép érvénybe.)

Ilyen módon biztosítottuk, hogy az interneten az összes DNS cache-ben legfeljebb 60 másodpercig lesz elavult érték, legfeljebb ennyi ideig keresik rossz helyen a web lapot a felhasználók. Persze az ilyen változtatási rendet nem csak a web lapok címénél, hanem minden DNS rekordnál, különösen NS rekord változtatásnál, például regisztrátor váltásnál érdemes követni.